

RESPONSABILIDADE PENAL DA PESSOA COLETIVA E O PRINCÍPIO DA CULPABILIDADE NOS CRIMES INFORMÁTICOS EM REDES SOCIAIS

Karina Silveira de Almeida Hammerschmidt¹

Décio Franco David²

RESUMO

A internet possibilita a socialização de informações e dados, sendo meio de comunicação rápido e amplamente utilizado, devendo seguir princípios éticos e morais da cibersociedade. Porém, diariamente diversos ilícitos afetam a sociedade, evidenciando falsidade informática e responsabilidade de pessoas coletivas. Diante deste desafio mundial, criou-se a Convenção de Budapeste; sendo que no Brasil, os ilícitos cibernéticos são enquadrados no Direito Penal, utilizando-se o modelo de heterorresponsabilidade, alinhado à Lei Ricochete. Neste contexto, teve-se objetivo de analisar a responsabilidade penal da pessoa coletiva e o princípio da culpabilidade nos crimes informáticos (falsidade informática) em redes sociais. Para tanto realizou-se estudo dedutivo sobre a temática. Os delitos cometidos na internet, realizados com utilização de dispositivos eletrônicos, evidenciam a importância do Direito buscar e promover efetiva proteção individual e coletiva. Alinhar preceitos do direito informático nos espaços virtuais, principalmente nas redes sociais, significa fomentar publicações com dados verdadeiros, evitando Fake News e trazendo segurança jurídica. Nos meios de comunicação virtuais, nem sempre é possível identificar o autor dos dados publicados, prejudicando a identificação do responsável pelos danos que podem ser causados, porém o conteúdo das publicações não exclui a responsabilidade coletiva, conforme Marco Civil da Internet. A dificuldade em identificar a origem do crime, âmbito individual e coletivo, prejudica e complexifica o ambiente jurídico, fomentando a discussão sobre a responsabilidade penal da pessoa coletiva nas redes sociais, com a culpabilidade da falsidade informática. O Direito Penal pode combater os crimes cibernéticos, visando gerar segurança jurídica.

Palavras-chave: Crime Cibernético. Delitos de Informática. Cibersociedade. Responsabilidade Penal da Pessoa Coletiva. Heterorresponsabilidade.

¹ Aluna do 7º período do curso de Direito da FAE Centro Universitário. Voluntária do Programa de Apoio à Iniciação Científica (PAIC 2022-2023). Doutora em Enfermagem pela Universidade Federal do Rio Grande. *E-mail:* ksalmeida@ufpr.br

² Orientador da Pesquisa. Doutor e Mestre em Ciência Jurídica pela Universidade Estadual do Norte do Paraná. Professor da FAE Centro Universitário. *E-mail:* decio.franco@fae.edu

INTRODUÇÃO

A evolução e aprimoramento das tecnologias de informação afetam a vida das pessoas em sociedade, tornando a utilização e dependência de computadores, celulares e redes de internet constante. A internet é fonte de possibilidades para socialização de informações e dados, sendo o meio de comunicação mais utilizado na atualidade.

Sousa e Santos (2017) destaca que conforme pesquisa do Banco Mundial, metade da população utiliza a rede mundial de computadores. Como efeito, tem-se a criação de cultura própria, em que a informação é compreendida como bem de valor, elemento protegido por direitos personalíssimos, mediante compartilhamento de opiniões ou ideias, principalmente em redes sociais.

Norbert Wiener, criador da cibernética, a definiu como *“control and communication theory, whether in the machine or in the animal”*, ou seja, a teoria do controle e da comunicação, no animal e na máquina (WIENER, 1970, p. 94). Limongi França, define a cibernética como *“a ciência da comunicação e do controle nos seres vivos e nas máquinas”* (FRANÇA, 1977, p. 119).

A expressão *“processo cibernético”*, indica utilização de técnicas comparativas e de controle do comportamento humano e computacional, sobretudo, mediante a utilização da inteligência artificial (PIMENTEL, 2019). Sobre esta temática, existe ampla discussão conceitual, sendo compreendido majoritariamente pela doutrina o espaço cibernético como sociedade digital ou cibersociedade.

A cibersociedade deve ser sustentada mutuamente por princípios éticos e morais (SOUZA; PEREIRA, 2009). Porém, a *“era da informação”* possibilita acesso a dados sobre pessoas e lugares em diferentes espaços, evidenciando preocupação com a circulação de informações descontroladas e alteradas, que podem gerar delitos. Os crimes cibernéticos, evidenciam diariamente falsidade informática, afetando a sociedade. Deste modo, as nomenclaturas *“crime cibernético”* ou *“delito informático”* são utilizadas, visto a inexistência do conceito dogmático pleno, com divergências teóricas.

Neste contexto o direito penal é instrumento que disciplina relações sociais, estabelecendo regras e condutas a serem observadas (MORAES, 2003). Convergindo com essa compreensão, em 2001, na Hungria, foi criado pelo Conselho da Europa a Convenção de Budapeste ou Convenção sobre o Cibecrime (BRASIL, 2023), em vigor desde 2004, com ratificação englobando mais de 20 países, apresentando tipificação dos principais crimes cometidos na internet. Trata-se de instrumento internacional estabelecido para promover cooperação entre países signatários no combate aos crimes praticados utilizando a internet e/ou uso de dispositivos eletrônicos (SOUZA; PEREIRA, 2009).

Os crimes cibernéticos podem ser de modalidade própria, quando há violação de dados, informações ou sistemas; ou modalidade imprópria, quando há fraudes eletrônicas. A Convenção de Budapeste destaca a falsidade informática, como item exposto no artigo 7º e a responsabilidade de pessoas coletivas no artigo 12º (COUNCIL OF EUROPE, 2021).

A falsidade informática envolve introdução, alteração, eliminação ou suspensão intencional e ilegítima de dados informáticos, produzindo informações não autênticas, com intenção de que estas sejam consideradas ou utilizadas para fins legais como se fossem verdadeiras. A responsabilidade coletiva destaca a possibilidade das pessoas coletivas serem responsáveis por infrações estabelecidas nos cibercrimes (pessoa coletiva atuante na direção) (COUNCIL OF EUROPE, 2021).

No Brasil, os crimes informáticos são condutas enquadradas no Direito Penal como ilícito em razão de atividades virtuais. O Código Penal brasileiro, destaca como objeto de proteção do Estado a atividade virtual, tendo legislação própria para tipificação criminal de delitos informáticos (BRASIL, 2012). As formas delitivas podem ser praticadas contra bens jurídicos difusos, vinculada sua realização a corporações, divididas hierarquicamente. A criminalidade empresarial, é baseada em convenções internacionais, como o Cibercrime (COUNCIL OF EUROPE, 2021), porém a responsabilidade penal das pessoas jurídicas, tem diversas propostas de modelos de imputação (CANESTRARO; JANUÁRIO, 2018).

Apesar da legislação brasileira ser fragmentada em relação a cibercrimes, para falsidade informática destaca-se a Lei nº 14.155/2021, § 2º A e B (BRASIL, 2021), e art nº 155 do Código Penal que prevê repressão a fraudes eletrônicas cometidas por meio de redes sociais. No referido país, a ênfase penal para estes crimes utiliza o modelo de heterorresponsabilidade, alinhado aos preceitos legais (Lei Ricochete), vinculando-se a necessidade de imputar a pessoa, fatos delituosos e evitar que a responsabilidade penal recaia sobre dirigentes e gestores, tornando a responsabilidade da pessoa jurídica subsidiária à da pessoa física.

A possibilidade de responsabilização das pessoas jurídicas pelos crimes informáticos, embasa-se no ente coletivo, destacando-se que nas empresas, nem sempre é possível determinar especificamente as ações ou pessoas que cometeram o ato lesivo. A compatibilidade de responsabilidade da pessoa jurídica, evita que as pessoas físicas sejam punidas por crimes que podem ser coletivos, bem como alinha-se a complexidade de identificação do agente/autor do ato criminoso (individualização do delito).

Diante do exposto, apresenta-se como objetivo analisar a responsabilidade penal da pessoa coletiva e o princípio da culpabilidade nos crimes informáticos (falsidade informática) em redes sociais.

Quanto ao método, explica-se que o estudo é dedutivo relacionado ao direito informático e responsabilidade coletiva nas redes sociais. Para fundamentação teórica foi realizada busca na literatura científica, no portal Revistas dos Tribunais, na busca pesquisa livre, com o descritor: responsabilidade penal *AND* internet (operador booleano *AND*), além de legislações.

Das buscas emergiram 190 doutrinas, que foram lidas e verificadas a aderência temática a esta pesquisa, conforme informações de título e resumo inicialmente, posteriormente com leitura do texto completo, sendo utilizado como corpus de análise 45 publicações. Realizou-se discussão dos materiais emergentes, alinhados às legislações e casos referência para a temática: *Cubby, Inc. vs. CompuServe, Inc* e *Stratton Oakmont, Inc versus Prodigy Service Co.*

1 DIREITO INFORMÁTICO NAS REDES SOCIAIS

O espaço cibernético consiste em camadas físicas, o hardware, que envolve a estrutura material por meio da qual a informação viaja; e sintáticas (ou lógicas): o software, inclui protocolos que permitem a informação ser roteada e codificada demonstrando que o ciberespaço pode ser onde as operações ocorrem, quanto o fim almejado. A falta de fronteiras possibilita condução simultânea de ações em escala global, com diferentes frentes, em que limitações físicas de distância e espaço não se aplicam (SILVA; STEINHÖFEL, 2021).

O ciberespaço inclui a “rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores” (FERNANDES, 2012, p. 53). Neste contexto, os dados podem transitar por diferentes espaços, de maneira rápida e irrevogável.

O amplo acesso ao ciberespaço remodelou padrões culturais, redimensionando preocupações e desafios para a sociedade, como os delitos cometidos na internet, evidenciando a importância do Direito buscar e promover efetiva proteção individual e coletiva. Conforme Jesus e Milagre (2016, p. 43) existe “conjunto de princípios, normas e entendimentos jurídicos oriundos de atividade informática, intitulado Direito informático”.

Atribuiu-se valor as informações isoladas, principalmente com evidências da *General Data Protection Regulation* (GDPR) pela União Européia, e da Lei de Proteção de Dados Pessoais, no Brasil (SALDANHA; SALDANHA, 2019; BRASIL, 2018). Assim, alinhar preceitos do direito informático nos espaços virtuais, principalmente naqueles utilizados extensivamente, como por exemplo nas redes sociais, fomenta publicações com dados

verdadeiros, refutando manipulação, alteração, inserção, como as *Fake News*. Apesar desta última (*Fake News*) não ser considerada crime passível de punição por parte do Estado brasileiro, pois não há no código penal dispositivo que tipifique o ato de criar ou disseminar notícias falsas, seja de forma individual ou coletiva, a mesma deve ser refutada.

O desafio das *fake news* está presente de forma desafiadora no Brasil, tendo notícias que trazem a ideia generalizada efetivando compartilhamento do distúrbio da informação, com aumento progressivo historicamente (SAMPAIO, 2023). Esse fato preocupa, visto que a Constituição da República Federativa do Brasil (1988), dispõe no seu artigo 5º, inciso IV, sobre a livre manifestação do pensamento, sendo vedado o anonimato, considerando-se como direito fundamental garantido pela Carta Magna, cláusula pétreia. Ancorado nesta questão, enfatiza-se que o direito à livre manifestação, não inclui a falsidade informática.

O surgimento de espaços de domínio cibernético pode contribuir para a conjuntura dos conflitos, *fake news* e ilícitos, visando evitar ou regular os impactos na sociedade. Com preocupação sobre as operações cibernéticas a Organização do Tratado do Atlântico-Norte (OTAN) elaborou por conjunto de experts o Manual Talinn 2.0 (Manual), com regras e dicas para operações cibernéticas. Trata-se de conceito amplo que abrange todo e qualquer tipo de operação no espaço cibernético, dentro ou fora do contexto de conflitos armados (SILVA; TEINHÖFEL, 2021).

As manifestações das redes sociais, acessos não autorizados ou não consentidos a base de dados ou sistemas alheios (*hacking*), podem visar diversos objetivos: ações destrutivas (*cracking*), interceptações de comunicações pessoais e coletivas, mensagem de correios eletrônicos adulteradas, expedição ou troca de documentos. A inclusão de informações (dados, imagens, som e voz) na rede, com conteúdo ilícito variados, transformando a rede em meio eficaz para a prática de delitos (CASABONA, 2011).

Nos “termos de uso, serviços e políticas de conteúdo” divulgados por empresas de tecnologia como o *Facebook/Meta, Instagram e o Twitter*, é comum a descrição de atuação como *neutral platforms*, sendo os seus usuários cientificados acerca da sua exclusiva responsabilidade sobre os conteúdos postados, principalmente por se tratar de mensagens pelos mesmos elaboradas, e que não representam a opinião das operadoras. Contudo, os provedores se reservam o direito de prever limitações quanto ao conteúdo e quanto a comportamentos permitidos na plataforma, sob pena de suspensão ou a cessação da conta, residindo justamente nessa espécie de poder moderador uma das maiores controvérsias a respeito da natureza dos serviços prestados pelas plataformas digitais (VENTURI, 2022).

Assim, diante da complexidade apresentada sobre a temática, debates sobre a responsabilidade penal no ciberespaço, envolvem a qualificação jurídica dos ambientes virtuais, bem como a natureza das empresas jurídicas envolvidas como pessoa coletiva.

2 RESPONSABILIDADE PESSOA COLETIVA

Não é possível considerar sujeitos ativos do delito as pessoas jurídicas, conforme princípio do *societas delinquere non potest*, que inspira a legislação de muitos países (DUARTE, 2015). Caso algum delito seja cometido através delas, a entidade, não poderá ser punida penalmente; poderá, no entanto, ser punida a administração, como consequência da prática de infração administrativa, nos casos e formas legalmente previstos.

A personalidade natural é reconhecida pelo Direito, e a personalidade jurídica, ao contrário, somente existiria por determinação da lei e dentro dos limites por ela fixados. Porém, tais argumentos não afastam, de per si, a teoria da pessoa jurídica como realidade técnica (ou jurídica), visto que o homem é dotado de personalidade jurídica quando e nos limites em que o ordenamento jurídico a reconhece (MORAES, 2011).

A infração indireta para a pessoa coletiva, envolve-se com a responsabilidade social, limitada geralmente aos dirigentes (MACHADO, 2009). A punição das pessoas que tenham realizado pessoalmente a conduta típica punível, quando em ambiente coletivo, para discussão principalmente na esfera da responsabilidade penal. Assim, a Convenção sobre Crime Cibernético (COUNCIL OF EUROPE, 2021; BRASIL, 2023) defende que a responsabilidade será de natureza civil, administrativa ou penal.

No tocante à responsabilidade penal, nos meios de comunicação virtuais, nem sempre é possível identificar o autor dos dados publicados, prejudicando a identificação do responsável pelos danos que podem ser causados. O conteúdo das publicações nas redes sociais não exclui a responsabilidade coletiva, sendo esta, responsabilidade vinculada a notificação do conteúdo danoso a vítima e após a comunicação, caso a empresa não realize as devidas providências, pode ser responsabilizada por omissão.

Na jurisprudência estrangeira, uma decisão ficou conhecida como o caso *Cubby, Inc. vs. CompuServe, Inc.* Trata-se de um dos primeiros julgados sobre difamação na internet, realizado pela Corte Distrital de Nova Iorque, decidindo pela inexistência de responsabilidade por parte da *CompuServe*, sob o fundamento de que a empresa enquanto provedora de conteúdo não teve viabilidade de visualização previamente sobre o conteúdo da publicação, antes de ser postada na rede, não podendo desta forma ser responsabilizada pela mensagem exposta (BARRETO JUNIOR; LEITE, 2017).

Este julgado, considerou os provedores de serviços de internet sujeitos à lei tradicional de difamação pelo conteúdo hospedado no ambiente virtual, incitou precedentes para a responsabilidade jurídica. O Tribunal após apuração dos fatos determinou julgamento sumário favorável à *CompuServe*, visto que esta não tem controle editorial sobre as publicações, para tanto teria que analisar individualmente

cada publicação; quando a reclamação de depreciação comercial, a empresa declarou desconhecer a natureza das declarações difamatórias, sendo não responsável pelo teor.

Assim o tribunal tratou os intermediários da internet sem envolvimento editorial dos distribuidores de informação no contexto das notícias da internet, removendo qualquer incentivo legal para monitoramento ou filtragem de conteúdo pelas empresas responsáveis pelos domínios do ciberespaço.

Em 1995, outro processo envolvendo *Stratton Oakmont, Inc versus Prodigy Service Co.* esclareceu responsabilidades dos provedores de internet. A *Prodigy* filtrava e ocasionalmente removia conteúdo ofensivo dos espaços que hospedava. Deste modo, o tribunal compreendeu que a empresa era editora, portanto, responsável pelo conteúdo divulgado (BARRETO JUNIOR; LEITE, 2017).

Como essas decisões não foram apeladas para tribunais superiores, não são precedentes obrigatórios. Porém, cabe destacar que estes julgados confirmam que os provedores que optam por não conhecer o seu conteúdo de publicação, estão imunes à responsabilidade, enquanto que os editoriais, mesmo de boa-fé, assumem total responsabilidade de editoração.

Em 1996, nos Estados Unidos, a Seção 230 da Lei Decência nas Comunicações, foi formalmente codificada como parte da Lei das Comunicações, concedendo aos provedores de internet imunidade de responsabilidade pelo conteúdo fornecido por outros, com algumas exceções. Esta legislação distingue serviços de computadores interativos, como provedores de internet e provedores de conteúdo, como usuários que postam as mensagens em fóruns; considerando que os serviços de computadores interativos não são considerados editores de conteúdo, não devendo ser responsabilizados penalmente.

Assim, no Brasil, com a intenção de pacificar o debate, foi promulgada legislação própria, Lei nº 12.965/2014 (BRASIL, 2014), conhecida popularmente como o Marco Civil da Internet. Esta lei foi responsável por regulamentar o uso da internet no Brasil e teve como principal objetivo garantir rede livre, unificando o entendimento jurisprudencial e doutrinário. A omissão de regulamentação própria, gerou decisões fundamentadas em dispositivos esparsos, por analogia ao Código Civil (BRASIL, 2002) ou ao Código do Consumidor (BRASIL, 1990), combinados com disposições da Constituição Federal de 1988.

A responsabilidade coletiva exige atribuição criminal que não acarreta a infração do princípio do *ne bis in idem*, caso acumulada a responsabilidade da pessoa física. Deste modo, cada uma responde a própria contribuição delitiva. Essa conjuntura da imputação da responsabilidade penal das pessoas jurídicas é complexa, diante da realidade do ciberespaço na sociedade (BRODT; MENGHIN, 2015).

No Brasil, principalmente nas redes sociais, pouco se discute sobre a responsabilidade individual e coletiva nas redes sociais. Sendo que, no país, a última legislação está relacionada ao modelo de heterorresponsabilidade, alinhado aos preceitos legais (Lei Ricochete), vinculando-se a necessidade de imputar fatos delituosos e evitar que a responsabilidade penal recaia sobre dirigentes e gestores jurídica. Neste contexto, a responsabilidade da pessoa jurídica é subsidiária à da pessoa física, garantindo segurança jurídica (SARCEDO, 2014).

A efetividade da persecução penal dos atos ilícitos cometidos no ciberespaço tem dificuldade de determinação do lugar e do tempo da prática do delito (*locus tempusque delicti commissi*). Deste modo, a teoria da ação, principalmente aquela vinculada ao delito realizado no local do trabalho (delitos informáticos), gera necessidade paradoxal de discussão de conflitos e responsabilidades.

As mudanças da cultura do ciberespaço exigem tratamento jurídico-penal em perspectiva ao princípio da personalidade e responsabilidade. A Convenção Européia sobre Crime Cibernético constituiu êxito nesta direção, apontando que os delitos cibernéticos colocam à prova a efetividade das instituições, com condenação, dos sujeitos responsáveis pelos delitos perpetrados no espaço cibernético (CASABONA, 2011).

Desta forma, deve-se investir esforços no sentido de conter a “criminalidade das pessoas coletivas” a partir da instrumentalização e aparelhamento humano e técnico dos órgãos estatais envolvidos na persecução criminal, no sentido de punição das condutas individuais perpetradas por agentes que atuam acobertados e tendo em vista os interesses da pessoa jurídica, mormente no plano dos interesses difusos (MORAES, 2003).

Alinhado a esta compreensão, a redação conferida aos artigos 18 e 19 da lei 12.965/2014 (BRASIL, 2014), implica em reconfiguração da natureza jurídica dos provedores, requalificando seu status, pois, condiciona a imputação de responsabilidade civil à desobediência de prévia ordem judicial. Assim, o legislador brasileiro desonerou as empresas provedoras de qualquer obrigação de valorar o conteúdo veiculado na internet por seus usuários. Isso implica, na realidade, no reconhecimento legislativo de que os provedores de internet passaram a ser considerados meras *neutral platforms* (VENTURI, 2022).

Trata-se de profunda alteração do status jurídico direcionado às empresas de tecnologia, refutando a discussão sobre a responsabilidade criminal no ciberespaço, trazendo efeitos nocivos a proteção das vítimas, imunizando operadoras, fomentando regime de irresponsabilidade sobre o ilícito e lesivo postado por seus usuários, exceto quando existem ordens judiciais para a supressão do conteúdo lesivo (VENTURI, 2022).

CONSIDERAÇÕES FINAIS

Diante do exposto, as características do ciberespaço contribuem para a disseminação rápida e irrevogável de inúmeras informações digitais. Ações virtuais, principalmente aquelas realizadas em redes sociais, podem degradar dados pessoais e informacionais, alterando o funcionamento de estruturas, dados pessoais, causando conflitos e ilícitos, com graves consequências para a sociedade.

Alguns materiais desenvolvidos internacionalmente e legislações brasileiras logram êxito em limitar o desenvolvimento de ações que prejudiquem outros. Em contrapartida, ainda há insuficiência para impedir que os crimes ocorram. A cultura digital não acompanhou as normativas jurídicas referentes à salvaguarda de dados informacionais, objetos e infraestruturas do ciberespaço.

O uso de espaço virtual, apesar de individualizado, pode estar no contexto coletivo, fomentando a responsabilidade penal da pessoa coletiva, principalmente em redes sociais, com culpabilidade da falsidade informática. Neste ínterim, mudanças do ciberespaço exigem tratamento jurídico-penal, em que delitos cibernéticos tenham condenação dos sujeitos responsáveis de forma solidariamente as pessoas coletivas. Assim, o Direito Penal pode combater os crimes cibernéticos, visando gerar segurança jurídica.

REFERÊNCIAS

BARRETO JUNIOR, I. F.; LEITE, B. S. F. **Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/15 (marco civil da internet)**. Revista Brasileira de Estudos Políticos, Belo Horizonte, n. 115, p. 391-438, jul./dez. 2017. Disponível em: <https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/479>. Acesso em: 05 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 out. 2022.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil. **Diário Oficial da União**, Brasília, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 28 mai. 2023.

BRASIL. Decreto-lei n. 3.689, de 03 de outubro de 1941. Código de Processo Penal (1941). **Diário Oficial da União**, Rio de Janeiro, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 28 out. 2022.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 fev. 2023.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 28 ago. 2023.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Diário Oficial da União**, Brasília, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 fev. 2023.

BRASIL. Lei n. 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. **Diário Oficial da União**, Brasília, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 28 out. 2022.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 mar. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 28 mar. 2023.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. Altera o Decreto Lei n. 2.848, de 7 de dezembro de 1940. **Diário Oficial da União**, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 28 mar. 2023.

BRODT, L. A. S.; MENEGHIN, G. S. Responsabilidade penal da pessoa jurídica: um estudo comparado. **Revista dos Tribunais**, v. 961, nov. 2015. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rtrib_n.961.10.PDF. Acesso em: 02 ago. 2023.

CANESTRARO, A. C.; JANUÁRIO, T. F. X. Responsabilidade penal da pessoa coletiva e princípio da culpabilidade: análise crítica do modelo português. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 39, p. 261-285, dez. 2018.

CASABONA, C. M. R. Dos delitos informáticos ao crime cibernético: uma aproximação conceitual e político-criminal. **Doutrinas Essenciais de Direito Penal Econômico e da Empresa**, v. 6, p. 509-552, jul. 2011.

COUNCIL OF EUROPE. **Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**. Estrasburgo: Council of Europe, 2021. Disponível em: <https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930>. Acesso em: 14 maio 2023.

DUARTE, A. A. A. R. Aspectos concernentes à responsabilidade penal da pessoa jurídica. **Banco do Conhecimento**, 2015. Disponível em: <https://www.tjrj.jus.br/documents/10136/30090/aspectos-concernentes-responsabilidade-penal-pessoa-juridica.pdf>. Acesso em: 08 set. 2023.

FERNANDES, J. P. T. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**, Lisboa, n. 33, p. 53-69, mar. 2012. Disponível em: www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-91992012000100005&lng=pt&nrm=iso. Acesso em: 29 mar. 2023.

FRANÇA, A. S. L. Cibernética jurídica. **Revista de Direito Civil**, São Paulo, n. 37, p. 119, 1977.

JESUS, D.; MILAGRE, J. A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MACHADO, F. G. P. Reminiscências da responsabilidade penal da pessoa jurídica e sua efetividade. **Revista Brasileira de Ciências Criminais**, v. 79, p. 75-100, set. 2009.

MORAES, R. I. Considerações sobre a responsabilidade criminal das pessoas jurídicas. **Revista dos Tribunais**, v. 813, p. 447-472, 2003.

PIMENTEL, A. F. Diagnóstico sobre a imprecisão das designações sobre o direito processual tecnológico: processo informático, eletrônico, telemático, digital, virtual ou cibernético? **Revista de Processo**, v. 296, p. 353-375, out. 2019.

SALDANHA, P. M.; SALDANHA, A. H. T. O alcance da penhora sobre o banco de dados de uma empresa judicialmente executada. **Revista de Processo**, v. 297, p. 117-132, nov. 2019. Disponível em: www.revistadostribunais.com.br/maf/app/widgetshomepage/resultList/document?&src=rl&srguid=i0ad6adc600000174604dc8bef18dd08d&docguid=I3205e0a0df0411e9a2c7010000000000&htguid=I3205e0a0df0411e9a2c7010000000000&spos=12&epos=12&td=572&context=8&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=true&startChunk=1&endChunk=1. Acesso em: 15 mar. 2023.

SAMPAIO, J. L. **A inteligência artificial: a (des)serviço do estado de direito**. Belo Horizonte: CAPES; Programa de Pós-graduação em Direito - PUC Minas; RTM, 2023. Disponível em: <https://www.pucminas.br/pos/direito/Documentos%20Gerais/Ebook%20final%20-%20IA.pdf>. Acesso em: 10 out. 2023.

SARCEDO, L. **Compliance e responsabilidade penal da pessoa jurídica: construção de um novo modelo de imputação, baseado na culpabilidade corporativa**. 2014. 325 f. Tese (Doutorado em Direito) — Faculdade de Direito, Universidade de São Paulo, 2014. Disponível em: https://teses.usp.br/teses/disponiveis/2/2136/tde-07122015-163555/publico/Leandro_Sarcedo_Tese_Versao_final.pdf. Acesso em: 01 maio 2023.

SILVA, A. B.; STEINHÖFEL, M. P. Operações cibernéticas e o princípio da distinção. A proteção de objetos civis sob o direito internacional dos conflitos armados. **Revista dos Tribunais**, São Paulo, ano 110, v. 1033, p. 165-194, nov. 2021. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000187329e47628882f532&docguid=l24eed9603b9d11ec96a7945cbf8b867d&hitguid=l24eed9603b9d11ec96a7945cbf8b867d&spos=1&epos=1&td=574&context=15&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 29 mar. 2023.

SOUZA, A. M. P.; SANTOS, K. G. Legislação penal simbólica e seus efeitos: uma análise jurídica e social. **Revista Integrart**, Vitória da Conquista, v. 1, n. 1, p.111-124, maio 2017.

SOUZA, G. L. M.; PEREIRA, D. V. A convenção de Budapeste e as leis brasileiras. In: SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, 1., 2009, João Pessoa. **Anais [...]**, João Pessoa: UFPB, 2009.

SYDOW, S. T. **Curso de direito penal informático**: partes geral e especial. 3. ed. Salvador: Juspodvim, 2022.

VENTURI, T. G. P. Responsabilidade civil das plataformas digitais: em busca de adequados marcos regulatórios. **Advocacia Faiad**, 31 mar. 2022. Disponível em: <http://www.advocaciafaiad.com.br/publicacao/responsabilidade-civil-das-plataformas-digitais-em-busca-de-adequados-marcos-regulatori>. Acesso em: 05 out. 2023.

WIENER, N. **Cibernética e sociedade**: o uso humano de seres humanos. São Paulo: Cultrix, 1970. p. 94.