

## CRIMES CIBERNÉTICOS: CONSEQUÊNCIAS JURÍDICAS E SOCIAIS

Paulo Ricardo Rodrigues urzedo<sup>1</sup>  
Jorge Barros Filho<sup>2</sup>

**RESUMO:** O direito à privacidade é um aspecto fundamental da dignidade humana, tendo evoluído ao longo do tempo para refletir as mudanças culturais e tecnológicas. Inicialmente ligado ao "direito de ser deixado em paz", hoje abrange conceitos como o direito ao esquecimento e a inviolabilidade de domicílio, correspondência e comunicações. A ascensão da sociedade da informação trouxe à tona a autodeterminação informativa, permitindo que os indivíduos exerçam maior controle sobre seus dados pessoais, promovendo a proteção tanto individual quanto social. A internet, no entanto, complicou a proteção de direitos, como o da imagem, devido à hiperexposição e à dificuldade em garantir segurança jurídica. A legislação, como a Lei nº 13.772/2018, foi adaptada para enfrentar esses novos desafios, enquanto o tema da privacidade ganhou destaque na Lei Geral de Proteção de Dados (LGPD). Além disso, a análise de delitos informáticos revelou lacunas conceituais que dificultam a aplicação das normas, uma vez que muitas leis são criadas sem considerar o avanço tecnológico. Crimes como a pornografia de vingança e o estelionato digital foram identificados, evidenciando a necessidade de uma abordagem legal mais robusta e atualizada. Em suma, a discussão sobre privacidade e crimes digitais é vital, considerando os desafios contemporâneos impostos pela era da informação.

**Palavras-chave:** Direito à Privacidade. Dignidade Humana. Sociedade Da Informação. Legislação. Crimes Digitais.

3895

**ABSTRACT:** The right to privacy is a fundamental aspect of human dignity, having evolved over time to reflect cultural and technological changes. Initially linked to the "right to be left alone," it now encompasses concepts such as the right to be forgotten and the inviolability of the home, correspondence, and communications. The rise of the information society has brought to light informational self-determination, allowing individuals to exert greater control over their personal data, promoting both individual and social protection. The internet, however, has complicated the protection of rights, such as the right to one's image, due to hyper-exposure and the difficulty in ensuring legal security. Legislation, such as Law No. 13,772/2018, has been adapted to address these new challenges, while the issue of privacy has gained prominence in the General Data Protection Law (LGPD). Furthermore, the analysis of cybercrimes has revealed conceptual gaps that hinder the application of norms, as many laws are created without considering technological advancements. Crimes such as revenge pornography and digital fraud have been identified, highlighting the need for a more robust and updated legal approach. In summary, the discussion of privacy and digital crimes is vital, given the contemporary challenges posed by the information age.

**Keywords:** Right to Privacy. Human Dignity. Information Society. Legislation. Digital Crimes.

<sup>1</sup> Discente- Universidade Unirg de Gurupi.

<sup>2</sup> Professor orientador da Universidade Unirg de Gurupi. Advogado.

## I INTRODUÇÃO

As interações virtuais têm ganhado destaque crescente, devido à necessidade de as pessoas se conectarem em diversos aspectos. Entretanto, esse ambiente não é explorado apenas para fins positivos, mas também por aqueles que o utilizam com intenções maliciosas. O ciberespaço, nome dado ao ambiente virtual, tem sido o palco para a prática de inúmeros crimes, muitas vezes cometidos por indivíduos que se escondem sob o véu da invisibilidade ou do anonimato.

Até os anos 1980, o uso da internet era praticamente exclusivo de universidades e órgãos governamentais. Contudo, nas últimas décadas, esse cenário mudou drasticamente, graças às melhorias nos serviços oferecidos pelos provedores, o que gerou um aumento expressivo no número de usuários de internet ao redor do mundo. Pesquisas recentes demonstram que, além do aumento significativo de internautas, o número de crimes virtuais também tem crescido.

As mídias digitais, móveis e sociais se tornaram parte indispensável da vida cotidiana global. Mais de 4,5 bilhões de pessoas agora acessam a internet, e os usuários de redes sociais superaram 3,8 bilhões. No entanto, o uso indevido de dados continua sendo uma preocupação, e cerca de metade dos internautas utiliza bloqueadores de anúncios.

Esse aumento no acesso ao ambiente virtual gerou debates sobre a necessidade de proteger novos bens jurídicos criados nesse espaço. É certo que, respeitando o princípio da intervenção mínima do direito penal, ele não deve criminalizar condutas meramente imorais. No entanto, após extensos debates sobre a criminalização de comportamentos no âmbito virtual e o surgimento de novos tipos penais e projetos de lei, tornou-se indispensável que o direito penal também se dedicasse à proteção desses novos bens jurídicos.

Foi apenas com a promulgação da Lei n. 12.737/2012 que os dados informáticos passaram a receber uma proteção penal mais clara, sendo reconhecidos como valores dignos de tutela jurídica. A partir desse momento, o tema ganhou mais relevância e passou a integrar discussões legislativas importantes.

Ademais, é importante destacar o caráter instantâneo das ações no ciberespaço. Uma vez divulgado um conteúdo no ambiente virtual, sua remoção ou exclusão muitas vezes se torna impossível se não for realizada imediatamente. Esse aspecto de permanência gera discussões complexas no âmbito jurídico.

Diante disso, é necessário compreender os conceitos e bens jurídicos envolvidos e como eles têm se transformado ao longo do tempo. Seja por meio da análise da evolução legislativa

ou doutrinária, é essencial entender como podemos cada vez mais combater, punir e prevenir condutas criminosas crescentes no ambiente digital.

Este artigo busca examinar a evolução de conceitos constitucionais, como dignidade humana, privacidade, intimidade, honra, imagem, correspondência e dados pessoais, sua inserção no mundo virtual e as mudanças nas premissas para a compreensão dos crimes cibernéticos. O objetivo é entender como esses novos conceitos influenciam a aplicação do direito penal.

O propósito deste estudo é analisar como o Estado pretende, atualmente, proteger os bens jurídicos consagrados pela Constituição Federal de 1988, em especial no que diz respeito aos ambientes virtuais, que transformaram radicalmente a estrutura da vida humana. Além disso, busca-se avaliar como e em que momentos o direito penal, uma construção histórica e pouco contemporânea, consegue ser eficaz na tutela desses bens em espaços imateriais e inovadores, desafiando os pressupostos tradicionais da aplicação da lei penal.

Por fim, será analisada a evolução dos direitos fundamentais frente à nova era dos dados, a forma como as inovações tecnológicas ampliam a atuação do direito penal e a necessidade de adaptação a uma variedade de novos crimes, com a devida abordagem dos conceitos essenciais que permeiam essa temática ao longo do estudo.

## 2 DOS DIREITOS FUNDAMENTAIS

Alguns dos primeiros direitos fundamentais reconhecidos pela Declaração Universal dos Direitos Humanos incluem o direito à vida, integridade física, liberdade, igualdade e propriedade. Contudo, inicialmente, não foram estabelecidos mecanismos eficazes para que o poder público garantisse esses direitos de forma preventiva, evitando danos a eles.

Os direitos fundamentais não surgiram de maneira uniforme, mas foram sendo reconhecidos gradualmente, conforme as demandas de cada época. Por isso, são classificados em gerações, de acordo com sua inserção nas constituições.

A primeira geração é composta pelos direitos civis e individuais, também chamados de direitos de liberdade, que limitam o poder do Estado e ampliam as liberdades individuais. Esses direitos surgiram com o liberalismo no século XVIII, como uma reação à arbitrariedade do Estado absolutista e às perseguições políticas e religiosas.

Superada a primeira geração, veio a segunda, que reconheceu os direitos sociais, como o direito ao trabalho, moradia e saúde. Cabia ao Estado promover o desenvolvimento da dignidade

humana. A aprovação da Segunda Declaração dos Direitos Humanos pela Assembleia Geral das Nações Unidas, em 10 de dezembro de 1948, representou um marco nesse sentido, consolidando um sistema de valores universais que materializava os ideais defendidos pelos jusnaturalistas.

A terceira geração de direitos fundamentais surgiu preocupada com a qualidade de vida e outros direitos personalíssimos, em resposta à industrialização e ao surgimento dos meios de transporte coletivo. Esses novos direitos surgiram em um contexto de crescente complexidade nas relações jurídicas, impulsionada pela revolução informacional e pela expansão dos meios de comunicação.

Com o avanço dos meios de transporte e o encurtamento das distâncias, inclusive no âmbito jurídico, e o desenvolvimento da tecnologia, surgiram os direitos fundamentais de quarta geração. Esses direitos dizem respeito ao direito de ser diferente, ao desenvolvimento da personalidade humana e à internacionalização das economias.

Diante dessa evolução, é essencial abordar o conceito de direitos fundamentais, conforme estabelecido na Constituição Federal de 1988. Esses direitos são entendidos como universais, garantindo aos cidadãos proteção contra abusos do Estado ou de particulares. Nesse contexto, os direitos fundamentais devem prevalecer sobre os interesses particulares ou estatais.

3898

No decorrer da história do constitucionalismo, observou-se uma evolução que culminou na construção e difusão de uma concepção de direitos fundamentais. Apesar de amplamente adotado no cenário constitucional moderno, esse conceito não é uniforme em todas as ordens jurídicas.

A Constituição de 1988 não previa o impacto que a internet teria sobre a vida cotidiana, como a transformação dos modos de viver, comprar e interagir. Em 1988, os direitos fundamentais tinham outra motivação, e sua perspectiva foi mudando ao longo do tempo.

Para Alexandre de Moraes:

O princípio que garante o sigilo de dados já considerava o uso de informações decorrentes da informática. Essa proteção, necessária devido ao surgimento de novas formas de armazenamento e transmissão de informações, deve se alinhar com os direitos à intimidade, honra e dignidade humana, a fim de impedir interceptações ou divulgações ilícitas.

Mesmo em 1988, as informações virtuais já eram vistas como merecedoras de inviolabilidade, embora de forma incipiente, recebendo uma proteção maior do que a oferecida ao sigilo bancário.

No final dos anos 1980, o Brasil ratificou os principais tratados internacionais de proteção aos direitos humanos e iniciou um processo intenso de produção legislativa. Em 2004, a Constituição de 1988 foi alterada para incluir a possibilidade de conferir status constitucional a normas internacionais de direitos humanos.

Quando se fala em direitos fundamentais e humanos no Brasil, questões como tortura, condições precárias nas prisões e altos índices de violência policial são frequentemente mencionadas. O Brasil está entre os países mais violentos do mundo, com suas condições prisionais sendo analisadas pela Corte Internacional de Direitos Humanos e a violência policial figurando entre as mais letais. No entanto, o debate sobre direitos humanos não se limita à violência física, prisional ou social. Outros fatores sociais também prejudicam o convívio e causam sérias consequências ao cotidiano. Nesse contexto, o Brasil ocupa a 5ª posição mundial em ataques cibernéticos.

A revolução tecnológica, inerente à sociedade da informação, trouxe novos desafios jurídicos, à medida que a internet, uma rede aberta e interativa, possibilita a atuação simultânea de diversos operadores. Isso gera consequências, especialmente no acesso irrestrito à informação. A ausência de fronteiras e a capacidade de alcançar inúmeras pessoas ao mesmo tempo tornam difícil apagar os rastros de ações online, o que coloca o direito à informação em uma nova perspectiva. Esse cenário exige reflexões inovadoras sobre as formas de proteção e controle desse direito.

## **2.1 Dignidade da pessoa humana**

O reconhecimento da dignidade humana pode se manifestar de várias formas, por meio de diferentes expressões, sem a necessidade de utilizar um termo específico para descrevê-la. A expressão "dignidade da pessoa humana" adquiriu relevância jurídica mais recentemente, sendo adotada quase de maneira universal por diversos países. Ao longo da história, várias civilizações foram, progressivamente, reconhecendo o conceito da dignidade humana.

No Brasil, a Constituição de 1988 foi o primeiro documento a mencionar a dignidade da pessoa humana de forma expressa, posicionando-a no preâmbulo como princípio que antecede os direitos fundamentais. Esse princípio reflete a intenção clara do constituinte de conferir aos princípios a força de normas que estruturam a ordem constitucional, elevando-os a fundamentos da República e do Estado Democrático de Direito.

Do ponto de vista jurídico, a dignidade da pessoa humana foi consagrada pela Constituição de 1988, especialmente no art. 1º, inciso III, que a reconhece como "fundamento da República". Essa dignidade também é mencionada em diversos outros dispositivos constitucionais, como os artigos 170, 226, 227 e 230. O Brasil ratificou e incorporou à sua legislação praticamente todos os tratados internacionais de direitos humanos que fazem referência à dignidade. Nos últimos quinze anos, a dignidade tornou-se um tema recorrente no discurso jurisdicional, o que gerou preocupações doutrinárias sobre a possível banalização do conceito.

Doutrinadores defendem que a dignidade é uma característica inerente e indissociável de todo ser humano, e que, em tese, o Estado e o Direito têm como objetivo respeitar e proteger essa qualidade. No entanto, o tema é controverso, sendo debatido tanto no campo doutrinário quanto na jurisprudência, devido às divergências sobre o significado e o conteúdo da dignidade para o ordenamento jurídico.

Para Guilherme de Souza Nucci, o princípio da dignidade humana deve ser interpretado sob duas perspectivas: objetiva e subjetiva. Sob o aspecto objetivo, a dignidade implica garantir um mínimo existencial para a pessoa, atendendo às suas necessidades vitais, conforme o art. 7.º, IV, da CF/1988, que trata do salário mínimo e das necessidades básicas de moradia, alimentação, educação, saúde, lazer, vestuário, higiene, transporte e previdência social. Subjetivamente, refere-se à autoestima e ao respeito intrínseco que a pessoa desenvolve ao longo da vida, interagindo em comunidade e merecendo reconhecimento, especialmente por parte do Estado.

3900

A dignidade é, portanto, uma qualidade inseparável de todo ser humano, conferindo-lhe direitos que devem ser respeitados, independentemente de suas características individuais. Ao longo do tempo, a noção de "ser pessoa" foi alterada drasticamente, sendo que, atualmente, todos os seres humanos, sem discriminação de raça, sexo, religião ou convicção política, têm o direito de serem tratados com dignidade, o que lhes garante direitos invioláveis por terceiros ou pelo Estado. Essa visão de dignidade fundamenta o conceito de Estado de Direito, que deve combater qualquer ação que atente contra essa qualidade humana.

Os direitos fundamentais derivam da própria existência humana e devem ser assegurados pelo Estado, como o direito à vida, à integridade física e à liberdade. O Estado, ao estabelecer garantias, assegura a instrumentalidade desses direitos, devendo seguir o devido processo legal, garantindo ampla defesa e contraditório para qualquer restrição à liberdade individual.

Ana Paula de Barcellos argumenta que a concepção de dignidade, para muitos brasileiros, está mais relacionada ao que o indivíduo possui ou faz, do que à sua simples condição de ser humano. Ela sugere que essa visão influencia a atuação de juízes e profissionais do Direito, afetando a formação de suas convicções e a escolha de suas prioridades.

Atualmente, a relação entre a dignidade da pessoa humana e os direitos fundamentais é reconhecida, mas muitas vezes a realização prática da dignidade ocorre por meio do exercício desses direitos. A dignidade, de caráter universal, é tanto a base quanto o objetivo dos direitos fundamentais, servindo como paradigma para sua aplicação.

Para Uadi Lamêgo Bulos, os princípios fundamentais são diretrizes básicas que orientam as decisões políticas essenciais à configuração do Estado brasileiro, determinando sua identidade e funcionamento.

Barcellos também divide os artigos constitucionais relacionados à dignidade humana em quatro níveis, conforme sua abrangência e precisão, destacando a importância da dignidade em diversos âmbitos da vida social.

Gustavo Tepedino reforça a relevância da dignidade humana como fundamento da República, associada ao objetivo de erradicar a pobreza e reduzir as desigualdades sociais, configurando-se como uma cláusula geral de tutela da pessoa humana, tomada como valor máximo pelo ordenamento jurídico.

Nesse sentido, a Constituição de 1988 atribuiu plena normatividade à dignidade da pessoa humana, reconhecendo que o Estado existe em função da pessoa, sendo o ser humano o fim principal das atividades estatais, e não um meio. O princípio da dignidade tornou-se um imperativo legal com ampla aplicação no direito brasileiro.

## 2.2 Direito a Privacidade

O direito à privacidade, embora atualmente considerado fundamental, não era sempre assim compreendido. No passado, era um privilégio reservado aos indivíduos com maior poder aquisitivo, dado que a posse de melhores condições financeiras lhes proporcionava a possibilidade de isolar-se do restante da população. Em 1890, a privacidade foi concebida como o "direito de ser deixado em paz", uma noção apresentada no artigo *The Right of Privacy*, que associava esse direito ao de estar só. No entanto, com o avanço da sociedade da informação a partir da década de 1960, a privacidade passou a ser entendida de forma mais ampla, englobando

o controle sobre a disseminação de informações pessoais, em vez de se limitar à ideia de isolamento.

Esse conceito evoluiu, especialmente em discussões sobre o direito ao esquecimento. Essa doutrina sustenta que um indivíduo deve ter o direito de desvincular-se de eventos embaraçosos ou vexatórios de seu passado, evitando assim que esses eventos prejudiquem sua honra, imagem e privacidade. Além disso, a privacidade é amparada por outros direitos fundamentais, como a inviolabilidade do domicílio e o sigilo de correspondências, consagrados no artigo 5º da Constituição Federal de 1988.

A noção de privacidade também foi objeto de estudos de diversos autores, como José Afonso da Silva, que definiu a intimidade e a vida privada como direitos autônomos, pertencentes ao gênero "direito à privacidade". A evolução desse direito, do liberalismo clássico para uma visão mais complexa nas relações sociais contemporâneas, merece uma análise detalhada, sobretudo no contexto de sua interação com os avanços tecnológicos.

No campo penal, o Supremo Tribunal Federal (STF) tem reconhecido o direito ao esquecimento como um princípio implícito na Constituição, derivado dos princípios da dignidade humana e da razoabilidade. Entretanto, o mesmo tribunal, ao julgar questões no âmbito cível, decidiu que o direito ao esquecimento é incompatível com a Constituição quando invocado para impedir a divulgação de fatos verídicos e legalmente obtidos.

3902

Além disso, a legislação brasileira, como o Marco Civil da Internet, estabelece princípios de proteção à privacidade nas plataformas digitais. O artigo 21 da Lei Federal n.º 12.965/2014 determina que provedores de internet podem ser responsabilizados se não tomarem medidas diligentes para remover conteúdos que violem a intimidade de usuários.

A tutela da privacidade, conforme apresentada por autores como Marcel Leonardi, vai além da proteção individual, sendo fundamental para a preservação da estrutura social. A privacidade, atualmente, não se refere mais apenas ao direito de estar só, mas ao direito de controlar as informações pessoais e o modo como são utilizadas.

### **2.3 Correspondência, comunicações telegráficas e telefônicas**

O direito ao sigilo das comunicações no Brasil tem suas raízes nas primeiras constituições do país, incluindo a de 1824, que já reconhecia a proteção à correspondência, e foi consolidado com a Constituição de 1988. Este direito abrange o sigilo da correspondência, das comunicações



telegráficas, telefônicas e, mais recentemente, eletrônicas, como e-mails e mensagens instantâneas enviadas por aplicativos como *WhatsApp* e *Telegram*.

A Constituição de 1988 introduziu uma limitação a esse sigilo ao permitir a interceptação de comunicações telefônicas, desde que por ordem judicial, exclusivamente para fins de investigação criminal ou instrução processual penal. Essa exceção não se aplica a outras formas de comunicação, como correspondências tradicionais e comunicações telegráficas, que permanecem amplamente protegidas. O Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ) têm reconhecido essa proteção tanto para comunicações físicas quanto eletrônicas.

A Lei nº 9.296/1996, conhecida como a Lei de Interceptação Telefônica, regulamenta essa possibilidade de quebra de sigilo, e desde então os tribunais têm permitido interceptações em conformidade com os requisitos legais. Apesar disso, o sigilo das comunicações eletrônicas, especialmente em tempos de criptografia e de maior uso de aplicativos de mensagens instantâneas, tem gerado novos desafios para a aplicação da lei.

No ambiente virtual, a criptografia de ponta a ponta, utilizada em aplicativos como *WhatsApp* e *Telegram*, garante uma proteção quase absoluta ao sigilo das comunicações. Em algumas ocasiões, esses aplicativos recusaram-se a fornecer informações ao Poder Judiciário, resultando na suspensão temporária de seus serviços no Brasil, como ocorreu com o *WhatsApp* em 2015 e 2016 e o *Telegram* em 2022.

Essas suspensões reacenderam o debate sobre a extensão do direito ao sigilo das comunicações no contexto digital. A criptografia dificulta ou até impede o acesso a dados por parte do Estado, o que levanta questões sobre o equilíbrio entre a proteção ao sigilo e a necessidade de fiscalização estatal em investigações criminais. A Carta Portuguesa de Direitos Humanos na Era Digital, por exemplo, reconhece a criptografia como um direito fundamental à privacidade, fortalecendo o sigilo das comunicações eletrônicas.

Contudo, essa proteção extrema tem gerado discussões sobre se o direito ao sigilo das comunicações não estaria sendo excessivamente garantido, a ponto de prejudicar a segurança pública e o controle social. As instâncias de justiça e os legisladores continuam a buscar um equilíbrio entre o direito à privacidade e a necessidade de acesso a informações em casos legais, especialmente diante dos desafios apresentados pelas novas tecnologias e pela criptografia.

### 3. CRIMES CIBERNÉTICOS

Agora, adentra-se nos aspectos dos principais crimes relacionados à prática de ilícitos pela internet, sendo necessário analisar e detalhar cada uma dessas condutas para compreender suas particularidades e os desafios impostos pelo mundo digital.

#### 3.1 Conceito de "crime cibernético"

A internet trouxe novos riscos de violação de direitos, especialmente no que tange aos direitos de personalidade, tornando essas violações mais complexas e frequentes. O direito penal, por sua natureza reativa, passou a se preocupar mais com a proteção de direitos ameaçados nos ambientes virtuais, oferecendo uma tutela mais forte com o tempo. Isso incluiu a criação de novos conceitos e termos voltados à proteção de direitos potencialmente violados no ambiente online.

Nesse sentido, Paulo Marco Ferreira Lima argumenta:

Diante da evolução tecnológica, há uma tendência social de reconhecer bens jurídicos informáticos, com destaque para o sigilo e a segurança de dados e informações eletrônicas” (LIMA, 2011).

O surgimento de uma nova área de proteção penal trouxe consigo termos e conceitos até então desconhecidos, que passaram a compor o que se denomina "crime cibernético". Antes de explorar as diferentes modalidades desses crimes e suas implicações, é necessário estabelecer um conceito preliminar de "crime cibernético".

3904

Embora seja possível abordá-lo sob uma perspectiva social e criminológica, interessa aqui a classificação dogmática penal, focando nos sujeitos (ativo e passivo), nos bens jurídicos protegidos e nas condutas. Assim, apesar da relevância social e criminológica do tema, o foco será na conceituação dogmática do delito cibernético.

Parte da doutrina se esforça para diferenciar crimes informáticos de crimes cibernéticos. Segundo Carlos María Romeo Casabona, o termo "crime informático" foi utilizado historicamente para designar:

- (i) condutas que violam gravemente bens jurídicos relacionados diretamente a dispositivos ou atividades informáticas, sendo o dispositivo ou seu conteúdo o objeto do delito;
- (ii) condutas tipificadas que podem ser cometidas através de dispositivos informáticos, mas cuja natureza não depende deles; e
- (iii) condutas em que o bem jurídico violado é o próprio dispositivo informático. Isso demonstra que a expressão "crimes informáticos" abrange várias situações, sem uma uniformidade metodológica que justifique tantas variações.

O crime cibernético, por outro lado, refere-se a condutas envolvendo o acesso, apropriação, troca e disponibilização de informações em redes telemáticas, sem consentimento ou autorização, ou utilizando conteúdos ilícitos, com potencial de lesar bens jurídicos individuais ou coletivos. Dessa forma, os crimes informáticos e cibernéticos podem coexistir, sendo os últimos uma "geração posterior" aos primeiros.

Alguns autores, como Helena Carrapiço, não distinguem entre crimes informáticos e cibernéticos. Ela afirma que o cibercrime pode ser classificado em dois tipos: (i) quando a informática é o alvo do crime, como no caso de alteração de dados de um sistema, e (ii) quando a informática é utilizada como instrumento para atacar bens jurídicos.

Além disso, algumas obras discutem o conceito de um "direito penal cibernético", que seria uma ferramenta preventiva usando tecnologias como biometria e monitoramento eletrônico para prevenir certos crimes.

Para este estudo, a definição mais adequada de crimes cibernéticos é aquela que os entende como delitos cometidos por meio da internet e dispositivos informáticos, ou contra esses dispositivos e seus conteúdos. Isso porque a distinção entre "crime informático" e "crime cibernético", apesar de relevante em certas discussões, parece mais teórica do que prática, uma vez que é raro falar de crimes cibernéticos que não sejam também informáticos.

A principal diferença entre um crime informático e um crime comum é que, no caso do crime informático, a conduta criminosa envolve diretamente o uso ou o ataque a dispositivos informáticos, enquanto no crime comum a proximidade física entre o agente e a vítima é geralmente uma característica importante. Esse aspecto traz um desafio para o direito penal clássico, que foi desenvolvido para lidar com crimes cometidos no mundo físico.

Com esses conceitos preliminares esclarecidos, é possível explorar os tipos penais relacionados a esses crimes, detalhando seus elementos constitutivos e demais aspectos relevantes.

### **3.2 Principais crimes cibernéticos**

Com base nas informações já discutidas, passamos agora à análise prática dos principais temas relacionados aos crimes digitais. Esse estudo é fundamental para compreender melhor o contexto, os problemas mais evidentes e as lacunas legais existentes nessa área, além de abordar as discussões doutrinárias ainda não resolvidas, trazidas pela nova realidade da era da internet.

#### **3.2.1 Estupro virtual**

Antes de aprofundarmos o conceito de estupro virtual, é necessário abordar o delito de estupro e suas modificações recentes. Até 2009, o crime de estupro era definido como o

constrangimento de uma mulher à conjunção carnal mediante violência ou grave ameaça. Esse conceito limitava o crime apenas à penetração vaginal e à vítima feminina, com pena prevista de seis a dez anos de reclusão.

Com a entrada em vigor da Lei nº 12.015/2009, houve mudanças significativas nas disposições sobre crimes sexuais no Código Penal. A nova legislação ampliou a definição de estupro, que não se restringe mais à conjunção carnal, e passou a reconhecer outras formas de violência sexual. José Ricardo Chagas explica que o artigo 213, na sua nova redação, contempla a conjunção carnal como uma das elementares do crime, mas também estende a figura da vítima para incluir homens, eliminando a exclusividade da mulher como sujeito passivo. Assim, a conjunção carnal não se limita apenas à cópula vaginal, abrangendo tanto relações vaginais quanto anais, com homens ou mulheres como vítimas.

Antes de 2009, o crime de "atentado violento ao pudor" também existia, caracterizado pela coerção de alguém, mediante violência ou ameaça, a praticar ou permitir que se praticasse ato libidinoso diverso da conjunção carnal. Com a nova lei, esse delito foi incorporado ao crime de estupro, passando a abranger uma gama mais ampla de condutas sexuais não consensuais. Além disso, o novo artigo 213 possibilitou que múltiplas condutas tipificadas como crimes sexuais fossem tratadas como um único delito, sendo considerado um tipo penal misto alternativo.

3906

A Lei nº 12.015/2009, portanto, unificou os crimes de estupro e atentado violento ao pudor, além de ampliar o reconhecimento da violência sexual contra qualquer pessoa, independentemente de gênero. Dessa forma, o estupro passou a ser caracterizado pela coerção de alguém, mediante violência ou grave ameaça, a praticar ou permitir a prática de atos libidinosos, ainda que sem contato físico ou proximidade entre agente e vítima, o que antes era impensável devido ao foco na conjunção carnal.

Com essa nova redação, o estupro inclui tanto a penetração vaginal quanto outros atos libidinosos, abrangendo qualquer ato sexual não consensual imposto mediante violência ou grave ameaça. Para que o delito seja caracterizado, é fundamental que se comprove a satisfação do autor com os atos praticados, demonstrando sua intenção ao cometer o crime. No entanto, a intenção pode ser manifestada sem a presença física, desde que haja coerção.

Outro ponto crucial é o consentimento, que distingue uma relação sexual consensual de um crime de estupro. O ato sexual deve ocorrer com o consentimento livre e esclarecido de todas as partes envolvidas. O estupro não exige necessariamente contato físico direto, podendo

ocorrer mesmo sem penetração, como em atos sexuais não consensuais cometidos através de coerção, violência ou ameaça.

Diante dessa concepção mais ampla, surge a possibilidade de que o estupro possa ser consumado de forma virtual. O termo "estupro virtual" se refere a casos em que a violência sexual ocorre online, sem contato físico direto, por meio de coerção ou ameaça através da internet, obrigando a vítima a participar de atividades sexuais contra sua vontade.

O Superior Tribunal de Justiça (STJ) já determinou que, tanto para o crime de estupro (art. 213), quanto para o estupro de vulnerável (art. 217-A), não é indispensável o contato físico. A dignidade sexual deve ser respeitada, e qualquer coerção sexual pode ser enquadrada como estupro, mesmo que ocorra em ambiente virtual. Um exemplo seria o ato de obrigar alguém, sob ameaça, a se despir enquanto o agressor se masturba, configurando estupro sem contato físico direto.

Portanto, o estupro pode ocorrer sem penetração física, desde que haja coerção ou ameaça, e a consumação do crime se dá com o constrangimento, não com o contato físico. O verbo central da definição legal é "constranger", no sentido de forçar a vítima a um ato sexual, seja pela prática da conjunção carnal ou por outros atos libidinosos.

No entanto, alguns doutrinadores questionam a viabilidade de se provar a intenção de obtenção de prazer sexual por parte do autor do crime em um cenário virtual, argumentando que, sem a presença física, seria difícil comprovar o elemento subjetivo do crime. Eles defendem que, sem uma grave ameaça que cause coação moral irresistível, não estaríamos diante de um estupro, mas sim de um constrangimento ilegal, o que resultaria em uma punição desproporcional ao ato praticado.

3907

### 3.2.2 Divulgação de Segredo

O crime de divulgação de segredo, previsto no artigo 153 do Código Penal de 1940, já indicava como conduta criminosa a divulgação, sem justa causa, de conteúdo de documento particular ou correspondência confidencial, desde que pudesse causar dano a outra pessoa. A definição de "segredo" refere-se à informação que uma pessoa deseja manter oculta, gerando um dever de sigilo para quem teve acesso a tal informação.

Guilherme de Souza Nucci sintetiza o conceito de segredo como algo "que não merece ser revelado a ninguém". Embora o artigo mencione a "correspondência", o bem jurídico protegido é a inviolabilidade da intimidade, não a correspondência em si. Assim, o crime de divulgação

de segredo não se confunde com o de violação de correspondência, já que ambos protegem bens jurídicos diferentes.

A divulgação de segredos somente se configura crime se a informação estiver contida em documento particular ou correspondência confidencial. Segredos revelados oralmente ou obtidos por outras fontes não são alcançados pela legislação penal neste caso. Entretanto, com o avanço da tecnologia, muitas informações sigilosas passaram a ser armazenadas em bancos de dados ou sistemas de informação, tornando insuficiente a proteção dada pela redação original do Código Penal.

Com a edição da Lei n. 9.983/2000, foi incluído o §1º-A no artigo 153 do Código Penal, ampliando o tipo penal para abarcar a divulgação de informações sigilosas ou reservadas contidas em sistemas de informação e bancos de dados da Administração Pública. A consumação do crime ocorre pela simples divulgação das informações, sem necessidade de um resultado naturalístico, caracterizando-se como crime formal.

A doutrina debate se os sistemas de informação mencionados no §1º-A pertencem exclusivamente à Administração Pública, embora haja uma tendência a interpretar o tipo penal dessa forma. De todo modo, o prejuízo à Administração Pública não é requisito para a consumação do crime, como sugere o §2º do artigo 153, mas apenas condição para que a ação penal seja incondicionada.

3908

Contudo, o tipo penal não prevê sanção mais severa para a divulgação de segredo por meios de comunicação de massa, como redes sociais, apesar do impacto significativamente maior dessas plataformas. Crimes contra a honra, por exemplo, têm penalidades mais graves quando cometidos em redes sociais, conforme o art. 141 do Código Penal, que triplica as penas para crimes de calúnia, injúria e difamação cometidos nesse contexto.

A divulgação de informações sensíveis em plataformas digitais é muito mais eficiente e abrangente, e deveria ser punida com maior rigor, assim como ocorre com crimes de indução ou instigação ao suicídio ou à automutilação. A Lei n. 13.968/2019 dobrou a pena para esses crimes quando cometidos por meio de redes sociais ou transmissão em tempo real.

Diante do aumento no uso de plataformas digitais e da facilidade de disseminação de informações, há uma necessidade crescente de adaptar o Código Penal para refletir essas mudanças tecnológicas. Portanto, a adequação das penalidades para crimes de divulgação de segredo em ambientes virtuais seria uma medida coerente com a evolução das práticas criminais e a política criminal adotada pelo legislador.

### 3.2.3 Invasão de dispositivo informático

A invasão de dispositivo informático foi tipificada no direito penal brasileiro pela Lei Federal n. 12.737/2012, conhecida como "Lei Carolina Dieckmann". Essa legislação foi aprovada após o incidente envolvendo a atriz Carolina Dieckmann, cujo dispositivo informático foi invadido, resultando no vazamento de fotos íntimas na internet. A lei visa proteger a inviolabilidade dos segredos, o direito à privacidade, à honra, e à livre manifestação de pensamento, sem a intromissão de terceiros.

Antes da promulgação da lei, invasões de dispositivos informáticos não eram tipificadas de forma clara, o que gerava insegurança jurídica. A Lei Carolina Dieckmann alterou o Código Penal Brasileiro (CP/1940), incluindo o artigo 154-A, posteriormente modificado pela Lei Federal n. 14.155/2021, que endureceu as penas para crimes cibernéticos como invasão de dispositivos, furto e estelionato eletrônico.

No entanto, ainda existem dúvidas sobre o conceito de "dispositivo informático" e se redes sociais, que também são vulneráveis a invasões, se enquadram nesse conceito. Enquanto dispositivos como computadores, smartphones e tablets são claramente classificados como dispositivos informáticos, as redes sociais, que podem ser alvo de invasões, são vistas como um ambiente distinto, mas igualmente sensível.

3909

Essa discussão é fundamental, uma vez que, segundo uma pesquisa do Ministério Público de Minas Gerais, a invasão de perfis de redes sociais foi um dos crimes cibernéticos mais frequentes em 2022. A doutrina traz um entendimento de que o dispositivo informático abrange qualquer equipamento que possa armazenar, processar ou transmitir dados digitais, incluindo computadores e *smartphones*.

Outro ponto relevante foi a alteração no texto da lei em 2021, que retirou a exigência de violação de mecanismos de segurança como condição para configurar a invasão, abrangendo qualquer acesso não autorizado ao dispositivo. A mudança foi vista como uma resposta a críticas anteriores, onde apenas invasões que envolvessem quebra de barreiras de segurança seriam puníveis, deixando outras formas de invasão desprotegidas.

Além disso, o conceito de "usuário" do dispositivo foi destacado na nova redação da lei, diferenciando-o do proprietário, ampliando a proteção para aqueles que utilizam o equipamento, independentemente de quem é o dono. A pena para o crime também foi aumentada, com a reclusão variando de 1 a 4 anos.

Por fim, a invasão qualificada ocorre quando a conduta resulta em obtenção de comunicações privadas, segredos comerciais ou industriais, ou controle remoto do dispositivo, elevando a pena para reclusão de 2 a 5 anos.

#### 4. CONCLUSÃO

O direito à privacidade é um direito essencial para a humanidade, intrínseco à própria condição humana, e busca proteger a dignidade da pessoa. Com o tempo, esse conceito evoluiu, partindo da ideia inicial de “direito de ser deixado em paz” para abarcar uma construção mais complexa, tanto cultural quanto tecnológica. Com o desenvolvimento da sociedade da informação, a privacidade passou a incluir o direito ao esquecimento, assim como a inviolabilidade do domicílio, correspondência e o sigilo das comunicações. Atualmente, a privacidade está mais associada à autodeterminação informativa, permitindo maior controle sobre os dados pessoais, com o objetivo de proteger não só o indivíduo, mas também o equilíbrio entre a vida privada e o direito à informação, que é um dos maiores pontos de conflito.

A internet aumentou a complexidade de proteger vários direitos, como o direito à imagem, devido à hiperexposição. A dificuldade em garantir a proteção jurídica desses direitos aumentou, especialmente considerando a estreita relação entre imagem e honra, que são conceitos difíceis de separar em casos de ofensas nas redes sociais. Isso motivou ajustes legislativos, como a criação da Lei nº 13.772/2018.

3910

Diante desse cenário, conceitos como a inviolabilidade da correspondência e das comunicações telegráficas e telefônicas foram significativamente atualizados com o tempo, não apenas devido aos avanços tecnológicos, mas também pela gravidade das violações desses direitos. O sigilo da correspondência sempre foi tratado como uma proteção pessoal, diferentemente do sigilo telefônico e telemático, que só começou a ser discutido seriamente com a Lei de Interceptação Telefônica, de 1996, que criminalizou a violação dessas formas de comunicação. As conversas via aplicativos de mensagens e redes sociais também foram incluídas nesse rol de proteção, dada a gravidade de suas violações.

Embora a questão não envolva diretamente o direito penal, sua relevância é evidente, especialmente com a inclusão de dados pessoais como um direito fundamental, destacada pela Lei Geral de Proteção de Dados (LGPD). Esta legislação trouxe à tona debates sobre o valor dos dados pessoais e a necessidade de proteção diante de seu potencial de causar danos quando expostos.



A pesquisa sobre delitos informáticos evidenciou várias lacunas conceituais que dificultam a aplicação das normas. Muitas leis são criadas sem acompanhar o ritmo das inovações tecnológicas, o que gera desafios para a aplicação da lei, devido à falta de definições claras e ao conhecimento técnico necessário sobre sistemas e o uso da internet em várias situações.

Além disso, observou-se que certos crimes, quando cometidos no ambiente virtual, recebem penas mais severas. É o caso dos crimes contra a honra, cujas penas foram recentemente triplicadas se ocorridos na internet, em razão do potencial lesivo ampliado pela rede, já que a internet permite uma divulgação permanente e difícil de apagar.

Outro crime que merece destaque é a pornografia de vingança, criminalizada em 2018 com a inclusão do artigo 218-C no Código Penal. Esse dispositivo visa proteger vítimas contra a divulgação de cenas íntimas sem consentimento, e prevê um aumento de pena quando o autor tem ou teve uma relação íntima com a vítima, tratando-se de um ato de vingança.

O crime de estelionato também foi remodelado para se adaptar às possibilidades trazidas pelo mundo digital. Ele pode ser facilmente identificado em fraudes como a criação de sites falsos e a compra de mercadorias usando dados de terceiros. Muitas dessas condutas são sofisticadas formas de enganar, baseadas em técnicas de engenharia social.

3911

Na engenharia social, o criminoso manipula a vítima para obter informações, sem precisar usar ferramentas tecnológicas avançadas, mas sim pela capacidade de convencimento e exploração de falhas no conhecimento dos usuários e nas vulnerabilidades dos sistemas.

Outro ponto relevante para essa pesquisa foi a menção aos inquéritos das "Milícias Digitais" e das "Fake News". O Inquérito 4.781, conhecido como das Fake News, investiga a disseminação em massa de informações falsas na internet, que ofendem e ameaçam autoridades. O inquérito sobre milícias digitais examina grupos que atuam de forma organizada para atacar a democracia e o Estado de Direito. Ambos os casos ressaltam a importância de se discutir os desafios impostos pela internet, que se tornou um meio difícil de controlar e cuja influência cresce exponencialmente.

## REFERÊNCIAS

AFFONSO, Filipe José Medon. O direito à imagem na era das deepfakes. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 27, n. 01, p. 260, mar. 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438>. Acesso em: 30 nov. 2022.

ANDRADE, Pedro Victor Silva de. Tutela da honra nas redes sociais: a contribuição possível da teoria da impolidez. 2019. Tese (Doutorado em Direito), Universidade Federal de Minas Gerais, Belo Horizonte, 2019. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/32323/7/Dissertac%cc%a7a%cc%83o%2ode%2oMestrado%2o-%>. Acesso em: 11 maio 2023.

ANDREUCCI, Ricardo Antonio. Manual de direito penal. 13. ed. São Paulo: Saraiva, 2019.

ARENDDT, Hannah. Eichmann em Jerusalém: um relato sobre a banalidade do mal. Trad. José Rubens Siqueira. São Paulo: Companhia das Letras, 1999.

ARROYO, César Landa. Dignidad de la persona humana. *Ius et Veritas*, v. 10, n. 21, 9 dez. 2000. Disponível em: <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15957>. Acesso em: 15 maio 2023.

AZEVEDO, Antônio Junqueira de. Caracterização jurídica da dignidade da pessoa humana. *Revista Trimestral de Direito Civil*, Rio de Janeiro: Padma, v. 9, p. 03, jan.-mar. 2002.

BADARÓ, Gustavo Henrique. Processo penal. 9. ed. São Paulo: Thomson Reuters, 2021 (ebook).

BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*. Rio de Janeiro, ano 3, n. 2, jul.-dez. 2014. Disponível em: <http://civilistica.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativoaconcretizacao-do-principio-dadignidade-da-pessoa-humana/>. Acesso em: 11 maio 2022.

3912

BARCELLOS, Ana Paula. Violência urbana, condições das prisões e dignidade humana. *Revista de Direito Administrativo*, n. 254, 2010.

BARRETO, Eduardo Mussnich. Terrorismo cibernético e cenários especulativos. *Revista Brasileira de Inteligência, ABIN*, v. 3, n. 4, Brasília, 2007.

BARROS, Flavio Augusto Monteiro de. Direito penal: parte geral. São Paulo: Saraiva, 2006.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo. 9. ed. São Paulo: SaraivaJur, 2020.

BERGONSO, Carlos Henrique Terçariol. Da fiscalização em face da Lei Geral de Proteção de Dados. In: OAB-SP. Comissão de Direito Digital, Tecnologia e Inteligência Artificial da OAB-SP. 116ª Subseção: Jabaquara – Saúde (org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo, 2020.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral. 22. ed. São Paulo:

Saraiva, 2016.

BITENCOURT, Cezar Roberto. Código Penal comentado. São Paulo: Saraiva, 2019. (ebook). Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788553615704/>. Acesso em: 12 maio 2023.

BORNHOLDT, Rodrigo Meyer. Liberdade de expressão e direito à honra: uma nova abordagem no direito brasileiro. Joinville: Bildung, 2010, p. 307 apud HARTMANN, Ivan Alberto Glasherster Martins Lange. Manifestação, honra e ódio na internet: a proteção da liberdade de expressão por meio da capacidade comunicativa e da autorregulação. 2018. Tese (Doutorado em Direito), Universidade do Estado do Rio de Janeiro (UERJ), Rio de Janeiro, 2018. Disponível em: <https://www.bdtd.uerj.br:8443/bitstream/1/9203/2/Tese%20%20Ivar%20Hartmann%20-%202018%20-%20Completa.pdf>. Acesso em: 22 nov. 2022.

BUFFON, Jaqueline Ana. Agente infiltrado virtual. In: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. Crimes cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. Brasília, MPF, 2018. 275 p. Coletânea de artigos v. 3. Disponível em: <https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticoscoletanea-de-artigos>. Acesso em: 12 maio 2023.

CABRAL, Camilla C. R. Interceptação telefônica: análise da Lei n. 9.296/96 segundo o entendimento dos Tribunais Superiores. Conteúdo Jurídico. 18 abr. 2016. Disponível em: <http://www.conteudojuridico.com.br/consulta/Artigos/46430/interceptacaotelefonicaanalise-da-lei-no-9-296-96-segundo-o-entendimento-dos-tribunais-superiores>. Acesso em: 26 dez. 2022.

3913

CARRAPIÇO, Helena. O crime organizado e as novas tecnologias: uma faca de dois gumes. Portugal: Instituto da Defesa Nacional. 2005. Disponível em: <http://hdl.handle.net/10400.26/1156>. Acesso em: 13 dez. 2022.

CASABONA, Carlos María Romeo. Dos delitos informáticos ao crime cibernético: uma aproximação conceitual e político-criminal. In: Ciências Penais, Revista da Associação Brasileira de Ciências Penais, v. 3, n. 4, p. 88-89, jan.-jun. 2006. São Paulo: RT, 2006. Disponível em: <http://bdjur.stj.jus.br/dspace/handle/2011/78605>. Acesso em: 13 dez. 2022.

COSTA NETO, João. Dignidade humana: visão do Tribunal Constitucional Alemão, do STF e do Tribunal Europeu. São Paulo: Saraiva, 2014.

COSTA, José de Faria. O direito penal, a informática e a reserva da vida privada. Portugal, Coimbra, Faculdade de Direito de Coimbra, 1996.

COENEN, Tanguy et al. Knowledge sharing over social networking systems: architecture, usage patterns and their application. In: OTM confederated international conferences on the move to meaningful internet systems. Springer, Berlin, Heidelberg, 2006.

CRETELLA JUNIOR, José. Comentários a Constituição Brasileira de 1988. v. I. 3 v. Rio de Janeiro: Forense, 1992.

CUSTÓDIO, Antônio Joaquim Ferreira. Constituição Federal interpretada pelo STF. 8. ed. São Paulo: Juarez de Oliveira, 2004.

DONEDA, Danilo. A proteção dos dados pessoais como direito fundamental. Espaço Jurídico Journal of Law, Chapecó, v. 12, n. 2, p. 93, dez. 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 11 set. 2022.

FERNANDES, Antônio Scarance. Considerações sobre a Lei 8.072/ 90, de 25 de julho de 1990 – crimes hediondos. São Paulo: RT, 1990.

FIGUEIREDO, Rudá. Crimes eletrônicos e Lei 14.155/2021. Disponível em: [https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/codigo\\_penal\\_-\\_parte\\_especial/crimes\\_eletronicos\\_e\\_lei\\_14.155-2021.pdf](https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/codigo_penal_-_parte_especial/crimes_eletronicos_e_lei_14.155-2021.pdf). Acesso em: 23 maio 2023.

FRANCO, Alberto Silva. Crimes hediondos: anotações sistemáticas à Lei n. 8.072/ 90. 4. ed. São Paulo: RT, 2000.

FRISTER, Die Notwehr im System der Notrechte, GA 1988, p. 29 1; HAFT, Strafrecht, 1994, p. 82-84; ROXIN, Strafrecht, 1997, § 15, n. 1.

GOMES, Luiz Flávio; MACIEL, Silvio. Interceptação telefônica e das comunicações de dados telemáticos: comentários à Lei 9.296/1996. 4. ed. São Paulo: RT, 2018.

GRECO, Rogério. Curso de direito penal: parte especial. Arts. 213 a 361 do Código Penal. v. 3. 3914  
São Paulo: GEN, 2022.

GRINOVER, Ada Pellegrini. Liberdades públicas e processo penal: as interceptações telefônicas. São Paulo: Saraiva, 1986.

HABERLE, Peter. Derecho constitucional y cultura. (coord.) Francisco Balaguer Callejón. Espanha: Tecnos, 2004.

HALL, Holly Kathleen. Deepfake videos: when seeing isn't believing, 27 CATH. U. J. L. & TECH 51, 2018, p. 57. Disponível em: <https://scholarship.law.edu/jlt/vol27/iss1/4>. Acesso em: 30 nov. 2022.

HELD, David; MCGREW, Anthony; GOLDBLATT, David; PERRATON, Jonathan. Global transformations politics, economics, and culture. Cambridge Politic Press, 1999.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O direito civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020.

JAKOBS, Günther. A imputação objetiva no direito penal. Trad. André Luís Callegari. São Paulo: RT, 2000.

JESUS, Damásio de. Direito penal: parte geral. 32. ed. São Paulo: Saraiva, 2011.

JESUS, Damásio de; MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

JUNQUEIRA, Gustavo; VANZOLINI, Patrícia. Manual de direito penal: parte geral. 5. ed. São Paulo: Saraiva Educação, 2019.

KUHL, Strafrecht, 1997, § 7, n. 41; ROXIN, Strafrecht, 1997, § 15, n. 24-25.

LEITE, George Salomão; LEMOS Ronaldo (coord.). Marco Civil da Internet. São Paulo: Atlas, 2014.

LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2012.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. Revista da Faculdade de Direito UFPR, Curitiba, PR, Brasil, v. 63, n. 3, p. 136-137, set.-dez. 2018. Disponível em: <https://revistas.ufpr.br/direito/article/view/59422>. Acesso em: 07 dez. 2022.

LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. São Paulo: Atlas, 2011.

LIMA, Renato Brasileiro de. Legislação criminal especial comentada. 8. ed. Salvador: JusPodivm, 2020.

LORENZETTI, Ricardo Luis. Fundamentos do direito privado. São Paulo: RT, 1998.

MACHADO, José Eduardo Marcondes. O direito ao esquecimento e os direitos da personalidade. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/cc13>. Acesso em: 8 mar. 2023.

MARTINI, Renato. Sociedade da informação – para onde vamos. São Paulo: Trevisan, 2017.

MAURACH/ZIPF, Strafrecht I, 1992, § 26, n. 8-21.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5.276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. Revista Brasileira de Políticas Públicas, v. 7, n. 3, 2017.

MORAES, Alexandre de. Constituição do Brasil interpretada e legislação constitucional. 5. ed. São Paulo: Atlas, 2005.

NOLASCO, Thiago Guilherme. A honra enquanto bem jurídico: sobre a tutela penal da autoestima e da consideração social. Rio de Janeiro: Lumen Juris, 2019.

NUCCI, Guilherme de Souza. *Princípios constitucionais penais e processuais penais*. 4. ed. Rio de Janeiro: Forense, 2015.

NUVOLONE, Pietro. *Il sistema del diritto penale*. Italia, Padova: Casa Editrice Dott Antonio Milani, 1975.

OLIVÉ, Juan Ferré; PAZ, Miguel Nunez; OLIVEIRA, William Terra de; BRITO, Alexis Couto de. *Direito penal brasileiro – parte geral*. São Paulo: RT, 2011.

PAYÃO, Felipe. Hackear perfis ou páginas de Facebook é crime e rende até 5 anos de prisão. *Tecmundo*, 21 set. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/134497-hackear-perfis-paginas-facebook-crime-rende-5-anos-prisao.htm>. Acesso em: 15 dez. 2022.

SANTOS, Maria do Rosário Laureano. Aspectos culturais da concepção de justiça na Roma antiga. Disponível em: <https://journals.openedition.org/cultura/1643>. Acesso em: 19 mar. 2023.

SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais constitucionais na Constituição Federal de 1988*. Porto Alegre: Livraria do Advogado, 2002.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. Sextorsão. *Revista dos Tribunais São Paulo*, n. 959, set. 2015. Disponível em: <http://dspace/xmlui/bitstream/item/21008/1.pdf?sequence=1>. Acesso em: 14 dez. 2022.