XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

FELIPE CHIARELLO DE SOUZA PINTO

EDMUNDO ALVES DE OLIVEIRA

DIOGO RAIS RODRIGUES MOREIRA

D597

Direito, governança e novas tecnologias I[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Felipe Chiarello de Souza Pinto, Edmundo Alves De Oliveira, Diogo Rais Rodrigues Moreira – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-308-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os artigos reunidos no *GT 8 – “Direito, Governança e Novas Tecnologias I”* do CONPEDI em São Paulo compuseram um conjunto significativo de reflexões acadêmicas sobre os impactos sociais, jurídicos e políticos das tecnologias digitais. As discussões evidenciaram a diversidade de abordagens presentes no campo, abrangendo desde desafios regulatórios até questões relacionadas à inclusão e aos direitos fundamentais na sociedade da informação. O GT foi coordenado pelos Professores Doutores *Felipe Chiarello de Souza Pinto* (Universidade Presbiteriana Mackenzie), *Diogo Rais Rodrigues Moreira* (Universidade Presbiteriana Mackenzie) e *Edmundo Alves de Oliveira* (Universidade de Araraquara).

Entre os temas apresentados, destacaram-se análises sobre *participação política, gênero e governança digital, com estudos que examinaram os direitos políticos das mulheres e a reprodução de desigualdades por meio de sistemas algorítmicos. Também foram discutidas perspectivas sobre **cidades inteligentes, **inclusão digital* e o uso da inteligência artificial como instrumento de apoio a pessoas com deficiência, apontando tanto potencialidades quanto limitações dessas tecnologias.

Os debates incluíram ainda reflexões sobre *movimentos sociais na internet, ciberativismo e seus efeitos nos processos democráticos, bem como investigações sobre **regulação tecnológica, com foco em modelos normativos de inteligência artificial, infocracia, soberania digital e responsabilidade civil. Aspectos práticos do uso da tecnologia no ambiente jurídico também estiveram presentes, com estudos envolvendo **crimes digitais, **herança digital, **georreferenciamento de imóveis* e a utilização de IA em mecanismos de resolução de disputas.

Além dos artigos apresentados no GT 8, *trabalhos relacionados às temáticas da digitalização e seus reflexos jurídicos foram apresentados em outros GTs do CONPEDI*, ampliando o escopo geral das discussões. Entre eles, destacam-se pesquisas sobre:

* conflitos entre *transparência processual e proteção de dados* no contexto do PJe;

* o uso da *inteligência artificial em crimes de estelionato e extorsão* e sua limitada abordagem jurisprudencial;

* os impactos da *IA na atuação do Poder Judiciário* e na concretização da cidadania;

* análises sobre *educação inclusiva, autismo e justiça social*, considerando a dedução integral de despesas educacionais no imposto de renda.

Em seu conjunto, os trabalhos apresentados nos diferentes GTs revelam a amplitude e a complexidade das relações entre tecnologia, direito e governança. As pesquisas demonstram que os desafios contemporâneos exigem abordagens multidisciplinares, éticas e regulatórias que considerem a centralidade das tecnologias digitais na vida social e institucional.

Prof. Dr. Felipe Chiarello de Souza Pinto

Prof. Dr. Edmundo Alves De Oliveira

Prof. Dr. Diogo Rais Rodrigues Moreira

SOBERANIA E NEOCOLONIALISMO DIGITAL: RESSIGNIFICANDO A RESPONSABILIDADE CIVIL NO BRASIL

DIGITAL SOVEREIGNTY AND NEOCOLONIALISM: REFRAMING CIVIL LIABILITY IN BRAZIL

Maria Fernanda Pereira Lima [1]
Cildo Giolo Junior [2]
Guilherme De Sousa Cadorim [3]

Resumo

Este estudo investiga os desafios da responsabilidade civil diante da ascensão dos sistemas inteligentes e da transformação digital. Parte-se da constatação de que os parâmetros clássicos, como conduta, dano, nexo causal e culpa não são suficientes para lidar com a autonomia e imprevisibilidade dos algoritmos, propõe-se, assim, a reformulação normativa da responsabilidade civil capaz de abarcar as complexidades da era digital. A pesquisa se preocupa também em analisar modelos internacionais como o AI Act da União Europeia, que categoriza riscos e propõe uma abordagem híbrida entre responsabilidade objetiva e critérios técnicos, já que o Brasil carece de normatização sobre sistemas inteligentes e precisa de referências sobre regulamentação. Assim diante da ausência de um marco regulatório específico que compromete a segurança jurídica e a proteção dos direitos fundamentais, percebe-se a necessidade de construção de um regime de responsabilidade digital que preserve a soberania nacional frente ao neocolonialismo informacional. Com base em levantamento bibliográfico e documental, incluindo dados do relatório da We Are Social (2024), o estudo propõe diretrizes para uma governança jurídica inclusiva, capaz de responder aos riscos das falhas operacionais dos sistemas automatizados.

Palavras-chave: Responsabilidade civil, Inteligência artificial, Plano de governança digital, Categorização dos riscos, Neocolonialismo digital

Abstract/Resumen/Résumé

This study investigates the challenges of civil liability in the face of the rise of intelligent systems and digital transformation. Based on the observation that traditional parameters, such as conduct, damage, causal connection, and fault, are insufficient to address the autonomy

[1] Advogada. Mestranda em Direito pelo PPGD da Faculdade de Direito de Franca, Brasil. Graduada no curso de Direito pela mesma faculdade. Pesquisadora pelo PIBIC 2020-2021

[2] Pós Doutor em Direitos Humanos pelo IGC/CDH da Faculdade de Direito da Universidade de Coimbra. Doutor em Direito pela Universidade Metropolitana de Santos. Doctor em Ciências Jurídicas y Sociales UMSA

[3] Mestrando em Direito e Pol. Públicas na Faculdade de Direito de Franca. Pós graduado em Direito Digital, LGPD, Direito Constitucional aplicado, Proteção ao Consumidor e Processo Civil Empresaria. Advogado

and unpredictability of algorithms, it proposes a normative reformulation of civil liability capable of encompassing the complexities of the digital age. The research also analyzes international models such as the European Union's AI Act, which categorizes risks and proposes a hybrid approach between strict liability and technical criteria, as Brazil lacks standardization on intelligent systems and requires regulatory references. Therefore, given the absence of a specific regulatory framework that compromises legal certainty and the protection of fundamental rights, the need to build a digital liability regime that preserves national sovereignty in the face of informational neocolonialism is evident. Based on a bibliographic and documentary survey, including data from the We Are Social report (2024), the study proposes guidelines for inclusive legal governance capable of responding to the risks posed by operational failures in automated systems.

Keywords/Palabras-claves/Mots-clés: Civil liability, Artificial intelligence, Digital governance plan, Risk categorization, Digital neocolonialism

1 INTRODUÇÃO

O Direito, enquanto sistema normativo voltado à regulação das condutas sociais, sempre esteve em constante diálogo com os fenômenos históricos, culturais e tecnológicos que moldam a realidade. Contudo, diante do dinamismo das transformações digitais impõe-se ao ordenamento jurídico um desafio inédito: a necessidade de se readaptar com agilidade e profundidade à vista de um mundo marcado pela automação, pela inteligência artificial e pela ubiquidade da informação. A era digital não apenas altera os meios pelos quais as relações sociais se desenvolvem, mas também modifica substancialmente os próprios fundamentos dessas relações, o que exige uma revisão acerca dos institutos jurídicos tradicionais.

Nesse contexto, a responsabilidade civil, um dos pilares do Direito Civil, revela-se insuficiente quando aplicada de forma estrita aos parâmetros clássicos. A lógica binária de conduta, dano, nexo de causalidade e culpa, embora ainda válida, não contempla adequadamente as complexidades envolvidas nas operações de sistemas inteligentes, que atuam de forma autônoma e probabilística. A imprevisibilidade dos riscos tecnológicos, aliada à dificuldade de atribuição de culpa em ambientes algorítmicos, demanda uma reformulação conceitual e normativa da responsabilidade civil, capaz de abarcar os novos contornos da realidade digital.

O Brasil, inserido nesse cenário de transformação global, encontra-se diante da urgência de regulamentar juridicamente as situações em que falhas operacionais de sistemas inteligentes causam danos a indivíduos, coletividades ou instituições. A ausência de um marco regulatório específico para a inteligência artificial compromete não apenas a segurança jurídica, mas também a proteção dos direitos fundamentais dos cidadãos. Assim, a construção de um regime de responsabilidade digital, adaptado às características da tecnologia, é condição essencial para garantir a efetividade do Direito e a preservação da soberania nacional frente aos desafios da globalização informacional.

A transformação da responsabilidade civil frente à era digital não precisa ocorrer em completo isolamento normativo. O ordenamento jurídico brasileiro pode e deve se inspirar em modelos regulatórios já consolidados internacionalmente, como o AI Act da União Europeia, que representa um marco na regulamentação da inteligência artificial. A categorização dos riscos proposta por esse regulamento, que distingue sistemas algorítmicos conforme seu potencial de causar danos permite a hibridização da responsabilidade civil, combinando elementos da responsabilidade objetiva com critérios técnicos e contextuais. Essa abordagem

favorece a criação de um modelo jurídico mais flexível, capaz de responder às especificidades dos sistemas inteligentes sem abandonar os fundamentos clássicos da reparação.

Justificada a presente discussão, a questão central que orienta esta pesquisa consiste em investigar: como se configura a responsabilidade civil por falhas operacionais de sistemas inteligentes, considerando os limites e possibilidades da soberania jurídica brasileira?

Dessa forma, para alcançar os resultados almejado o percurso metodológico adotado neste estudo foi o método dedutivo, já que se partiu da premissa de que o instituto tradicional da responsabilidade civil demanda reformulação conceitual e normativa para ser eficazmente aplicado às novas dinâmicas digitais. Ainda assim, reconhece-se que persistem obstáculos significativos para a consolidação de um regime jurídico nacional que assegure a soberania brasileira na regulação dessas tecnologias emergentes.

Fez-se necessário também o uso do método auxiliar comparativo, com o objetivo de examinar experiências normativas estrangeiras que possam servir de referência para o ordenamento jurídico brasileiro, destacando-se a análise da categorização de riscos proposta pelo AI Act da União Europeia. Para tanto, esta pesquisa se caracteriza por ser qualitativa, pois parte da análise do instituto da Responsabilidade civil, de modo a adaptá-lo a realidade digital. Posto isso, o presente relato é também prescritivo, pois tem o objetivo de propor ideias de normatização com base na atribuição da responsabilidade adequada a cada tipo de risco advindo das falhas nos sistemas automatizados.

Em sua maior parte, a pesquisa foi orientada por meio de levantamento bibliográfico, doutrinário e documental. Esta última baseou-se, sobretudo, nas informações disponibilizadas no relatório digital global mais recente da organização *We Are Social*, datado de 31 de janeiro de 2024. A análise desses dados teve como propósito evidenciar a crescente preocupação da sociedade brasileira com a gestão de seus dados pessoais, bem como ressaltar a urgência da implementação de políticas eficazes de responsabilização aplicáveis aos sistemas algorítmicos.

É dessa maneira que este estudo tem como objetivo geral promover a adequação do instituto da responsabilidade civil à realidade algorítmica, com vistas à proposição de um marco regulatório eficiente voltado à normatização dos sistemas inteligentes. Para tanto foram estabelecidos objetivos específicos que orientaram o desenvolvimento da investigação. Em primeiro lugar, procedeu-se à revisão crítica das teorias clássicas da responsabilidade civil. Em seguida, realizou-se uma análise da **c**ategorização de riscos proposta pelo ordenamento regulatório europeu.

Por fim, a pesquisa dedicou-se à identificação e ao exame dos desafios relacionados à efetividade do Direito brasileiro, considerando os impactos da globalização informacional e do

chamado neocolonialismo digital. A investigação buscou compreender como a fragmentação regulatória internacional e a assimetria de poder entre Estados e corporações tecnológicas afetam a capacidade normativa nacional, apontando caminhos para o fortalecimento da soberania jurídica por meio de uma governança digital estruturada e inclusiva.

2 DOS FUNDAMENTOS CLÁSSICOS DA RESPONSABILIDADE CIVIL

A responsabilidade civil, em seu conceito clássico, configura-se como o instituto jurídico que impõe ao causador de um dano a obrigação de repará-lo, buscando restabelecer, tanto quanto possível, o status quo ante da vítima. Esse instituto revela-se fundamental à pacificação social e à efetividade do ordenamento jurídico, pois traduz, em termos práticos, o princípio da reparação integral. Trata-se de uma obrigação jurídica que emerge em decorrência da violação de um dever primário, tendo por finalidade recompor o dano causado (Cavalieri Filho, 2021). Em sua acepção tradicional, tal instrumento encontra fundamento não apenas na proteção individual, mas também na preservação da confiança e da segurança nas relações sociais, sendo indispensável para o equilíbrio entre interesses privados e coletivos.

Em âmbito doutrinário, ressalta-se que a responsabilidade civil é construída a partir de elementos estruturantes que lhe conferem coerência e operacionalidade. Esses elementos tais quais, conduta, dano, nexo de causalidade e culpa, são considerados, no paradigma clássico, requisitos indispensáveis à configuração da obrigação de indenizar. A conduta, entendida como o comportamento humano voluntário, seja comissivo ou omissivo, é o marco inicial para a análise da responsabilização. Tal comportamento deve ser juridicamente relevante e contrário ao direito, representando uma ação ou omissão imputável ao agente. A ausência de conduta exclui, de plano, a possibilidade de imputação de responsabilidade civil, pois não há ato a ser correlacionado ao dano.

O dano, enquanto segundo elemento da responsabilidade civil, refere-se à violação de um interesse juridicamente tutelado, podendo manifestar-se sob a forma de prejuízo patrimonial ou de lesão a direitos de natureza extrapatrimonial. A obrigação de indenizar somente se configura diante de um prejuízo efetivo, suscetível de avaliação, ainda que estimativa, ou quando se verifica afronta à dignidade da pessoa humana, ensejando o reconhecimento do dano moral (Gagliano, Pamplona Filho 2018). A concepção tradicional do instituto não admite a responsabilização dissociada da existência de dano, uma vez que este representa não apenas um requisito lógico, mas também um imperativo ético que legitima a pretensão reparatória. Nesse sentido, a responsabilidade civil tem por escopo assegurar a recomposição plena da esfera

jurídica lesada, abrangendo tanto o reembolso por perdas materiais quanto a compensação por sofrimentos de ordem subjetiva, conforme delineado pelo ordenamento jurídico vigente.

O nexo de causalidade, por sua vez, é o vínculo que une a conduta ao dano, estabelecendo a relação de causa e efeito. No sistema clássico, sem esse liame causal não há que se falar em responsabilidade, pois o evento lesivo poderia decorrer de fatores alheios à atuação do agente. É possível enfatizar, portanto, que o nexo causal cumpre a função de limitar a imputação, evitando que o dever de indenizar se estenda a quem não contribuiu de forma relevante para o resultado danoso (Cavalieri Filho, 2021). As teorias da causalidade adequada e da equivalência das condições são referências metodológicas nesse campo, sendo a primeira mais utilizada no direito contemporâneo por permitir filtragem valorativa das causas juridicamente relevantes, afastando fatores meramente remotos ou irrelevantes.

O elemento culpa, no modelo tradicional, remete à ideia de reprovação pela conduta contrária ao dever jurídico, podendo manifestar-se sob a forma de dolo (intenção de causar o dano) ou culpa stricto sensu (negligência, imprudência ou imperícia). A responsabilidade subjetiva, como regra no direito civil clássico, pressupõe a demonstração da culpa para que se imponha a reparação. Essa exigência decorre do princípio da justiça corretiva aristotélica, segundo o qual somente deve responder aquele que agiu de forma censurável (Tartuce, 2022). Contudo, o ordenamento admite hipóteses de mitigação desse paradigma por meio da responsabilidade objetiva, em que a obrigação de indenizar decorre da mera comprovação do dano e do nexo causal, independentemente de culpa, fundamentando-se na teoria do risco e em normas específicas que atribuem dever de reparar a determinadas atividades.

A distinção entre responsabilidade subjetiva e objetiva é, portanto, central para a compreensão do instituto. Na primeira, exige-se a prova da culpa do agente, sendo aplicável como regra geral nas relações civis, em consonância com os artigos 186 e 927, caput, do Código Civil. Já a responsabilidade objetiva, prevista no parágrafo único do artigo 927 do mesmo diploma, bem como em legislações especiais como o Código de Defesa do Consumidor, estabelece que determinadas atividades, pela sua natureza ou pelo risco que geram, impõem ao agente o dever de indenizar independentemente da verificação de culpa. Essa ampliação visa tutelar bens jurídicos sensíveis e assegurar a reparação célere em contextos de risco acentuado, o que reflete um movimento de transição do paradigma estritamente subjetivo para modelos híbridos e funcionalizados à proteção da vítima (Rosenvald, 2023).

Os fundamentos clássicos da responsabilidade civil permanecem, no entanto, como se discutirá nos capítulos subsequentes desta pesquisa, a emergência de riscos associados ao ambiente digital e a atuação de sistemas inteligentes vem tensionando esses conceitos, o que

exigi releitura de suas bases para garantir a efetividade da proteção jurídica diante de novas modalidades de dano e de agentes não humanos.

2.1 Adaptação da teoria da responsabilidade civil ao ambiente digital

Sendo a Responsabilidade civil o mecanismo jurídico por meio do qual se busca a reparação de danos injustamente sofridos por terceiros e fundamentada na ideia de justiça corretiva, tal instituto tem por escopo restabelecer o equilíbrio rompido entre as partes, mediante a imposição de um dever de indenizar àquele que, por ação ou omissão, causou prejuízo a outrem. A evolução social e o aumento de riscos derivados de atividades complexas impuseram uma ampliação dessa função, agregando-lhe um viés preventivo. Ou seja, a responsabilidade civil não mais se limita a recompor perdas já consolidadas, mas também atua como mecanismo de inibição de condutas potencialmente lesivas. Essa perspectiva preventiva torna-se particularmente relevante no ambiente digital, no qual a antecipação de riscos pode evitar danos de larga escala e difícil reparação.

O deslocamento do foco da responsabilidade civil para a prevenção é perceptível quando se observa o novo tipo de dano emergente no contexto tecnológico: aquele não necessariamente causado por uma ação humana direta, mas por decisões autônomas de sistemas algorítmicos. Com a crescente sofisticação de sistemas de inteligência artificial, significativos resultados prejudiciais decorrem de processos de aprendizado de máquina e de tomada de decisão automatizada, nos quais a intervenção humana é mínima ou inexistente (Tartuce, 2024). Essa característica rompe com a lógica clássica, na qual a conduta humana voluntária era o ponto de partida para a responsabilização. No ambiente tecnológico, o dano pode ser produto de cadeias causais complexas, envolvendo tanto programadores quanto usuários, empresas mantenedoras de plataformas e até fornecedores de dados, o que exige, portanto, uma reavaliação dos critérios de imputação.

Assim, necessário se faz analisar a adequação da responsabilidade civil ao contexto digital, tendo em vista a expressiva presença da população brasileira no ambiente virtual. Conforme dados divulgados em janeiro de 2024, o Brasil ocupa a segunda posição no ranking mundial de tempo médio diário de uso da internet (We are social, 2024). Os usuários brasileiros, com idade entre 16 e 64 anos, permanecem conectados por aproximadamente 9 horas e 13 minutos ao dia, superando significativamente a média global, que é de cerca de 6 horas e 40 minutos (We are social, 2024).

Apesar do elevado tempo de permanência dos brasileiros na internet, observa-se que aproximadamente 50% dos usuários nacionais, com idade entre 16 e 64 anos, demonstram preocupação quanto ao modo como as empresas utilizam seus dados pessoais (We are social, 2024). Tal porcentagem evidencia não apenas a vulnerabilidade dos indivíduos diante da coleta massiva de dados, mas também a influência exercida pelas plataformas digitais na modelagem de comportamentos e decisões, especialmente em um cenário marcado pela ausência de regulamentação robusta capaz de limitar práticas abusivas e garantir maior transparência nos processos algorítmicos.

Essa vulnerabilidade técnica dos usuários é outro fator que provoca a adaptação do instituto da Responsabilidade Civil. A assimetria de informação entre operadores de sistemas tecnológicos e seus usuários cria um cenário em que estes últimos não apenas desconhecem o funcionamento interno das tecnologias que utilizam, como também não possuem meios eficazes de prevenir ou mitigar danos decorrentes de seu uso. A fragilidade dos consumidores digitais não se restringe à dimensão informacional, mas abrange aspectos como a dependência de infraestrutura digital e a opacidade dos processos decisórios algorítmicos (Cohen, 2022). Sob essa ótica, a proteção jurídica deve considerar que, para o usuário comum, é inviável identificar falhas técnicas, prever comportamentos do sistema ou adotar medidas preventivas adequadas, o que justifica a ampliação de hipóteses de responsabilidade objetiva.

A categorização dos casos em que se aplica responsabilidade objetiva ou subjetiva no ambiente tecnológico deve partir dessa constatação de vulnerabilidade e da análise da natureza da atividade desenvolvida. A responsabilidade objetiva, fundamenta-se na teoria do risco, sendo aplicável quando a atividade, pela sua própria essência, expõe terceiros a riscos anormais ou acima do padrão socialmente tolerado (Cavalieri Filho 2021). No contexto digital, enquadram-se nessa categoria situações como o fornecimento de plataformas de inteligência artificial generativa, sistemas de recomendação automatizada que possam induzir danos massivos, e dispositivos autônomos conectados à Internet das Coisas. Nesses casos, a ausência de necessidade de provar a culpa do agente garante uma proteção mais célere e efetiva à vítima, refletindo a função preventiva da responsabilidade civil e incentivando o desenvolvimento de mecanismos de segurança mais robustos.

Por outro lado, a responsabilidade subjetiva mantém relevância quando a atividade tecnológica não apresenta, por si só, riscos extraordinários, ou quando é possível identificar e provar a culpa do agente. Essa modalidade é adequada para situações em que o dano decorre de falhas de operação, negligência no uso de ferramentas digitais ou violação de deveres contratuais específicos por parte de um profissional qualificado (Tartuce, 2024). Assim, a

responsabilidade subjetiva preserva seu papel como instrumento de imputação proporcional e individualizada, compatível com atividades de risco ordinário e com a possibilidade de prova da culpa.

Essa adaptação da responsabilidade civil ao ambiente tecnológico revela-se no futuro do Direito brasileiro, já que é um movimento de pluralização normativa, no qual coexistem funções reparatória e preventiva em equilíbrio dinâmico. A função reparatória continua essencial, assegurando a recomposição de prejuízos e a justiça corretiva; já a função preventiva assume caráter estratégico, buscando desestimular condutas e projetos tecnológicos potencialmente lesivos antes mesmo de sua concretização. Essa dupla função não deve ser entendida como ruptura com a tradição, mas como ampliação necessária diante da complexidade e da imprevisibilidade dos riscos digitais (Rosenvald, 2023). Nesse cenário, a categorização entre responsabilidade objetiva e subjetiva torna-se ferramenta de calibragem da proteção jurídica, assegurando tanto a eficiência na reparação quanto a efetividade na prevenção, especialmente em um contexto no qual a decisão algorítmica e a vulnerabilidade técnica do usuário se tornaram elementos centrais na análise da responsabilidade civil.

3 CATEGORIZAÇÃO DOS RISCOS PARA APLICAÇÃO DA RESPONSABILIDADE CIVIL HÍBRIDA

A responsabilidade civil híbrida surge como uma resposta a essa demanda, propondo a combinação de elementos da responsabilidade subjetiva e objetiva. Não se trata de uma nova modalidade de responsabilidade, mas sim de uma abordagem que permite a aplicação conjunta ou complementar de diferentes regimes, adaptando-se à complexidade dos danos causados por tecnologias digitais. Essa hibridização reconhece que, em uma parcela de casos, a atribuição de culpa exclusiva a um único agente é inviável, seja pela opacidade dos algoritmos, pela cadeia de fornecimento de serviços digitais ou pela própria autonomia dos sistemas de IA.

No Brasil, a regulamentação da responsabilidade civil no ambiente digital ainda está em construção, mas já é possível identificar elementos que apontam para a adoção de um modelo híbrido. O Marco Civil da Internet, Lei nº 12.965/2014, e a Lei Geral de Proteção de Dados Pessoais LGPD, Lei nº 13.709/2018, são marcos importantes nesse sentido, estabelecendo princípios e diretrizes que podem ser interpretados à luz da responsabilidade civil híbrida.

O Marco Civil da Internet, por exemplo, ao tratar da responsabilidade dos provedores de aplicações de internet, adota um regime que mescla elementos de responsabilidade subjetiva e objetiva. Provedores de conteúdo, em regra, só são responsabilizados por danos decorrentes de

conteúdo gerado por terceiros se, após ordem judicial, não removerem o material. Já os provedores de conexão não são responsabilizados por conteúdo de terceiros (Brasil, 2014). Essa distinção demonstra preocupação em equilibrar a liberdade de expressão com a necessidade de proteção dos usuários, sem, contudo, impor uma responsabilidade excessiva que pudesse inviabilizar a inovação.

A LGPD, por sua vez, ao estabelecer um regime de responsabilidade solidária entre o controlador e o operador de dados pessoais em caso de danos decorrentes do tratamento de dados, também aponta para uma abordagem híbrida (Brasil, 2018). Embora a lei preveja a possibilidade de excludentes de responsabilidade, a regra geral é a responsabilização conjunta, o que reflete a complexidade da cadeia de tratamento de dados e a dificuldade de individualizar a culpa em caso de vazamento ou uso indevido. A LGPD, ao focar na proteção dos direitos fundamentais de liberdade e privacidade, impõe um dever de cuidado que se aproxima da responsabilidade objetiva, ao mesmo tempo em que permite a análise da conduta dos agentes.

Ao considerar o andamento da situação, importante se faz analisar o Regulamento de Inteligência Artificial da União Europeia (AI Act), embora recente, essa normativa representa um marco global na tentativa de regulamentar a IA de forma abrangente e baseada em riscos. Sua abordagem inovadora classifica os sistemas de IA em diferentes categorias de risco: inaceitável, alto, limitado e mínimo, dessa forma impõem obrigações proporcionais a cada nível, com o objetivo de garantir a segurança, a ética e a proteção dos direitos fundamentais dos cidadãos.

Por riscos inaceitáveis é abordado algoritmos que representam uma ameaça clara aos direitos fundamentais e à segurança dos indivíduos, sendo, portanto, proibidos. É possível citar como exemplo sistemas de identificação biométrica remota em tempo real em espaços públicos para fins de aplicação da lei, com algumas exceções estritas (European Commission, 2024). Já os classificados como de alto risco são aqueles que podem causar danos significativos à saúde, segurança ou direitos fundamentais das pessoas. Para esses sistemas, o AI Act impõe obrigações rigorosas, como a necessidade de avaliação de conformidade antes da colocação no mercado, gestão de riscos, governança de dados, documentação técnica, supervisão humana, robustez, precisão e segurança cibernética (European Commission, 2024).

Os riscos limitados, por sua vez, caracterizam-se por sistemas inteligentes que apresentam riscos específicos de manipulação ou falta de transparência, mas que não são considerados de potencial elevado de perigo. As obrigações para esses sistemas são mais leves e focam principalmente na transparência, exigindo que os usuários sejam informados de que estão interagindo com sistema de IA, por exemplo, chatbots e sistemas de reconhecimento de

emoções (European Commission, 2024). Por último o risco mínimo ou nulo, é a categoria em que se enquadra a maioria dos agentes inteligentes, já que inclui aplicações de baixo risco, como filtros de spam ou jogos baseados em IA. Para esses sistemas, o AI Act não impõe obrigações legais adicionais, incentivando, no entanto, a adoção voluntária de códigos de conduta (European Commission, 2024).

A adoção de uma abordagem baseada em riscos, similar à do AI Act, pode ser uma alternativa promissora para o Brasil na regulamentação da IA e na aplicação da responsabilidade civil híbrida. Ao categorizar os sistemas de inteligência artificial de acordo com o potencial de dano, é possível estabelecer um regime de responsabilidade proporcional, que incentive a inovação ao mesmo tempo em que protege os direitos dos cidadãos.

Além disso, a categorização de riscos facilitaria a identificação dos agentes responsáveis em cada etapa do ciclo de vida de um sistema de inteligente, como desenvolvedor, fornecedor, implementador, usuário, o que permite a aplicação de diferentes regimes de responsabilidade conforme a natureza do risco e a capacidade de controle de cada agente. Isso evita a imposição de responsabilidades desproporcionais e garante que a reparação do dano seja efetiva. Dessa forma, a flexibilidade do modelo híbrido de responsabilidade civil se alinha adequadamente nessa estrutura, o que permite que a responsabilidade seja atribuída de forma mais eficaz, ao considerar a complexidade e o potencial de dano de cada sistema inteligente.

3.1 Desafios da efetividade do Direito brasileiro na aplicação de normas de soberania nacional quanto a responsabilidade digital

A era digital, caracterizada pela ubiquidade da internet e pela crescente automação impulsionada pela Inteligência Artificial, reconfigurou as relações sociais, econômicas e jurídicas em escala global. Nesse cenário de profunda transformação, a governança digital emerge como campo de estudo e prática essencial para a formulação de políticas públicas e marcos regulatórios que busquem equilibrar inovação tecnológica, desenvolvimento econômico e proteção de direitos fundamentais. No Brasil, a efetividade do Direito na aplicação da responsabilidade digital enfrenta desafios complexos, especialmente no que tange à jurisdição e territorialidade em plataformas transnacionais, ao fenômeno do neocolonialismo digital e à necessidade de diretrizes claras para a responsabilização em casos de falhas de algoritmos.

A internet, por sua natureza global e descentralizada, desafia os conceitos tradicionais de jurisdição e territorialidade, que são pilares do direito internacional e nacional. Em um ambiente em que dados e informações fluem sem fronteiras físicas, a aplicação de leis nacionais a

condutas praticadas em plataformas digitais transnacionais torna-se um dos maiores entraves para a efetividade do Direito brasileiro na aplicação da responsabilidade digital (Tiburcio, Albuquerque, 2023).

Tradicionalmente, a jurisdição de um Estado está atrelada ao seu território, ou seja, à sua capacidade de exercer poder soberano sobre pessoas e bens dentro de suas fronteiras geográficas. No entanto, as plataformas digitais, muitas vezes sediadas em outros países, com servidores distribuídos globalmente e usuários em diversas jurisdições, complexificam essa lógica (Tiburcio, Albuquerque, 2023). Um ato ilícito praticado por um usuário no Brasil, por exemplo, pode ter seus efeitos sentidos em outros países, e a plataforma que hospeda esse conteúdo pode estar sujeita a leis e regulamentações de diferentes jurisdições.

No Brasil, o Marco Civil da Internet tentou endereçar parte dessa questão ao estabelecer que a lei brasileira será aplicada às operações de tratamento de dados pessoais realizadas em território nacional, independentemente do local de sede do operador ou do controlador dos dados, desde que o objetivo seja a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil (Brasil, 2014). Essa disposição, embora importante, não resolve integralmente o problema da jurisdição em casos de danos causados por plataformas transnacionais, especialmente quando se trata de conteúdo ilícito ou de responsabilidade por falhas em sistemas de IA.

Os desafios na aplicação da lei brasileira a plataformas transnacionais são multifacetados e vão desde as dificuldades de notificação e citação, conflito de leis entre países e execução de decisões judiciais até a assimetria de poder e as situações de Forum Shopping. Ou seja, grandes empresas de tecnologia, com vastos recursos jurídicos possuem maior poder de barganha do que Estados individuais, além disso, esses conglomerados tecnológicos aproveitam da fragmentação regulatória para escolher jurisdições mais favoráveis, onde as leis são menos rigorosas ou a fiscalização é menos intensa, o que prejudica a efetividade da proteção dos direitos dos usuários (Camargo, 2017).

Diante desses desafios, a busca por soluções passa necessariamente pela cooperação internacional e pela harmonização legislativa. Apesar de o avanço tecnológico ter se apresentado como um vetor de desenvolvimento e democratização, uma análise mais aprofundada revela que a distribuição e o controle dessas tecnologias não são equitativos, dando origem a um fenômeno que tem sido denominado de neocolonialismo digital.

Inicialmente, cumpre destacar que a colonialidade configura um sistema global de poder marcado por assimetrias estruturais e pela imposição de subjetividades subordinadas. De modo análogo, o neoliberalismo representa a expressão contemporânea do capitalismo,

caracterizando-se por uma racionalidade política e econômica que concebe o mundo como um mercado competitivo, composto por entidades empresariais voltadas à incessante busca por progresso (Silveira, 2021). No contexto da era digital, observa-se a intensificação da lógica capitalista mediante a informatização da produção simbólica e a expansão das redes digitais em escala planetária. Tal dinâmica promove um fluxo unidirecional de dados, consolidando o domínio informacional nas mãos de atores que, historicamente, já detinham posições privilegiadas de poder.

O neocolonialismo digital, portanto, é uma extensão do conceito tradicional de neocolonialismo, que se refere à exploração econômica e cultural de nações mais fracas por nações mais fortes, sem a necessidade de controle político direto (Faustino, Lippold, 2021). Este conceito descreve a perpetuação de relações de dependência e dominação entre países desenvolvidos, detentores da tecnologia e da infraestrutura digital, e países em desenvolvimento, que se tornam meros consumidores e provedores de dados, sem autonomia para definir seus próprios rumos tecnológicos.

Uma das formas de manifestação desse fenômeno é por meio da imposição de padrões e normas (Faustino, Lippold, 2021). As normas técnicas e regulatórias que governam o ciberespaço são frequentemente definidas por organismos internacionais dominados por países desenvolvidos, que tendem a refletir seus próprios interesses e valores, marginalizando as perspectivas e necessidades dos países em desenvolvimento.

Diante do cenário de neocolonialismo digital, a busca pela soberania tecnológica torna-se um imperativo para o Brasil. A soberania digital brasileira só acontecerá após um plano de governança robusto que estabeleça um marco regulatório nacional. Ou seja, a capacidade do Estado brasileiro em controlar autonomamente suas infraestruturas digitais, fluxos de dados e o desenvolvimento de suas próprias tecnologias, garantindo que as decisões sobre o futuro digital do país sejam tomadas em seu próprio interesse, e não ditadas por potências estrangeiras, advém de regras nacionais claras para a atuação de plataformas transnacionais no Brasil, o que garante a aplicação da lei do país.

3.2 Governança Digital como pilar para a responsabilidade digital

A governança digital é um campo em constante evolução que busca estabelecer princípios, estruturas e processos para gerenciar o desenvolvimento e o uso das tecnologias digitais, garantindo que elas sirvam ao bem-estar social, à justiça e à sustentabilidade. Diante de um contexto virtual marcado pela infosfera, em que dados, informações e comunicações

digitais circulam e interagem, a governança do digital deve ser guiada por uma "ética suave", que se concentra na prevenção de danos e na promoção do florescimento humano na infosfera (Floridi, 2018).

É possível observar que a governança digital eficaz exige uma abordagem que vai além da mera regulamentação legal, incorporando aspectos éticos, sociais e técnicos. Propõem-se que a responsabilidade não deve ser atribuída apenas aos indivíduos, mas também aos sistemas e às organizações, reconhecendo a agência distribuída no ambiente digital (Floridi, 2018). Assim, tal gestão estratégica eletrônica deve ter como característica a centralidade no ser humano, ter processos decisórios transparente de sistemas inteligente, inclusiva e equitativa, responsável e responsabilizável.

Por outro lado, ao basear-se na teoria da sociedade em rede (Castells, 2005) a governança digital, torna-se um instrumento de redistribuição de poder, capaz de equilibrar as relações entre grandes corporações tecnológicas e os cidadãos. Dessa maneira se caracterizada por redes complexas de atores, em que o poder não reside apenas nos Estados, mas também em corporações transnacionais e movimentos sociais. Essa governança eletrônica, portanto, é um processo dinâmico de negociação e conflito entre esses diferentes atores que promove interoperabilidade entre sistemas e a harmonização de normas em escala global. Isso implica reconhecer a responsabilidade dos Estados, das empresas e da sociedade civil na definição dos rumos da transformação digital (Castells, 2015).

A governança digital, em suas diversas concepções, é um pilar fundamental para a efetividade do Direito brasileiro na aplicação da responsabilidade tecnológica. Ao estabelecer princípios claros, estruturas de supervisão e mecanismos de responsabilização, ela cria o ambiente necessário para que as tecnologias digitais sejam desenvolvidas e utilizadas de forma ética e segura. É preciso entender que planos de governança robustos permite que os sistemas de IA sejam transparentes em seu funcionamento e que seus algoritmos sejam explicáveis, facilitando a identificação de falhas e a atribuição de responsabilidade.

Além disso, estabelece mecanismos para verificar o desempenho e o impacto dos sistemas inteligente, o que permite a detecção precoce de problemas e a correção das redes ao determinar diretrizes de condutas a serem seguidas. Sempre alinhada a proteger os direitos fundamentais, bem como os princípios democráticos, a governança digital não se trata de conceito teórico, mas uma necessidade prática para enfrentar os desafios da era digital. Por isso, a colaboração entre diferentes atores para um projeto de governança digital efetivo é essencial.

Apesar de cada instituição possuir interesses e prioridades distintas, já que Governos buscam soberania e controle, enquanto empresas visam lucro e inovação, a sociedade civil foca

em direitos e inclusão, e a academia busca conhecimento e ética. Faz-se necessário estabelecer órgãos consultivos permanentes, com representação equitativa de governos, setor privado, sociedade civil e academia, para debater e propor soluções para questões de governança digital

Embora o Direito Digital se apresente como campo emergente e marcado por inovações tecnológicas disruptivas, sua construção dogmática não prescinde do diálogo com teorias clássicas consolidadas no ordenamento jurídico. A aplicação de paradigmas consolidados, como o modelo da tríplice hélice, criada em 1995 por Henry Etzkowitz e Chunyan Zhou, revela-se particularmente pertinente na formulação de um plano de governança digital nacional. Esse modelo, ao propor a articulação sinérgica entre academia, governo e setor produtivo, oferece uma base teórica e prática para o desenvolvimento de soluções colaborativas voltadas à preservação da soberania tecnológica brasileira, logo, podem atuar conjuntamente na definição de caminhos regulatórios que viabilizem a normatização adequada dos sistemas autônomos

CONSIDERAÇÕES FINAIS

Dessa forma, de maneira a responder à questão da pesquisa: como se configura a responsabilidade civil por falhas operacionais de sistemas inteligentes, considerando os limites e possibilidades da soberania jurídica brasileira? É que se sugere um modelo propositivo de reformulação do instituto da responsabilidade civil, adaptando-o ao ambiente digital por meio de um formato híbrido baseado na categorização dos riscos tecnológicos. Essa abordagem visa garantir reparação proporcional e eficaz diante da complexidade dos danos causados por tecnologias autônomas.

Apesar dos desafios como a indefinição da jurisdição competente no ciberespaço, bem como a situação do colonialismo digital, em que ambos comprometem a soberania jurídica de nações como o Brasil, é que se indica a construção de um plano de governança digital nacional sólido. Tal plano visa reequilibrar as relações entre grandes corporações tecnológicas e os cidadãos, de modo a fortalecer o objetivo da autonomia regulatória brasileira.

Partindo da constatação de que os modelos tradicionais desse instituto jurídico se revelam insuficientes quando aplicados de forma restrita às dinâmicas tecnológicas contemporâneas, propôs-se uma releitura da responsabilidade civil clássica, especialmente no que tange à ocorrência de falhas em sistemas inteligentes. Para tanto, tornou-se necessário revisitar os conceitos estruturantes da responsabilidade civil como conduta, dano, nexo de causalidade e culpa, com vistas a estabelecer um ponto de partida teórico sólido para sua reinterpretação no contexto digital.

Na sequência, o estudo dedicou-se à análise da adaptação da responsabilidade civil às novas configurações tecnológicas, considerando a crescente imprevisibilidade dos riscos associados à inteligência artificial e à automação de decisões. Nesse cenário, destacou-se a relevância da dupla função da responsabilidade civil: a função reparatória, voltada à compensação dos danos sofridos, e a função preventiva, orientada à dissuasão de condutas lesivas e à promoção de boas práticas. A pesquisa também se preocupou em examinar os critérios de aplicação da responsabilidade objetiva e subjetiva no ambiente digital, reconhecendo que a natureza da atividade desenvolvida e a vulnerabilidade dos usuários são elementos determinantes para a definição do regime jurídico mais adequado.

Com o intuito de oferecer subsídios normativos, analisou-se o Regulamento de Inteligência Artificial da União Europeia (AI Act), que propõe uma classificação dos sistemas de IA em quatro categorias de risco: inaceitável, alto, limitado e mínimo. Essa abordagem permite a construção de um regime de responsabilidade proporcional, em que o grau de exigência normativa se ajusta ao potencial de dano associado à tecnologia utilizada. A categorização de riscos, nesse sentido, revela-se como ferramenta essencial para a formulação de políticas públicas eficazes e para a proteção dos direitos fundamentais em ambientes digitais complexos e dinâmicos.

Em seguida, a pesquisa se debruçou sobre os desafios enfrentados pelo ordenamento jurídico brasileiro na aplicação de normas de soberania nacional no contexto da responsabilidade digital. A natureza global e descentralizada da internet impõe obstáculos significativos aos conceitos tradicionais de jurisdição e territorialidade, dificultando a efetividade das decisões judiciais e a aplicação uniforme da legislação nacional. A ausência de mecanismos de cooperação internacional e de harmonização legislativa contribui para o agravamento do fenômeno conhecido como neocolonialismo digital, no qual países em desenvolvimento permanecem subordinados aos interesses tecnológicos e regulatórios das potências digitais.

Diante desse cenário, propõe-se a elaboração de um plano de governança digital como alternativa estratégica para enfrentar os desafios da responsabilidade civil no ambiente tecnológico. Tal plano deve contemplar a definição de princípios normativos, estruturas institucionais e processos administrativos voltados à regulação e ao uso ético das tecnologias digitais, com vistas à promoção do bem-estar coletivo, da justiça social e da sustentabilidade. Conclui-se, portanto, que embora a transição da responsabilidade civil clássica para sua aplicação no contexto digital envolva transformações teóricas e práticas, o futuro do Direito

brasileiro aponta para a construção de um marco regulatório robusto, baseado na categorização de riscos e sustentado por uma governança digital eficiente e inclusiva.

REFERÊNCIAS

ANDRADE, Walmar. **AI Act: análise do Regulamento Europeu de Inteligência Artificial.** Walmar Andrade, 2024. Disponível em: https://walmarandrade.com.br/ai-act/. Acesso em: 14 ago. 2025.

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.

CAMARGO, Solano de**. Forum Shopping: a escolha da jurisdição mais favorável**. São Paulo: Intelecto Editora, 2017.

CARVALHO, André; BELCHIOR, Felipe. **Soberania digital: (neo)colonialismo e infraestruturas públicas digitais.** Legal Grounds Institute, 22 maio 2025. Disponível em: https://legalgroundsinstitute.com/blog/soberania-digital-neocolonialismo-e-infraestruturas-publicas-digitais. Acesso em: 14 ago. 2025.

CASTELLS, Manuel. **A sociedade em rede.** 8. ed São Paulo: Paz e Terra, 2005.

CASTELLS, Manuel. **Comunicação e poder**. Lisboa: Fundação Calouste Gulbenkian, 2015.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 13. ed. São Paulo: Atlas, 2021.

COHEN, Julie E. **From Lex Informatica to the Control Revolution.** Berkley Technology Law Journal, v. 36, n.3, 2022.

COSTA, Caio Vilela; FREITAS, Fernanda Martins; MOTA, Gustavo Rodrigues Gentil da**. REsp 2.147.711/SP e os limites da extraterritorialidade na internet**. Migalhas, São Paulo, 14 ago. 2025. Disponível em: https://www.migalhas.com.br/depeso/436705/resp-2-147-711-sp-e-os-limites-da-extraterritorialidade-na-internet. Acesso em: 14 ago. 2025.

ETZKOWITZ, Henry; ZHOU, Chunyan. **Hélice Tríplice: inovação e empreendedorismo universidade-indústria-governo.** Estudos Avançados, São Paulo, v. 31, n. 90, mai./ago. 2017. Disponível. Disponível em: https://doi.org/10.1590/s0103-40142017.3190003. Acesso em: 15 agosto 2025.

EU ARTIFICIAL INTELLIGENCE ACT**.** Article 6: Classification Rules for High-Risk AI Systems. 2026. Disponível em: https://artificialintelligenceact.eu/article/6/. Acesso em: 14 ago. 2025.

EUROPEAN COMMISSION. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Brussels, 21.4.2021 COM(2021) 206 final.

EUROPEAN COMMISSION. **Regulamento Inteligência Artificial – Shaping Europe's digital future**. Bruxelas: European Commission, 2024. Disponível em: https://digital-strategy.ec.europa.eu/pt/policies/regulatory-framework-ai. Acesso em: 14 ago. 2025.

FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana.** [S.l.]: Google Books, 2021. Disponível em: Google Books – Colonialismo digital. Acesso em: 14 ago. 2025.

FLORIDI, Luciano. **Ethics, Governance and Policies for the Digital Age.** Oxford: Oxford University Press, 2021.

FLORIDI, Luciano. **Soft Ethics and the Governance of the Digital. Philosophy & Technology,** v. 31, 2018. Disponível em: SpringerLink. Acesso em: 14 ago. 2025.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo**. Novo Curso de Direito Civil.** Volume 3: Responsabilidade Civil. 16. ed. São Paulo: Saraiva, 2018.

GIOLLO JUNIOR, Cildo; TOFFANO, Marcelo; ARAÚJO, Eduarda Calixto Rezende de. **Estruturas algorítmicas e exclusão social: necessidade de políticas públicas para prevenir a perpetuação de preconceitos**. CONGRESSO NACIONAL DO CONPEDI, Virtual, 2024. Florianópolis: CONPEDI, 2024. Disponível em: https://site.conpedi.org.br/publicacoes/v38r977z/8435z800/O0ad7KJW1O06Q7ni.pdf. Acesso em: 25 Set, 2025.

GIOLO JUNIOR; Cildo. SARAIVA; José Sérgio. **A Adoção Teoria da Tríplice Hélice como Política Pública.** Disponível: https://periodicos.ufms.br/index.php/revdir/article/view/18893.

ONETRUST. **Lei de IA da UE: soluções para conformidade com a legislação europeia sobre inteligência artificial**. OneTrust, 21 nov. 2024. Disponível em: https://www.onetrust.com/pt/solutions/eu-ai-act-compliance/. Acesso em: 14 ago. 2025.

PIRES, Guilherme Moreira; SILVA, Patrícia Cordeiro da**. (Neo)colonialismo digital: subordinação tecnológica na sociedade de controle**. Empório do Direito, 20 nov. 2024. Disponível em: https://emporiododireito.com.br/leitura/neo-colonialismo-digital-subordinacao-tecnologica-na-sociedade-de-controle. Acesso em: 14 ago. 2025.

ROSENVALD, Nelson. **Responsabilidade civil e proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2023.

SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce. Colonialismo de dados: como opera as trincheiras algorítmicas na guerra neoliberal. 1. ed. São Paulo: Autonomia Literária, 2021.

TARTUCE, Flávio. **Manual de Direito Civil: volume único**. 14. ed. Rio de Janeiro: Método, 2024..

TIBURCIO, Carmen; ALBUQUERQUE, Felipe. **Territorialidade, jurisdição e internet: alguns aspectos de direito internacional privado**. Revista Eletrônica de Direito Processual, Rio de Janeiro, n. 24, p. 1–30, 2023. Disponível em: https://www.e-publicacoes.uerj.br/redp/article/download/79553/538/287246. Acesso em: 14 ago. 2025.

VLK ADVOGADOS**. AI Act: mapa interativo de obrigações e das categorias de riscos**. São Paulo: VLK Advogados, 18 abr. 2024. Disponível em: https://vlklaw.com.br/wp-content/uploads/2024/04/AI-Act-Mapa-Interativo-de-Obrigacoes-e-das-Categorias-de-Riscos-VLK-Advogados.pdf. Acesso em: 14 ago. 2025.

WE ARE SOCIAL; MELTWATER. Digital 2024: 5 billion social media users. Londres: We Are Social, 2024. Disponível em: https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users. Acesso em: 03 jul. 2025.

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder***. Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2021. e-book.