

RESPONSABILIDADE PENAL DA INTELIGÊNCIA ARTIFICIAL NOS CRIMES CIBERNÉTICOS: LIMITES DA IMPUTAÇÃO PENAL E PROPOSTA DE CORRESPONSABILIDADE TECNOLÓGICA

Letícia da Silva Reis¹

Lucas Azevedo de Lima²

Pedro Ivan dos Santos Ferreira³

RESUMO

Atualmente, o avanço das tecnologias de inteligência artificial tem tomado espaço significativo no dia a dia da população brasileira e também na esfera global, promovendo a automação de tarefas e apoio à tomada de decisões. Entretanto, esse desenvolvimento apresenta desafios para o ordenamento jurídico, especialmente no contexto dos crimes cibernéticos. Este artigo analisa os limites da imputação penal diante da utilização da inteligência artificial como instrumento facilitador de ilícitos penais, destaca a impossibilidade de atribuição de responsabilidade penal direta aos sistemas automatizados devido à ausência de consciência, vontade e culpabilidade. A pesquisa também analisa o viés algorítmico das ferramentas inteligentes, demonstrando como sistemas aparentemente neutros podem produzir distorções presentes nos dados de treinamento e melhoria das inteligências artificiais, como evidenciado no caso do sistema COMPAS nos Estados Unidos. Com base na análise realizada, propõe-se uma abordagem de solidariedade da responsabilidade penal, distinguida em três níveis: o usuário como autor direto do crime, o desenvolvedor do sistema em situações de negligência ou ausência de mitigação de riscos previsíveis, e a empresa fornecedora quando disponibiliza tecnologias sem mecanismos adequados de governança e controle. Por fim, o estudo defende a aplicação analógica de estruturas jurídicas já consolidadas no ordenamento bra-

¹ Graduanda em Direito na Faculdade ASA de Brumadinho – Instituição Educacional Cecília Maria de Melo Barcelos. Orientador: Prof^a. MSc^a. Lucas Azevedo de Lima. E-mail: leticiareis0915@gmail.com

² Mestre em Direito Ambiental e Desenvolvimento Sustentável. Professor na Faculdade ASA de Brumadinho – Instituição Educacional Cecília Maria de Melo Barcelos. E-mail: professorlucaslima@gmail.com

³ Graduando em Direito na Faculdade ASA de Brumadinho – Instituição Educacional Cecília Maria de Melo Barcelos. Orientador: Prof. MSc. Lucas Azevedo de Lima. E-mail: pedroivandossantos14@gmail.com

sileiro, como a responsabilidade objetiva prevista no Código de Defesa do Consumidor e a teoria do risco da atividade, como estratégias para enfrentar os desafios jurídicos decorrentes da expansão da inteligência artificial no ambiente digital.

Palavras-chave: Inteligência artificial; Crimes cibernéticos; Responsabilidade penal; Viés algorítmico; Responsabilidade tecnológica.

ABSTRACT:

Currently, the advancement of artificial intelligence technologies has taken up significant space in the daily lives of the Brazilian population and also globally, promoting the automation of tasks and supporting decision-making. However, this development presents challenges for the legal system, especially in the context of cybercrimes. This article analyzes the limits of criminal liability in the face of the use of artificial intelligence as a facilitating instrument for criminal offenses, highlighting the impossibility of attributing direct criminal responsibility to automated systems due to the absence of consciousness, will, and culpability. The research also analyzes the algorithmic bias of intelligent tools, demonstrating how seemingly neutral systems can produce distortions present in the training and improvement data of artificial intelligences, as evidenced in the case of the COMPAS system in the United States. Based on the analysis carried out, a joint and several liability approach is proposed, distinguished at three levels: the user as the direct perpetrator of the crime, the system developer in situations of negligence or lack of mitigation of foreseeable risks, and the supplier company when it provides technologies without adequate governance and control mechanisms. Finally, the study advocates for the analogical application of legal structures already established in the Brazilian legal system, such as the strict liability provided for in the Consumer Protection Code and the theory of risk of activity, as strategies to address the legal challenges arising from the expansion of artificial intelligence in the digital environment.

INTRODUÇÃO

Analisando o cenário atual, podemos observar que a inteligência artificial (IA) deixou de ser um simples recurso experimental para se tornar uma verdadeira ferramenta de suporte polarizada de transformação digital moderna. Com grande capacidade de processamento de dados, aprender padrões e tomar decisões baseados nos conhecimentos armazenados, sua aplicação se estende à análise de dados, gestão logística até a cibersegurança, entre muitos outros. No entanto, o mesmo potencial que gera avanços também amplia riscos, especialmente no cenário dos crimes cibernéticos.

Ataques como phishing, ransomware, malware, invasões de dispositivos e deepfakes têm sido cada vez mais potencializados por sistemas de inteligência artificial, que podem ser utilizados tanto para fortalecer mecanismos de defesa quanto para executar práticas ilícitas de forma cada vez mais efetiva. A autonomia de alguns modelos, especialmente aqueles baseados em aprendizado autônomo e adaptativo, que aprendem a todo instante com o banco de dados e interação ao método de sua aplicação, levanta questões jurídicas complexas: quem deve responder penalmente quando um sistema atua de forma independente e causa danos? O programador, o operador, a empresa proprietária ou a própria IA?

Em diversos países, incluindo o Brasil, o direito penal ainda não possui regras específicas para lidar com a autonomia desses sistemas de inteligência artificial. Entretanto, já podemos observar avanços relevantes como o Projeto de Lei nº 2.338/2023, que propõe diretrizes para utilização responsável e segura das ferramentas de IA. A grande dificuldade de enquadramento jurídico de personalidade a uma ferramenta despersonalizada pode gerar tanto impunidade quanto responsabilização indevida, evidenciando a necessidade de um olhar mais atento para essa situação.

O presente artigo analisa os desafios e as perspectivas jurídicas sobre a responsabilização criminal da inteligência artificial nos crimes cibernéticos. Além de evidenciar as principais correntes doutrinárias, avaliar a aplicabilidade das normas existentes e em tramitação, além de refletir sobre possibilidades legislativas que conciliem inovação tecnológica, segurança jurídica e proteção da sociedade.

INTELIGÊNCIA ARTIFICIAL E CRIMES CIBERNÉTICOS

Popularizada por sua sigla IA, a inteligência artificial tem ganhado espaço e extrema relevância no cotidiano da população brasileira e até mesmo mundial. Segundo pesquisa da Forbes Tech, 93% dos brasileiros já interagiram e/ou ainda interagem com alguma ferramenta integrante deste ramo da ciência da tecnologia.

Para compreendermos de forma mais precisa a inserção dessas ferramentas no cotidiano dos usuários, a mesma pesquisa de 2025 realizada pela Conversion, a maior agência de SEO no Brasil, em parceria com a Escola Superior de Propaganda e Marketing, demonstra que 49,7% utilizam IA todos os dias e 86,4% ao menos uma vez por semana. Nesse contexto, plataformas como ChatGPT, Gemini, Copilot, entre muitas outras, estão se tornando ferramentas de apoio em estudos, trabalho e no processo de assimilação de novos conteúdos.

A inteligência artificial vem se desenvolvendo desde a década de 1950, como um campo da ciência da computação dedicado ao estudo de métodos capazes de reproduzir, em máquinas e softwares, determinados aspectos do comportamento humano em realização de tarefas e decisões automatizadas. Atualmente, essas tecnologias estão disponíveis na palma da nossa mão, presentes em uma assistente de voz, nas redes sociais, sistemas de reconhecimento facial, carros autônomos e de muitas outras formas. Essas ferramentas são capazes de aprender com novas informações e experiências, ou seja, quanto mais utilizadas e alimentadas por bancos de dados online e pelo contato com os usuários, podem agir de forma independente, reduzindo a necessidade de uma intervenção humana constante.

Com a difusão dessa tecnologia na sociedade, levantam-se outros questionamentos significativos, especificamente na confiabilidade das informações absorvidas e replicadas pela inteligência artificial, a imputação e responsabilização da falha sistêmica dessas ferramentas e principalmente nos impactos jurídicos no que diz respeito à utilização dessas máquinas e softwares como ferramenta para prática de ilícitos penais.

A partir do momento que a inteligência artificial passaram a possuir capacidade analítica e produtora de conteúdo em massa, ela também passa a auxiliar na produção de emails e mensagens automatizados de phishing (ataques digitais que tentam roubar dados pessoais, informações bancárias em sites que parecem legítimos), analisando inclusive as redes sociais e informações das vítimas para criação de golpes personalizados e mais convincentes elevando e sofisticando o nível do estelionato previsto no artigo 171 do Código Penal Brasileiro para uma esfera cada vez maior.

De forma semelhante à inteligência artificial que alimenta as redes sociais para entretenimento e comunicação digital com criação de vídeos, áudios e imagens falsas extremamente realistas, podem ser utilizadas para a criação de deepfakes (conteúdos audiovisuais que disseminam desinformações), gera nova insegurança das provas digitais em processos, falsidade ideológica, fraude, extorsão e vinculação da imagem de terceiros em pornografia.

LACUNAS LEGISLATIVAS DIANTE DO AVANÇO DA INTELIGÊNCIA ARTIFICIAL

O desenvolvimento normativo brasileiro não tem acompanhado na mesma intensidade o avanço das criações tecnológicas. Apesar de existirem normas voltadas à proteção do ambiente digital e à repressão de crimes informáticos, não existe regulamentação específica que trate da responsabilidade penal relacionada à prática de ilícitos penais mediados pela inteligência artificial.

Em 2012, foi promulgada a Lei Carolina Dieckmann, que alterou o Código Penal para abranger a tipificação de crimes relacionados à invasão de dispositivos informáticos, motivada por caso infortúnio anterior, no qual imagens íntimas da atriz Carolina Dieckmann foram divulgadas sem autorização após uma invasão de seu computador pessoal por agentes criminosos. Na época, o caso trouxe à tona uma fragilidade do ordenamento jurídico nas respostas aos crimes cibernéticos, e mais uma vez o sistema judiciário teve que tomar uma ação reparadora ao invés de preventiva, especificando na lei dispositivos voltados para a proteção da privacidade e da segurança das informações digitais.

Outro episódio relevante foi o Marco Civil da Internet, sancionado em 23 de abril de 2014, considerado uma espécie de direcionador, uma “Constituição da internet brasileira”. Elaborado em um contexto de crescimento exponencial da internet e preocupação com a governança digital, foi instigado por debates internacionais sobre vigilância digital, neutralidade da rede e proteção da privacidade. Somente depois desse marco foram estabelecidos direitos e deveres claros para o uso da internet, abrangendo temas como responsabilidade dos provedores de aplicações, proteção da privacidade e guarda de registros de acesso, mas ainda assim sem abordar diretamente a responsabilidade penal relacionada ao uso de sistemas de inteligência artificial na prática de crimes, devido à baixa utilização dessa tecnologia naquela época.

No mesmo sentido, podemos destacar a Lei Geral de Proteção de Dados (LGPD), promulgada em 14 de agosto de 2018, quando surgiu a necessidade de regular o uso indiscriminado de dados pessoais por empresas e organizações, derivada do aumento de casos de vazamento de dados e exploração indevida de informações pessoais em plataformas digitais. A lei padroniza e estabelece critérios para coleta, armazenamento, consentimento, tratamento e compartilhamento de dados pessoais, introduzindo no ambiente digital princípios como a transparência, segurança e responsabilidade no tratamento dessas informações.

Diante do cenário histórico, legislativo e jurídico, o ordenamento legal brasileiro possui importantes dispositivos que regulam o ambiente digital, mas ainda existe uma lacuna normativa no que diz respeito à responsabilidade penal envolvendo crimes realizados com a facilitação da inteligência artificial.

O ordenamento jurídico atualmente concentra-se na proteção da privacidade, na tutela dos dados pessoais dos usuários e na regulação do uso da internet, mas não aborda de forma direta a problemática central da responsabilização de sistemas automatizados na prática de ilícitos penais. Torna-se pertinente voltar as atenções para a realidade digital e analisar alternativas interpretativas

já existentes, capazes de suprir essa lacuna normativa de forma mais expressiva e geral. Uma dessas possibilidades é a aplicação, por similaridade, do comportamento de estruturas jurídicas já consolidadas em outras searas do direito, como a responsabilidade solidária pelo fato do produto contida no Código de Defesa do Consumidor, bem como a teoria do risco da atividade.

A partir dessa estruturação jurídica de mediação e repressão à utilização indevida dos sistemas digitais inteligentes, é possível discutir a responsabilidade dos agentes envolvidos em toda a cadeia, desde o desenvolvimento e disponibilização até a utilização direta das inteligências artificiais, especialmente quando utilizadas como instrumentos facilitadores da prática de crimes cibernéticos.

LIMITES DA RESPONSABILIDADE PENAL DA INTELIGÊNCIA ARTIFICIAL

A culpabilidade é um princípio basilar na estrutura da teoria do crime, derivado do latim “*Nullum crimen sine culpa*”, não há crime sem culpa, ou seja, o indivíduo não pode ser imputado de crime ou apenação sem que a conduta criminosa seja reprovada. Com origem na Idade Média foi objeto de superação as concepções medievais da responsabilização objetiva enraizadas em superstições e crenças religiosas da época.

Alvo de discussão por muito tempo, a culpabilidade hoje implica ao direito penal três análises fundamentais da aplicação dela como elemento que integra o conceito analítico de crime, como princípio medidor da pena e como impedor da responsabilidade penal objetiva.

Apesar de não estar expresso na Constituição da República Federativa do Brasil de 1988 podemos encontra-la de forma implícita deduzindo e relacionando-o com o princípio da dignidade humana conforme a citação do renomado jurista Guilherme Nucci, O princípio da culpabilidade encontra-se previsto de maneira implícita na Constituição, justamente porque não se pode, num estado Democrático de Direito, transformar a punição mais gravosa que o ordenamento pode impor (pena) em simples relação de causalidade, sem que exista vontade ou previsibilidade do agente. (NUCCI, 2013).

O Código Penal, já influenciado pela teoria da culpabilidade expressa no seu artigo 18, tem a responsabilidade subjetiva no seu texto vigente desde 1940.

Art. 18 – Diz-se o crime:

I – doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo;

II – culposo, quando o agente deu causa ao resultado por imprudência, negligência ou imperícia.

Parágrafo único – Salvo os casos expressos em lei, ninguém pode ser punido por fato previsto como crime, senão quando o pratica dolosamente.

(BRASIL, 1940).

A culpa associada a uma ação é um sentimento baseado na psique do indivíduo, conforme diversos autores e doutrinas da psicologia. Sendo assim, não podemos aplicar a culpabilidade à Inteligência Artificial, sendo que se trata de um produto e, como produto, constitui uma infraestrutura inimputável.

Na culpa, sentimos que não podemos ser nós mesmos. Não encontramos lugar, experimentamos algo como rejeição ou iminência de morte, uma sensação de falta de naturalidade, uma atitude contraída para com as demais pessoas ou mesmo para o ambiente que nos cerca. Sentimo-nos como estranhos, como se algo se interpusesse entre a natureza e nós – como se dela tivéssemos sido aliados ou abortados. O mundo não nos aninha. É algo como uma vergonha não localizada, gratuita, que nos deixa desconfortáveis. Temos ânsia de fazer algo para remediar, mas não sabemos o quê (Carvalho, 1997, p. 46).

A atribuição da responsabilidade penal à inteligência artificial relativiza os princípios básicos do direito penal, especialmente os que regem elementos subjetivos que são indispensáveis para a configuração da culpabilidade, principalmente a consciência e a vontade direta à prática da conduta criminosa. O ordenamento jurídico brasileiro, baseia a responsabilidade penal subjetiva na presença de dolo ou culpa para imposição de pena, requisitos estes incompatíveis com a natureza instrumental da inteligência artificial.

VIÉS ALGORÍTMICO E RESPONSABILIDADE DOS DESENVOLVEDORES

Embora associem os resultados entregues pelas ferramentas de inteligência artificial à imparcialidade e à confiabilidade técnica da informação, erroneamente, não há correlação nessa associação. O método de aprendizagem e desenvolvimento de uma inteligência artificial, seja ela generativa ou preditiva, é baseado em fontes de informação públicas e no contato com o usuário, que em grande parte estão maculadas com preconceitos estabelecidos, mesmo que de forma velada.

No cenário internacional, fazendo menção a essa falha enviesada do algoritmo, nos Estados Unidos foi utilizado o sistema de inteligência artificial COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) nos tribunais norte-americanos com o intuito de estimar a probabilidade de reincidência criminal dos agentes de condutas criminosas, auxiliando os juízes em suas tomadas de decisões referentes à liberdade provisória e à definição da pena. No julgamento

do caso Estado contra Loomis, a defesa do réu questionou a utilização do algoritmo na fundamentação da decisão judicial, tendo em vista a impossibilidade de auditoria por leigos em programação e também em relação à base de informações utilizada para comparar as respostas dos agentes com estigmas sociais de acessibilidade ao ensino anterior à conduta, moradia e infraestrutura do lar, antecedentes criminais familiares, cor da pele, renda familiar, entre outras classificações que reproduziam generalização e depreciação social.

Posteriormente, a ProPublica, uma redação independente e sem fins lucrativos que produz jornalismo investigativo de interesse público, realizou uma investigação que apontou essas distorções étnico-raciais, quando a inteligência artificial classificava indivíduos negros com maior risco de reincidência do que indivíduos brancos em circunstâncias semelhantes. A inteligência artificial, por si só, não é capaz de reproduzir esses preconceitos se não estiverem previamente contidos nos algoritmos implementados pelos próprios desenvolvedores ou na base de dados utilizada como fonte matriz, representando uma fragilidade sistêmica e/ou negligência por parte de seus desenvolvedores.

INTELIGÊNCIA ARTIFICIAL COMO PRODUTO TECNOLÓGICO

Tendo em vista que a inteligência artificial é um produto tecnológico, devemos compreendê-la como um meio facilitador para os crimes cibernéticos. Assim, ela sai da figura de agente por não possuir culpabilidade, consciência e vontade própria, tornando-se instrumento intermediário na cadeia de causalidade entre fabricante, desenvolvedor e o agente direto do crime. Dessa forma, a responsabilidade dos desenvolvedores e das empresas fornecedoras pode ser atribuída por analogia à responsabilidade imputada às instituições financeiras nos casos de fraude, aplicando-se a teoria do risco da atividade.

Segundo o Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990, a responsabilidade é solidária entre fabricante e desenvolvedor nas falhas decorrentes e derivadas da utilização do produto, podendo a estes ser imputada também responsabilidade criminal.

Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. (BRASIL, 1990)

Art. 18. Os fornecedores de produtos de consumo duráveis ou não duráveis respondem solidariamente pelos vícios de qualidade ou quantidade que os tornem impróprios ou inadequados ao consumo a que se destinam ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade com as indicações constantes do recipiente, da embalagem, rotulagem ou mensagem publicitária, respeitadas as variações decorrentes de sua natureza, podendo o consumidor exigir a substituição das partes viciadas. (BRASIL, 1990)

Dessa forma, a inteligência artificial deve ser entendida como ferramenta tecnológica, não como sujeito ativo do crime, tendo em vista que a utilização inadequada ou insegura do produto pode escalar e potencializar a prática de crimes cibernéticos. Nesse sentido, é fundamental a adoção de políticas de segurança e governança tecnológica visando a segurança e transparência por parte das empresas desenvolvedoras.

TEORIA DA CORRESPONSABILIDADE TECNOLÓGICA

Diante dessa projeção, é possível separar os diferentes níveis de responsabilização dentro desse contexto de utilização da inteligência artificial como facilitadora da prática de ilícitos penais, sendo compartilhada, na medida de sua intenção e conhecimento, a responsabilidade entre o agente direto que executa a prática delitiva, bem como os sujeitos que participaram do desenvolvimento, disponibilização e implementação dessas tecnologias.

No primeiro nível de responsabilização, temos o autor direto que utiliza a inteligência artificial como meio instrumental para praticar o delito. Assim, permanece a imputação penal típica e expressa do Código Penal, com as agravantes em que incorre.

Em um segundo nível, deve-se analisar a responsabilidade do desenvolvedor do sistema, especialmente nos casos que demonstrarem negligência, imprudência ou imperícia no exercício de suas atividades de construção do algoritmo e nas etapas associadas à funcionalidade do sistema inteligente, bem como a ausência de mecanismos de mitigação de falhas sistêmicas previsíveis na utilização do sistema. Tal conduta pode ser caracterizada como omissiva imprópria relevante dentro da cadeia causal do dano, respondendo o desenvolvedor como possível garantidor, enquadrando-se nas tratativas que o Direito Penal adota para esses agentes.

Por fim, deve-se responsabilizar solidariamente as empresas fornecedoras das máquinas e softwares inteligentes por disponibilizarem a tecnologia no mercado sem uma adequada projeção

de riscos e sem governança tecnológica eficaz, considerando especialmente o elevado potencial de impacto social decorrente da venda do produto e de sua ampla aderência no mercado.

Assim, a aplicação da lei não deve se limitar apenas ao agente direto, mas deve considerar toda a cadeia de desenvolvimento, produção e disponibilização da tecnologia no mercado, aplicando, por analogia, como sugerido, estruturas jurídicas já consolidadas no ordenamento brasileiro, como a responsabilidade objetiva prevista no Código de Defesa do Consumidor e a teoria do risco da atividade, minimizando impactos derivados da criação desenfreada motivada pelo consumismo tecnológico.

CONCLUSÃO

O desenvolvimento acelerado da inteligência artificial coloca novos desafios à tona para o ordenamento jurídico, principalmente na estrutura de responsabilização jurídica. Embora esses sistemas inteligentes apresentem autonomia operacional, ainda não possuem em si consciência, vontade ou culpa, elementos característicos para configuração da responsabilidade penal. Portanto, a inteligência artificial não pode ser considerada sujeito ativo do crime, devendo ser considerada como ferramenta tecnológica na cadeia causal da conduta delitiva.

Nesse contexto, é necessário ampliar a responsabilidade delitiva, não restringindo-a somente ao agente direto do crime, reconhecendo a participação indireta das figuras contidas no ciclo de desenvolvimento e disponibilização dessas tecnologias, como desenvolvedores e entidades responsáveis pela comercialização dessas inteligências artificiais. A responsabilização do usuário permanece à conduta tipificada no Código Penal, uma vez que ele utiliza a ferramenta para prática de crime já expresso. Contudo, em determinadas circunstâncias, os desenvolvedores e responsáveis por negligência ou omissão praticada pela ausência de mecanismos de controle podem contribuir de forma relevante para a ocorrência do dano.

A análise do viés algorítmico coloca em evidência que os sistemas de inteligência artificial não são neutros, produzem distorções sociais presentes nas bases de dados utilizadas em seu treinamento, e são dotados de preconceitos já contidos em seu algoritmo ou desenvolvido durante seu contato com o usuário, como demonstrado no caso do sistema COMPAS. Reforçando a necessidade de mecanismos de governança tecnológica, auditoria e mitigação de riscos no desenvolvimento e implementação dessas ferramentas.

Diante disso, é coerente a aplicação analógica de estruturas jurídicas já consolidadas no ordenamento brasileiro, como a responsabilidade objetiva prevista no Código de Defesa do Consumidor

e a teoria do risco da atividade, sendo um caminho possível para enfrentar os desafios decorrentes da utilização da inteligência artificial. Assim, a apenação e responsabilidade das falhas tecnológicas devem considerar toda a cadeia de desenvolvimento, produção e disponibilização dessas tecnologias, buscando equilibrar inovação tecnológica, segurança jurídica e proteção social.

REFERÊNCIAS

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 15 mar. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. *Código Penal*. *Diário Oficial da União*: Rio de Janeiro, RJ, 31 dez. 1940.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 12 set. 1990.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. *Diário Oficial da União*: Brasília, DF, 3 dez. 2012.

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

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

CARVALHO, Olavo de. O jardim das aflições: de Epicuro à ressurreição de César – ensaio sobre o materialismo e a religião civil. Rio de Janeiro: Diadorim, 1997.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

PINHEIRO, Patrícia Peck. Direito digital. 7. ed. São Paulo: Saraiva Educação, 2021.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.