

ESPIONAGEM ECONÔMICA, SOBERANIA DIGITAL E LIVRE CONCORRÊNCIA NAS ECONOMIAS DIGITAIS SUL- AMERICANAS

ECONOMIC ESPIONAGE, DIGITAL SOVEREIGNTY, AND FREE COMPETITION
IN SOUTH AMERICAN DIGITAL ECONOMIES

Ciências Sociais Aplicadas • 21/09/2026

REGISTRO DOI: [10.70773/revistatopicos/789966270](https://doi.org/10.70773/revistatopicos/789966270)

Aryel Licker da Silva¹

João Enir Ghislani dos Santos²

Leonardo Somavilla Binotto³

RESUMO

A economia digital transformou a informação e o conhecimento em ativos estratégicos, ampliando a relevância da proteção jurídica contra a espionagem econômica corporativa. Entretanto, essa expansão pode gerar efeitos concorrenciais adversos ao restringir a circulação do conhecimento e inovação, a interoperabilidade, a engenharia reversa e a mobilidade profissional, especialmente em economias digitais caracterizadas por elevada concentração tecnológica. Este estudo analisa os limites jurídicos da proteção dos ativos informacionais nas economias digitais sul-americanas, examinando sua compatibilidade com os princípios da livre concorrência e da soberania digital. Adota-se a abordagem qualitativa, exploratória e explicativa, utilizando método dedutivo, pesquisa bibliográfica e análise jurídico-comparativa dos modelos normativos do Brasil, Argentina, Chile e Colômbia. Os resultados indicam que a hiperproteção dos ativos informacionais reforça barreiras à entrada, consolida posições dominantes e amplia a dependência tecnológica regional. Conclui-se que a tutela jurídica deve restringir-se às hipóteses de obtenção ilícita de informações estratégicas, preservando mecanismos de conhecimento essenciais à concorrência, à inovação e ao fortalecimento da soberania digital.

Palavras-chave: Ativos informacionais; Dependência tecnológica; Hiperproteção; Interoperabilidade.

ABSTRACT

The digital economy has transformed information and knowledge into strategic assets, heightening the relevance of legal protection against corporate economic espionage. However, this expansion can generate adverse competitive effects by restricting the circulation of knowledge and innovation, interoperability, reverse engineering, and professional mobility, especially in digital economies characterized

by high technological concentration. This study analyzes the legal limits of protecting information assets in South American digital economies, examining their compatibility with the principles of free competition and digital sovereignty. A qualitative, exploratory, and explanatory approach is adopted, using the deductive method, bibliographic research, and comparative legal analysis of the normative models of Brazil, Argentina, Chile, and Colombia. The results indicate that the hyper-protection of information assets reinforces barriers to entry, consolidates dominant positions, and broadens regional technological dependence. The study concludes that legal protection should be restricted to cases of illicit acquisition of strategic information, preserving knowledge mechanisms essential for competition, innovation, and the strengthening of digital sovereignty.

Keywords: Information assets; Technological dependence; Hyper-protection; Interoperability.

1. INTRODUÇÃO

A ascensão da economia digital mudou radicalmente as bases tradicionais da atividade econômica, movendo gradualmente o foco da criação de valor dos ativos físicos para recursos intangíveis que se baseiam em informação, dados, conhecimento e tecnologia. A crescente interconexão entre plataformas digitais, inteligência artificial, computação em nuvem, big data, Internet das Coisas (IoT) e sistemas automatizados de análise transformou os fluxos de informação em componentes essenciais para a competitividade das empresas, a inovação tecnológica e a própria estrutura dos mercados modernos. Consequentemente, o domínio desses recursos imateriais consolidou-se como o pilar central que define o poder econômico e a estrutura dos mercados modernos.

Nesse cenário, a informação deixou de ser um mero insumo secundário para assumir um papel estratégico nas economias digitais, consolidando-se como um ativo de alto valor. Essa mudança reconfigurou a concorrência, uma vez que as vantagens de mercado passaram a ser definidas pela capacidade de processar grandes volumes de dados e de controlar as infraestruturas tecnológicas de circulação. Assim, o domínio exclusivo desses recursos acentuou as assimetrias entre os agentes, tornando a proteção legal da informação determinante para a consolidação do poder econômico.

Ao mesmo tempo, a crescente concentração de plataformas digitais e ecossistemas integrados gerou profundas assimetrias informacionais entre os agentes econômicos. Esse desequilíbrio estrutural, impulsionado pelo controle sobre serviços de nuvem e inteligência artificial, tem permitido que corporações solidifiquem posições dominantes no mercado. Diante dessa desigualdade, a busca por mecanismos jurídicos capazes de proteger os ativos informacionais das empresas ganhou uma importância sem precedentes na nova ordem econômica mundial.

A espionagem econômica corporativa ganha uma nova dimensão, diferente daquela associada às práticas industriais do século XX. Com a facilidade de reproduzir, armazenar e transmitir informações digitalmente, além da internacionalização das cadeias produtivas e do aumento dos fluxos de dados entre fronteiras, o valor econômico dos segredos empresariais cresceu consideravelmente, assim como a vulnerabilidade das organizações à obtenção indevida de informações estratégicas. Como resultado, vivencia-se um movimento global que busca fortalecer as ferramentas jurídicas para proteger segredos comerciais, ativos informacionais e a inteligência competitiva das empresas.

Por outro lado, o recrudescimento dessas medidas protetivas suscita tensões complexas quando analisado sob a ótica do direito concorrencial aplicado às economias digitais. Embora seja inegavelmente fundamental coibir a apropriação indevida de informações estratégicas para preservar os incentivos ao investimento privado em pesquisa e desenvolvimento, a hiperproteção jurídica desses ativos pode gerar severas externalidades negativas. Quando levada ao extremo, a exclusividade cega sobre dados e conhecimentos técnicos transforma-se em um mecanismo indireto de bloqueio à disseminação tecnológica. Desse modo, o excesso de blindagem ameaça sufocar o dinamismo inerente ao mercado, restringindo drasticamente processos legítimos e essenciais.

Nos mercados digitais contemporâneos, a presença de fortes efeitos de rede e de economias de escala informacional impulsiona uma concentração tecnológica. Nesse ambiente propenso ao oligopólio, a ampliação indiscriminada da exclusividade jurídica sobre ativos informacionais acaba por desvirtuar sua finalidade original. O que deveria atuar precipuamente como uma salvaguarda para assegurar o retorno do investimento privado converte-se em um instrumento estratégico das grandes corporações. Como reflexo dessa distorção, as ferramentas protetivas transformam-se em mecanismos que, de forma indireta, consolidam o poder econômico preexistente e erguem barreiras à novos competidores.

Essa problemática adquire contornos cruciais e singulares quando transposta para a realidade estrutural das economias sul-americanas. Em nítido contraste com os polos hegemônicos de inovação global, nações como Brasil, Argentina, Chile e Colômbia integram-se à economia digital sob um pano de fundo de

acentuada vulnerabilidade tecnológica. Esse quadro regional é marcado por uma forte dependência de plataformas estrangeiras, escassa soberania sobre as infraestruturas digitais essenciais e pela importação contínua de tecnologias estratégicas provenientes de centros econômicos internacionais.

Nesse contexto, a definição dos limites jurídicos aplicáveis aos ativos informacionais transcende o âmbito estrito das relações privadas de concorrência. Trata-se de uma questão que impacta diretamente a inovação, a soberania digital e a competitividade macroeconômica da região. Em economias fortemente dependentes de infraestruturas, nuvens corporativas e tecnologias controladas por potências estrangeiras, a expansão indiscriminada da exclusividade monopolizadora sobre esses ativos aprofunda as assimetrias preexistentes. Como desdobramento dessa distorção, criam-se barreiras intransponíveis ao surgimento de capacidades inovadoras endógenas e autônomas (Lima et al., 2022; UNCTAD, 2025).

O recorte temporal adotado compreende o intervalo de 2008 a 2026, marco histórico que delimita a consolidação da economia digital. Trata-se do período em que os dados e a informação ascenderam definitivamente à condição de ativos estratégicos centrais para a atividade econômica global. Ao longo desse arco temporal, as discussões regulatórias sobre a proteção informacional, a concorrência em mercados digitalizados e a soberania estatal ganharam densidade sem precedentes. Desse modo, o recorte reflete rigorosamente as transformações estruturais, econômicas e jurídicas que constituem o núcleo analítico desta pesquisa (Bertarini, 2023; UNCTAD, 2025).

A hipótese inicial sustenta que o excesso de proteção aos ativos informacionais gera efeitos anticompetitivos ao limitar mecanismos essenciais aos mercados digitais, agravando a vulnerabilidade de economias dependentes de plataformas estrangeiras. Partindo desse pressuposto, o objetivo principal consiste em analisar os limites legais da proteção contra a espionagem corporativa na América do Sul, investigando as tensões entre a segurança empresarial, a livre concorrência e o fluxo informacional. Para alcançar esse propósito, o estudo desdobra-se em três etapas analíticas complementares: a fundamentação teórica da economia digital, o mapeamento regulatório comparado e a avaliação crítica dos impactos sobre a soberania regional.

Sob o prisma metodológico, este estudo adota o método dedutivo, partindo de aportes teóricos sobre economia digital, direito concorrencial e soberania. O propósito central reside em empreender uma análise crítica dos limites jurídicos aplicáveis à espionagem econômica na América do Sul. Quanto à abordagem, a pesquisa caracteriza-se como qualitativa, de natureza exploratória e explicativa, desenvolvida precipuamente por meio de investigação bibliográfica. Tal percurso metodológico engloba o exame de artigos científicos, obras especializadas, documentos e relatórios técnicos de organismos internacionais.

Ademais, o estudo emprega o método jurídico-comparativo ao examinar os modelos normativos vigentes no Brasil, na Argentina, no Chile e na Colômbia. A investigação detém-se sobre os critérios de tutela dos segredos empresariais, as hipóteses de obtenção lícita e ilícita de dados estratégicos, as restrições informacionais e as salvaguardas concorrenciais de cada ordenamento. Por fim, o cotejo analítico almeja identificar convergências, divergências e lacunas

regulatórias, propiciando a formulação de parâmetros normativos que conciliem a segurança empresarial, a livre concorrência, a inovação e a soberania digital.

2. INFORMAÇÃO E PODER ECONÔMICO NA ECONOMIA DIGITAL

A compreensão da dinâmica contemporânea dos mercados exige, primariamente, reconhecer que a sociedade informacional transcende a mera ubiquidade de computadores e redes eletrônicas, configurando uma mutação profunda na organização econômica e social (Bertarini, 2023, p. 7). Essa transição altera substancialmente a forma como a informação é instrumentalizada nas atividades produtivas, nas relações sociais e nas estruturas institucionais. Como desdobramento desse rearranjo, a digitalização acentuou um descompasso entre a velocidade da inovação tecnológica e a capacidade adaptativa das políticas e normas tradicionais, concebidas em um arranjo anterior à era digital.

Entretanto, a adoção tecnológica desacompanhada de substrato intelectual mostra-se insuficiente para assegurar o desempenho econômico, pois a efetividade na exploração de sistemas digitais vincula-se diretamente ao capital intelectual acumulado. Embora a digitalização forneça a infraestrutura básica, são as capacidades humanas e organizacionais que operam a filtragem de dados relevantes e a ressignificação de processos produtivos. Desse modo, o ecossistema digital consolida-se como uma economia do conhecimento, na qual os ativos intangíveis gravitam como determinantes primordiais da competitividade empresarial (Akhtar; Senadjki; Kumaran, 2025, pp. 21-26).

A extensão dessa transformação digital difere acentuadamente entre as nações, visto que os países desenvolvidos dispõem de melhores condições para explorar tecnologias emergentes. Em contrapartida, nas economias em desenvolvimento, a escassez de infraestrutura, capital e capacitação técnica impede que a digitalização se traduza em autonomia produtiva genuína. Embora a participação nas redes globais seja imperativa para a inserção econômica, ela frequentemente aprofunda a dependência de infraestruturas, nuvens e sistemas analíticos controlados por potências estrangeiras. (Bertarini, 2023, pp. 47-48; UNCTAD, 2025, p. 7).

A transformação da informação em ativo econômico pulsa por meio da expansão contínua da coleta, processamento e análise de dados, cadeia que, como argumenta Bertarini (2023, pp. 67-70), constitui a verdadeira espinha dorsal da economia orientada por dados. Sendo continuamente alimentado por transições cotidianas, dispositivos conectados e fluxos comportamentais nas plataformas, o valor estratégico desse ecossistema não reside no registro individualizado, mas na capacidade de cruzar, interpretar e reutilizar os dados em múltiplas frentes empresariais.

Conforme argumenta Santaella (2022, pp. 82-83), a valoração dos dados vincula-se umbilicalmente aos modernos modelos de negócios, visto que dados e metadados ascenderam da condição de subprodutos para a de recursos reutilizáveis de elevado valor estratégico. Esses insumos alimentam sistemas preditivos, refinam algoritmos e viabilizam estratégias de publicidade direcionada. Sob essa ótica, as grandes plataformas digitais superam a mera função de intermediárias de tráfego, estruturando sua atividade primordial

em torno da captura, armazenamento e exploração intensiva do capital informacional gerado pelas interações em seus ecossistemas.

Tal dinâmica reconfigura profundamente a concorrência nos mercados digitais, onde a disputa mercantil transcende os parâmetros tradicionais de preços e quantidades para gravitar em torno do controle e da monetização dos fluxos informacionais. Como aponta Lupacchini (2026, pp. 421-423), a suposta gratuidade de determinados serviços digitais oculta modelos de financiamento sustentados pela captura da atenção e pela exploração econômica dos dados gerados no intercurso com o usuário. A ausência de um preço monetário direto, portanto, não anula a lógica de troca, mas substitui a contraprestação financeiro-mercantil por dados, tráfego de atenção e capacidade de direcionamento comportamental.

Os ecossistemas digitais consubstanciam o ápice da concentração econômica na modernidade, superando a lógica de mercados fragmentados pela aglutinação sistêmica de serviços interconectados. Grandes corporações tecnológicas passam a ofertar, de maneira verticalizada e integrada, sistemas operacionais, comércio eletrônico, computação em nuvem e inteligência artificial. Embora esse arranjo traga conveniência e interoperabilidade, o domínio sobre uma infraestrutura central acaba sendo instrumentalizado para alavancar posições dominantes em setores adjacentes, convertendo a integração corporativa em um vetor central de distorção competitiva (ACCC, 2023, pp. 3-6).

Segundo Bertarini (2023, pp. 69, 75-76), a incidência dos efeitos de custos de substituição não configura uma anomalia concorrencial, podendo refletir ganhos legítimos de eficiência e a preferência dos usuários. O desvio emerge quando tais mecanismos corroem de

maneira persistente a contestabilidade do mercado, uma vez que a dependência imposta a usuários e fornecedores ergue barreiras para entrantes desprovidos de bases equivalentes de dados, infraestrutura e escala. Consequentemente, a dinâmica concorrencial sofre uma mutação estrutural: a disputa restringe-se ao momento inicial de conquista do ecossistema, sendo rapidamente sucedida pela consolidação perpétua do operador dominante.

A restrição ou exclusividade no acesso a dados consolida-se como uma das barreiras mais intransponíveis para a entrada de novos concorrentes nos mercados digitais (ACCC, 2023, pp. 143-145). Ao atuarem como intermediárias de infraestruturas essenciais, as plataformas monitoram as atividades comerciais de terceiros, recolhendo métricas sobre desempenho, demanda e comportamento do consumidor. Dessa forma, a vantagem competitiva nos ecossistemas digitais transcende a supremacia financeira, assentando-se sobre o monopólio da inteligência estratégica gerada no interior do próprio ambiente competitivo.

A ascensão da inteligência artificial acentua a assimetria competitiva nos mercados digitais, visto que seu desempenho operacional depende de bases colossais de dados, poder computacional e expertise especializada. Corporações que já controlam infraestruturas de nuvem, ecossistemas operacionais e bases massivas de usuários detêm condições estruturais privilegiadas para treinar, aprimorar e difundir ferramentas de IA em múltiplos setores. Essa convergência tecnológica entre aprendizado de máquina, redes de sensores e computação descentralizada não apenas catalisa a inovação, mas viabiliza a rápida transferência de capacidades acumuladas de um mercado para outro,

transformando a inteligência artificial em um mecanismo decisivo de petrificação do poder de mercado (CMA, 2023, p. 5).

A concentração de mercado também se reflete no domínio tecnológico, impondo desafios cruciais à soberania digital. No contexto brasileiro, observa-se que parcela significativa da infraestrutura e das aplicações de inteligência artificial permanece atrelada a corporações de matiz internacional (Lima et al., 2022, pp. 179-182). Essa assimetria escancara a centralização global da pesquisa tecnológica e a vulnerabilidade estrutural frente aos polos hegemônicos do Norte Global. Consequentemente, a mera adoção de arquiteturas externas por setores nacionais amplia a eficiência operacional a curto prazo, mas aprofunda uma dependência sistêmica que compromete a autonomia tecnológica duradoura.

Conforme sistematiza Lupacchini (2026, pp. 422-424), a assimetria informacional nos mercados digitais ramifica-se em múltiplos e complexos planos estruturais, manifestando-se na vigilância assimétrica exercida pelas controladoras sobre as empresas dependentes e concorrentes que operam em sua infraestrutura (ACCC, 2023, pp. 143-145). Projeta-se, por fim, no desequilíbrio geopolítico entre economias centrais e periféricas, alimentado pela concentração global de capacidade computacional e tecnológica (Lima et al., 2022, pp. 179-182). Em todos esses patamares, a informação transborda sua função econômica tradicional para consolidar-se como o eixo central de dominação e assimetria de poder.

O monitoramento competitivo contemporâneo processa-se em um ambiente saturado por sinais digitais ininterruptos, nos quais transações, interações, deslocamentos e o consumo de conteúdo

geram um fluxo contínuo de dados comportamentais. A capacidade de decodificar esses fluxos permite que as corporações reduzam incertezas, segmentem mercados com precisão e antecipem oscilações na demanda. Essa vantagem estratégica, contudo, não decorre da mera acumulação passiva de registros brutos, mas da filtragem e interpretação rigorosa de informações que se alinham diretamente aos objetivos de expansão das plataformas (ACCC, 2023, pp. 104-107; CMA, 2023, pp. 54-57).

A vantagem informacional estratégica decorre, primordialmente, da posição estrutural que os operadores ocupam no centro do ecossistema digital. Ao controlarem a infraestrutura subjacente, as plataformas detêm a prerrogativa de monitorar em tempo real a atividade de vendedores, desenvolvedores e prestadores terceirizados (ACCC, 2023, pp. 143-145). Assim, as métricas granulares sobre oferta, demanda, retenção, picos de vendas e margens de lucratividade revelam-se diretamente às controladoras, dispensando o recurso a pesquisas externas ou fontes públicas e conferindo-lhes uma inteligência competitiva inalcançável para os demais concorrentes.

Essa configuração oblitera a fronteira conceitual entre infraestrutura neutra e agente concorrente, permitindo que uma mesma corporação modele o ecossistema, intermedeie o acesso aos consumidores e dispute mercados diretamente com os usuários de seu próprio sistema. A apuração analítica decorrente dessa intermediação confere às controladoras uma vantagem informacional incomensurável e inviável de ser replicada por agentes externos. Desse modo, o desequilíbrio estrutural resultante culmina na apropriação predatória de funcionalidades, na depressão

dos incentivos ao investimento independente e na asfixia financeira de entrantes inovadores (ACCC, 2023, pp. 143-145).

Para Mattoo e Meltzer (2018, pp. 769-770), a relevância estratégica da inteligência competitiva amplia-se exponencialmente com a circulação transnacional de dados, cujos fluxos irrestritos sustentam parcelas crescentes da atividade econômica global. Essa infraestrutura de transferência transfronteiriça viabiliza ecossistemas digitais, serviços de computação em nuvem e a fragmentação internacional da cadeia de valor. Desse modo, a mobilidade informacional entre distintas jurisdições atua como catalisadora da difusão tecnológica, comprimindo custos operacionais e redefinindo os contornos do comércio internacional de bens e serviços.

A internacionalização dos ativos informacionais engendra uma profunda tensão estrutural, caracterizada pela fragmentação operacional e geográfica dos dados, de acordo com Mattoo e Meltzer (2018, pp. 769-770). Sob esse arranjo transnacional, informações podem ser coletadas em um território, processadas em outro e armazenadas em servidores distribuídos, operados por corporações desvinculadas das jurisdições de origem. Conforme essa dinâmica se consolida, a atividade empresarial desterritorializa-se, enquanto as capacidades regulatórias e tecnológicas estatais permanecem fragmentadas e assimétricas. Desse modo, a mera localização física da infraestrutura perde a capacidade de indicar quem, de fato, exerce o controle econômico e estratégico sobre o ativo informacional.

Os fluxos transfronteiriços constituem o alicerce operacional da economia digital contemporânea, exigindo interoperabilidade técnica robusta e confiança sistêmica ao longo das cadeias globais

de valor. A ausência de compatibilidade normativa e técnica entre sistemas fragmenta os mercados e inflaciona os custos de transação. Em contrapartida, a liberalização irrestrita da circulação de dados, desprovida de mecanismos de governança públicos, acentua as vulnerabilidades de indivíduos, empresas e Estados. Desse modo, o desenvolvimento sustentável da economia digital impõe a construção de arquiteturas regulatórias capazes de viabilizar o intercâmbio transnacional sem renunciar à salvaguarda dos interesses soberanos envolvidos (UNCTAD, 2025, pp. 135-136).

A circulação global de dados potencializa a centralidade estratégica da informação para a soberania estatal, uma vez que infraestruturas tornaram-se indispensáveis para a sustentação de serviços públicos, atividades econômicas vitais e aparatos de segurança nacional, segundo Haswell (2026, pp. 20-23). Quando a gestão dessas capacidades essenciais concentra-se nas mãos de um oligopólio de corporações transnacionais, as decisões estratégicas dessas empresas ultrapassam a esfera estritamente comercial, invadindo ecossistemas informacionais soberanos e reconfigurando os próprios fundamentos da organização do poder nacional.

A dependência de infraestruturas privadas não expressa um antagonismo irreconciliável entre Estados e corporações, estabelecendo-se sob a égide de relações de complementaridade e interdependência. Sob essa dinâmica, os governos capitalizam a inovação e a eficiência técnica providas pelo setor privado, enquanto as corporações dependem de contratos públicos, respaldo institucional e segurança jurídica para operar. A assimetria estrutural manifesta-se, portanto, quando o custo e a complexidade da substituição dessas infraestruturas tornam-se proibitivos para o Estado (Haswell, 2026, pp. 21-23).

No âmbito da economia contemporânea, a soberania digital não equivale ao isolamento autárquico ou à retenção absoluta de dados no território nacional, visto que a participação em fluxos internacionais é indispensável à vitalidade digital e à captura de ganhos de escala, eficiência e segurança, de modo que o verdadeiro desafio reside em como uma economia pode integrar tais correntes transnacionais sem abdicar do controle soberano sobre infraestruturas críticas, competências tecnológicas e a tomada de decisões autônomas (UNCTAD, 2025, pp. 135-136; Haswell, 2026, pp. 22-23).

Conforme apontam Akhtar, Senadjki e Kumaran (2025, pp. 21, 24-26), a inteligência competitiva contemporânea transcende a mera acepção de uma atividade de pesquisa intraorganizacional, vinculando-se visceralmente a estruturas de governança avançadas, à captação de fontes externas, à posição estratégica das firmas em redes digitais e à habilidade de operar em fluxos internacionais. Sob essa perspectiva, a informação estratégica encontra-se difusa em plataformas, cadeias produtivas e sistemas automatizados, convertendo a dinâmica concorrencial em uma disputa pautada pelo controle sobre as infraestruturas que condicionam a produção, a acessibilidade e a apropriação dos ativos informacionais.

Nos mercados digitais, as vantagens competitivas tendem a se acumular de forma cumulativa e autossustentada, visto que corporações dotadas de bases massivas de usuários coletam volumes superiores de dados, aprimoram seus algoritmos, potencializam a personalização e atraem novos fluxos de interações (Bertarini, 2023, pp. 69, 75-76). Sob essa lógica, o conhecimento gerado pelo uso contínuo retroalimenta o aperfeiçoamento do próprio serviço. Quando esse ciclo virtuoso se articula com

externalidades de rede, infraestruturas integradas e robustez financeira, a barreira informacional erigida torna-se praticamente intransponível para novos entrantes (CMA, 2023, pp. 54-57).

Conforme a *Australian Competition and Consumer Commission* (ACCC, 2023, pp. 117-145), o acúmulo corporativo de dados não constitui um fenômeno nocivo, podendo representar antes um reflexo legítimo de inovação, confiança dos usuários e eficiência operacional. Paralelamente, a livre circulação irrestrita de todas as informações não se traduz em vantagem econômica, uma vez que a competitividade das firmas também depende de ativos proprietários e capacidades desenvolvidas internamente. O cerne do dilema regulatório e econômico reside, portanto, em discernir com precisão em quais circunstâncias a apropriação de dados atua como incentivo à inovação e quando, inversamente, degenera-se em barreira que restringe a entrada de novos integrantes.

A economia de plataformas intensifica essa complexidade regulatória, visto que o operador do ecossistema assume, simultaneamente, o controle da infraestrutura subjacente, da arquitetura normativa e dos fluxos informacionais (ACCC, 2023, pp. 117-145). Sob essa configuração, a prerrogativa de estipular as condições de acesso articula-se organicamente com a posse massiva de dados sobre o comportamento dos participantes. Desse modo, a vantagem competitiva consolida-se pela capacidade de moldar o próprio ambiente onde as alternativas concorrentes operam, permitindo que a plataforma manipule a compatibilidade técnica, o acesso a funcionalidades e a distribuição de informações estratégicas.

O controle informacional viabiliza, ademais, a transferência de vantagens competitivas entre distintos mercados adjacentes, de modo que dados colhidos em um serviço otimizam a penetração em novos nichos, ecossistemas de contas integradas reduzem os custos de aquisição de clientes e a capilaridade de ferramentas de pagamento, publicidade ou nuvem simplifica a expansão sistêmica. A articulação sinérgica desses ativos intangíveis consolida uma verdadeira economia de escopo informacional, a qual, embora capaz de fomentar ganhos de eficiência e aprimorar a experiência do usuário, eleva substancialmente os custos de transição e consolida barreiras intransponíveis para a atuação de concorrentes especializados em segmentos específicos (ACCC, 2023, pp. 104-107; CMA, 2023, pp. 18-20).

A inovação tecnológica permanece como vetor determinante da competitividade, de modo que a convergência sinérgica entre inteligência artificial, computação em nuvem, redes avançadas e análise de dados viabiliza a gestão de produtos e serviços inviáveis sob o escopo de tecnologias isoladas, permitindo que as firmas capazes de arquitetar arranjos tecnológicos eficientes inauguram novos mercados ou reestruturem os já consolidados, embora as corporações entrincheiradas, detentoras de acesso privilegiado a infraestruturas e bases massivas de dados, absorvam essas inovações com maior celeridade para neutralizar ou dificultar a ascensão de rivais emergentes (CMA, 2023, pp. 5, 13-14).

Em contextos periféricos ou emergentes, a vantagem competitiva assume uma projeção eminentemente nacional, visto que as firmas locais encontram nas plataformas globais um canal para escalar o alcance de consumidores, comprimir custos e absorver tecnologias de ponta, embora a concentração de funções estratégicas e

infraestruturas críticas em fornecedores externos resulte na migração de parcela expressiva do valor gerado e da soberania decisória para fora das fronteiras nacionais, aprofundando, a longo prazo, uma perigosa dependência estrutural (Lima et al., 2022, pp. 179-182).

Consoante Haswell (2026, pp. 20-23), a intersecção entre a confidencialidade informacional e o poder de concorrência revela uma profunda ambivalência, visto que, embora o sigilo proteja investimentos proprietários, métodos e estratégias legítimas, a opacidade sistêmica restringe a discernibilidade dos critérios que governam o acesso ao mercado. Se, por um lado, a proteção de dados restritos a operações estritamente intraorganizacionais resguarda a iniciativa privada, por outro, o enclausuramento de informações que estruturam a arquitetura de interações para milhares de agentes econômicos extrapola a esfera privada, projetando externalidades deletérias sobre a integridade da concorrência como um todo.

Haswell (2026, pp. 20-23) também aponta que a dependência tecnológica constitui fator axial para a erosão da soberania econômica, à medida que corporações detentoras do monopólio sobre sistemas de tecnologia estabelecem um patamar de dependência incontornável para agentes públicos e privados. Sob esse prisma, a supremacia dessas firmas emana menos de sua mera fatia de mercado e mais da intransponibilidade de suas infraestruturas e da extrema escassez de alternativas de substituição, permitindo que deliberações estritamente corporativas condicionem fluxos informacionais, determinem rumos da atividade econômica e debilitem a autonomia institucional dos Estados.

Por outro lado, segundo Mattoo e Meltzer (2018, pp. 770-771), a circulação transnacional do conhecimento consolida-se como pilar para a dinâmica da inovação, uma vez que o livre fluxo de dados catalisa a difusão tecnológica, otimiza a coordenação global e viabiliza a expansão das exportações digitais. Sob essa ótica, restrições desmedidas ou fragmentadas elevam os custos de transação, bloqueiam o acesso a mercados externos e cerceiam a habilidade de firmas emergentes em capitalizar o arcabouço de conhecimentos disponíveis em escala global, gerando o risco de que marcos regulatórios rígidos penalizem tanto a infraestrutura interna quanto a competitividade internacional.

A materialização de efeitos anticompetitivos indiretos revela-se exequível diante da vantagem informacional opera como um ativo cumulativo e sistemicamente integrado às arquiteturas de mercado, de modo que a robustez das bases de dados retroalimenta a eficiência algorítmica, atrai novos contingentes de usuários e amplia a rigidez dos custos de substituição em ecossistemas hipertrofiados. Nessa dinâmica, a proteção jurídica conferida a dados, modelos, interfaces ou métodos proprietários acopla-se a esses mecanismos de feedback econômico, cristalizando posições dominantes preexistentes sob o pretexto normativo de salvaguardar ativos intelectuais legítimos (Mattoo; Meltzer, 2018, pp. 770-771).

Por outro lado, a ausência de mecanismos adequados de proteção jurídica pode deprimir os incentivos à inovação e expor as empresas a apropriações que anulam o retorno sobre investimentos, evidenciando que o dilema regulatório não se resume a uma dicotomia entre livre acesso e proteção absoluta, mas exige a calibragem de instrumentos normativos capazes de salvaguardar o esforço inovador sem permitir que o monopólio informacional

resulte no fechamento estrutural dos mercados, mediante a ponderação obrigatória das peculiaridades econômicas entre os participantes e das vulnerabilidades tecnológicas das economias emergentes (UNCTAD, 2025, pp. 20-22, 135-137; ACCC, 2023, pp. 104-145).

Outrossim, a informação e o conhecimento desempenham função análoga à dos insumos produtivos tradicionais, constituindo pilares para a inovação, a personalização de serviços, a governança de cadeias de valor, a expansão internacional e a consolidação de posições hegemônicas no mercado. Sob esse prisma, a dinâmica concorrencial contemporânea transcende a disputa tradicional pela comercialização de bens e serviços, assentando-se, sobremaneira, no domínio informacional, na capacidade computacional de processamento e na soberania sobre as infraestruturas que regem a circulação de dados na economia digital (UNCTAD, 2025, pp. 20-22, 135-137; ACCC, 2023, pp. 104-145).

Os advogados Falavigna e Lins (2025) sinalizam que, dado o papel da informação empresarial como ativo central da economia digital, torna-se imperativo examinar o alcance da proteção jurídica, as formas ilícitas de apropriação combatidas e os limites normativos aplicáveis a esse regime. Sob essa ótica, a tutela contra a espionagem econômica e o desvio de segredos opera em um ambiente altamente estratégico, incidindo diretamente sobre mercados onde o acesso a dados e o fluxo de conhecimentos condicionam a própria inovação, a contestabilidade econômica e a autonomia tecnológica.

Portanto, a qualificação jurídica dos dados infraestruturais e algoritmos de controle sob o manto protetivo dos segredos de

negócio agrava a opacidade sistêmica dos ecossistemas digitais. Ao invocarem a prerrogativa da confidencialidade, as plataformas hegemônicas blindam suas arquiteturas operacionais contra o escrutínio regulatório e concorrencial, inviabilizando a auditoria de práticas discriminatórias e o acesso de terceiros a bases informacionais críticas. Consequentemente, impõe-se uma reconfiguração hermenêutica capaz de distinguir o resguardo legítimo da inteligência inovadora da instrumentalização abusiva do sigilo, sob pena de a tutela jurídica converter-se em um escudo inexpugnável para a perpetuação de assimetrias estruturais e monopólios informacionais (UNCTAD, p. 21).

3. PROTEÇÃO DOS ATIVOS INFORMACIONAIS, LIVRE CONCORRÊNCIA E SOBERANIA DIGITAL

O verdadeiro desafio consiste em definir quais informações merecem proteção jurídica e quais fluxos de conhecimento devem permanecer livres. A apropriação indevida de segredos empresariais por meio de fraude, abuso de acesso ou cooptação de funcionários difere da obtenção legítima de conhecimento decorrente da experiência prática, da mobilidade de trabalhadores, da engenharia reversa, do compartilhamento, do acesso a dados abertos ou do desenvolvimento independente. Quando essa distinção se torna tênue, mecanismos destinados a combater a espionagem podem acabar restringindo práticas fundamentais à concorrência e à inovação (Phillips; Pohl, 2025, pp. 143-147; Liang, 2016, pp. 2-4).

A dinâmica de acesso à informação empresarial divide-se entre métodos ilícitos de apropriação e canais legítimos de absorção tecnológica, visto que condutas como intrusão, fraude, cooptação e extração clandestina violam diretamente o controle informacional

(Phillips; Pohl, 2025, pp. 143-147). Em contrapartida, mecanismos de difusão fundados na observação imitativa, mobilidade de pessoal, transferência contratual de tecnologia, análise de produtos e desenvolvimento autônomo integram outra dimensão normativa, consubstanciando, a depender dos contornos jurídicos aplicáveis, vias lícitas para a assimilação e circulação da inteligência competitiva (Liang, 2016, pp. 2-4).

A proteção jurídica dos segredos empresariais possui relevante fundamento econômico e estratégico, pois preserva os incentivos à inovação. Busca-se impedir que terceiros se beneficiem, sem os correspondentes custos, dos resultados de investimentos em pesquisa, desenvolvimento e geração de conhecimento. Assim, ao resguardar informações estratégicas, assegura-se às empresas o retorno de seus investimentos, o que torna essa tutela essencial à promoção da inovação e à preservação da concorrência leal (Rimmer, 2021, pp. 76-77; Hacoheh, 2026, pp. 280-282).

O aumento da relevância econômica dos dados, algoritmos, softwares e conhecimentos técnicos justifica o fortalecimento dos mecanismos de proteção empresarial. Embora essa tendência possua fundamento econômico legítimo, não resolve a questão dos limites dessa tutela. Isso porque a mesma informação que confere vantagem competitiva ao seu titular pode também impulsionar a inovação, a pesquisa e o ingresso de novos concorrentes no mercado. É nesse ponto que a proteção dos segredos empresariais se relaciona com a livre concorrência e a circulação do conhecimento (Rimmer, 2021, pp. 76-77; Hacoheh, 2026, pp. 280-282).

Essa observação mostra que não podemos encarar a circulação do conhecimento como algo que acontece naturalmente só porque temos tecnologias avançadas à disposição. A habilidade das empresas em absorver esse conhecimento é fundamental para que consigam reconhecer e aplicar informações externas. Empresas que não têm capital tecnológico, pessoal qualificado ou a infraestrutura podem acabar sem conseguir transformar a informação disponível em produtividade. Por isso, a proteção da circulação deve ser acompanhada pelo fortalecimento das capacidades locais de aprendizado (Liang, 2016, pp. 1-5, 19).

A engenharia reversa enfrenta um dilema semelhante, uma vez que desafia a definição dos limites entre a proteção dos segredos empresariais e a promoção da concorrência e da inovação. No contexto do direito ao reparo, restrições de propriedade intelectual, barreiras tecnológicas e a ausência de informações técnicas podem dificultar a atuação de prestadores independentes. Já a engenharia reversa de software está historicamente associada à interoperabilidade, à manutenção e ao desenvolvimento de soluções compatíveis, embora seus limites variem conforme o ordenamento jurídico aplicável (Rimmer, 2021, pp. 14, 76-81).

O compartilhamento de dados não pessoais reflete essa tensão em uma escala maior. A abertura pode impulsionar a inovação, aumentar a eficiência e fomentar a pesquisa e o desenvolvimento de novos serviços, mas também traz à tona custos organizacionais, riscos legais, falta de padrões, formatos incompatíveis e o medo de perder a vantagem competitiva. Apenas decidir compartilhar dados, sem estabelecer regras claras sobre segurança, remuneração, qualidade e responsabilidade, pode desestimular a produção desses dados. Por outro lado, manter uma exclusividade total pode barrar

que agentes externos criem produtos complementares, auditem sistemas ou concorram em segmentos que dependem daquela informação (Batura et al., 2023, pp. 47-55; Hacoheh, 2026, pp. 277-293).

Informações que são realmente secretas e têm valor econômico devido ao seu sigilo, quando protegidas por medidas razoáveis, merecem proteção contra a obtenção, uso ou divulgação indevidos. Por outro lado, dados públicos, conhecimentos gerais, habilidades profissionais e informações essenciais para interoperabilidade, pesquisa ou reparo não devem ser automaticamente tratadas com o mesmo nível de restrição. Nesses casos, mecanismos como licenciamento, compartilhamento seguro, remuneração proporcional, acesso federado, anonimização e ambientes controlados podem ajudar a preservar interesses legítimos sem exigir uma abertura total (Batura et al., 2023, pp. 24, 58-61; Hacoheh, 2026, pp. 291-305; Narechania, 2022, pp. 1610-1612).

Nos mercados digitais, os riscos dessa expansão são amplificados pelas características econômicas das atividades que dependem de dados e aprendizado de máquina. O desenvolvimento inicial de certos sistemas pode demandar investimentos significativos em coleta e preparação de dados, treinamento, capacidade computacional e pesquisa, enquanto o uso posterior tende a ter custos marginais bem mais baixos. Quando esses custos fixos se combinam com efeitos de rede, a empresa que atinge a escala primeiro consegue mais dados, aprimora seu sistema, atrai novos usuários e expande ainda mais sua base de informações, criando um ciclo cumulativo de vantagem (Narechania, 2022, pp. 1543, 1549-1552).

Assim, a exclusividade informacional assume um papel estrutural. Dados de treinamento protegidos como segredos comerciais, contratos exclusivos de compartilhamento e controle privado da infraestrutura computacional podem dificultar que empresas concorrentes desenvolvam aplicações semelhantes. A barreira não surge necessariamente da superioridade do produto final, mas da dificuldade de acessar os insumos necessários para competir. O titular pode, ainda, usar sua posição em um mercado para impor condições (Narechania, 2022, pp. 1610-1613).

Esse efeito também se verifica nos mercados de dados não pessoais. A concentração de dados, sua retenção estratégica, a discriminação de preços e os contratos de exclusividade podem dificultar o acesso de pequenas e médias empresas. Além disso, os elevados custos de obtenção, gestão e processamento de dados, aliados à falta de padronização e à escassez de grandes bases de dados, favorecem organizações já consolidadas. Como a análise de dados envolve custos fixos elevados e custos marginais reduzidos, o controle de grandes volumes de informações pode gerar retornos crescentes e reforçar posições dominantes no mercado (Batura et al., 2023, pp. 53-55).

A exclusividade não se limita apenas a proibições legais explícitas. Termos de uso restritivos, limitações técnicas à portabilidade, interfaces fechadas, bloqueios na coleta de dados e incertezas jurídicas podem dificultar pesquisas, auditorias e o desenvolvimento de aplicações complementares. As empresas podem restringir acessos sem diferenciar entre atividades parasitárias e usos voltados à crítica, aprendizado, investigação ou inovação. Essa combinação de restrições legais e barreiras técnicas eleva o custo de contestação

e favorece o controle privado de recursos informacionais que são relevantes para a coletividade (Hacohen, 2026, pp. 280-283, 291).

Os efeitos anticompetitivos podem comprometer a inovação incremental, pois muitos novos produtos dependem da compreensão, da compatibilidade ou da adaptação de sistemas já existentes. Quando informações de diagnóstico, interfaces, padrões ou dados operacionais recebem proteção excessiva, concorrentes podem ser impedidos de aperfeiçoar funcionalidades, prestar serviços de manutenção ou desenvolver soluções interoperáveis. Nesse contexto, a ampliação da confidencialidade para além do que é necessário à proteção da tecnologia pode preservar a posição do agente incumbente em detrimento da inovação promovida por agentes independentes ou complementares (Rimmer, 2021, pp. 14, 76-81).

A mobilidade profissional pode ser alcançada quando as obrigações de confidencialidade são elaboradas de forma a incluir toda a experiência que o trabalhador adquiriu. Embora seja importante proteger documentos e informações específicas para combater a espionagem, restrições que impeçam o uso de conhecimentos gerais e habilidades técnicas podem limitar a troca de saberes entre empresas. Como a movimentação de profissionais é um dos meios reconhecidos de disseminação tecnológica, bloquear esse fluxo de forma indiscriminada pode beneficiar os já estabelecidos e dificultar o surgimento de concorrentes inovadores (Liang, 2016, pp. 2-4).

Além disso, a resposta competitiva não deve ser feita de maneira indiscriminada. Regras de acesso, compartilhamento ou controle de preços mal ajustadas podem diminuir o retorno sobre o investimento, desestimular a criação de bases de dados e impor

padrões de qualidade que tornem a atividade inviável. Condições excessivamente favoráveis aos usuários dos dados podem acabar transferindo todos os custos para o produtor, enfraquecendo os incentivos que a proteção buscava garantir. Vale lembrar que uma situação de monopólio natural pode ser temporária, desaparecendo com inovações tecnológicas, redução de custos computacionais ou o surgimento de novos métodos (Narechania, 2022, pp. 1612-1614).

A promoção da concorrência e da inovação nos mercados de dados exige mecanismos que conciliem proteção e compartilhamento de informações. Nesse contexto, mostram-se relevantes instrumentos como ambientes seguros de compartilhamento, cláusulas contratuais padronizadas, formatos interoperáveis e legíveis por máquina, proteção de conjuntos de dados mistos e obrigações específicas de acesso, quando justificadas pela posição do titular. Assim, a aplicação dessas medidas deve considerar a natureza dos dados, a finalidade do acesso, o poder econômico das partes envolvidas e os riscos de reidentificação ou divulgação indevida (Batura et al., 2023, pp. 58-62).

Nisto, verifica-se que hiperproteção acontece quando a ênfase na propriedade privada ignora de forma sistemática os custos competitivos que vêm com o fechamento. Nessa situação, a proteção não se limita a impedir que alguém copie o resultado do investimento de outra pessoa; ela passa a exigir que nenhuma nova alternativa tecnológica possa ser criada sem a autorização do detentor original. O verdadeiro problema não é apenas a existência do segredo, mas sim seu uso como uma ferramenta de controle sobre mercados ou atividades que vão além do que é legitimamente protegido (Batura et al., 2023, pp. 58-62).

Assim, a hipótese da pesquisa encontra respaldo na análise. O fortalecimento das medidas contra a espionagem pode aumentar a segurança dos investimentos e diminuir os incentivos para a apropriação indevida. No entanto, se essa proteção se estender a conhecimentos gerais, engenharia reversa permitida, circulação profissional, dados essenciais, interoperabilidade e inovação independente, isso poderá criar barreiras à entrada e reforçar tendências de concentração. A proteção só se mantém em harmonia com a concorrência quando garante espaços institucionalmente seguros para aprendizado e contestação dos que já estão estabelecidos (Xiong, 2026, pp. 17-21).

Aplicar essas conclusões às economias sul-americanas exige uma reflexão sobre sua posição na divisão internacional da economia digital. O conceito de soberania digital, que surge da perspectiva do Sul Global, não deve ser confundido com autarquia tecnológica. A autonomia pode ser construída em níveis nacional, regional ou multilateral, sem que cada país precise dominar todas as etapas das cadeias digitais internamente. O objetivo é manter uma capacidade suficiente para decidir sobre dados, infraestrutura, governança e desenvolvimento tecnológico, reduzindo dependências que possam limitar a formulação de políticas próprias (Xiong, 2026, pp. 17-21).

O modelo analisando organiza a soberania digital em dimensões. A primeira, a independência sobre dados, envolve a proteção legal, o controle dos fluxos de dados entre fronteiras e a prevenção da apropriação exclusiva do valor informacional por empresas privadas ou estrangeiras. A segunda dimensão, a independência de infraestrutura, abrange hardware, software essencial, serviços em nuvem, aplicações e a segurança da informação. Já a independência de governança se refere à capacidade de legislar, regular e participar

na criação de normas internacionais. Por fim, a independência de capacidades envolve pesquisa, formação de pessoal, engenharia e a articulação das tecnologias digitais com as estratégias nacionais de desenvolvimento (Xiong, 2026, pp. 17-19).

A estrutura internacional da economia digital caracteriza-se pela concentração de hardware, software e infraestrutura em um número reduzido de organizações. Esse fenômeno está associado à extração de dados e à captura de valor econômico gerado por usuários localizados em outras regiões, além da dependência de produtos e serviços desenvolvidos no exterior. Assim, a vinculação prolongada a plataformas e infraestruturas estrangeiras pode restringir o desenvolvimento de empresas nacionais e limitar a capacidade de inovação tecnológica local (Nothias, 2025, pp. 387-388).

O Brasil ocupa posição singular e privilegiada na América do Sul por ter sido o único país da região submetido a uma avaliação sistemática de soberania digital. Essa análise revelou significativa dependência de empresas estrangeiras, especialmente norte-americanas, bem como a ausência de uma política de transição capaz de ampliar o controle autônomo sobre ativos e infraestruturas digitais. Assim, apesar dos avanços legislativos já alcançados, persistem fragilidades em áreas estratégicas, como armazenamento de dados e de informações, fluxos transfronteiriços, infraestrutura tecnológica, pesquisa, software e capacidade industrial (Silveira; Xiong, 2025, pp. 44-47).

A dependência de hardware, sistemas operacionais, serviços em nuvem e aplicações estrangeiras torna essa vulnerabilidade ainda mais evidente. O mercado interno se concentra na prestação de serviços e na terceirização, com uma capacidade limitada de

pesquisa e produção independente em áreas essenciais. A infraestrutura de nuvem está, em sua maioria, ligada a grandes fornecedores internacionais, enquanto empresas estrangeiras desempenham um papel significativo no fornecimento de software e serviços utilizados por instituições tanto públicas quanto privadas (Silveira; Xiong, 2025, pp. 44-47).

Essas características estruturais impactam o equilíbrio entre proteção, segurança e concorrência. Em mercados onde as empresas locais já enfrentam barreiras para acessar dados, infraestrutura computacional, padrões e capital tecnológico, a ampliação indiscriminada da exclusividade informacional tende a favorecer aqueles que controlam os principais insumos. Se dados de treinamento, interfaces, sistemas de nuvem e padrões de interoperabilidade continuarem a ser submetidos a exclusividades amplas, as empresas locais terão que arcar com custos que os incumbentes já conseguiram amortizar ou aceitar condições impostas unilateralmente pelos detentores (Narechania, 2022, pp. 1549-1553, 1610-1613; Batura et al., 2023, pp. 53-60).

4. MODELOS JURÍDICOS DE PROTEÇÃO CONTRA A ESPIONAGEM ECONÔMICA CORPORATIVA E SEUS LIMITES CONCORRENCIAIS NAS ECONOMIAS SUL-AMERICANAS

Na Argentina, a proteção dos segredos empresariais encontra-se amparada por um arcabouço jurídico específico voltado à tutela de informações confidenciais. A legislação assegura proteção contra a revelação, aquisição ou utilização indevida de informações legitimamente controladas, desde que permaneçam secretas, possuam valor comercial em razão dessa condição e sejam objeto de medidas razoáveis de proteção. Assim, esse regime é

complementado por normas trabalhistas, penais, civis e comerciais, bem como pelo sistema de repressão à concorrência desleal, formando um modelo abrangente de tutela da confidencialidade empresarial (Correa et al., 2025, pp. 20-23, 42-43).

Este último abrange a divulgação ou exploração não autorizada de segredos que foram obtidos de maneira legítima sob obrigação de sigilo ou adquiridos de forma ilegítima, incluindo espionagem e práticas semelhantes que visam obter vantagem ou causar dano à concorrência. A exigência de uma finalidade econômica ou prejudicial impede, pelo menos em teoria, que toda circulação não autorizada de informações seja automaticamente considerada espionagem empresarial (Correa et al., 2025, pp. 20-23, 42-43).

No Chile, a regulamentação é mais clara ao definir o que é um segredo comercial. A legislação de propriedade industrial protege informações que estão sob o controle de seu titular, que podem ser utilizadas em atividades produtivas, industriais ou comerciais, que não sejam amplamente conhecidas ou facilmente acessíveis, que tenham valor comercial por serem secretas e que tenham sido submetidas a medidas razoáveis de preservação (Egaña Bertoglia, 2024, pp. 68-70; Correa et al., 2025, pp. 44-45).

A legislação chilena considera ilegal a aquisição, divulgação ou exploração não autorizada de segredos, incluindo a violação de deveres de confidencialidade, especialmente quando há a intenção de obter vantagens ou causar prejuízos. Reformas recentes ampliaram o escopo do que é protegido, que antes era interpretado de forma muito restrita, agora incluindo informações que podem ser utilizadas em atividades produtivas, industriais ou comerciais. Essa mudança foi uma resposta às dificuldades que surgiram em

disputas onde planos e informações comerciais não eram reconhecidos como segredos, simplesmente porque não tinham um conteúdo estritamente industrial (Egaña Bertoglia, 2024, pp. 79-80).

O sistema penal chileno agora detalha comportamentos como a entrada não autorizada em instalações, o uso de dispositivos de gravação, o acesso a sistemas informáticos superando mecanismos de segurança, e a reprodução e divulgação de informações protegidas. A referência da norma penal à definição da legislação de propriedade industrial ajuda a criar uma maior unidade conceitual. No entanto, a ampliação da responsabilidade criminal para violações de deveres de confidencialidade exige uma distinção clara entre segredos comerciais, informações confidenciais comuns e conhecimentos profissionais gerais. Sem essa diferenciação, obrigações contratuais privadas poderiam, indiretamente, ampliar o alcance da criminalização (Egaña Bertoglia, 2024, pp. 80-81).

Na Colômbia, a proteção vem da legislação sobre concorrência desleal, das normas da Comunidade Andina e da disciplina penal. O segredo abrange informações não divulgadas, que são legitimamente possuídas, utilizáveis em atividades produtivas, industriais ou comerciais, e que podem ser transmitidas a terceiros, desde que sejam secretas, tenham valor comercial devido à sua confidencialidade e sejam objeto de medidas razoáveis de proteção (Correa et al., 2025, pp. 29-30, 45-46).

O regime colombiano traz uma lista não exaustiva de práticas desleais, como espionagem industrial, descumprimento de obrigações contratuais, violação de confiança ou lealdade, e a indução de terceiros a essas ações. As medidas que podem ser tomadas incluem ações de natureza declaratória, condenatória,

preventiva ou proibitória. A legitimidade para agir não se limita apenas ao titular formal da informação; ela pode se estender a agentes do mercado, entidades representativas e, em certas situações que envolvem o interesse público e a livre concorrência, até mesmo a órgãos estatais. A responsabilização civil caminha lado a lado com as penalidades relacionadas à violação de segredos industriais ou comerciais (Correa et al., 2025, pp. 55-56, 76-78).

A Superintendência de Indústria e Comércio tem um papel único, pois combina competências administrativas e jurisdicionais, além de lidar com informações confidenciais em processos de integração empresarial e concorrência. O processo permite uma ampla produção de provas, a participação de especialistas, medidas de busca em computadores e ações que podem ser realizadas sem que a parte adversa tenha conhecimento prévio. A eficácia desse modelo depende de salvaguardas que evitem que a própria investigação se torne um meio de divulgação de segredos, por isso são utilizados mecanismos de acesso restrito e garantias de confidencialidade processual (Correa et al., 2025, pp. 93-96).

Em síntese, Argentina, Brasil, Chile e Colômbia compartilham o objetivo de proteger informações economicamente valiosas contra sua obtenção ou exploração desleal. Contudo, os ordenamentos jurídicos desses países diferem quanto à precisão conceitual, à especialização institucional, à extensão das sanções e à definição dos limites da tutela conferida. Assim, Argentina e Chile se destacam por apresentarem disciplina normativa mais detalhada acerca das condutas ilícitas e de suas finalidades, sendo que o Chile reconhece expressamente hipóteses de aquisição lícita de informações, como a engenharia reversa e o desenvolvimento (Egaña Bertoglia, 2024, pp. 68-70; Correa et al., 2025, pp. 44-45).

O Brasil e a Colômbia adotam modelos distintos de proteção dos segredos empresariais, o que influencia a segurança jurídica e a dinâmica concorrencial. No Brasil, a tutela ocorre de forma mais ampla por meio das normas de concorrência desleal, embora as definições legais e os limites da proteção sejam menos sistemáticos. Já a Colômbia combina o regime andino de proteção com a atuação da autoridade de indústria e comércio nas esferas administrativa e jurisdicional. Assim, essas diferenças afetam diretamente a previsibilidade dos respectivos sistemas e os riscos de utilização estratégica da confidencialidade em prejuízo de concorrentes, trabalhadores ou autoridades públicas (Correa et al., 2025, pp. 93-96).

A proteção dos segredos empresariais desempenha importante função de incentivo à inovação, mas também pode gerar custos concorrenciais relevantes. Diferentemente da patente, o segredo não exige divulgação pública nem está sujeito a prazo legal de vigência, permitindo a manutenção prolongada da exclusividade informacional. Assim, quanto mais ampla for a categoria de informações protegidas e mais restritivas forem as limitações impostas ao seu uso, maiores tendem a ser os obstáculos à mobilidade dos trabalhadores, à difusão tecnológica e à entrada de novos concorrentes no mercado (Schultz; Lippoldt, 2014, pp. 11-13, 21-23).

Embora a proteção dos segredos empresariais possa estimular investimentos, crescimento individual e a atividade inovadora, ela também pode gerar efeitos restritivos sobre a concorrência. Isso ocorre porque a ampliação da tutela da confidencialidade pode limitar o processo cumulativo por meio do qual novos agentes aprendem, adaptam e aperfeiçoam conhecimentos já existentes. Assim, os efeitos econômicos desse regime não dependem apenas

da intensidade da proteção conferida, mas também da adequação entre o objeto protegido, as condutas vedadas e as salvaguardas destinadas à preservação da concorrência (Schultz; Lippoldt, 2014, pp. 11-13, 21-23).

A proporcionalidade constitui elemento essencial para delimitar a proteção dos segredos empresariais. Nesse contexto, condutas como espionagem, fraude, invasão de sistemas, violação de confiança e indução ao descumprimento de deveres justificam repressão, pois substituem a competição baseada no mérito pela apropriação indevida de informações alheias. Em contrapartida, a criação independente, a observação legítima, a análise de produtos regularmente adquiridos e a engenharia reversa autorizada integram a dinâmica ordinária da concorrência. Assim, equiparar tais comportamentos significaria eliminar a distinção entre a repressão à deslealdade e a concessão de exclusividade sobre o conhecimento (Schultz; Lippoldt, 2014, p. 8; Correa et al., 2025, pp. 53-55).

O Chile se destaca por apresentar a formulação mais clara dessa distinção nos materiais analisados, reconhecendo de forma explícita a independência criativa, a engenharia reversa e o acesso a fontes públicas. Nos outros países, a abertura concorrencial surge principalmente da própria definição do que é segredo, da exigência de aquisição que contraria as práticas comerciais honestas e da exclusão de informações que são públicas ou evidentes. A falta de limitações expressas, especialmente no Brasil, não implica que toda descoberta paralela seja ilegal, mas sim que diminui a segurança jurídica e aumenta a dependência de interpretações judiciais que variam caso a caso (Correa et al., 2025, pp. 43-55).

As medidas processuais desempenham papel fundamental na tutela dos segredos empresariais, especialmente para prevenir a divulgação irreversível de informações confidenciais. Nesse contexto, providências como busca e apreensão, acesso a sistemas informáticos, proibição imediata de uso e restrições à atividade empresarial podem ser necessárias para assegurar a efetividade da proteção. Assim, sua utilização deve observar critérios rigorosos de proporcionalidade, de modo a conciliar a proteção do segredo com as garantias processuais e a livre concorrência (Schultz; Lippoldt, 2014, pp. 16-21).

O direito comparado evidencia a necessidade de cautela na adoção de medidas destinadas à proteção de segredos empresariais. Embora tais providências possam ser essenciais para impedir o uso indevido de informações confidenciais, sua utilização também pode gerar riscos relevantes. Em especial, essas medidas podem ser empregadas de forma abusiva, interferindo na atividade empresarial de concorrentes ou permitindo o acesso a informações sigilosas do próprio demandado. Assim, sua concessão deve estar condicionada à demonstração inicial consistente da existência do segredo protegido, à delimitação rigorosa da diligência e à preservação bilateral da confidencialidade (Schultz; Lippoldt, 2014, pp. 16-21).

A intervenção do Estado também precisa ser analisada em relação à coerência entre a política de concorrência, a proteção da propriedade intelectual e a regulação econômica. Os direitos sobre ativos imateriais podem estimular a pesquisa e o desenvolvimento, mas cláusulas de licenciamento, transferência de tecnologia e confidencialidade podem se tornar restritivas se usadas para fixar preços, impedir exportações, bloquear inovações independentes ou controlar agentes que já não precisam da informação protegida. A

legalidade não pode ser simplesmente inferida da existência de um segredo ou de outro direito intelectual; é necessário avaliar a estrutura do mercado, o poder econômico, as barreiras à entrada, a duração da restrição e as eficiências geradas (Echeverri Uribe; Díaz Rivera; Mick Forero, 2006, pp. 16, 22-28).

A experiência brasileira apresentada nos materiais reforça essa interação. Os contratos de transferência de tecnologia e a exploração de segredos continuam a estar sob a égide do direito concorrencial. Cláusulas que impõem restrições injustificadas ao acesso ao mercado, à formação de preços ou à liberdade comercial podem ser vistas como incompatíveis com a ordem econômica. A proteção não garante automaticamente controles permanentes sobre conhecimentos que já se tornaram públicos, nem obrigações de confidencialidade que não estejam ligadas à real preservação do segredo (Caffé; Abenza; Torres, 2021, pp. 94, 99).

Nesse contexto, a experiência comparada demonstra que o sigilo pode ser relativizado quando necessário à preservação da concorrência e ao exercício das funções regulatórias do Estado. Na Argentina, admite-se que a autoridade determine a divulgação de informações necessárias para corrigir práticas anticoncorrenciais, enquanto, no Brasil, o acesso a algoritmos e dados empresariais pela autoridade concorrencial deve limitar-se ao estritamente necessário, com observância de mecanismos de confidencialidade institucional. Assim, a tutela do segredo empresarial deve ser compatibilizada com a proteção da concorrência e com outras finalidades legalmente justificadas (Correa et al., 2025, pp. 85-90, 102-105).

No Chile, o uso de segredos empresariais para impedir a entrada de competidores ou restringir a concorrência pode caracterizar abuso

de posição dominante, inclusive em hipóteses de recusa de acesso a tecnologias essenciais. Assim, na Colômbia, cláusulas de transferência de tecnologia que imponham preços de revenda, determinem a cessão de direitos sobre aperfeiçoamentos ou restrinjam exportações podem ser submetidas ao controle concorrencial, demonstrando a necessidade de compatibilizar a proteção do sigilo com a preservação de mercados competitivos (Correa et al., 2025, pp. 85-90, 102-105).

O Estado, ao realizar uma intervenção que funciona em duas frentes, precisa agir para evitar a apropriação clandestina ou desleal da informação, criando um ambiente que favoreça o investimento e a colaboração entre empresas. Por outro lado, é fundamental que o Estado impeça que segredos sejam usados para esconder práticas restritivas, obstruir investigações ou aumentar artificialmente posições dominantes. A proteção que se busca não é nem a máxima nem a mínima; é aquela que mantém a vantagem obtida por meio de investimentos legítimos, sem eliminar do mercado as formas justas de descoberta, aprendizado, mobilidade e competição (Correa et al., 2025, pp. 102-105; UNCTAD, 2021, pp. 82-83).

A informação digital traz características que desafiam as categorias tradicionais. Embora possa ser acessada ao mesmo tempo por diversos agentes, seu acesso pode ser limitado por meio de ferramentas jurídicas e tecnológicas. As plataformas que conseguem coletar grandes quantidades de dados têm uma posição privilegiada na cadeia de valor, transformando dados brutos em inteligência comercial, capacidade preditiva e melhorias contínuas nos serviços. O controle acumulado de dados, combinado com efeitos de rede, economias de escala e escopo, altos custos iniciais e baixos custos marginais, pode gerar mercados que tendem

à concentração e criar barreiras que são difíceis de superar para novos entrantes (UNCTAD, 2021, pp. 22, 82-83).

No contexto da economia digital, a proteção dos segredos empresariais assume papel estratégico na preservação de ativos intangíveis. A confidencialidade de algoritmos, bancos de dados, métodos de análise e arquiteturas de sistemas pode constituir instrumento legítimo para proteger investimento. Contudo, a classificação indiscriminada desses ativos como segredos empresariais pode restringir auditorias, interoperabilidade, portabilidade, explicabilidade e o acesso a insumos essenciais. Assim, a tutela da confidencialidade deve ser compatibilizada com mecanismos que promovam transparência, inovação e concorrência nos mercados digitais (UNCTAD, 2021, pp. 82-83).

Na economia digital, a vantagem competitiva decorre cada vez menos da posse isolada de informações e mais da capacidade de gerar, processar e reutilizar fluxos contínuos de dados. Nesse contexto, o crescimento da base de usuários tende a aperfeiçoar o desempenho dos serviços e atrair novos usuários, produzindo um ciclo de retroalimentação que fortalece a posição de mercado das plataformas. Assim, quando associada a esses efeitos de rede, a proteção da confidencialidade pode reforçar barreiras estruturais à entrada e ampliar as vantagens competitivas já detidas pelos agentes (UNCTAD, 2021, pp. 82-83).

A relação entre segredo empresarial e direito concorrencial não deve se restringir apenas à punição de abusos após o fato. É fundamental que essa relação também ajude a definir o próprio alcance da proteção. Quando uma empresa alega que um determinado conjunto de informações é confidencial, a autoridade deve não

apenas confirmar a existência dos requisitos para o segredo, mas também entender o papel dessa informação na dinâmica do mercado. A análise deve levar em conta a substituíbilidade, replicabilidade, custos de obtenção independente e a capacidade da informação de atuar como uma infraestrutura de acesso ao mercado (Correa et al., 2025, pp. 85-90, 93-96, 102-105).

Na Argentina, o segredo pode ser deixado de lado quando se trata de corrigir práticas anticoncorrenciais. No Brasil, o CADE tem a capacidade de receber informações confidenciais e mantê-las em sigilo, revelando-as apenas quando for absolutamente necessário para a investigação ou para a solução de problemas concorrenciais. No Chile, o uso excessivo ou injustificado do controle sobre informações tecnológicas pode ser visto como um abuso de posição dominante. Já na Colômbia, a autoridade de indústria e comércio possui competências que permitem conectar concorrência desleal, proteção de segredos, atos de concentração e restrições contratuais (Correa et al., 2025, pp. 85-90, 93-96, 102-105).

A inovação também está ligada à mobilidade das pessoas. Nos setores digitais, uma parte significativa do conhecimento está nas equipes, nas rotinas e nas experiências acumuladas. A proteção deve se concentrar em informações que possam ser claramente identificadas, e não na memória geral do trabalhador, em sua experiência profissional ou em seu conhecimento técnico. Restrições pós-contratuais só são justificáveis quando são bem definidas em termos de tempo, espaço e atividades, protegem um interesse legítimo e, dependendo do sistema, oferecem uma compensação proporcional (Schultz; Lippoldt, 2014, pp. 12, 19-20; Correa et al., 2025, pp. 85-96).

Essa reflexão conecta a proteção dos segredos empresariais ao conceito de soberania digital. Nesse contexto, aplicações extraterritoriais excessivamente amplas podem induzir outros países a adotar padrões regulatórios mais restritivos do que aqueles previstos em seus próprios ordenamentos. Assim, embora a atuação exclusivamente nacional se revele insuficiente diante de plataformas globais, fluxos transfronteiriços de dados e práticas de espionagem apoiadas em infraestruturas distribuídas, a preservação de espaços decisórios autônomos continua sendo elemento central da soberania digital (Effron, 2003, pp. 1513-1517; UNCTAD, 2021, pp. 180-181).

Interoperabilidade, portabilidade e padrões abertos surgem como ferramentas importantes para diminuir dependências, mas precisam ser implementados com respeito à confidencialidade empresarial e a outros direitos protegidos. Não existe uma solução única que sirva para todos os mercados. A abertura de dados pode incentivar a concorrência em uma área, mas em outra pode expor segredos legítimos ou aumentar vulnerabilidades. O critério regulatório deve considerar a necessidade de acesso em relação à função que a informação desempenha, adotando medidas técnicas e jurídicas que minimizem a divulgação ao estritamente necessário (UNCTAD, 2021, pp. 180-181).

A eficiência econômica não se confunde com a ampliação da exclusividade informacional. Para que haja eficiência dinâmica, é necessário preservar incentivos à criação, mas também à entrada de novos agentes, à recombinação de conhecimentos e à substituição de tecnologias. Embora a repressão à espionagem e à fraude possa favorecer a inovação, uma proteção excessiva pode restringir a descoberta independente, a mobilidade profissional e o acesso a

insumos. Assim, cabe ao direito concorrencial verificar se a confidencialidade efetivamente protege investimentos legítimos ou se funciona como instrumento de exclusão e reforço de posições dominantes (Schultz; Lippoldt, 2014, pp. 10-13, 21).

A luta contra a espionagem econômica corporativa é bem fundamentada. A obtenção clandestina de processos, estratégias, informações comerciais ou projetos permite que o infrator evite os custos de pesquisa, desenvolvimento e organização que o titular teve que arcar. Isso também aumenta os gastos defensivos das empresas, diminui a disposição para compartilhar informações nas cadeias produtivas e compromete a confiança necessária para relações de emprego, investimento e cooperação tecnológica. Sem uma proteção adequada, a competição poderia se basear na apropriação desleal, em vez de na eficiência, na inovação ou no desenvolvimento autônomo (Schultz; Lippoldt, 2014, pp. 10-13, 21).

A legitimidade da proteção, no entanto, não permite que ela se expanda sem limites. O segredo empresarial pode durar indefinidamente, não precisa ser divulgado publicamente e pode incluir uma vasta gama de informações. Quando essas características se juntam a uma criminalização ampla, medidas cautelares invasivas, contratos de não concorrência ou interpretações que proíbem a engenharia reversa e a criação independente, a proteção pode acabar tendo efeitos semelhantes ou até mais intensos do que um direito exclusivo, sem as limitações temporais e informacionais que estão ligadas a outras formas de propriedade intelectual (Effron, 2003, pp. 1477-1481; Schultz; Lippoldt, 2014, pp. 11-13).

O limite jurídico da proteção deve recair sobre a qualificação da informação. Apenas informações secretas, dotadas de valor econômico e submetidas a medidas razoáveis de proteção podem ser resguardadas como segredos empresariais. Além disso, sua identificação deve ser precisa para que empregados, concorrentes e autoridades compreendam o alcance da tutela. Assim, expressões genéricas, como “todas as informações da empresa”, não bastam para fundamentar sanções severas, especialmente na esfera penal, tampouco para converter qualquer violação de dever contratual em infração relativa a segredo empresarial (Egaña Bertoglia, 2024, pp. 68-70, 80-81; Correa et al., 2025, pp. 41-46).

O segundo limite ramificado trata da distinção entre métodos desleais e práticas competitivas legítimas. A espionagem, a fraude, a invasão de sistemas, o roubo de arquivos, a violação intencional de deveres específicos e a indução à quebra de confiança são situações que justificam uma intervenção. Por outro lado, a descoberta independente, a experiência profissional geral, a análise de fontes públicas e a engenharia reversa legal devem ficar fora do alcance da repressão. Essa delimitação ajuda a manter a função concorrencial do instituto: evitar a apropriação desonesta sem dar ao titular controle sobre todo o conhecimento equivalente (Schultz; Lippoldt, 2014, p. 8; Correa et al., 2025, pp. 53-55).

O terceiro limite diz respeito ao elemento subjetivo e à relação de causa e efeito. A responsabilização, especialmente no âmbito criminal, deve exigir a prova de que o agente tinha consciência do caráter secreto da informação e que pretendia ou assumia conscientemente sua obtenção, divulgação ou uso indevido. Benefícios econômicos distantes, vantagens hipotéticas ou relações causais muito longas não são suficientes para caracterizar

espionagem. A exigência de um resultado provável, direto ou natural diminui a chance de que ações periféricas sejam englobadas por tipos de sanções criados para práticas mais graves (Schultz; Lippoldt, 2014, pp. 16-21; Egaña Bertoglia, 2024, pp. 68-70, 80-81).

O quarto limite refere-se à proporcionalidade das medidas de urgência. Como a divulgação de um segredo pode eliminar seu valor econômico, a tutela preventiva muitas vezes se mostra necessária. Contudo, medidas como busca e apreensão, acesso a dispositivos ou restrições à atividade empresarial devem ser delimitadas quanto ao objeto, à duração e à finalidade. Assim, o requerente deve identificar a informação protegida, comprovar seu controle e demonstrar o risco concreto de uso indevido, cabendo ao juízo resguardar tanto o alegado segredo empresarial quanto eventuais informações confidenciais do demandado (Schultz; Lippoldt, 2014, pp. 16-21; Correa et al., 2025, pp. 63-78, 85-96).

O quinto limite refere-se às relações de trabalho. Embora as obrigações de confidencialidade possam subsistir após o término do contrato, elas não devem impedir o exercício profissional nem abranger habilidades e conhecimentos gerais do trabalhador. Da mesma forma, pactos de não concorrência somente se justificam quando necessários à proteção de interesse legítimo, observados limites de tempo, espaço e atividade. Assim, a proteção dos segredos empresariais não pode ser utilizada como mecanismo de retenção de trabalhadores ou de restrição à criação de novos empreendimentos (Schultz; Lippoldt, 2014, pp. 12, 19-20; Correa et al., 2025, pp. 85-96).

O sexto limite refere-se ao controle concorrencial da confidencialidade. A autoridade deve poder acessar informações

essenciais à investigação de práticas restritivas, assegurada sua proteção contra divulgações indevidas. O titular, por sua vez, não pode invocar o segredo empresarial para ocultar condutas anticoncorrenciais, como cartéis, discriminação, fechamento de mercado ou restrições contratuais injustificadas. Além disso, a recusa de acesso merece escrutínio quando a informação controlada for indispensável à interoperabilidade ou à atuação de concorrentes no mercado (Correa et al., 2025, p. 89-90, 102-105; ITU; The World Bank, 2020, pp. 52-53).

O sétimo limite decorre da dimensão transfronteiriça da proteção dos segredos empresariais. A aplicação de normas nacionais não deve desconsiderar a soberania regulatória de outros países nem impor, por via extraterritorial, modelos de proteção mais abrangentes. Isso porque condutas como engenharia reversa, mobilidade de trabalhadores e obrigações contratuais podem receber tratamento distinto conforme a jurisdição envolvida. Assim, embora a cooperação internacional seja essencial para investigar ataques digitais e preservar evidências, ela deve respeitar os limites territoriais e as legítimas escolhas de política regulatória de cada Estado (Effron, 2003, pp. 1513-1517).

Os modelos da América do Sul que foram analisados já possuem elementos que podem ajudar a manter esse equilíbrio. Os requisitos de sigilo, valor e medidas razoáveis atuam como um filtro inicial; a concorrência desleal restringe a proteção a formas inadequadas de aquisição ou uso; tanto a Argentina quanto o Chile dão importância à finalidade econômica ou prejudicial; o Chile reconhece claramente meios legais de descoberta; Argentina e Brasil permitem um acesso estatal qualificado para a defesa da concorrência; a Colômbia conta com uma autoridade que possui competências bem articuladas; e

os quatro sistemas impõem limites, mesmo que de maneira desigual, às restrições trabalhistas (Correa et al., 2025, pp. 41-56, 85-105).

O Brasil ainda carece de uma definição autônoma mais detalhada e de uma sistematização clara das hipóteses de aquisição lícita, enquanto a ampliação da tutela penal no Chile reforça a necessidade de distinguir segredo empresarial de mera confidencialidade. Na Argentina, a efetividade do regime depende da articulação entre diferentes diplomas normativos e autoridades, ao passo que, na Colômbia, a integração institucional não é acompanhada de evidências suficientes para uma avaliação conclusiva do controle concorrencial. Assim, em todos os países analisados, a tutela pode ser comprometida pela demora processual, pelo elevado custo da prova técnica, pela dificuldade de demonstrar aquisições digitais clandestinas (Correa et al., 2025, pp. 61-62, 85-96).

Do ponto de vista regulatório, o modelo mais adequado às economias digitais abertas não é o que confere proteção máxima, mas aquele capaz de distinguir claramente a apropriação desleal da concorrência legítima. A tutela deve ser rigorosa diante de fraudes, invasões, subtrações, violações de confiança e práticas de espionagem, sem comprometer a criação independente, a engenharia reversa lícita, a mobilidade profissional e a circulação de conhecimentos públicos. Assim, a confidencialidade não pode servir como instrumento de preservação artificial de poder econômico, impondo-se o controle concorrencial sempre que seu uso dificultar a entrada de novos agentes ou restringir investigações legítimas (Schultz; Lippoldt, 2014, pp. 11-13, 16-23; UNCTAD, 2021, pp. 82-83).

Com base nos elementos analisados, a hipótese central da pesquisa é confirmada, especialmente em sua dimensão jurídico-estrutural. Verifica-se a existência de mecanismos com potencial para gerar efeitos anticompetitivos, como a duração indeterminada dos segredos empresariais, a amplitude das categorias protegidas, as restrições à mobilidade profissional, o risco de criminalização excessiva, as medidas cautelares de elevado impacto e o uso da confidencialidade como barreira à entrada. Além disso, o poder econômico das plataformas digitais tende a intensificar esses riscos nas economias contemporâneas (Schultz; Lippoldt, 2014, pp. 11-13, 16-23; UNCTAD, 2021, pp. 82-83).

A análise comparativa dos modelos jurídicos do Brasil, Argentina, Chile e Colômbia confirma a hipótese da pesquisa no que diz respeito ao plano jurídico-estrutural. Embora todos esses sistemas reconheçam a importância de proteger os segredos empresariais e combater a espionagem econômica, a investigação revelou que, quando a proteção jurídica é ampliada sem limites claros em termos materiais, processuais e concorrenciais, isso pode ir além da proteção do investimento legítimo (Correa et al., 2025, pp. 61-62, 85-96).

Em determinadas circunstâncias, a proteção dos segredos empresariais pode converter a confidencialidade em um instrumento de fechamento informacional. Isso ocorre porque a ampliação excessiva de proteção tende a restringir o acesso a informações necessárias ao desenvolvimento de tecnologias complementares. Nesses casos, mecanismos concebidos para coibir a obtenção desleal de informações acabam por restringir práticas legítimas, como a engenharia reversa, a criação independente e a mobilidade profissional. Assim, essa proteção excessiva da

informação dificulta formas legítimas de circulação do conhecimento, essenciais à inovação das economias digitais (Correa et al., 2025, pp. 61-62, 85-96).

Os regimes analisados incorporam mecanismos relevantes para equilibrar proteção da informação e concorrência. Entre eles, Salgado e Fiuza (2015, p. 12-15) destacam a exigência de valor econômico do segredo, a adoção de medidas razoáveis de proteção, a exclusão de informações públicas, o reconhecimento de formas lícitas de obtenção de conhecimento e a atuação das autoridades concorrenciais. Contudo, a efetividade desses instrumentos depende de uma aplicação coerente e sistemática, orientada por critérios de qualidade regulatória, transparência e coordenação institucional, de modo a compatibilizar a tutela da inovação com a livre concorrência e a soberania digital.

Dessa forma, o modelo jurídico mais adequado às economias digitais da América do Sul é aquele que concilia proteção da informação, concorrência e desenvolvimento econômico. Conforme a literatura sobre qualidade regulatória, a intervenção estatal deve ser necessária, proporcional e orientada por evidências, evitando a criação de barreiras excessivas ou custos regulatórios desnecessários. Assim, a proteção dos segredos empresariais deve preservar os incentivos à inovação sem comprometer a contestabilidade dos mercados e a competitividade regional (Salgado; Fiuza, 2015, pp. 12-15).

Em síntese, a análise comparada dos modelos jurídicos sul-americanos demonstra que a proteção dos segredos empresariais constitui instrumento legítimo de estímulo à inovação e à concorrência baseada no mérito. Contudo, conforme advertem

Schultz e Lippoldt (2014, pp. 10-23), a eficiência econômica não decorre da máxima expansão da confidencialidade, mas da adequada delimitação de seu objeto, de seus mecanismos de tutela e de seus limites concorrenciais. Por essa razão, a tutela dos segredos empresariais deve ser interpretada à luz dos princípios da proporcionalidade, da livre concorrência e da qualidade regulatória, preservando os incentivos à criação sem comprometer a circulação legítima do conhecimento, a contestabilidade dos mercados e o desenvolvimento tecnológico regional.

5. CONCLUSÃO

A crescente relevância econômica da informação tem transformado a dinâmica competitiva das economias digitais. Dados, algoritmos, conhecimentos técnicos e outros ativos informacionais passaram a ocupar posição central na geração de valor, na inovação e na competitividade empresarial. Nesse contexto, a espionagem econômica corporativa deixa de representar apenas uma forma ilícita de obtenção de vantagens competitivas e passa a influenciar diretamente a estrutura dos mercados digitais. Por isso, a proteção jurídica dos segredos empresariais deve ser analisada não apenas sob a perspectiva patrimonial, mas também à luz dos princípios da livre concorrência, da inovação e da soberania digital.

A pesquisa realizada mostrou que proteger os ativos informacionais é essencial para garantir segurança jurídica aos investimentos das empresas, estimular a pesquisa e o desenvolvimento, e combater práticas que buscam obter informações estratégicas de forma ilícita. Assim, manter a confidencialidade de segredos empresariais que têm relevância econômica é, sem dúvida, compatível com a ordem econômica constitucional e se revela um importante mecanismo

para fomentar o desenvolvimento tecnológico, a inovação e a eficiência nos mercados.

Embora a proteção dos segredos empresariais seja necessária para preservar incentivos à inovação e resguardar investimentos privados, a análise da literatura, da economia da informação, do direito concorrencial e da experiência sul-americana demonstra que a ampliação dessa tutela produz efeitos que vão além de seus objetivos originais. Quando a exclusividade informacional passa a abranger conhecimentos técnicos, engenharia reversa, interoperabilidade, mobilidade profissional e o compartilhamento de informações relevantes para o progresso tecnológico, ela deixa de atuar apenas como mecanismo de proteção do investimento e passa a influenciar a dinâmica concorrencial dos mercados.

A pesquisa mostrou que esse fenômeno se torna ainda mais significativo nas economias digitais, que são marcadas pela presença simultânea de efeitos de rede, economias de escala baseadas em dados, altos custos fixos para o desenvolvimento tecnológico, baixos custos marginais de reprodução e uma concentração considerável de recursos computacionais, infraestruturas digitais e fluxos informacionais. Nesses contextos, a expansão indiscriminada da proteção jurídica fortalece vantagens competitivas já existentes, aumenta as barreiras de entrada, dificulta a contestação dos mercados e diminui os incentivos à inovação incremental, prejudicando a concorrência como um motor de desenvolvimento econômico.

A análise comparativa dos modelos jurídicos do Brasil, Argentina, Chile e Colômbia reforça essa conclusão. Embora todos reconheçam a necessidade de proteger informações empresariais confidenciais

contra sua obtenção, uso ou divulgação indevidos, diferem quanto ao objeto da proteção, às hipóteses de aquisição lícita de informações, ao tratamento da engenharia reversa, à mobilidade profissional e às salvaguardas concorrenciais. Assim, as experiências examinadas demonstram que a efetividade do sistema não depende apenas da intensidade da proteção conferida, mas da capacidade de estabelecer limites jurídicos que conciliem inovação, segurança dos investimentos e concorrência nos mercados.

Os resultados obtidos confirmam a hipótese desta pesquisa. Verificou-se que a ampliação dos mecanismos de proteção contra a espionagem econômica corporativa, quando desacompanhada de limites concorrenciais adequados, pode produzir efeitos restritivos sobre a livre concorrência nas economias digitais sul-americanas. A expansão da exclusividade informacional tende a reforçar posições dominantes, dificultar a circulação legítima do conhecimento, elevar barreiras à entrada, reduzir a interoperabilidade tecnológica e limitar a inovação incremental, especialmente em mercados fortemente dependentes de dados, algoritmos e infraestrutura digital.

Nas economias sul-americanas, essa questão assume relevância ainda maior em razão da dependência tecnológica, da concentração internacional das infraestruturas digitais e da limitada autonomia regional em relação a dados, plataformas e tecnologias estratégicas. Nesse contexto, a ampliação excessiva da exclusividade sobre ativos informacionais pode aprofundar assimetrias tecnológicas, dificultar o desenvolvimento de capacidades produtivas locais, restringir o fortalecimento de empresas nacionais e comprometer a construção da soberania digital. Dessa forma, a proteção dos segredos empresariais somente se justifica quando preserva os incentivos à inovação sem comprometer a livre concorrência.

Em conclusão, a preservação da concorrência não exige a redução da proteção dos segredos empresariais, mas a definição clara de seus limites jurídicos. A tutela deve concentrar-se na repressão à obtenção ilícita de informações valiosas, sem restringir práticas legítimas de aprendizado tecnológico, desenvolvimento, engenharia reversa, mobilidade profissional e circulação do conhecimento. Portanto, a pesquisa demonstra que o equilíbrio entre proteção empresarial, livre concorrência e soberania digital constitui condição para o desenvolvimento tecnológico e para a competitividade sustentável das economias digitais sul-americanas.

REFERÊNCIAS BIBLIOGRÁFICAS

AKHTAR, Farah; SENADJKI, Abdelhak; KUMARAN, Viknisiwari Vija. **Navigating the digital era: role of intellectual capital in enhancing the financial performance.** Atlantis Press, pp. 21-60, 2026. DOI: 10.2991/978-94-6463-666-6_3. Disponível em: <https://www.atlantispress.com/proceedings/bafe-24/126009210>. Acesso em: 2 set. 2026.

AUSTRALIAN COMPETITION AND CONSUMER COMMISSION. **Digital Platform Services Inquiry 2020-25.** Austrália: ACCC, 2023. Disponível em: <https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries-and-monitoring/digital-platform-services-inquiry-2020-25>. Acesso em: 26 mai. 2026.

BATURA, Olga; WION, Axel; GONZALEZ, Sofia N.; MARCUS, J. Scott; GODLOVITCH, Ilsa; WIEWIORRA, Lukas; KROON, Peter; TAS, Serpil; STEFFEN, Nico. **The emergence of non-personal data markets.** Luxembourg: European Parliament, 2023. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740098/IPOL_STU\(2023\)740098_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740098/IPOL_STU(2023)740098_EN.pdf). Acesso em: 05 jun. 2026.

BERTARINI, Beatrice. **European Union digital single market: legal framework and challenges**. Milano: FrancoAngeli, 2023. Disponível em:

<https://www.econstor.eu/bitstream/10419/279839/1/1865944661.pdf>.

Acesso em: 4 mai. 2026.

CAFFÉ, Cândida; ABENZA, Mariana; TORRES, Rodrigo. **Trade secrets - Brazil**. les Nouvelles, pp. 93-99, 2021. Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3832047. Acesso

em: 4 mai. 2026.

COMPETITION AND MARKETS AUTHORITY. **Trends in digital markets: a CMA horizon scanning report**. Reino Unido: CMA, 2023.

Disponível em: <https://www.gov.uk/government/publications/trends-in-digital-markets-a-cma-horizon-scanning-report>. Acesso em: 15

jun. 2026.

CORREA, Juan; CABANELLAS, Guillermo; WEGBRAIT, Pablo; FEKETE, Elisabeth Kasznar; ZARATE, José Manuel Alvarez; MINUTTI, Karla Fiorella; BARRIOS, Andrea. **Trade secrets and data protection in Latin America: a comparative study**. Munich: Max Planck Institute for Innovation and Competition, 2025. Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5225765. Acesso

em: 14 mai. 2026.

ECHEVERRI URIBE, Andrés; DÍAZ RIVERA, Jorge Alberto; MICK FORERO, Juan Pablo. **Prácticas restrictivas de la competencia en Latinoamérica y el Caribe**. Bogotá: Pontificia Universidad Javeriana, 2006. Disponível em:

<https://cendoc.sc.gob.sv/textocompleto/932.pdf>. Acesso em: 23 mai. 2026.

EFFRON, Robin J. **Secrets and spies:** extraterritorial application of the Economic Espionage Act and the TRIPS Agreement. New York: New York University Law Review, v. 78, pp. 1475-1517, 2003. Disponível em: <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1494&context=faculty>. Acesso em: 04 mai. 2026.

EGAÑA BERTOGLIA, Juan Pablo. **Información no divulgada y secretos comerciales en Chile.** Revista de Actualidad Mercantil, n. 8, pp. 68-81, 2024. Disponível em: <https://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/28772/26390>. Acesso em: 15 mai. 2026.

FALAVIGNA, Leandro; LINS Thiago Vitor; **O furto de informações e seu o vácuo legislativo.** Migalhas: 2025. Disponível: <https://www.migalhas.com.br/depeso/443218/o-furto-de-informacoes-e-seu-o-vacuio-legislativo>. Acesso em: 3 set. 2026.

HACOHEN, Uri Y. **Fostering open data.** Berkeley: Berkeley Technology Law Journal, v. 41, n. 1, pp. 259-305, 2026. DOI: 10.15779/Z38M61BS11. Disponível em: <https://lawcat.berkeley.edu/record/1333883?v=pdf>. Acesso em: 14 mai. 2026.

HASWELL, Christopher. **Simulated accountability:** Big Tech, transparency reports, and Russian disinformation in the Baltic States. Athens: University of Georgia, 2026. Disponível em: <https://openscholar.uga.edu/record/27965/files/2026-Haswell-SimulatedAccountabilityThesis.pdf%20.pdf>. Acesso em: 07 jun. 2026.

INTERNATIONAL TELECOMMUNICATION UNION; THE WORLD BANK. **Manual de reglamentación digital.** Geneva: 2020. Disponível

em: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-TRH.1-2020-PDF-E.pdf. Acesso em: 14 mai. 2026.

LIANG, Feng Helen. **Does foreign direct investment improve the productivity of domestic firms?** Technology spillovers, industry linkages, and firm capabilities. Research Policy: 2016. DOI: 10.1016/j.respol.2016.08.007. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0048733316301263>. Acesso em: 7 jun. 2026.

LIMA, Luciana Piazzon Barbosa; JEREISSATI, Tatiana; MACAYA, Javiera F. M.; VARELLA, Guilherme. **An analysis of Artificial Intelligence uses and its implications for cultural diversity in Brazil.** Artificial Intelligence and culture: perspectives for cultural diversity in the digital age. São Paulo: Comitê Gestor da Internet no Brasil, pp. 125-190. Disponível em: https://cetic.br/media/docs/publicacoes/7/20220927095231/sectoral_studies-artificial_intelligence_and_culture.pdf. Acesso em: 15 jun. 2026.

LUPACCHINI, Beatrice. **Disruptive business models in data-driven markets: rethinking EU competition law through the lens of privacy.** Atlantis Press: pp. 421-434. 2026. DOI: 10.2991/978-94-6239-622-7_25. Disponível em: <https://www.atlantispress.com/proceedings/icech-25/126023132>. Acesso em: 08 jun. 2026.

MATTOO, Aaditya; MELTZER, Joshua P. **International data flows and privacy:** the conflict and its resolution. Journal of International Economic Law: v. 21, pp. 769-789, 2018. DOI: 10.1093/jiel/jgy044. Disponível em: <https://academic.oup.com/jiel/article-abstract/21/4/769/5227421>. Acesso em: 15 jun. 2026.

NARECHANIA, Tejas N. **Machine learning as natural monopoly.** Iowa Law Review: v. 107, pp. 1543-1614, 2022. Disponível em: https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/A4_Narechania.pdf. Acesso em: 15 mai. 2026.

NOTHIAS, Toussaint. **An intellectual history of digital colonialism.** Journal of Communication: v. 75, n. 5, pp. 385-397, 2025. DOI: 10.1093/joc/jqaf003. Disponível em: <https://academic.oup.com/joc/article/75/5/385/8078024>. Acesso em: 11 jun. 2026.

PHILLIPS, Peter J.; POHL, Gabriela. **Industrial espionage: window of opportunity.** Information Security Journal: A Global Perspective: v. 34, n. 2, pp. 143-155, 2025. DOI: 10.1080/19393555.2024.2378755. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/19393555.2024.2378755>. Acesso em: 23 mai. 2026.

RIMMER, Matthew. **A submission on the right to repair.** Brisbane: Queensland University of Technology, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891319. Acesso em: 15 mai. 2026.

SALGADO, Lúcia Helena; FIUZA, Eduardo P. S.; Marcos regulatórios no Brasil: aperfeiçoando a qualidade regulatória. Rio de Janeiro: Ipea, 2015. Disponível em: <https://repositorio.ipea.gov.br/bitstreams/f10c7ab1-1e0e-4d4a-85ae-3ceec318174f/download>. Acesso em: 5 set. 2026.

SANTAELLA, Lucia. **Artificial Intelligence and culture: opportunities and challenges for the Global South.** Artificial Intelligence and culture: perspectives for cultural diversity in the

digital age. São Paulo: Comitê Gestor da Internet no Brasil, pp. 69-95. 2022. Disponível em: https://cetic.br/media/docs/publicacoes/7/20220927095231/sectoral_studies-artificial_intelligence_and_culture.pdf. Acesso em: 4 mai. 2026.

SCHULTZ, Mark F.; LIPPOLDT, Douglas C. **Approaches to protection of undisclosed information (trade secrets):** background paper. Paris: OECD Publishing, 2014. DOI: 10.1787/5jz9z43w0jnw-en. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/01/approaches-to-protection-of-undisclosed-information-trade-secrets_g17a245f/5jz9z43w0jnw-en.pdf. Acesso em: 10 mai. 2026.

SILVEIRA, Sergio Amadeu; XIONG Jeff. **Índice de soberania digital:** o caso do Brasil. Liinc em Revista: v. 21, 2025. Disponível em: <https://revista.ibict.br/liinc/article/view/7451>. Acesso em: 09 mai. 2026.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Digital Economy Report 2021:** cross-border data flows and development: for whom the data flow. Geneva: UNCTAD, 2021. Disponível em: https://unctad.org/system/files/official-document/der2021_en.pdf. Acesso em: 24 mai. 2026.

_____. **Implementing World Summit on the Information Society outcomes: a twenty-year review.** Geneva: UNCTAD, 2025. Disponível em: <https://unctad.org/publication/implementing-world-summit-information-society-outcomes-twenty-year-review>. Acesso em: 4 mai. 2026.

XIONG, Jie. **Digital sovereignty from a Global South perspective:** national attitudes and measurement systems. BRICS Digital Sovereignty Index Report. Global South Academic Forum; IDEAS: pp.

9-21, 2026. Disponível em: https://thetricontinental.org/wp-content/uploads/2026/05/BRICS_Digital_Sovereignty_Index_Report_EN.pdf. Acesso em: 14 mai. 2026.

¹ Especialista em Direito Empresarial, Fundação Getúlio Vargas (FGV), Santa Maria, Rio Grande do Sul, Brasil. E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0009-0003-7543-0478>.

² Residente Jurídico no Ministério Público do Rio Grande do Sul. Especializando em Direito Penal e Criminologia pela PUC-RS. E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0009-0009-6799-0073>.

³ Especialista em Direito de Família e Sucessões, Centro Educacional Dom Alberto (FDA), Santa Maria, Rio Grande do Sul, Brasil. E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0009-0000-3465-1299>.