RGe ISSN: 2177-3246

# RESPONSABILIDADE CIVIL POR RISCO ALGORÍTMICO: ANÁLISE CRÍTICA DO MODELO BRASILEIRO DE REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL À LUZ DO PL Nº 2.338/2023

# CIVIL LIABILITY FOR ALGORITHMIC RISK: CRITICAL ANALYSIS OF THE BRAZILIAN MODEL FOR THE REGULATION OF ARTIFICIAL INTELLIGENCE IN LIGHT OF BILL NO. 2,338/2023

# RESPONSABILIDAD CIVIL POR RIESGO ALGORÍTMICO: UN ANÁLISIS CRÍTICO DEL MODELO BRASILEÑO DE REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL A LA LUZ DEL PROYECTO DE LEY N.º 2.338/2023

10.56238/revgeov17n4-094

**Renata Dantas de Oliveira Mercadante**
Doutoranda em Direito Constitucional
Instituição: Universidade de Fortaleza (UNIFOR)
E-mail: renata@jereissatioliveira.com.br
Orcid: https://orcid.org/0000-0002-7018-785
Lattes: http://lattes.cnpq.br/1497682211499041

**Thales de Oliveira Machado**
Doutorando em Direito Constitucional com ênfase em Direito Privado
Instituição: Universidade de Fortaleza (UNIFOR)
E-mail: thalesmachado@hlpadvogados.com.br
Orcid: https://orcid.org/0000-0002-7732-1625
Lattes: http://lattes.cnpq.br/9285100570040542

**RESUMO**
Investigam-se os desafios de imputação de responsabilidade civil em danos decorrentes de sistemas de inteligência artificial, destacando a inadequação dos modelos tradicionais de responsabilidade subjetiva diante da opacidade estrutural, da natureza probabilística e dos diferentes graus de autonomia algorítmica. Parte-se da hipótese de que o ordenamento jurídico brasileiro necessita adotar um regime híbrido de responsabilidade objetiva graduada, ancorado na teoria do risco tecnológico e na categoria de risco algorítmico intolerável, com imputação solidária imperfeita entre desenvolvedores e empresas usuárias de acordo com o controle exercido e a contribuição causal ao risco. Metodologicamente, emprega-se análise dogmático-crítica do Projeto de Lei nº 2.338/2023 em diálogo com a regulação responsiva e com os fundamentos da responsabilidade civil por atividade de risco. A investigação demonstra que, embora o projeto avance ao classificar sistemas conforme níveis de risco, persiste um déficit regulatório quanto à definição de causalidade probabilística, aos critérios de imputação entre agentes da cadeia tecnológica e à distribuição dinâmica do ônus probatório em cenários de opacidade algorítmica. Conclui-se pela necessidade de um modelo regulatório integrado, estruturado em deveres ex ante de governança algorítmica e auditoria técnica, responsabilidade objetiva agravada para sistemas de alto risco, mecanismos de inversão do ônus da prova ancorados na teoria das cargas

dinâmicas e regime de solidariedade imperfeita, capaz de assegurar tutela efetiva aos lesados sem comprometer a inovação tecnológica.

**Palavras-chave:** Inteligência Artificial. Responsabilidade Civil Objetiva. Risco Algorítmico. Governança Regulatória. Teoria do Risco.

**ABSTRACT**
This research examines the challenges of assigning civil liability for damages arising from artificial intelligence systems, emphasizing the inadequacy of traditional fault-based liability models when confronted with structural opacity, probabilistic behavior, and varying degrees of algorithmic autonomy. The study proceeds from the hypothesis that the Brazilian legal system must adopt a hybrid model of graduated strict liability, anchored in the theory of technological risk and in the category of intolerable algorithmic risk, with imperfect joint and several liability between developers and user companies according to the degree of control exercised and the causal contribution to the risk. Methodologically, a dogmatic-critical analysis of Bill No. 2,338/2023 is employed, in dialogue with responsive regulation and with the foundations of strict liability for risk-intensive activities. The investigation demonstrates that, although the bill advances by classifying systems according to risk levels, a regulatory deficit persists with respect to the definition of probabilistic causation, the criteria for allocation of liability among agents in the technological chain, and the dynamic distribution of the burden of proof in contexts of algorithmic opacity. The study concludes by proposing the need for an integrated regulatory model structured around ex ante duties of algorithmic governance and technical auditing, aggravated strict liability for high-risk systems, mechanisms for burden-shifting grounded in the theory of dynamic evidentiary burdens, and a regime of imperfect joint and several liability, capable of ensuring effective protection for harmed parties without hindering technological innovation.

**Keywords:** Artificial Intelligence. Strict Civil Liability. Algorithmic Risk. Regulatory Governance. Risk Theory.

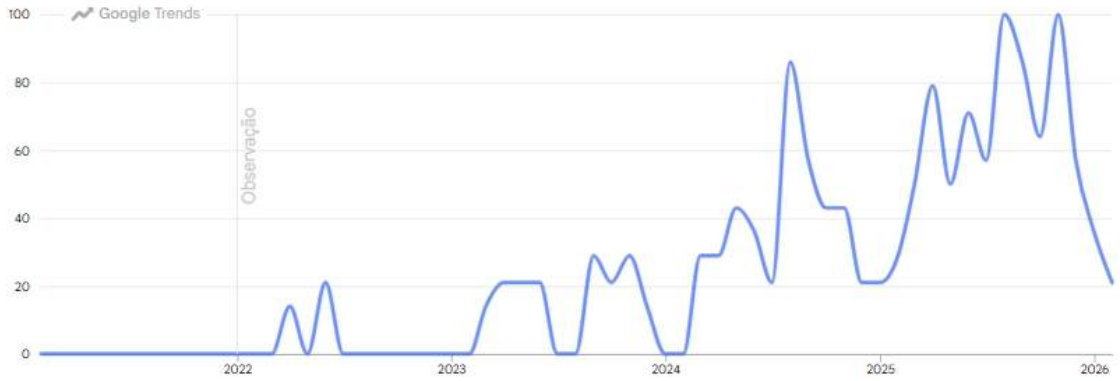
**RESUMEN**
Este estudio investiga los desafíos de imputar responsabilidad civil por daños derivados de sistemas de inteligencia artificial, resaltando la insuficiencia de los modelos tradicionales de responsabilidad subjetiva ante la opacidad estructural, la naturaleza probabilística y los diferentes grados de autonomía algorítmica. Se plantea la hipótesis de que el ordenamiento jurídico brasileño necesita adoptar un régimen híbrido de responsabilidad objetiva gradual, fundamentado en la teoría del riesgo tecnológico y la categoría de riesgo algorítmico intolerable, con responsabilidad solidaria imperfecta entre desarrolladores y empresas usuarias según el control ejercido y la contribución causal al riesgo. Metodológicamente, se emplea un análisis dogmático-crítico del Proyecto de Ley N° 2.338/2023 en diálogo con la regulación receptiva y los fundamentos de la responsabilidad civil por actividades riesgosas. La investigación demuestra que, si bien el proyecto avanza en la clasificación de sistemas según niveles de riesgo, persiste un déficit regulatorio en cuanto a la definición de causalidad probabilística, los criterios de imputación entre agentes en la cadena tecnológica y la distribución dinámica de la carga de la prueba en escenarios de opacidad algorítmica. Se concluye que se necesita un modelo regulatorio integrado, estructurado en funciones ex ante de gobernanza algorítmica y auditoría técnica, responsabilidad objetiva agravada para sistemas de alto riesgo, mecanismos para invertir la carga de la prueba basados en la teoría de cargas dinámicas y un régimen de responsabilidad conjunta imperfecta, capaz de garantizar una protección efectiva para los perjudicados sin comprometer la innovación tecnológica.

**Palabras clave:** Inteligencia Artificial. Responsabilidad Objetiva. Riesgo Algorítmico. Gobernanza Regulatoria. Teoría del Riesgo.

## 1 INTRODUÇÃO

A rápida expansão da inteligência artificial (IA) tem intensificado o debate sobre responsabilidade civil, especialmente diante de situações em que a causalidade se torna opaca ou probabilística. Uma simples pesquisa no Google Trends pelos termos de pesquisa “responsabilidade” “inteligência” e “artificial” permite evidenciar uma tendência crescente de pesquisas na plataforma a partir de 2023, conforme Figura 1.

Figura 1 – Tendência de busca sobre responsabilidade da inteligência artificial no Google




Fonte: Google Trends, 2026.

A autonomia dos sistemas, a imprevisibilidade de seus resultados e a dificuldade de rastrear decisões algorítmicas geram um cenário em que danos podem ocorrer sem que seja possível identificar, de modo tradicional, a conduta, o nexo causal e a culpa. Esses elementos exigem uma revisão crítica dos modelos clássicos da responsabilidade civil, cuja lógica foi construída para relações lineares, transparentes e controláveis.

Nesse contexto, ganha relevância a noção de risco tecnológico, compreendido como a potencialidade de dano decorrente do desenvolvimento e uso de sistemas de IA, especialmente os de aprendizado de máquina. Esses sistemas operam com modelos estatísticos complexos, gerando decisões cuja lógica nem sempre é acessível ou explicável, o que compromete a demonstração do nexo causal. Surge, assim, o risco algorítmico, marcado pela dificuldade de se atribuir responsabilidade quando os danos decorrem de interações probabilísticas, ajustes automáticos ou critérios internos não observáveis.

A doutrina contemporânea tem apontado que modelos puramente subjetivos de responsabilização são insuficientes para lidar com tais situações. A adoção de enfoques objetivos, aliados à inversão ou dinamização do ônus da prova, tem sido sugerida como forma de equilibrar a assimetria técnica entre desenvolvedores, operadores e vítimas. Além disso, a incorporação de elementos prospectivos – como governança algorítmica, auditorias independentes e mecanismos de explicabilidade – desponta como alternativa capaz de reduzir a opacidade e favorecer uma responsabilização mais eficiente e justa.

No Brasil, o debate se intensificou com a tramitação do Projeto de Lei (doravante PL) nº 2.338/2023, que estabelece princípios, deveres e mecanismos de governança para sistemas de IA, aproximando-se das diretrizes do *AI Act* Europeu (Brasil, 2023). Embora o projeto avance ao tratar de obrigações de transparência, gestão de riscos e supervisão humana, ainda há desafios quanto à responsabilização por danos decorrentes de sistemas altamente autônomos ou pouco explicáveis. A discussão revela a necessidade de modelos híbridos, que conciliem responsabilidade objetiva, análise probabilística do nexo e deveres de governança técnica.

Importa, ainda, avaliar como a causalidade probabilística pode servir de base para um regime jurídico mais adequado aos riscos algorítmicos. A ideia de que determinados danos podem ser imputados mesmo sem certeza plena sobre a causa individual – desde que haja elevada probabilidade e falhas de governança – tem ganhado espaço no cenário internacional. Esse enfoque evita que a vítima suporte integralmente os custos da incerteza técnica, ao mesmo tempo em que incentiva o fornecedor a implementar práticas robustas de mitigação de riscos.

Assim, esta pesquisa tem como objetivo examinar como a responsabilidade civil pode responder aos desafios trazidos pela IA, com ênfase na causalidade probabilística, no risco algorítmico e nas obrigações de governança. Busca-se demonstrar que modelos tradicionais são insuficientes, propondo-se um regime que combine elementos objetivos, parâmetros probabilísticos e deveres específicos de prevenção.

Metodologicamente, a pesquisa adota uma abordagem dedutiva. A discussão se desenvolve a partir da doutrina nacional e estrangeira, bem como da análise comparada entre o ordenamento brasileiro e iniciativas regulatórias internacionais. O desenvolvimento da pesquisa está organizado em três seções: na primeira se aprofunda a noção de risco algorítmico como elemento central para a compreensão da responsabilidade civil; a segunda seção se dedica à atuação do Estado brasileiro na regulação do exercício da atividade econômica baseada no uso da IA; na terceira, aliam-se as reflexões das seções anteriores para enfrentar a questão da responsabilidade civil do uso da IA a partir da teoria do risco algorítmico.

## 2 O RISCO ALGORÍTMICO E OS FUNDAMENTOS DA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL

O desenvolvimento e a incorporação da IA nas atividades econômicas e sociais introduziram um novo tipo de risco jurídico: o risco algorítmico, caracterizado pela imprevisibilidade e pela autonomia parcial das decisões computacionais. Diferentemente das tecnologias tradicionais, a IA baseia-se em processos de aprendizado de máquina que podem gerar comportamentos não previstos pelos desenvolvedores, produzindo danos a consumidores, usuários e terceiros. Como observa Rodotà e Moraes (2008, p. 217), a inovação tecnológica cria “novas formas de vulnerabilidade que o direito

deve antecipar e governar, sob pena de se tornar reativo e ineficaz". Assim, compreender a natureza desse risco é o ponto de partida para discutir a responsabilidade civil e a necessidade de intervenção regulatória.

O desenvolvimento e a incorporação da IA nas atividades econômicas e sociais introduziram um novo tipo de risco jurídico: o risco algorítmico, marcado pela imprevisibilidade e pela autonomia parcial das decisões computacionais. Diferentemente de tecnologias tradicionais, sistemas de aprendizado de máquina podem gerar comportamentos não previstos pelos desenvolvedores, produzindo danos a consumidores e terceiros. Como aponta Rodotà e Moraes (2008, p. 217), a inovação tecnológica cria novas vulnerabilidades que o Direito deve antecipar, sob pena de se tornar reativo e ineficaz. Assim, compreender a natureza desse risco constitui etapa fundamental para discutir responsabilidade civil e intervenções regulatórias.

O conceito de risco algorítmico, central para este estudo, pode ser definido como o conjunto de probabilidades de danos jurídicos decorrentes de decisões automatizadas baseadas em IA, caracterizado por três elementos estruturantes, conforme Tabela 1.

Tabela 1 – Elementos estruturantes do risco algorítmico

| **Elemento estruturante** | **Função** | **Efeito** |
|---|---|---|
| Opacidade epistêmica | Resulta da complexidade dos modelos de *deep learning* e redes neurais | Impede a compreensão *ex post* da lógica decisória pelos próprios desenvolvedores |
| Autonomia adaptativa | Permite ao sistema modificar seus parâmetros mediante aprendizado não supervisionado | Produz comportamentos emergentes não previstos no design inicial |
| Potencial de dano difuso | Atinge milhares de indivíduos simultaneamente em decorrência da conectividade informacional | Gera externalidades negativas em escala sistêmica |

Fonte: elaborado pelos autores.

Essa tríplice configuração – opacidade, autonomia e difusão – exige repensar os fundamentos da responsabilidade civil, deslocando o foco da culpa individual para gestão preventiva de riscos tecnológicos.

A doutrina reconhece que o risco algorítmico rompe paradigmas clássicos de causalidade e culpa, impondo reformulações na responsabilidade civil. Para Pagallo (2013, p. 92), a responsabilidade em ambientes de IA passa a se orientar pela previsibilidade objetiva do dano no contexto funcional do sistema, e não pela vontade humana individual. Assim, ainda que ausente dolo ou culpa, o desenvolvedor pode ser responsabilizado quando o dano decorre de falhas estruturais de design, treinamento enviesado, insuficiência de testes de robustez ou ausência de medidas preventivas disponíveis. Essa compreensão se aproxima da teoria do risco criado, segundo a qual quem introduz atividade geradora de riscos especiais deve assumir os ônus decorrentes (Cavalieri Filho, 2020, p. 153), deslocando o foco da conduta subjetiva para a causalidade objetiva entre atividade e dano.

Um dos principais desafios consiste na demonstração do nexo causal em danos algorítmicos. Modelos de IA baseados em aprendizado de máquina funcionam por relações probabilísticas e multifatoriais, e não por lógica determinística, o que compromete a aplicação das teorias tradicionais de causalidade. Selbst (2017, p. 128) denomina esse obstáculo de "problema da informação significativa", diante da impossibilidade de rastrear fatores determinantes de uma decisão automatizada. Nesses contextos, admite-se a adoção de causalidade probabilística ou a inversão do ônus da prova, atribuindo ao desenvolvedor a responsabilidade de demonstrar a ausência de nexo causal, fundamentada no princípio da aptidão para a prova e na teoria das cargas dinâmicas.

Esse cenário evidencia a necessidade de repensar os fundamentos regulatórios da IA segundo abordagem de governança por riscos, substituindo modelos estritamente punitivos por mecanismos preventivos. Conforme Giddens (1999, p. 27), a sociedade contemporânea é marcada por riscos fabricados, oriundos de decisões tecnocientíficas, exigindo estruturas regulatórias capazes de agir prospectivamente. Assim, o Direito passa a assumir funções preventivas e orientadoras, moldando a conduta de agentes privados mediante incentivos, deveres de governança e auditorias, priorizando mitigação antes da ocorrência de danos irreversíveis. Essa transição encontra amparo em Sunstein (2005) e na regulação responsiva de Ayres e Braithwaite (1992), que defendem intervenções graduais conforme a gravidade do risco e a capacidade de autorregulação empresarial.

A implementação de modelo preventivo, porém, enfrenta desafios conhecidos da teoria econômica da regulação, especialmente o risco de captura regulatória. Como apontam Stigler (1971) e Posner (1974), agências podem ser influenciadas pelos interesses das indústrias que fiscalizam, gerando regulação subótima. No campo da IA, a elevada assimetria informacional entre reguladores e empresas de tecnologia intensifica esse risco. Carpenter e Moss (2014, p. 18) destacam formas de captura cultural e informacional, nas quais reguladores incorporam valores da indústria. Por isso, é essencial fortalecer expertise técnica, ampliar transparência, assegurar participação da sociedade civil e estabelecer mecanismos robustos de accountability.

Nesse contexto, o princípio da precaução tecnológica tornou-se diretriz importante para decisões regulatórias em cenários de incerteza. Segundo Sarlet (2021, p. 44), a precaução impõe atuação preventiva na presença de risco potencial de dano grave, ainda que ausente certeza científica. Aplicado à IA, exige implementação de mecanismos de segurança, testes rigorosos e auditorias contínuas. O modelo europeu do *AI Act* reforça tais exigências, impondo obrigações de documentação, rastreabilidade, supervisão humana e avaliação de conformidade a sistemas classificados como de alto risco (União Europeia, 2024, arts. 9º a 15). Contudo, Sunstein (2005, p. 18) adverte para o paradoxo da precaução: o excesso de cautela pode inviabilizar tecnologias capazes de reduzir riscos superiores, impondo equilíbrio entre inovação e segurança.

A regulação por riscos, alternativa ao comando e controle tradicional, adota instrumentos flexíveis e graduais ajustados à dinâmica tecnológica. Black (2008, p. 144) destaca que esse modelo se baseia na responsividade regulatória, combinando *hard law* com mecanismos de *soft law*, como códigos de conduta, certificações, auditorias independentes e padrões técnicos colaborativos. Ayres e Braithwaite (1992, p. 35) descrevem essa abordagem por meio da "pirâmide regulatória", em que o Estado inicia com instrumentos persuasivos e avança para sanções severas apenas quando a cooperação voluntária falha.

A aplicação desse modelo à IA exige postura jurídica interdisciplinar, capaz de compatibilizar inovação e tutela de direitos fundamentais. Como observa Zuboff (2019, p. 137), sistemas inteligentes operam sob lógica de vigilância e coleta massiva de dados, ampliando assimetrias informacionais. Assim, a regulação deve incorporar mecanismos de transparência algorítmica, voltados à auditoria pública e à rastreabilidade das decisões. Hildebrandt (2016, p. 88) lembra que a IA produz efeitos coletivos invisíveis que dificultam a identificação de agentes lesivos, reforçando a necessidade de responsabilidade objetiva baseada na teoria do risco (Cavalieri Filho, 2020, p. 157).

O Estado, portanto, deve atuar como mediador entre inovação e segurança, equilibrando custos da precaução e do risco, como destaca Sunstein (2005, p. 67). Na prática, isso requer instrumentos proporcionais, de exigências de conformidade a sanções por negligência, para criar ambiente confiável para o uso da IA. No Brasil, Doneda e Monteiro (2021, p. 144) identificam tendência a modelo híbrido influenciado pela LGPD e pelo Marco Civil da Internet, articulando normas obrigatórias e incentivos à autorregulação, aproximando-se do movimento internacional de compliance algorítmico.

Em síntese, a análise dos fundamentos da regulação da IA demonstra que o risco algorítmico é elemento estruturante da economia digital, exigindo arcabouço jurídico capaz de conciliar desenvolvimento tecnológico e proteção contra danos sistêmicos. Essa tensão será aprofundada na próxima seção, que examina o papel do Estado e das agências reguladoras na consolidação de um modelo brasileiro de governança da IA, com atenção ao PL nº 2.338/2023 e à influência do direito europeu na futura Lei Brasileira de Inteligência Artificial (LBIA).

## 3 GOVERNANÇA REGULATÓRIA E O PAPEL DO ESTADO NA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

A governança regulatória da IA constitui desenvolvimento direto do modelo contemporâneo de Estado regulador e pressupõe articulação coordenada entre normas gerais, regulação setorial e mecanismos permanentes de supervisão de sistemas operados em ambiente de incerteza e impacto social difuso. Regular a IA significa enfrentar uma tecnologia em rápida evolução e sujeita à constante obsolescência normativa, o que exige instrumentos flexíveis, principiológicos e capazes de acompanhar o amadurecimento tecnológico e a consolidação de padrões sociais de uso (os usos e

costumes tecnológicos). Trata-se, portanto, de sistema regulatório dinâmico, no qual o Estado deve equilibrar estabilidade institucional com adaptabilidade diante de transformações rápidas e imprevisíveis.

Nesse cenário, destaca-se a necessidade de abordagem multinível de governança, na qual legislador, autoridades reguladoras independentes, órgãos de controle, setor privado e sociedade civil compartilham responsabilidades (BIONI, 2021, p. 75). O objetivo é compatibilizar estímulo à inovação com salvaguardas institucionais que previnam discriminação algorítmica, violações de privacidade, riscos sistêmicos e assimetrias informacionais. Instrumentos como compliance regulatório, auditorias algorítmicas, avaliações de impacto, certificações técnicas e regimes sancionatórios proporcionais tornam-se elementos centrais dessa estrutura. A governança policêntrica permite maior capacidade de supervisão e evita que a regulação se torne rígida ou insuficiente.

Identificam-se três eixos essenciais da governança da IA:

a) deveres de diligência tecnológica impostos a desenvolvedores e empresas usuárias;
b) dever do Estado de evitar tanto a sub-regulação quanto a sobre-regulação que comprometa inovação; e
c) dever das autoridades reguladoras de agir com transparência, coerência e coordenação institucional.

O desenvolvimento e a incorporação da Inteligência Artificial nas atividades econômicas e sociais introduziram o chamado risco algorítmico, caracterizado pela imprevisibilidade e pela autonomia parcial das decisões computacionais. Diferentemente das tecnologias convencionais, os sistemas de aprendizado de máquina operam como "caixas-pretas", gerando comportamentos que podem não ser totalmente antecipados por seus criadores, o que resulta em danos a consumidores e terceiros. Como observa Frank Pasquale (2016, p. 158) essa opacidade intrínseca aos algoritmos cria formas de vulnerabilidade, exigindo que o Direito desenvolva mecanismos para governar processos que escapam ao controle humano direto.

A governança da IA no Brasil, assim, não pode limitar-se à edição de normas gerais. O papel estatal transcende a atuação sancionadora *ex post* e passa a envolver o desenho institucional de incentivos, a criação de *sandboxes* regulatórios, a emissão de diretrizes técnicas com homologação de certificações, a coordenação entre agências e a manutenção de diálogo constante com academia e sociedade civil. Essa dimensão ampliada da atuação estatal busca conferir flexibilidade regulatória sem comprometer proteção contra riscos intoleráveis e assegurar que o desenvolvimento e uso da IA permaneçam alinhados à Constituição e aos direitos fundamentais.

A futura LBIA — representada pelo Projeto de Lei n.º 2.338/2023, aprovado pelo Senado e atualmente em tramitação na Câmara — insere-se nesse movimento internacional de construção de

arcabouço regulatório. O PL adota modelo híbrido de governança baseado no risco e inspirado no *AI Act* europeu.

De acordo com Monteiro (2026, p. 7-8), o texto classifica sistemas de IA segundo quatro categorias: risco excessivo, alto risco, risco moderado e risco mínimo. A partir delas, distribui-se obrigações graduadas de transparência, documentação, testes de conformidade, supervisão humana e responsabilização, de modo a adequar o rigor regulatório ao potencial de dano.

a) sistemas de **risco excessivo**, como pontuação social ou manipulação subliminar de comportamento, seriam proibidos;
b) sistemas de **alto risco**, aplicados em saúde, educação, crédito, infraestrutura crítica e justiça criminal, estariam sujeitos a avaliação prévia de conformidade, registro obrigatório, supervisão humana efetiva, rastreabilidade técnica e auditorias periódicas;
c) sistemas de **risco moderado ou mínimo** receberiam exigências mais leves, centradas em transparência e princípios de não discriminação.

Essa estrutura normativa visa prevenir danos antes que ocorram, impondo deveres substantivos de diligência a desenvolvedores e provedores, o que representa avanço em relação a modelos puramente reativos da responsabilidade civil tradicional. A lógica preventiva desloca o foco da reparação para a mitigação sistemática de riscos, aproximando o regime jurídico brasileiro das tendências regulatórias predominantes em ambientes altamente tecnologizados.

Contudo, a análise crítica do PL nº 2.338/2023 revela lacunas relevantes, sobretudo no tocante aos mecanismos de responsabilização e à definição de competências institucionais, conforme Tabela 2.

Tabela 2 – Lacunas relevantes do PL nº 2.338/2023

| Lacuna | Consequência |
|---|---|
| Não oferece critérios claros de imputação causal em cenários de opacidade algorítmica | Indefinição da prova do nexo causal quando o processo decisório é tecnicamente opaco ou inacessível |
| Não há disciplina precisa sobre a distribuição de responsabilidades na cadeia tecnológica, envolvendo desenvolvedor originário, fornecedor de dados, integrador, operador e usuário final | Gera incerteza quanto às esferas de imputação |
| Não prevê mecanismos específicos de inversão do ônus da prova ou presunções de causalidade | Poder Judiciário desenvolve soluções casuisticamente, o que compromete previsibilidade e segurança jurídica |
| Indeterminação da definição da autoridade reguladora competente, não esclarece se será novo órgão, ampliação da ANPD ou coordenação interinstitucional | Pode gerar fragmentação regulatória e conflitos de competência |
| Não disciplina adequadamente modelos de *sandbox* regulatório | Afeta o equilíbrio da inovação com supervisão técnica em outras instâncias de controle |

Fonte: elaborado pelos autores.

Como observa Doneda (2019, p. 74), a coexistência de múltiplos órgãos com atribuições concorrentes exige coordenação clara para evitar fragmentação regulatória e insegurança jurídica. A regulação da IA no Brasil, portanto, deve equilibrar dois imperativos: reconhecer que aplicações de IA permeiam diversos setores econômicos, cada qual com sua agência especializada; e, simultaneamente, assegurar existência de autoridade central com mandato transversal para padronizar critérios técnicos, evitar arbitragem regulatória e garantir coerência sistêmica. Esse equilíbrio entre coordenação horizontal e autoridade centralizada constitui condição essencial para efetividade regulatória.

Por fim, é indispensável reconhecer que a governança regulatória da IA se vincula diretamente à responsabilização dos agentes tecnológicos, sobretudo desenvolvedores e provedores de sistemas que introduzem riscos algorítmicos na sociedade. A atuação estatal deve integrar mecanismos preventivos (regulação *ex ante*) com instrumentos reparatórios (regulação *ex post*), de modo a garantir proteção dos usuários e fomentar inovação responsável amparada em autorregulação supervisionada. Como defendem Baldwin e Cave (1999, p. 38), modelos de corregulação permitem que o setor tecnológico desenvolva códigos de conduta, padrões de segurança e processos de certificação, desde que sujeitos à supervisão estatal e ao escalonamento para intervenção direta quando necessário. Este arranjo híbrido constitui alternativa promissora para equilibrar eficiência regulatória, adaptabilidade tecnológica e preservação dos direitos fundamentais.

## 4 RESPONSABILIDADE DOS DESENVOLVEDORES E A EMPRESA USUÁRIA DE APLICATIVOS DE IA: ENTRE O DEVER DE DILIGÊNCIA E O RISCO ALGORÍTMICO

A definição sobre quem deve responder civilmente pelos danos decorrentes do uso de IA em aplicativos configura um dos debates mais desafiadores da regulação tecnológica contemporânea. A complexidade reside na autonomia funcional dos algoritmos de aprendizado de máquina, que operam com base em fluxos contínuos de dados e podem produzir efeitos não antecipados, mesmo quando não há falha técnica evidente. Doneda (2019, p. 112) observa que o cerne da questão não é apenas apontar o agente causal, mas compreender de que modo o risco tecnológico deve ser distribuído entre os diversos sujeitos envolvidos no desenvolvimento, integração e operação da IA, reconhecendo que cada etapa do ciclo de vida algorítmico contribui, em maior ou menor grau, para a materialização do dano.

No cenário jurídico brasileiro, a aplicação das categorias tradicionais de responsabilidade civil mostra-se insuficiente para lidar com os desafios trazidos pelos sistemas algorítmicos. Como destaca Mello (2021, p. 63), o reconhecimento de um direito fundamental autônomo à proteção de dados pessoais pelo Supremo Tribunal Federal impõe deveres de proteção que transcendem a mera análise de culpa. Diante da opacidade estrutural da IA, a tutela desse direito fundamental exige mecanismos de transparência e governança que garantam o controle sobre o fluxo informativo. Nesse sentido, a doutrina defende que a eficácia dessa proteção constitucional depende da adoção de regimes de

responsabilidade e deveres de cuidado que assegurem a mitigação de riscos e a prestação de contas, independentemente da demonstração de negligência ou imperícia no desenvolvimento do sistema.

Dentro dessa lógica, a teoria do risco tecnológico surge como solução intermediária que busca harmonizar inovação e proteção jurídica. Gasser e Almeida (2017, p. 60) defendem que a IA deve ser enquadrada como uma atividade de risco qualificado, sujeita a padrões reforçados de diligência e governança. Assim, o desenvolvedor assume o dever de projetar mecanismos de controle, auditoria e atualização constante do sistema, reduzindo vulnerabilidades previsíveis. A empresa usuária, por sua vez, torna-se responsável quando usufrui da tecnologia sem implementar salvaguardas compatíveis com a complexidade operacional do sistema ou sem observar padrões mínimos de conformidade.

A partir dessa construção, ganha relevo o princípio da precaução tecnológica, segundo o qual a incerteza científica sobre os potenciais impactos da IA não exonera os agentes das obrigações preventivas. Floridi (2023, p. 145) defende que o dever de diligência deve ser exercido de modo antecipatório, impondo aos desenvolvedores a postura de identificar e mitigar riscos antes que eles se concretizem. Importado de campos como o Direito Ambiental e a Bioética, esse princípio encontra particular pertinência na regulação da IA, dada a possibilidade de danos amplos, sistêmicos e difusos decorrentes de decisões automatizadas.

Contudo, analisar a responsabilidade civil exclusivamente sob a ótica do desenvolvedor seria insuficiente, pois o ciclo de vida da IA envolve uma rede complexa de agentes, cada qual com diferentes níveis de informação e capacidade de intervenção. Mendes (2021, p. 119) ressalta que programadores, fornecedores de bases de dados, integradores e empresas usuárias compõem uma cadeia algorítmica interdependente, de modo que a responsabilidade deve ser graduada conforme a contribuição causal de cada agente para o resultado danoso. Essa visão sistêmica reforça a noção de corresponsabilidade e evidencia a necessidade de parâmetros regulatórios que permitam clareza, previsibilidade e equilíbrio entre inovação e segurança.

Nesse cenário, a natureza técnica da IA desafia o ordenamento jurídico, que corre o risco de se tornar reativo e ineficaz perante a velocidade das transformações digitais. Para Pasquale (2016, p. 135) o enfrentamento desse risco exige uma regulação que promova a transparência e a prestação de contas sobre os sistemas automatizados. Assim, a compreensão profunda da natureza do risco algorítmico e da autonomia dos sistemas constitui a etapa fundamental para o estabelecimento de novos regimes de responsabilidade civil e intervenções regulatórias que protejam efetivamente o usuário final.

Nesse contexto ampliado, a empresa usuária de sistemas baseados em IA adquire papel essencial, pois é ela quem operacionaliza e aplica os resultados gerados pelo algoritmo. Doneda, Mendes e Cueva (2020, 216) defendem que a efetividade da proteção de dados impõe aos agentes de tratamento um dever de diligência contínuo, o qual obsta a exclusão de responsabilidade baseada na mera utilização passiva de sistemas automatizados. Na perspectiva dos autores, a empresa que decide

pela implementação de IA assume o papel de garantidora da conformidade com os princípios da segurança e da prevenção, devendo assegurar a integridade técnica e ética de todo o fluxo informacional. Assim, a responsabilidade do controlador decorre da ausência de uma governança proativa e da falha em mitigar riscos inerentes à tecnologia, tornando a supervisão jurídica um requisito indispensável, sobretudo em operações de alto impacto que envolvam o tratamento de dados sensíveis ou decisões que afetem direitos fundamentais.

A experiência europeia, consagrada no AI Act e na AI Liability Directive, indica que a regulação eficaz depende de uma abordagem multinível, que articule deveres de diligência, mecanismos de sanções proporcionais. A experiência europeia, consolidada por normas como o GDPR e refletida no debate sobre o AI Act, fundamenta-se em uma lógica de 'regulação por riscos' que exige governança proativa. Conforme analisa Mello (2021, p. 34), a influência desse modelo no ordenamento brasileiro reforça a necessidade de instrumentos como a avaliação de impacto e o dever de prestação de contas para salvaguardar o direito fundamental à proteção de dados. Essa estrutura normativa desloca o foco da mera reparação posterior para a prevenção *ex ante*, impondo aos agentes o dever de demonstrar que o sistema opera dentro de padrões de segurança e conformidade, o que, na prática, atenua os desafios probatórios gerados pela opacidade algorítmica.

A realidade brasileira, entretanto, ainda carece de uma lei geral de IA que estabeleça parâmetros uniformes sobre responsabilidade. Santos (2022, p. 49) esclarece que, embora o Marco Civil da Internet e a LGPD forneçam diretrizes relevantes – como a obrigação de adotar medidas de segurança e a exigência de transparência no tratamento de dados – eles não abarcam adequadamente a complexidade dos sistemas autônomos de decisão. Nesse contexto, o PL nº 2.338/2023 representa avanço ao prever obrigações específicas de governança algorítmica, impondo padrões de conduta e responsabilidade proporcionais ao grau de controle exercido pelos agentes.

Com efeito, a proposta de regulação prevê a exigência de avaliações de impacto algorítmico para as IAs de alto risco. Monteiro (2026, p. 19) entende que o modelo brasileiro traz essa ferramenta como um “processo iterativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco”

A construção de um modelo regulatório apto a lidar com os desafios da IA demanda, portanto, uma arquitetura normativa que conjugue instrumentos de *soft law* (como guias técnicos, códigos de conduta e padrões internacionais) com normas cogentes capazes de assegurar proteção efetiva contra danos previsíveis. Mendes (2021, p. 127) argumenta que esse modelo híbrido preserva a flexibilidade necessária ao desenvolvimento tecnológico, ao mesmo tempo em que estabelece um núcleo rígido de obrigações mínimas, imprescindíveis à segurança jurídica. Para tanto, torna-se essencial fortalecer a atuação coordenada de agências reguladoras, com competências específicas para monitorar e mitigar riscos decorrentes de algoritmos autônomos.

Nesse ambiente, cabe ao Estado assumir papel de indutor da confiança tecnológica, e não apenas de agente sancionador. Gasser e Almeida (2017, p. 61) defendem um modelo de governança multinível que envolva agências reguladoras, sociedade civil e setor privado na formulação de padrões éticos e técnicos, permitindo que a regulação acompanhe o ritmo da inovação sem criar barreiras desnecessárias. Essa abordagem colaborativa reforça a necessidade de que tanto desenvolvedores quanto empresas usuárias assumam responsabilidades proporcionais à sua posição no ciclo tecnológico.

A criação de uma autoridade reguladora especializada em IA surge, assim, como alternativa capaz de reduzir a fragmentação institucional e uniformizar critérios técnicos. Mulholland (2020, p. 62) argumenta que a dispersão normativa e a multiplicidade de órgãos decisórios constituem entraves significativos à proteção jurídica na sociedade digital, motivo pelo qual uma instância especializada poderia promover maior coerência e previsibilidade na governança algorítmica.

Ainda assim, a intervenção estatal deve observar limites constitucionais, como os princípios da livre iniciativa e da proporcionalidade. Fenwick, Vermeulen e Corrales (2018, p. 89) (2021, p. 131) enfatiza que a regulação da IA não pode suprimir o potencial inovador do setor tecnológico, devendo, ao contrário, criar incentivos para a adoção voluntária de padrões éticos e práticas de autocontrole. Dessa forma, o Estado deixa de atuar como freio e passa a ser garantidor da confiança pública e da proteção dos direitos fundamentais frente aos riscos inerentes às decisões automatizadas.

O debate sobre responsabilidade civil aplicada à IA vincula-se, em última análise, à noção de risco socialmente aceitável. Pagallo (2013, p. 97) sustenta que, diante da impossibilidade de eliminação completa dos riscos tecnológicos, o direito deve assegurar que eles sejam distribuídos de maneira equitativa entre os agentes envolvidos. Assim, o desenvolvedor responde objetivamente por danos derivados de falhas estruturais, enquanto a empresa usuária assume responsabilidade solidária quando aplica a tecnologia sem observar parâmetros mínimos de conformidade, segurança e supervisão responsável.

Nesse sentido, o estudo de Silva e Melo (2025, p. 19) aponta para os papeis que a opacidade e a transparência algorítmicas exercem no tratamento da responsabilidade civil, para fins de enquadramento numa responsabilidade mais ou menos objetiva para desenvolvedores e operadores dos sistemas tecnológicos com uso de IA. Em outras palavras, o maior ou menor grau de explicabilidade e de abertura do acesso aos códigos gera um risco inversamente proporcional para o desenvolvedor e a empresa usuária da solução de IA.

A partir desse panorama, torna-se possível perceber que a responsabilidade civil no ecossistema da IA demanda harmonização entre técnica, direito e governança, de modo a evitar tanto lacunas normativas quanto excessos regulatórios que inviabilizem a inovação. A distinção entre deveres do desenvolvedor e da empresa usuária não deve ser compreendida como dicotomia rígida, mas como

eixo de distribuição funcional do risco tecnológico, assegurando que cada agente responda conforme sua capacidade real de controle e intervenção no ciclo algorítmico. Essa compreensão integrada cria as bases para a conclusão do capítulo, na qual se examinam os desafios estruturais, as escolhas regulatórias possíveis e os caminhos para um modelo equilibrado que proteja direitos, favoreça a inovação e ofereça segurança jurídica diante da crescente complexidade da IA.

## 5 CONSIDERAÇÕES FINAIS

O avanço das tecnologias de IA e a disseminação de sistemas de alto impacto tornam evidentes as limitações dos modelos tradicionais de responsabilidade civil para lidar com danos decorrentes do risco algorítmico. A opacidade estrutural, o funcionamento probabilístico e os diferentes graus de autonomia desafiam categorias clássicas como culpa e nexo causal linear, deslocando o debate para a gestão institucional do risco e a adequada distribuição dos custos dos danos na cadeia algorítmica. O ordenamento brasileiro dispõe de instrumentos relevantes, como o Código Civil e a LGPD, mas ainda não oferece um regime específico para danos decorrentes de IA de alto risco. O PL nº 2.338/2023 representa avanço ao adotar abordagem regulatória baseada em risco, inspirada no *AI Act*, prevendo avaliação de impacto, direitos dos afetados e estrutura de governança, embora ainda não estabeleça um modelo de responsabilidade civil adequado à causalidade probabilística e à corresponsabilidade entre agentes.

A partir desse diagnóstico, defendeu-se um modelo híbrido que combine deveres densos de diligência tecnológica com responsabilidade objetiva calibrada pelo risco, de modo que a atuação do Direito abarque simultaneamente prevenção e reparação. A responsabilidade dos desenvolvedores e usuários não pode ser tratada como matéria contratual isolada nem como risco transferível ao usuário final, pois a decisão de projetar, treinar e empregar sistemas críticos gera dever jurídico de diligência reforçada.

O modelo regulatório proposto organiza-se em cinco pilares:

a) responsabilidade objetiva graduada conforme o risco, com proibição de sistemas de risco inaceitável e manutenção da responsabilidade subjetiva apenas em cenários de menor potencial lesivo;
b) solidariedade imperfeita entre agentes da cadeia algorítmica, com direito de regresso proporcional ao controle exercido sobre o risco, incentivando cooperação e investimentos preventivos;
c) facilitação probatória robusta, com possibilidade de inversão do ônus da prova em casos de opacidade e descumprimento de deveres de documentação e avaliação de impacto;

d) deveres substanciais *ex ante* de governança algorítmica — mitigação de vieses, supervisão humana significativa, monitoramento pós-mercado e canais de contestação — juridicamente exigíveis e diretamente vinculados à imputação de responsabilidade; e
e) fortalecimento de autoridade reguladora especializada, com poderes fiscalizatórios, capacidade sancionatória e função coordenadora entre agências setoriais, atuando em diálogo contínuo com academia, setor privado e sociedade civil.

A ética tecnológica não constitui mero adorno retórico, mas fundamento de legitimidade jurídica e social do desenvolvimento da IA. Estruturar a responsabilidade civil por risco algorítmico a partir de um arranjo regulatório robusto — orientado pela precaução, transparência, *accountability* e proteção de direitos fundamentais — é condição para que a IA se integre ao ambiente econômico e institucional brasileiro sem aprofundar desigualdades e assimetrias informacionais. O desafio para legislador, autoridades reguladoras e tribunais é transformar esse desenho normativo em prática efetiva, com rigor técnico, coragem intelectual e compromisso constitucional com a dignidade humana.

## REFERÊNCIAS

AYRES, Ian; BRAITHWAITE, John. Responsive Regulation: Transcending the Deregulation Debate. Oxford: Oxford University Press, 1992. Disponível em: https://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf. Acesso em: 24 fev. 2026.

BALDWIN, Robert; CAVE, Martin. Understanding Regulation: Theory, Strategy, and Practice. Oxford: Oxford University Press, 1999.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2021.

BLACK, Julia. Forms and Paradoxes of Principles-Based Regulation. Law & Policy, v. 29, n. 1, p. 1-36, 2008.

BRASIL. Senado Federal. Projeto de Lei n° 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 24 fev. 2026.

CARPENTER, Daniel; MOSS, David Alan (org.). Preventing Regulatory Capture: Special Interest Influence and How to Limit It. Cambridge: Cambridge University Press, 2014. Disponível em: https://tobinproject.org/sites/default/files/assets/Introduction%20from%20Preventing%20Regulatory%20Capture.pdf. Acesso em: 24 fev. 2026.

CAVALIERI FILHO, Sérgio. Programa de Responsabilidade Civil. São Paulo: Atlas, 2020.

DONEDA, Danilo. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados no Brasil. 2021. 385 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

FENWICK, Mark; VERMEULEN, Erik Phillip Maria; CORRALES, Marcelo. Business and Regulatory Responses to Artificial Intelligence: Dynamic Regulation, Innovation Ecosystems and the Strategic Management of Disruptive Technology. In: CORRALES, Marcelo et al. (ed.). Robotics, AI and the Future of Law. Singapore: Springer, 2018. p. 81-103. Disponível em: https://arxiv.org/pdf/2407.19439. Acesso em: 24 fev. 2026.

FLORIDI, Luciano. The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford: Oxford University, 2023.

MULHOLLAND, Caitlin. Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade civil. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). Inteligência Artificial e Direito: ética, regulação e responsabilidade. 2. ed. São Paulo: Thomson Reuters, 2020. p. 32-74.

GASSER, Urs; ALMEIDA, Virgílio Augusto. A Layered Model for AI Governance. Computer Law & Security Review, v. 33, n. 5, p. 56-72, 2017.

GIDDENS, Anthony. Risk and Responsibility. Modern Law Review, v. 62, n. 1, p. 1–10, 1999.

HILDEBRANDT, Mireille. Smart Technologies and the End(s) of Law. Cheltenham: Edward Elgar, 2016.

SARLET, Wolfgang Sarlet. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. Revista Privacidade e Proteção de Dados, v. 10, p. 12-49, 2021.

DONEDA, Danilo; MENDES, Laura Schertel, CUEVA, Ricardo Villas Bôas. Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Revista dos Tribunais, 2020.

MELLO, Patrícia Perrone Campos. O Supremo Tribunal Federal e a Proteção Constitucional dos dados Pessoais: rumo a um direito fundamental autônomo. In: MENDES, Laura Schertel. DONEDA, Danilo. SARLET, Ingo Wolfgang. RODRIGUES JR, Otávio Luiz. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 7-61.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. A LGPD e o princípio da não discriminação. Revista de Direito do Consumidor, v. 138, n. 3, p. 175-199, dez. 2021.

MONTEIRO, Giovanna Voorn. Avaliações de impacto da inteligência artificial: regulação jurídica no Brasil e União Europeia. Direito & TI, Porto Alegre, v. 1, n. 22, p. 1-24, jan./jul. 2026. Disponível em: https://direitoeti.com.br/direitoeti/article/view/293/188. Acesso em: 24 fev. 2026.

PAGALLO, Ugo. The Law of Robots: Crimes, Contracts and Torts. Londres: Springer, 2013.

POSNER, Richard Allen. Theories of Economic Regulation. Bell Journal of Economics, v. 5, n. 2, p. 335–358, 1974.

RODOTÀ, Stefano; MORAES, Maria Celina Bodin de. A Vida na Sociedade da Vigilância: privacidade hoje. Rio de Janeiro: Renovar, 2008.

SELBST, Andrew David. Disparate Impact in Big Data Policing. Georgia Law Review, v. 52, p. 109–195, 2017. Disponível em: https://georgialawreview.org/wp-content/uploads/2025/01/Andrew-D.-Selbst-Disparate-Impact-in-Big-Data-Policing-52-Georgia-Law-Review-2018.pdf. Acesso em: 24 fev. 2026.

SILVA, Breno Oto da; MELO, Álisson José Maia. Algoritmos de caixa preta e relações privadas: transparência, accountability e proteção dos direitos humanos na era da IA. In: MAKIYA, E.H.G.; ROCHA, J.F.; GUIMARÃES, J.A.S.A. (Coords.). Regulação da inteligência artificial III. VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA). Belo Horizonte: Skema Business School, 2025. Disponível em: https://site.conpedi.org.br/publicacoes/czk1u677/36031285/716qWaSjCy6E55x3.pdf. Acesso em: 24 fev. 2026.

PASQUALE, Frank. The Black Box Society: the secreet algorithms that control money em information. Cambridge: Harvard University Press, 2016.

STIGLER, George Joseph. The Theory of Economic Regulation. Bell Journal of Economics, v. 2, n. 1, p. 3–21, 1971.

SUNSTEIN, Cass Robert. Laws of Fear: Beyond the Precautionary Principle. Cambridge: Cambridge University Press, 2005.

UNIÃO EUROPEIA. Artificial Intelligence Act. Bruxelas: Parlamento Europeu e Conselho da União Europeia, 2024.

UNIÃO EUROPEIA. Parlamento Europeu. Artificial Intelligence Act. Regulamento (UE) 2024. Bruxelas, 2024.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism. Nova York: PublicAffairs, 2019.