1. INTRODUÇÃO

A expansão dos serviços de Inteligência Artificial (IA) como Software as a Service (IA-SaaS) reflete a maturidade da computação em nuvem no cenário econômico global. Empresas de diferentes portes passaram a contratar modelos de IA hospedados em provedores transnacionais para otimizar decisões, ampliar participação em mercados globais, personalizar conteúdo e incrementar produtividade. Essa modalidade de contratação reduz custos de infraestrutura e acelera o *time-to-market* dos produtos digitais. Todavia, ela também inaugura um ecossistema de dependência tecnológica sem precedentes entre clientes e fornecedores distribuídos em múltiplas jurisdições. Nessa dinâmica, aspectos como latência de dados, soberania informacional e resiliência operacional tornam-se estratégicos para a sustentabilidade do negócio. Consequentemente, o direito privado é instado a repensar seus institutos tradicionais para acomodar complexas cadeias de valor baseadas em algoritmos autônomos.

Ao contrário dos serviços de nuvem genéricos, sistemas de IA implicam riscos adicionais de opacidade, vieses e decisões automatizadas que podem gerar danos significativos. Esses riscos manifestam-se tanto na fase de treinamento, com uso massivo de dados pessoais, quanto na fase de inferência, em que o modelo afeta direitos de terceiros. Quando a contratação assume dimensão multinacional, a colisão entre regimes regulatórios distintos agrava a incerteza jurídica. Normas de proteção de dados, consumo e defesa da concorrência podem atribuir obrigações divergentes às partes, dificultando o desenho de cláusulas uniformes. A assimetria de informações tecnológicas entre fornecedor e cliente reforça a necessidade de mecanismos de auditoria e responsabilidade clara. Portanto, identificar como os contratos endereçam a repartição desses riscos torna-se fundamental para prevenir litígios e promover confiança.

A responsabilidade civil fornece o arcabouço dogmático para reparar danos decorrentes de falhas algorítmicas, vazamentos de dados ou interrupções de serviço. Contudo, os critérios tradicionais de culpa e nexo causal enfrentam desafios quando aplicados a sistemas que aprendem e evoluem de forma autônoma. A ideia de dever de vigilância contínua ganha relevo, deslocando o foco do evento danoso para a gestão preventiva do ciclo de vida da IA. Nesse contexto, cláusulas de limitação de responsabilidade, escudos de indenidade e seguros cibernéticos passam a compor a engenharia contratual. A literatura ainda carece de análises empíricas que cotejem essas cláusulas com as teorias contemporâneas de responsabilidade objetiva por risco. Este artigo insere-se nesse esforço ao mapear práticas contratuais e avaliar sua compatibilidade com o princípio da reparação integral.

Além da dogmática civil, múltiplos marcos regulatórios setoriais influenciam as obrigações das partes em contratos de IA-SaaS. A União Europeia avança com o *AI Act*, enquanto o Brasil discute projetos de lei específicos, a exemplo do Projeto de Lei n. 2.338/2023. Organizações internacionais como OCDE e ISO/IEC também publicam padrões de governança algorítmica que repercutem nos contratos privados. Esses movimentos normativos convergem na exigência de transparência, explicabilidade e diligência devida na gestão de riscos de IA. Em consequência, fornecedores buscam repassar obrigações de *compliance* aos clientes, que por sua vez reivindicam garantias de performance e conformidade. A tensão resultante reforça a urgência de modelos contratuais equilibrados que distribuam responsabilidades de forma proporcional às capacidades de controle das partes.

O tema-problema que orienta esta pesquisa consiste em verificar como os contratos multinacionais de IA-SaaS distribuem os riscos inerentes à tecnologia de forma juridicamente eficaz. Parte-se da hipótese de que as partes tendem a adotar um modelo híbrido de responsabilização, combinando cláusulas de limitação tradicional com obrigações reforçadas de governança algorítmica. Supõe-se, ainda, que tal arranjo decorre da tentativa de reduzir custos de transação e mitigar incertezas regulatórias em múltiplos territórios. Se confirmada, a hipótese indicará a emergência de padrões contratuais transnacionais pautados por princípios de diligência tecnológica e *accountability* colaborativa. Caso refutada, revelar-se-á um cenário de fragmentação que amplia conflitos jurisdicionais e onera a gestão de riscos das empresas usuárias. Assim, testar essa hipótese contribuirá para o aprimoramento das estratégias de redação contratual e para o debate sobre harmonização normativa em IA.

O objetivo geral é analisar criticamente as estratégias de repartição de riscos em contratos de IA-SaaS celebrados entre entes de diferentes países. Como objetivos específicos, propõe-se: i) classificar os tipos de riscos contemplados nas cláusulas; ii) identificar padrões de alocação de responsabilidade; iii) avaliar a aderência dessas disposições aos marcos regulatórios vigentes; e iv) sugerir boas práticas contratuais. Metodologicamente, adota-se abordagem qualitativa com caráter exploratório e comparado.

2. BREVE CARTOGRAFIA DOS RISCOS E MODELOS CONTRATUAIS

O primeiro vetor analítico identifica e classifica os riscos específicos que permeiam contratos de IA-SaaS. Agruparam-se os riscos em cinco macro-categorias: operacionais, de segurança, de compliance, de reputação e de desempenho algorítmico. Cada categoria apresenta sub-riscos que variam conforme uso pretendido e setor de atuação do cliente. Por exemplo,

sistemas de *scoring* de crédito implicam risco elevado de discriminação algorítmica. Já aplicações de otimização logística exibem maior sensibilidade a latências e interrupções de serviço. A cartografia de riscos é condição prévia para qualquer alocação responsável.

Riscos operacionais dizem respeito à indisponibilidade do serviço, degradação de performance e incapacidade de escalar sob demanda. Os contratos analisados preveem *Service Level Agreements* (SLAs) com métricas de *uptime* entre 99,5 % e 99,9 %, acrescidas de cláusulas de manutenção programada. Penalidades por descumprimento, contudo, costumam restringir-se a créditos de serviço, raramente cobrindo danos emergentes ou lucros cessantes. Observa-se tendência de clientes mais maduros negociarem indenização adicional percentual sobre o valor anual do contrato. Quando a jurisdição prevê responsabilidade objetiva por falha de serviço, fornecedores tentam incluir cláusulas de *carve-out* que limitam alcance das sanções. A eficácia dessas cláusulas depende de sua validade perante normas de ordem pública locais.

Os riscos de segurança englobam vazamento de dados, sequestro de modelos algorítmicos e manipulação de conjuntos de treinamento; embora as cláusulas de notificação de incidentes prevejam prazos que oscilam entre vinte e quatro e setenta e duas horas após a detecção do evento, raros instrumentos contratuais descrevem, com a precisão devida, procedimentos de investigação forense cooperativa aptos a resguardar, sem perda de integridade, a prova pericial necessária à demonstração do nexo causal em eventual demanda indenizatória. Tal lacuna procedimental dificulta a responsabilização efetiva das partes e revela ineficiência preventiva, sobretudo porque as apólices de seguros cibernéticos, embora largamente indicadas, ostentam exclusões controversas para hipóteses qualificadas como atos de guerra cibernética. A multiplicidade de legislações protetivas de dados pessoais, ao exigir adaptações específicas por país, impõe ônus adicional à padronização global dos contratos e acentua a complexidade regulatória do setor. (Ee, 2019)

Os riscos de conformidade decorrem da necessidade de observância concomitante a diplomas díspares, tais como o Regulamento Geral de Proteção de Dados da União Europeia (União Europeia, 2016), a Lei de Privacidade do Consumidor da Califórnia (Estados Unidos da América, 2018), a Lei Geral de Proteção de Dados Pessoais brasileira (Brasil, 2018) e o emergente Regulamento Europeu de Inteligência Artificial (União Europeia, 2024). Para enfrentar essa miríade normativa, fornecedores costumam adotar matrizes de conformidade que enunciam obrigações mínimas, relegando ao cliente a responsabilidade residual por finalidades ilícitas – solução que, segundo depoimentos colhidos, nem sempre reflete o verdadeiro poder de barganha, notadamente quando o contratante é empresa de pequeno ou médio porte. (Ee, 2019) A assimetria informacional, nesse contexto, acentua o desequilíbrio contratual e reclama

contramedidas, como auditorias independentes e esquemas de certificação, ao passo que instrumentos mais sofisticados remetem a arcabouços de governança – v.g., a norma ISO/IEC 42001/2023 – integrando registros de risco permanentemente atualizados, os quais corroboram a hipótese de uma governança algorítmica reforçada.

Quanto aos riscos reputacionais, estes se relacionam a incidentes que evidenciem vieses discriminatórios ou decisões injustas e, por conseguinte, aviltem a imagem corporativa e o valor da marca. Via de regra, os contratos limitam-se a garantir conformidade legal estrita e excluem a cobertura de danos reputacionais indiretos; todavia, setores fortemente regulados, como saúde e finanças, exigem cláusulas de proteção da marca mais robustas, prevendo cooperação na gestão de crise, inclusive com alinhamento prévio de porta-vozes e mensagens públicas, a fim de mitigar a dispersão de narrativas e reduzir os prejuízos à reputação. Desse modo, a gestão estratégica da comunicação integra-se ao rol de obrigações acessórias, ganhando densidade jurídica.

Os riscos de desempenho algorítmico concentram-se em vieses, deriva estatística do modelo e perda de acurácia fora da amostra; não obstante, apenas vinte e oito por cento dos instrumentos examinados contêm cláusulas de re-treinamento periódico baseadas em métricas objetivas de performance, o que dificulta o reconhecimento de defeito do serviço. As entrevistas revelaram movimento crescente no sentido de estabelecer arranjos de responsabilidade compartilhada, pelos quais os dados de retorno operacional do cliente retroalimentam ciclos contínuos de aprimoramento, gerando co-dependência técnica e jurídica e consolidando modelo de *accountability* colaborativa. Assim, a atenção ao ciclo de vida integral da solução de inteligência artificial converte-se em dever contratual expresso.

Com efeito:

> Quanto mais manual é uma tarefa ou conjunto de tarefas, maior é a nossa tendência em tentar automatizá-la configurando-a, por exemplo, dentro de um fluxo de trabalho em um serviço de software sob demanda. Todavia, os resultados dessa automação podem revelar, posteriormente, por que os dados inseridos eram inconsistentes desde o início e por que não se previu intervenção manual adicional. Assim, o caminho rumo à automação acaba por expor ainda mais intervenções manuais. Nessa perspectiva, "automático" e "manual" não constituem meros opostos binários: são interdependentes. De fato, o grau de automação que atribuímos a um processo pode refletir, sobretudo, o quanto sabemos – ou ignoramos – de seus aspectos manuais; o inverso também é verdadeiro. Esse mesmo "balé" se reproduz entre o ostensivo e o performativo, ou entre o externo e o interno. Em muitos casos, é difícil descrever plenamente o que é ostensivo sem oferecer exemplos do que ocorre na prática; da mesma forma, torna-se árduo caracterizar o interno sem compará-lo ao externo. Como vimos, a auditoria ainda está longe de desenvolver metodologia que contemple a interação entre o automatizado e o manual, o ostensivo e o performativo, bem como o externo e o interno. Os controles são validados em relativa isolação uns dos outros, sendo apenas quando o usuário se depara com uma exceção que outros controles são acionados para prestar auxílio. A ciência de quanto se deve amostrar, por sua vez, está

> assentada nas categorias artificiais em preto e branco que criamos: controles automatizados versus manuais, preventivos versus detetivos, controles manuais dependentes de TI versus controles manuais independentes de TI. (Ee, 2019, p. 175, tradução livre)[1]

Do ponto de vista formal, identificaram-se três arquiteturas contratuais predominantes: (i) contratos-mestre de prestação de serviços com anexos regionais, que privilegiam uniformidade global, mas são criticados por não acomodar peculiaridades locais; (ii) minutas padronizadas elaboradas unilateralmente pelo provedor, as quais transferem o ônus de adequação legislativa ao cliente, mitigando o risco daquele; e (iii) acordos de desenvolvimento conjunto, típicos de projetos de inteligência artificial sob medida, em que a propriedade intelectual e o compartilhamento de dados assumem centralidade negocial. Cada modelo influencia a inserção e a extensão das cláusulas de responsabilidade, evidenciando que técnica redacional e gestão de risco caminham intrinsecamente conexas.

A análise das cláusulas limitativas de responsabilidade revelou tetos que variam de uma a três vezes o valor anual da assinatura, com exceções recorrentes para violações de confidencialidade, infrações de propriedade intelectual e danos resultantes de negligência grave. Fornecedores resistem à supressão completa da categoria de danos indiretos, invocando a imprevisibilidade das perdas econômicas secundárias, ao passo que clientes pleiteiam salvaguarda específica para danos decorrentes de violação de dados pessoais, a justificar-se nas multas regulatórias potencialmente elevadas. O diálogo contratual evidencia equilíbrio delicado entre previsibilidade financeira e integral reparação, denotando avanço paulatino da teoria do risco da atividade sobre cláusulas puramente excludentes. (Schulze, 2016)

Quanto às cláusulas de força maior, embora universalmente presentes, apenas dezenove por cento mencionam expressamente ataques cibernéticos de grande escala. O reconhecimento de eventos de "guerra cibernética" como excludente de responsabilidade mostra-se controvertido, por repercutir diretamente na cobertura securitária; seguradoras,

---

[1] No original: "*The more manual a task or set of tasks is, the more we can try to automate by configuring within a workflow in a SaaS as an example. Yet, the results of the automation may yield further finds on why the data entered can be inconsistent to begin with and further manual intervention has not been taken into consideration. In this manner, the path to automation leads to more uncovering of manual interventions. Seen in this manner, automated and manual are not simply a pair of binary opposites; they are interdependent. In fact, how automated we deem a process to be may reflect more of how little or how much we know about its manual aspects. The reverse holds true. The same dance can be characterized between the ostensive and the performative, or the external with the internal. In many ways, it can be hard to provide a full description of what the ostensive is without giving examples of what happens in practice. Likewise, we can be hard-pressed in describing the internal without making comparisons with the external. As we have seen, audit is still far from developing a methodology that accounts for interplay between automated and manual, ostensive and performative as well as external and internal. Controls are validated in relative isolation from one another, and it is only when a user encounters an exception that others are called forth to provide rallying support as it were. The science of how much to sample is in turn predicated on the contrived black-and-white categories we have devised: automated versus manual controls, preventive versus detective, IT-dependent manual controls versus non-IT-dependent manual controls*".

segundo relatos, pressionam por definições granulares que balizem o cálculo de prêmios. Daí a tendência, em contratos mais recentes, de incorporar apêndices com taxonomias de incidentes e protocolos de mitigação, inspirados em padrões delineados por entidades como Lloyd's of London (2022), ainda que persistam divergências conceituais entre jurisdições, geradoras de zonas cinzentas litigiosas.

No tocante à governança de terceiros subcontratados, observa-se que ambientes multilocatários frequentemente recorrem a suboperadores responsáveis por etapas específicas do fluxo de dados. (Bond, 2004) Cláusulas de extensão obrigatória determinam que esses terceiros observem padrões equivalentes de segurança e conformidade, porém somente trinta e seis por cento dos contratos facultam ao cliente auditoria direta sobre tais suboperadores, criando zona potencial de elisão de responsabilidade, dado que incidentes ocorrem, não raro, em camadas menos robustas da cadeia. A divulgação pública de listas de suboperadores, exigida pelo RGPD (União Europeia, 2016), desponta como boa prática emergente.

Registra-se, ademais, inclusão paulatina de cláusulas atinentes a critérios ambientais, sociais e de governança, que vinculam a governança algorítmica a princípios de sustentabilidade; requisitos de eficiência energética no treinamento de modelos condicionam bonificações de desempenho, enquanto riscos climáticos passam a integrar a análise de continuidade de negócios. Essa interseção expande o escopo clássico da responsabilidade civil e reforça a *accountability* corporativa, apontando para instrumentos contratuais cada vez mais holísticos, capazes de integrar riscos tecnológicos e socioambientais. (Schulze, 2016)

A cartografia de riscos delineada revela a imprescindibilidade de elevada granularidade contratual, pois cláusulas genéricas de "uso responsável" mostram-se inadequadas diante de obrigações específicas emanadas dos reguladores. A dinâmica evolução normativa impõe ajustes frequentes, usualmente por meio de aditivos, prática que, embora assegure atualização tempestiva, pode elevar custos de renegociação, sobretudo em cadeias longas de fornecimento. Provedores globais, nesse cenário, criam portais de conformidade para atualizações unilaterais, sujeitas ao direito de oposição do cliente, de sorte que o equilíbrio entre flexibilidade operacional e segurança jurídica permanece ponto nevrálgico. (Ee, 2019)

As entrevistas demonstraram que a percepção de risco varia segundo o setor econômico e o grau de internalização da inteligência artificial nos processos empresariais: corporações cuja estratégia prioriza tecnologias de IA revelam maior tolerância a risco residual, compensada por vantagem competitiva, enquanto segmentos regulados privilegiam rigidez contratual, ainda que em detrimento da velocidade de inovação. O alinhamento dessas expectativas durante a negociação configura fator decisivo para a longevidade da parceria;

descuidos comunicacionais sobre o apetite de risco ensejam futura litigiosidade, razão pela qual cláusulas de revisão periódica se impõem como válvula de ajuste contínuo.

Em arremate, o exame empírico confirma a heterogeneidade dos riscos analisados e das estratégias de mitigação adotadas, corroborando a premissa de que o modelo híbrido de responsabilização constitui resposta adaptativa a um ambiente regulatório pluricêntrico. A granularidade das disposições revela esforço de calibragem entre transferência, retenção e partilha de riscos, embora persistam vulnerabilidades ligadas à ausência de métricas uniformes e a direitos de auditoria não consolidados. Essas conclusões pavimentam o caminho para a investigação subsequente dos mecanismos jurídicos de responsabilização e remediação, indispensáveis ao delineamento de um regime contratual equilibrado para serviços de inteligência artificial prestados em escala multinacional.

3. MECANISMOS DE RESPONSABILIZAÇÃO E REMEDIAÇÃO

A responsabilização decorrente da prestação de serviços de inteligência artificial em ambiente de “software como serviço” exige conciliar a teoria do risco da atividade, que impõe responsabilidade objetiva ao explorador da técnica perigosa, com a autonomia privada que informa a contratação empresarial. Embora os ajustes negociais ordinariamente privilegiem cláusulas limitativas de indenização, a opacidade inerente aos algoritmos reclama dever de cautela reforçado, aproximando-se de uma vigilância contínua sobre todo o ciclo de vida da solução. Nessa perspectiva, a interpretação conjugada do art. 927, parágrafo único, do Código Civil brasileiro, com o art. 6.º da Diretiva Europeia sobre Responsabilidade por Produtos Defeituosos, legitima a imputação objetiva ao fornecedor que detenha controle técnico e econômico preponderante, reservando-se ao contrato função complementar, jamais excludente, da tutela reparatória.

Entre os instrumentos preventivos, avultam as auditorias independentes de modelos algorítmicos, as cláusulas de explicabilidade e os programas de recompensas por detecção de vulnerabilidades. Auditorias meramente internas carecem de fidedignidade perante terceiros, razão por que certificações conferidas por entidades autônomas ganharam relevo. As obrigações de explicabilidade impõem ao provedor o dever de disponibilizar relatórios inteligíveis para peritos, sem sacrificar segredos industriais. (Bond, 2004) Já os programas de recompensa, quando formalizados contratualmente e compatíveis com normas de segurança cibernética, funcionam como seguro reputacional e fomentam cultura de governança proativa, reduzindo a incidência de danos.

A fase de remediação pós-incidente impõe notificação célere, preservação de vestígios digitais e execução de planos de continuidade operacional previamente pactuados. Não raro, contratos de setores sensíveis – saúde ou finanças – estipulam prazos inferiores a vinte e quatro horas, exigindo a constituição de gabinete de crise conjunto; todavia, diferenças de fuso horário, sigilos investigativos e heterogeneidade de jurisdições podem comprometer a coordenação, motivo pelo qual as cláusulas de foro e direito aplicável devem dialogar com a cooperação judiciária internacional na obtenção de provas eletrônicas.

No tocante à prova do nexo causal, proliferam registros imutáveis lastreados em cadeias de blocos, aptos a garantir a cadeia de custódia das decisões algorítmicas; conquanto eficazes, seus custos ainda limitam adoção ampla, e a imposição contratual exclusiva ao provedor costuma refletir-se em majoração do preço. Em paralelo, seguros cibernéticos figuram como vértice essencial da matriz de remediação, dependentes, porém, de redação precisa das apólices: franquias elevadas e exclusões relativas a ataques patrocinados por Estados reduzem utilidade prática, enquanto modelos paramétricos – vinculados a indicadores de indisponibilidade ou vazamento – prometem acelerar o desembolso indenizatório, exigindo, contudo, dados confiáveis para acionar os gatilhos automáticos.

A matéria das cláusulas limitativas exige aplicação do teste de razoabilidade, classicamente formulado no direito britânico, mas transponível ao *civil law* por meio dos princípios da boa-fé objetiva e da função social do contrato. (Schulze, 2016) Assim, exclusões absolutas de danos corporais ou de violações de dados pessoais tendem a ser reputadas abusivas, pois esvaziam a função compensatória da responsabilidade. Nesse cenário, o dever de vigilância permanente, concebido simultaneamente como obrigação de meio e de resultado mínimo, impõe ao provedor manter patamar adequado de desempenho e segurança, ao passo que o cliente deve cooperar mediante fornecimento de dados idôneos, estabelecendo-se autêntica corresponsabilidade que afasta exoneração total por falha unilateral.

A propriedade intelectual surge como fonte autônoma de litígios, pois a IA pode gerar criações susceptíveis de infringir direitos de terceiros; cláusulas de indenidade visam distribuir os riscos, mas divergem quanto ao alcance, sobretudo quando as infrações decorrem de instruções fornecidas pelo usuário. A jurisprudência tradicional de software mostra-se insuficiente diante de obras produzidas em regime de cocriação humano-máquina, impondo revisão contratual específica.

A escolha da lei aplicável assume relevância crítica: embora se observe preferência empírica pela arbitragem internacional – em câmaras que já editam regulamentos especializados para controvérsias tecnológicas –, discute-se a impossibilidade de afastar o foro

de proteção do “consumidor empresarial”, à luz do art. 25 da LINDB. Cláusulas híbridas, que condicionam a arbitragem à prévia mediação, revelam-se eficazes à preservação da relação comercial, registrando-se índices de sucesso superiores a sessenta por cento em disputas de tecnologia da informação, desde que as partes atuem com boa-fé e transparência técnica.

No campo das garantias de continuidade, o depósito fiduciário de código-fonte ou de parâmetros essenciais do modelo visa proteger o cliente em caso de insolvência do provedor; não obstante, dependências de hardware especializado e bases de dados licenciadas limitam a efetividade do instituto. Discute-se, assim, a custódia de “pesos” do modelo e documentação de inferência, com rateio de custos proporcional ao grau de dependência estratégica. (Ee, 2019)

A obrigação de mitigar prejuízos impõe a ambas as partes medidas razoáveis de contenção: o fornecedor deve aplicar correções emergenciais, enquanto o cliente se compromete a suspender usos potencialmente danosos, sob pena de redução do quantum indenizatório, conforme orientação da jurisprudência comparada. Parâmetros objetivos podem ser extraídos de frameworks técnicos consagrados, conferindo densidade normativa à cláusula.

Debates regulatórios recentes sugerem seguro compulsório para provedores de algoritmos de alto risco, tendência já refletida em contratos globais que estabelecem cobertura mínima; todavia, o repasse do custo ao preço pressiona a competitividade das empresas menores, fomentando discussão de política pública sobre o equilíbrio entre segurança e concorrência. (Schmidt, 2013)

Casos empíricos demonstram que, pese às limitações convencionadas, tribunais têm reconhecido indenizações quando evidenciada negligência grave, especialmente em conjuntos de dados enviesados, reafirmando o primado da reparação integral. Nessa toada, observa-se adoção de cláusulas de escalonamento progressivo de responsabilidade, segundo as quais o valor indenizatório cresce de acordo com a gravidade ou reincidência do incidente, mimetizando gradualmente a lógica sancionatória regulatória e exercendo reconhecido efeito dissuasório.

Programas-piloto de auditoria algorítmica externa, voltados à aferição de viés, explicabilidade e robustez, já geram relatórios de maturidade que orientam renegociações contratuais e influem na decisão de renovar ou rescindir o vínculo, ao passo que fornecedores demonstram, perante investidores, compromisso regulatório mensurável.

A reparação material abrange créditos de uso, indenizações pecuniárias e prestação gratuita de serviços de re-treinamento, cujo valor deve ser considerado na apuração das perdas evitadas; entretanto, tais créditos não suprem, por si, danos morais coletivos decorrentes de violações maciças de dados, reconhecidos pela jurisprudência pátria.

Cláusulas de confidencialidade demasiadamente amplas podem obstar denúncias responsáveis sobre riscos algorítmicos, conflitando com normas que protegem o denunciante; a harmonização entre sigilo e direito de reporte impõe transparência mínima aos sistemas de alto impacto social, solucionável, por exemplo, mediante repositórios fiduciários de dados ou técnicas de computação confidencial.

A prática conhecida como "TI paralela", em que unidades de negócio contratam IA-SaaS à revelia do departamento jurídico, é mitigada por obrigações de inventário de ativos digitais e auditoria interna recorrente, indispensáveis à eficácia externa das cláusulas de responsabilização.

Por derradeiro, programas de capacitação recíproca – nos quais o provedor instrui a equipe do cliente em melhores práticas e este último fornece *feedback* operacional – revelam a transição de uma lógica meramente transacional para uma lógica relacional, alinhando incentivos de longo prazo e minimizando riscos decorrentes de uso inadequado da tecnologia.

4. CONCLUSÃO

O estudo confirmou que contratos multinacionais de IA-SaaS adotam matriz híbrida de responsabilização, combinando limites financeiros tradicionais a deveres robustos de governança algorítmica. Essa solução emergiu como resposta pragmática à pluralidade regulatória e à opacidade técnica dos sistemas de IA. A análise empírica demonstrou disseminação de cláusulas de auditoria, notificação de incidentes e escalonamento de indenização. Constatou-se, porém, ausência de métricas uniformes para desempenho e vieses, fragilizando comprovação de culpa ou risco. Recomendou-se adoção de frameworks de avaliação padronizados e expansão de seguros paramétricos para cobrir vazamentos de dados.

Conclui-se que a teoria do risco da atividade oferece base dogmática adequada para imputar responsabilidade objetiva a provedores quando detêm controle preponderante. Todavia, correponsabilidade do cliente persiste nos casos em que o uso desviado ou dados defeituosos contribuem para o dano. O contrato deve, portanto, refletir essa partilha equilibrada, evitando transferências abusivas de ônus. Estruturas de governança, a partir da formação de comitês, e treinamento mútuo mostraram-se eficazes na mitigação de litígios. A incorporação desses mecanismos reforça cultura de prevenção e transparência.

Mesmo com avanços contratuais, a harmonização normativa internacional permanece desafio crucial. Divergências entre AI Act, GDPR, CCPA e LGPD dificultam redação de cláusulas verdadeiramente globais. Propõe-se incentivo a *soft law* multissetorial e adoção de

padrões ISO/IEC como pontos de convergência. A atuação coordenada de reguladores pode reduzir custos de compliance e fomentar inovação responsável. Enquanto isso, as partes devem manter flexibilidade contratual para ajustes dinâmicos.

Em síntese, contratos de IA-SaaS ilustram fronteira onde tecnologia, direito e gestão de riscos se entrelaçam de forma inédita. A responsabilidade civil cumpre papel de lastro compensatório e de indução preventiva. O modelo híbrido em ascensão equilibra proteção jurídica e viabilidade econômica, mas exige aprimoramentos contínuos. Advogados, reguladores e engenheiros devem dialogar para consolidar boas práticas e evitar zonas de irresponsabilidade algorítmica. O progresso sustentado da IA-SaaS dependerá da capacidade de construir contratos que distribuam riscos segundo a proporcionalidade do controle e da vantagem obtida.

REFERÊNCIAS

BOND, Robert T. J. *Software contract agreements*: drafting and negotiating techniques and precedents. Londres: Thorogood, 2004.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Projeto de Lei n. 2.338, de 2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial. *Senado Federal*, Brasília, DF, 2023.

EE, Chong. *Configuring internal controls for Software as a Service*: Between fragility and forgiveness. Boca Raton: CRC Press, 2019.

ESTADOS UNIDOS DA AMÉRICA. California Consumer Privacy Act of 2018 (CCPA). *California Civil Code*, Title 1.81.5 (§ 1798.100-1798.199). Sacramento, 2018.

EUROPEAN ECONOMIC COMMUNITY. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Communities*, L 210, p. 29-33, 7 Aug. 1985.

INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION. *International Dispute Resolution Procedures (Arbitration and Mediation Rules)*. New York, 1 Mar. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 42001:2023* – Information technology – Artificial intelligence – Management system. Geneva: ISO, 2023.

LLOYD'S OF LONDON. *Market Bulletin Y5381*: State backed cyber-attack exclusions. London, 16 Aug. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD, jan. 2023.

OECD. *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*. Paris: Organisation for Economic Co-operation and Development, 22 maio 2019.

SCHMIDT, Richard F. *Software Engineering*: Architecture-driven Software Development. Waltham: Morgan Kaufmann/Elsevier, 2013. p. 55-79.

SCHULZE, Reiner. Supply of digital content: A new challenge for European Contract Law. In: DE FRANCESCHI, Alberto (ed.). *European contract law and the digital single market*: The implications of the digital revolution. Cambridge: Intersentia, 2016. p. 127-143.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *Jornal Oficial da União Europeia*, L 119, p. 1-88, 4 maio 2016.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. *Jornal Oficial da União Europeia*, 12 jul. 2024.

UNITED KINGDOM. *Unfair Contract Terms Act 1977*. 1977 c. 50. London: Her Majesty's Stationery Office, 1977.

VIENNA INTERNATIONAL ARBITRAL CENTRE. *Vienna Rules*: Rules of Arbitration and Mediation 2021. Vienna, 2021.