# O Segredo Empresarial Como Opção De proteção Dos Ativos Intangíveis Na Sociedade Contemporânea[1]

Mariana Piovezani Moreti[2]

Wilker Caetano[3]

**Resumo**

Na contemporaneidade as criações autorais e industriais, know-how e segredo empresarial, dados e outras informações se destacam como ativos essenciais para a prática das atividades empresariais, além de agregarem valor e ampliarem negociações. Nesse cenário, identificou-se o desafio de proteger os ativos intangíveis ao se considerar o gargalo entre os bens protegidos pela propriedade intelectual por direito de exclusiva e outros conhecimentos protegidos enquanto posição jurídica, bem como um aumento da opção pelo uso do segredo. Assim, o objetivo do presente estudo foi compreender o uso do segredo como mecanismo de proteção do conhecimento empresarial. Através de uma metodologia dedutiva baseada em pesquisa bibliográfica e documental, o estudo mostrou que o segredo pode ser qualquer informação, conhecimento ou dado ("informação"), desde que seja confidencial, conceda vantagem competitiva, sejam eivados esforços pelo titular para manter a informação em segredo, não esteja em domínio público, não seja facilmente determinável ou acessado por meios lícitos. Com base nessas premissas, foi possível identificar algumas ferramentas de proteção preventivas, porque se a fuga ocorrer a informação deixa de ser secreta e a vantagem competitiva se perde.

**Palavras-chave:** Vantagem Competitiva. Concorrência desleal. Segredo comercial. Propriedade intelectual. Saber-fazer.

**Abstract**

In contemporary, copyright, industrial inventions, know-how and business secrets, data and other information stand out as essential assets for the practice of business activities, in addition to adding value and expanding negotiations. In this scenario, the challenge of protecting intangible assets was identified when considering the bottleneck between assets protected by exclusive right and other knowledge protected as a legal position, as well as an

[1] Este artigo é fruto da dissertação de mestrado intitulada "O conhecimento empresarial não protegido por direito de exclusiva: uma orientação para proteção do segredo empresarial" apresentada no Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação – PROFNIT – Ponto Focal Universidade Estadual de Maringá – UEM, 2023, defendida em 27 de Junho de 2023.

[2] Mestra em Propriedade Intelectual e Transferência de Tecnologia para Inovação pelo PROFNIT – Ponto Focal da Universidade Estadual de Maringá - UEM. Pós-graduanda em Propriedade Intelectual pela PUC-RJ. E-mail: marianapmoreti@gmail.com.

[3] Pós Doutor no Instituto de Física da Universidade de São Paulo (IFUSP). Professor na Universidade Estadual de Maringá e do PROFNIT PROFNIT – Ponto Focal da Universidade Estadual de Maringá - UEM. E-mail: wcaetano@uem.br.

increase in the option for the use of trade secret. Thus, the objective of this study was to understand the use of trade secret as a mechanism for protecting business knowledge. Through a deductive methodology based on bibliographical and documentary research, the study showed that the secret can be any information, knowledge, or data ("information"), as long as it is confidential, grants a competitive advantage, efforts are made by the holder to keep the information secret, not in the public domain, not easily discoverable or lawfully accessed. Based on these premises, it was possible to identify some preventive protection tools, because if the leak occurs, the information is no longer secret and the competitive advantage is lost.

**Keywords:** Competitive advantage. Unfair competition. Trade secret. Intellectual property. Know how.

## 1 INTRODUÇÃO

No contexto empresarial contemporâneo, em que a busca por diferencial competitivo é praticamente condição para permanência no mercado, o conhecimento, trabalho ou o resultado intelectual (não corpóreo) proveniente da mente humana, ganha posição de destaque na inovação. Nesse cenário, a inovação não se restringe às capacidades técnico-científicas, mas a competências voltadas ao conhecimento da estrutura dos mercados, oportunidades, riscos e estratégias, que nada mais são do que a utilização do conhecimento para geração de valor. Portanto, as empresas voltam atenções aos seus ativos intangíveis, onde o conhecimento gera riqueza e se torna vantagem competitiva no ambiente concorrencial.

Ocorre que, os ativos intangíveis possuem valor comercial porque constituem propriedade da empresa (SVEIBY, 1998), ou seja, geram riqueza a partir do momento em que a eles é conferido um título de exclusividade (propriedade), que garante a exploração econômica em detrimento dos concorrentes, ou possui um valor econômico que, apesar de não gerar um título de exclusividade, garante uma posição no mercado que lhe gera vantagens frente aos concorrentes.

É a propriedade intelectual que assume o papel do conjunto de princípios, normas, regras e procedimentos que regulam a produção e o acesso ao conhecimento, transformando os bens intelectuais em bens apropriáveis. (GANDELMAN, 2004). Grande parte dos ativos intangíveis de uma empresa como a marca, as patentes, o desenho industrial, software, bem como outros elementos produzidos pela indústria criativa, são bens protegidos pelas leis de Propriedade Intelectual. No entanto, parte extremamente importante desses elementos, que geram vantagem competitiva, como o know-how, dados de clientes e fornecedores, metodologias e gestão de projetos, relações mercadológicas, estratégia de marketing, entre

outros, são fenômenos que não são objeto de exclusividade legal, seja em razão de sua inapropriabilidade ou pela ausência de expressa previsão legal.

Tais figuras se caracterizam como uma oportunidade concorrencial resultante da detenção de certas informações em torno de um segredo ou confidencialidade, que geram escassez suficiente que lhes dotem de valor competitivos, e possuem proteção em uma variedade de normas, mas em especial como valores concorrenciais. (BARBOSA, 2017).

Nesta perspectiva, apesar da existência, os mecanismos de proteção desses ativos intangíveis não geram um título de exclusividade (propriedade) para exploração do bem no mercado, mas se resumem em uma situação de fato: a posição de uma empresa que lhe dá vantagem na concorrência, porquanto o que define a vantagem não é uma técnica, um sinal, um desenho industrial, mas a falta de acesso por parte dos concorrentes ao conhecimento específico gerado dentro da empresa (BARBOSA, 2017).

Nesse cenário, de ausência de forma jurídica protetiva própria, há uma tendência no estudo da proteção dos bens não respaldados por direito de exclusiva que justifica a presente pesquisa. Isso se dá em virtude da era da transformação digital, em que manter informação é um desafio constante, mas uma necessidade. De acordo com o relatório organizado pela World Intellectual Property Organization (2019) empresas e governos estão dando mais importância para a proteção dos conhecimentos comerciais[4] e diversos países, como os membros da União Europeia, Japão, China e Estados Unidos da América, promulgaram ou editaram suas legislações sobre a matéria, trazendo uma abordagem mais convergente.

No mesmo documento, foram listadas quatro razões pelas quais o conhecimento empresarial de valor tem chamado atenção. São elas: (a) o fato da digitalização ter transformado tudo em dados, que transformados em informação se tornam um importante ativo do negócio; (b) que a proteção do conhecimento exerce um papel fundamental nos negócios colaborativos; (c) mobilidade de pessoal qualificado, como consequência direta da globalização e da mudança dos modelos de negócios, o que faz com que as empresas estejam mais vigilantes sobre qual

[4] O documento referenciado trata do instituto "trade secret", que em tradução livre significa Segredo Comercial. Contudo, esse termo não será utilizado neste trabalho uma vez que o conceito, quando traduzido, importa em algumas diferenciações em face das legislações e doutrina brasileira. Para a finalidade pretendida nesta introdução, vale entender que o conhecimento empresarial de valor se refere as seguintes modalidades: (a) segredo de fábrica; (b) segredo de negócio; (c) Know-how; (d) informações confidenciais. O documento referenciado, apesar de tratar do termo "trade secret", abrange as modalidades indicadas.

informação pode ser compartilhada com seus funcionários; (d) a vulnerabilidade da informação e dos dados (WIPO, 2019).

De igual forma, Ciuriak e Patashkina (2021) afirmam que os governos do mundo inteiro estão introduzindo legislações para tratar ou aperfeiçoar o tratamento do conhecimento empresarial, especialmente em razão da aceleração da inovação baseada em dados, em que as posições jurídicas proporcionadas pelo conhecimento empresarial se tornam fundamentais para a criação de estratégias de propriedade intelectual, em parte porque os dados e algoritmos que exploram esses dados não são patenteáveis ou protegidos por direito autoral, mas também porque se torna mais fácil utilizar técnicas para manter o conhecimento em segredo em detrimento do sistema tradicional de propriedade intelectual, especialmente em razão da fluidez, flexibilidade e rapidez do ambiente de inovação em que as empresas funcionam atualmente.

Assim, a pergunta que orienta essa pesquisa é a seguinte: como as empresas podem se valer de uma posição jurídica para evitar a fuga do conhecimento e garantir a exploração dessa vantagem competitiva?

Procurando responder à pergunta de pesquisa que norteia este estudo, foi definido como objetivo geral compreender o uso do segredo como mecanismo de proteção do conhecimento empresarial. Na busca do objetivo geral, foram definidos como objetivos específicos: a) compreender a proteção de uma posição jurídica sob a perspectiva concorrencial e a modalidade do segredo empresarial na legislação brasileira; b) analisar a opção do segredo como ferramenta de proteção; c) apontar mecanismos de proteção quando da opção pelo segredo empresarial.

Para atingir os propósitos definidos, a pesquisa será conduzida por meio de pesquisa bibliográfica (livros e artigos científicos do campo do Direito) e documental (legislação, regulamentos nacionais e internacionais, jurisprudências, memoriais, pesquisas, reportagens, dentre outros), com abordagem qualitativa, de natureza aplicada e objetivo exploratório.

## 2 PROPRIEDADE INTELECTUAL: DIREITO DE EXPLORAÇÃO EXCLUSIVA E TEMPORÁRIA SOB BENS IMATERIAIS E POSIÇÃO JURÍDICA

Juridicamente, a concepção patrimonial exclusivista sob a expressão humana se consubstanciou em duas espécies: o Direito Autoral e a Propriedade Industrial. A primeira espécie "[...] sobreleva a originalidade como fator determinante à apropriação de representações simbólicas de condão literário, artístico e científico" (ARRABAL, 2018, p. 32). Por outro lado, a segunda, tem o condão de conferir "legitimidade monopolística sobre novas soluções técnicas – a Propriedade Industrial" (ARRABAL, 2018, p. 32).

No arcabouço legislativo da propriedade intelectual também são encontradas legislações específicas sobre determinado bem jurídico protegido, chamadas de "sui generis". Trata-se de uma categoria do direito de propriedade intelectual que possui figuras jurídicas intermediárias entre a propriedade industrial e o Direito Autoral, e que possuem legislações próprias, envolvendo a topografia de circuito integrado, a cultivar bem como os conhecimentos tradicionais e o acesso ao patrimônio genético, sendo cada tipo de proteção regulamentada por legislação própria.

As formas tradicionais de proteção da propriedade intelectual são reduzidas aos bens protegidos, legalmente previstos nas legislações de Direito Autoral (Lei 9610/98), de Propriedade Industrial (Lei 9279/96), Programa de Computador (Lei 9609/98), Cultivares (Lei 9456/97), Topografia de Circuito Integrado (Lei 11484/2007), e Conhecimento Tradicional e Patrimônio Genético (Lei 13123).

Para além do exercício classificatório da propriedade intelectual através dos bens protegidos, é preciso conhecer sua perspectiva desenvolvimentista e econômica consistente no direito de exclusiva sobre bens imateriais.

O detentor de bens incorpóreos "em princípio, pode assegurar sua exclusividade de fato. Só uma restrição de direito assegura a apropriação". (BARBOSA, 2010, p. 28). O mecanismo que concede a exclusividade sobre um invento, obra literária ou posição de mercado se dá pela propriedade industrial ou propriedade literária. "A exclusividade jurídica da utilização de um bem imaterial, idéia, forma, ou posição no mercado dão uma mínima certeza de que se terá a vantagem econômica da escassez" (BARBOSA, 2010, p. 29). A propriedade intelectual, portanto, cria uma ficção jurídica que torna um bem imaterial, em termos econômicos, rival e exclusivo (direitos de exclusiva), sendo que apenas seus titulares podem usar, gozar, fruir e dispor desses bens perante o mercado, gerando a ideia de escassez.

Sob a perspectiva concorrencial, essa concepção vai além dos direitos exclusivos, pois há a tutela de posições jurídicas que não são exclusivas, na medida que os agentes econômicos concorrentes podem "[...] deter oportunidade total ou parcialmente idênticas sem que o Direito exclua qualquer deles do uso lícito do item em questão." (BARBOSA, 2010, p. 31). A título exemplificativo, Denis Barbosa (2010, p. 31) aponta uma situação:

> Isso acontece, por exemplo, quando uma empresa tem um conhecimento técnico não patenteado, que não seja livremente acessível; saber fazer um pudim de pão que algum seu concorrente não saiba (embora outros restaurantes tenham o mesmo pudim no cardápio) dá ao que sabe uma oportunidade vantajosa na competição perante o que não sabe fazer o doce, e a possibilidade de pelo menos empatar com os demais, que sabem fazer o mesmo pudim que o primeiro. Não há nesse caso um direito de exclusividade. O que pode haver, conforme a situação fática, é a garantia de um comportamento leal na concorrência. Não posso evitar que o concorrente que não saiba fazer o pudim, um dia aprenda pelo ensaio e erro, e empate comigo na oportunidade de mercado. O que posso impedir é que ela aprenda por um método desleal, por exemplo, subornando meu chef para conseguir a receita do pudim. Não tenho exclusividade, mas tenho uma garantia jurídica de um comportamento conforme ao que esperado no mercado.

Seguindo a linha de raciocínio e a título exemplificativo, o desenvolvimento de um modelo de negócio inovador e sua inserção no mercado não garante exclusividade sobre ele. Isso porque, não há proteção do modelo de negócio pelas ferramentas tradicionais de propriedade intelectual. Basta observar o exemplo da Uber , uma plataforma de mobilidade urbana que revolucionou o mercado de transporte com seu modelo de negócio. Na sequência, outras empresas surgiram oferecendo o mesmo modelo de negócio aos consumidores (como a 99 , Cabify , Lift ), sem que isso ofendesse propriedade da pioneira Uber.

Por outro lado, caso um colaborador da Uber quebrasse o sigilo de melhorias sendo desenvolvidas no aplicativo e repassasse tais informações aos concorrentes, estaríamos diante de um comportamento desleal que retirou a vantagem que a Uber detinha perante os demais. Portanto, não há um direito de exclusiva, mas uma situação em que determinada posição, que gera vantagem competitiva, é deslealmente prejudicada por seus concorrentes.

Alguns fenômenos, portanto, apesar de não encontrarem proteção enquanto direito de exclusiva, expressam situações de fato em que a posição de uma empresa que detém conhecimentos, técnicos ou não, lhe dão vantagem competitiva no mercado. Não há, portanto, propriedade, mas "oponibilidade relativa e condicional que deriva das regras de concorrência leal" (BARBOSA, 2010, p.63). Da mesma forma, José Manuel Otero Lastres (WIPO, 2019) afirma que esse tipo de conhecimento empresarial é protegido com base em condutas e não por direitos de exclusividade.

Dentro dessa perspectiva, informações dotadas de valor competitivo num determinado mercado, estão acobertadas pela noção dos objetos de Propriedade Intelectual, dentre elas, a modalidade de segredo empresarial.

## 2.1 Segredo Empresarial

No Brasil, o segredo, por si só, reflete uma vastidão de significados. Sob a perspectiva jurídica, da mesma forma, consegue ser tratado em diversos diplomas legais[5]. Para a finalidade dessa pesquisa, o segredo receberá atenção em situações de uso empresarial[6] que o direito exigir sua manutenção em razão de uma finalidade econômica, sob o regime da repressão à concorrência desleal. Por essa razão, a análise do conceito do segredo se alicerça no artigo 195 da Lei 9279/96, o qual apresenta regras aplicáveis ao sigilo.

> Art. 195. Comete crime de concorrência desleal quem:
>
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
>
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude;

Cometido o ato de divulgar, explorar ou utilizar-se de um conhecimento, informação ou dados confidenciais, há a caracterização do crime de concorrência desleal (art. 195, Lei 9279/96). Segundo Denis Barbosa (2017, p. 372), o ato de divulgar compreende "o episódio de lançar a informação em disponibilidade pública, reduzindo ou eliminando a vantagem concorrencial, como o repassar a terceiros, especialmente a concorrentes, eliminando a vantagem em face do receptor"; o ato de explorar designa o uso das informações em proveito próprio de forma lesiva à concorrência. Ainda, os verbos que compõem a tipologia do delito requerem a ausência de autorização ou o excesso de uma autorização limitada do titular.

Segundo Davi Monteiro Diniz (2003, p. 141), para a compreensão do sigilo, três

[5] No Direito Privado, por exemplo, encontra guarida no art. 229 do Código Civil (sigilo em razão do estado ou profissão); art. 157 da Lei 6404/76 (direito ao sigilo dos administradores de sociedades anônimas); art. 482, "g" da Consolidação das Leis do Trabalho – CLT (violação de segredo de empresa pelo empregado). No Direito Público, por exemplo, o art. 198 do Código Tributário Nacional - CTN (vedação de divulgação de informação do sujeito passivo ou de terceiros); art. 325 do Código Penal – CP (violação de sigilo funcional).

[6] Relativo à empresa (organização).

faces da sua composição devem ser avaliadas: “quais as informações a que ele se refere, os sujeitos que podem ocupar os polos da relação jurídica que disciplina e o alcance dos direitos e obrigações correspondentes”.

No tocante a informação, decorre da lei (LPI) que ela não deve ser de conhecimento público, nem evidente para pessoas com formação técnica na área do conhecimento a que o sigilo diz respeito. A obrigação de sigilo forma-se por um negócio bilateral ou por obrigação decorrente de lei, tem como receptor (sujeito passivo) qualquer pessoa que tenha acesso à informação e tome conhecimento do seu status de sigilosa, e como comunicador (sujeito ativo) qualquer pessoa que detenha a informação. Assim como os sujeitos, o alcance do direito também decorre da Lei 9279/96. As informações sigilosas não podem ser divulgadas, exploradas ou utilizadas sem autorização, sob pena de caracterizar um ilícito penal e/ou civil. Inclusive, a proteção do sigilo garante ao titular da informação não somente a repressão pela divulgação ilícita do segredo, mas também a faculdade de impedir o prosseguimento de sua utilização ilegal. (DINIZ, 2003).

Observa-se que na perspectiva de Davi Monteiro Diniz, a informação que compõem o sigilo e sua proteção é avaliada a partir do elemento de exclusão legal, ou seja, a partir do que a lei aponta como não sendo um segredo (não é sigiloso aquilo que é de conhecimento público ou evidente para pessoas com formação técnica na área do conhecimento). Referida informação pode designar elementos de características distintas dentro da empresa, o que acaba por originar nomenclaturas diversas para o segredo.

Seguindo a classificação de José Antônio Gómez Segade (1974) quando utilizada a nomenclatura segredo de fábrica ou industrial, diz respeito ao setor técnico-industrial da empresa que está sendo objeto de segredo; quando relativa aos aspectos comerciais ou negociais, a informação será designada como segredo comercial ou de negócio; ao passo que, quando não representar um caráter industrial/fabril ou comercial/negocial, mas se traduzir em um conhecimento valioso para os competidores, estaremos diante de um Know-How ou informação confidencial pura, essa última é aquela que não pode ser negociada, tal como a situação financeira de uma empresa, mas que importa em uma vantagem deter seu conhecimento.

As nomenclaturas são essenciais para a organização e gestão do conhecimento dentro de uma empresa, mas a natureza da informação é indiferente para sua proteção. Basta que a informação “possa assegurar ao seu titular uma vantagem competitiva dentro do seu

mercado ou afetar, por qualquer meio, a posição relativa de seu titular dentro do seu mercado" (LEONARDOS, 1997, p. 75).

James Pooley (2015) compartilha uma visão extremamente objetiva sobre o tema, simplificando as coisas para os empresários. Para ele, todas as nomenclaturas utilizadas (segredo comercial, informação confidencial, dentre outras) se referem a mesma coisa: aquilo que você não quer que a competição saiba. Tecnicamente, é qualquer informação que dê a empresa uma vantagem competitiva, que não seja de conhecimento público, e que a empresa tenha tomado providências razoáveis para proteger referido conhecimento.

Assim, a vantagem competitiva, sigilosa, pode estar relacionada a uma informação técnica que poderia ser patenteada, mas não foi por opção do titular; a elementos internos e estratégicos da empresa não cobertas pelo sistema de proteção às tecnologias; ao conjunto de conhecimentos e experiências; a informações confidenciais (proteção da informação). Em todas essas hipóteses inexiste um direito de propriedade como se tem nas patentes, marcas e desenho industrial; o segredo deve ser respeitado por quem tem acesso a ele em vista de uma lealdade empresarial.

## 3 A OPÇÃO PELO SEGREDO COMO MECANISMO DE PROTEÇÃO DO CONHECIMENTO EMPRESARIAL

No mercado globalizado, caracterizado pela extrema competitividade, os ativos intangíveis são capazes de proporcionar vantagem para todos os tipos de empresas e setores econômicos (EUIPO, 2018). Por esse motivo, as estratégias relacionadas com propriedade intelectual têm tomado importância e crescido dentro das empresas (CIURIAK; PTASHKINA, 2021). Contudo, ao inovar, nem sempre o resultado preenche os requisitos para que o titular tenha exclusividade de exploração do bem imaterial, o que faz com que o segredo se torne uma ferramenta para que as companhias possam proteger o conhecimento empresarial. O mesmo pode ser dito quando empresas, apesar de desenvolverem criações que poderiam ser protegidas, preferem não tornar suas inovações públicas, ou ainda para startups que não possuem recursos financeiros para os procedimentos de registro (EUIPO, 2018).

O fato é que o segredo empresarial se tornou uma ferramenta atrativa para empresas no nível prático, uma vez que cobre praticamente qualquer tipo de informação com valor

econômico, tem duração indeterminada, é flexível no sentido da desnecessidade de modificações para assegurar inovações incrementais, e pode ser invocado sempre que estiver abordado em contratos e medidas internas de segurança (CIURIAK; PTASHKINA, 2021).

Mark Schultz (WIPO, 2022a) afirma que na última década o segredo tem se tornado de extrema importância nos EUA, e dentre os motivos desse movimento, o primeiro diz respeito ao aumento do valor dos bens intangíveis, o segundo está calcado no fato de que o segredo tem sido considerado a estratégia mais importante de propriedade intelectual, especialmente por ser mais prático.

A explicação para o crescimento do uso do segredo, segundo James Pooley (2015, p. 19), pode ser vista sobre diversas perspectivas, dentre elas a adoção do modelo de inovação colaborativo entre empresas e o próprio cenário atual de modelos de redes globais de fornecimento e distribuição.

> Aqui está o resultado final: os negócios modernos são cada vez mais feitos por meio de colaborações globais, onde informações valiosas precisam ser compartilhadas e a eficiência da cadeia de suprimentos é otimizada. O bom gerenciamento de segredos comerciais permite que você garanta o benefício e controle os riscos inerentes a esse ambiente e tome decisões inteligentes sobre como implantar seus ativos mais importantes. (tradução livre)7.

Para Elisabeth Kasznar Fekete (WIPO, 2019), o segredo é uma opção em situações particulares, como inovações em estágios iniciais ou quando a inovação não pode ser patenteada ou protegida por outra ferramenta formal de propriedade intelectual, tal como um processo biológico, ideias abstratas, procedimentos de negócios, métodos e planos. Segundo Kappos (WIPO, 2019), o novo ambiente de inovação faz com que as companhias se utilizem tanto do sistema de patentes quanto da opção pelo segredo, sustentando sua afirmação no fato de que recentes estudos mostram o crescente uso do modelo de colaboração entre empresas para promover a inovação, que se sustentam no segredo empresarial, especialmente quando as companhias estão distantes geograficamente.

De acordo com Lena Pauschenwein (WIPO, 2022a), o aumento da competitividade pela inovação está crescendo mais dependente de bens intangíveis tal como o *know-how* e o *trade secret*, e essas ferramentas são utilizadas não apenas quando a propriedade intelectual de exclusivos é insuficiente, mas como uma estratégia de proteção, inclusive para pequenos negócios, especialmente para ambientes de inovação colaborativos.

[7] Here´s the bottom line: modern business is increasingly done through global collaborations, where valuable information has to be shared, and supply chain efficiency is optimized. Good trade secret management allows you to secure the benefit and control the risks inherent in this environment, and to make intelligent decisions about how do deploy your most important assets.

Assim como pontuado por Lena Pauschenwein, o destaque para o uso do segredo empresarial como ferramenta de proteção do conhecimento na atualidade não é apenas privilégio de grandes empresas. Muthu de Silva (WIPO, 2022c) indica que é uma opção bastante utilizada por médias e pequenas empresas e compartilha os resultados de sua pesquisa onde constata que: (a) o uso do segredo é mais popular entre as PMEs quando se referem a dados, processo e conhecimento tecnológico, e conhecimento negocial; (b) os conhecimentos gravados como segredo, mais compartilhados pelas PMEs se referem ao conhecimento dos colaboradores (habilidades, experiências etc) e informações relacionadas a produtos, tecnologias e P&D; (c) os segredos menos compartilhados são referentes a dados sobre informação negocial, conhecimento de mercado, fórmulas e software.

Outro motivo de destaque para o uso do segredo, mas que exige profunda discussão, é o fato da inexistência de fronteiras, ou seja, diferente dos direitos de exclusiva protegidos pela propriedade intelectual, o segredo não é territorial, o que, em uma economia global, faz com que as companhias inclinem suas estratégias para essa escolha (James Pooley, WIPO, 2022b).

No entanto, o uso do segredo, apesar de crescente, é desafiador na medida em que sua proteção se torna cada vez mais difícil na era digital. Por exemplo, empregados poderiam sair das empresas com inúmeros documentos salvos em um USB, um pesquisador poderia compartilhar dados da pesquisa com apenas um clique no mouse e dispersar todo o conhecimento produzido (WIPO, 2019), documentos estratégicos arquivados em nuvem poderiam ser acessados por invasores externos, assim como câmeras internas que registram o dia a dia dos colaboradores poderiam ser acessadas e indicar ferramentas e procedimentos utilizados, dentre inúmeras outras situações. Assim, manter o segredo também é um risco. De acordo com Pallavi Steh (WIPO, 2019, p. 11) "segredos comerciais são compartilhados com funcionários e parceiros comerciais, eles podem ser submetidos a engenharia reversa e descobertos de forma independente. O custo para manter essa proteção é alto e segredos comerciais podem dificultar a mobilidade da mão de obra"[8].

A dificuldade em gerir o segredo, potencializada pela era digital, chega a ser contraditória na medida em que os mesmos fatores que levam as empresas a utilizarem o segredo como ferramenta de proteção são fatores que tornam essa escolha arriscada, como a colaboração para inovação, utilização de redes de fornecimento e distribuição globais, a própria

[8] Tradução livre de "trade secrets are shared with employees and commercial partners, they can be reverse engineered and discovered independently. The cost to maintain this protection is high, and trade secrets could hinder labor mobility ".

evolução da internet e as possibilidades de uso das informações (Big Data, Internet das Coisas, dentre outras), o uso de dispositivos móveis (Laptops e Smartphones) etc. A título exemplificativo, Pooley (2015) compartilha a experiência de uma empresa atuante na área climática, situada em San Francisco, que usou a "big data" em seu benefício ao analisar dados estatísticos públicos sobre o clima/tempo disponíveis publicamente e, por meio de um software proprietário, passou a vender conselhos para agricultores com base nesse conhecimento gerado. Segundo o autor (2015, p. 19), "a empresa foi recentemente adquirida por um bilhão de dólares. Em que se baseia essa nova riqueza? É o algoritmo secreto para transformar todas essas informações de dados, e as próprias informações, que são protegidas por segredo"[9]. No entanto, apesar dessas possibilidades quase que ilimitadas, é de fundamental atenção que a empresa assegure toda essa informação, já que os riscos de um ataque cibernético são grandes.

Portanto, para proteger o conhecimento empresarial por meio do segredo, é necessário uma estratégia interna sólida e boas práticas. Empresas que se utilizam do Segredo, como Space X , Xenometrix , Ycorp Corp´s , e Zheijang Weixing New Building Materials , compartilham suas estratégias: acordos de confidencialidade com sócios, empregados e terceiros; a existência de uma equipe de tecnologia da informação (TI) comprometida, com ferramentas de monitoramento dos dados e mecanismos efetivos de proteção da informação (criptografia); que as equipes sejam orientadas sobre o segredo e sua importância, no sentido de impedir, por exemplo, que fotos sejam tiradas em ambientes restritos e publicadas em redes sociais , criando, portanto, uma cultura de respeito da confidencialidade da empresa e de terceiros; desenvolver orientações/políticas internas que ensinam e indicam como o segredo é tratado na companhia; utilizar o conceito de "need to know", ou seja, identificar efetivamente quem precisa ter acesso ao conhecimento (WIPO, 2019).

Assim, o segredo é um mecanismo utilizado como forma de proteger o conhecimento empresarial não abrangido por direito de exclusiva, mas que dá vantagem competitiva pelo seu valor econômico. No entanto, para que a proteção seja efetiva, algumas ferramentas precisam ser desenvolvidas por quem opta pelo uso do segredo.

[9] Tradução livre de "the company was recently purchased for a billion dollars. What tis that new wealth based on? It´s the secret algorithm for turning all of that data information, and the information itself, which is protected by secrecy".

## 4 A PROTEÇÃO DO SEGREDO EMPRESARIAL

Tanto para HALLIGAN, R. M. e WEYAND, R.F (2016), quanto para SPRANKLING, J.G. e SPRANKLING, T. G (2020), como para POOLEY, J. (2015) para que o conhecimento empresarial não amparado por direito de exclusiva, mas que gera vantagem competitiva, esteja protegido por segredo é indispensável compreender o conceito do instituto.

Segundo John G. Sprankling e Thomas G. Sprankling (2020), o segredo empresarial está fundamentado na preservação da moralidade comercial e no encorajamento da inovação quando não existem mecanismos de proteção, sendo a livre concorrência e a liberdade do empregado os limites do amparo legal. Com essas premissas, o conceito por eles apresentado está baseado na Uniform Trade Secret Act (UTSA) e Defend Trade Secret Act (DTSA), nos quais o segredo empresarial significa a informação que tenha valor econômico atual ou potencial, não seja de conhecimento geral e não seja razoavelmente determinável por meios adequados por outras pessoas que possam obter valor econômico de sua divulgação ou uso, e tenha existido esforços razoáveis pelo titular para manter a informação em segredo.

Ocorre que, os autores indicam que o conceito trazido acima deve ser desmembrado a fim de um melhor entendimento sobre o que as legislações querem dizer ao se referirem com: i) informação; ii) valor econômico independente da informação; iii) não ser de conhecimento geral e não ser determinável por meios adequados; iv) esforços razoáveis.

No tocante à informação, a UTSA e DTSA trazem compreensão distintas. Enquanto a UTSA indica que as informações se referem a fórmula, padronizações, compilações, programas, dispositivos, métodos, técnicas ou processos, que o titular tenha eivado esforços para manter em segredo e a informação tenha valor econômico; a DTSA é um pouco mais limitada, na medida em que indica que as informações se referem a formulários e tipos de informações financeiras, negocial, científica, técnica, econômica ou de engenharia, incluindo padronizações, planos, compilações, dispositivos de programa, formulas, designs, protótipos, métodos, técnicas, processos, procedimentos, programas, códigos, tangíveis ou intangíveis, independente da forma de armazenamento, que o titular tenha eivado esforços para manter em segredo e desde que a informação tenha valor econômico.

A limitação trazida pela DTSA em comparação com a UTSA se refere ao tipo de informação protegida. Na UTSA o tipo de informação não é delimitado, ou seja, abrange toda e qualquer informação, desde que os demais requisitos estejam presentes. Na DTSA, os tipos

de informações protegidas seriam apenas aquelas financeiras, negociais, científicas, técnicas, econômicas ou de engenharia (uma informação de marketing, por exemplo, não encontraria respaldo).

Ainda, para os autores, existem informações que dão vantagem competitiva, mas não preenchem todas as características do segredo empresarial, sendo que nesses casos a informação é considerada proprietária e a proteção se dá exclusivamente por meio de contratos. (SPRANKLING; SPRANKLING, 2020).

No tocante ao valor econômico independente, significa que a informação também precisa ser de valia para terceiros além do seu titular. Ou seja, se a informação estiver em poder de outros competidores no mercado eles ganharão vantagem competitiva ou retirarão a vantagem competitiva do titular originário.

Sobre o requisito "não ser de conhecimento geral e não ser determinável por meios adequados" os autores John G. Sprankling e Thomas G. Sprankling (2020) compartilham que dizer que uma informação é de conhecimento geral significa que outras pessoas possuem acesso àquela mesma informação, de maneira que a informação secreta deve ser diferente do que se conhece. Na prática, provar que uma informação não é de conhecimento geral e por isso protegida por segredo empresarial, segundo os autores, pode se dar por meio da demonstração dos gastos que a empresa teve para desenvolver aquela informação, a extensão das medidas tomadas pela empresa para manter a informação em segredo, além de outros pontos levados em consideração pelos tribunais estadunidenses como declarações de experts no assunto sobre a novidade, a vontade de terceiros em adquirir a informação, o uso de meios impróprios por terceiros para conseguir a informação, e a existência do pedido ou preparo de patente (se for o caso) baseado na informação.

No tocante a determinação, a informação secreta não pode ser facilmente encontrada por meios (adequados) como a invenção independente, engenharia reversa, descoberta em razão de uma licença, observação de uso ou obtida por meio da literatura. Nessas hipóteses, a informação não está protegida. (SPRANKLING; SPRANKLING, 2020).

Adiante, demonstrar a existência de esforços razoáveis praticados pelo titular da informação para evitar a fuga desse conhecimento é desafiador e depende do caso concreto. No entanto, John G. Sprankling e Thomas G. Sprankling (2020) apontam dois elementos que geralmente são considerados como indicativos da proteção: medidas de segurança e procedimentos de confidencialidade.

No que diz respeito as medidas de segurança, os autores trazem alguns exemplos, como senhas, criptografia de dados, cofres para documentos secretos, barreiras, guardas, protocolos de lixo, vigilância por vídeos. No tocante aos procedimentos de confidencialidade, os exemplos são acordos de confidencialidade, marcas em documentos, manuais para os empregados, orientações para os empregados desligados, políticas internas, restrições de acesso a documentos. (PRANKLING; SPRANKLING, 2020).

James Pooley (2015), ao tratar do conceito de segredo empresarial, procura trazer uma linguagem mais acessível ao ambiente empresarial e, genericamente, aponta que o segredo empresarial se refere a tudo aquilo que o titular não queira que seus competidores saibam. Contudo, em complemento técnico, o autor indica que a proteção está nas informações que dão vantagem competitiva ao negócio, que não seja de conhecimento geral e que tenha sido objeto de esforços do titular para manter a informação protegida. Na sua linha de raciocínio, as diferenças trazidas entre a UTSA e DTSA no tocante ao tipo de informação são meramente exemplificativas, de forma que todas as informações, incluindo as denominações know-how, informação confidencial e dados proprietários, podem designar segredos de uma companhia na modernidade, em que pese decisões em sentido contrário.

Para Pooley (2015), existem duas categorias de informações protegidas: i) tecnológica; ii) negocial. A primeira (tecnológica) diz respeito a informações sobre máquinas, design, fórmula, técnica de manufatura, método negocial (como um processo de transações na internet), etc. A segunda diz respeito a lista de clientes, planos de marketing, estudos de competitividade, relatórios financeiros, uma oferta negociada, entre outros.

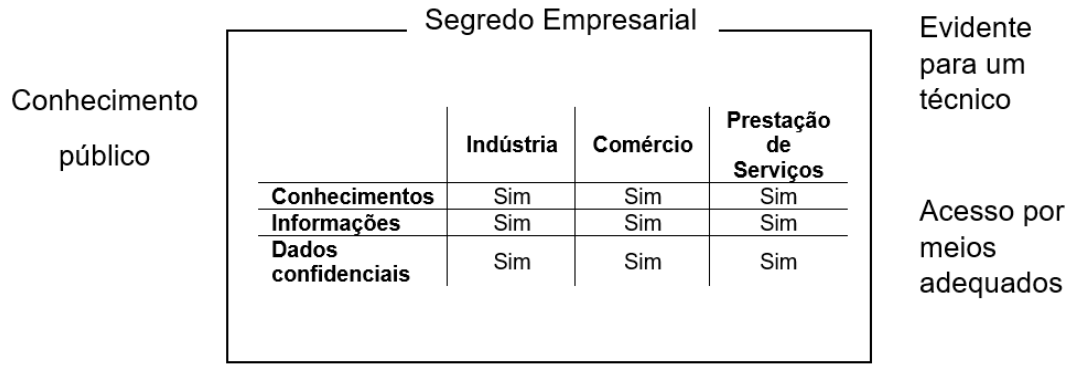
Assim, seguindo Pooley (2015), não estariam protegidos como segredo empresarial aquilo que advém da habilidade individual de determinada pessoa, informações que são de conhecimento geral, e aquelas informações facilmente determináveis (que qualquer pessoa pode criar ou ter acesso com o mínimo esforço ou por meios adequados como, por exemplo, a engenharia reversa).

Para os autores R. Mark Halligan e Richard F. Weyand (2016), o segredo empresarial se constitui em um bem intangível, gênero de propriedade intelectual, e se refere a informação que é valiosa por não ser de conhecimento comum e que o titular tenha eivado esforços razoáveis para protegê-la. Ou seja, o segredo empresarial é um bem porque traz vantagem competitiva ao negócio, só é protegido se mantido em segredo, e o seu titular deve tomar medidas para que essas informações permaneçam em segredo.

Alguns exemplos são referenciados pelos autores, a saber: a) o segredo empresarial pode existir no campo da P&D, engenharia, e pode incluir: resultados de testes laboratoriais, protótipos de equipamentos, design de produtos etc.; b) na área de marketing: resultados de pesquisas, planos para propagandas, estrutura de desconto, análise de mercado etc.; c) na área de vendas: informações de contato de consumidores e fornecedores, dentre outras. (HALLIGAN; WEYAND, 2016).

Já na legislação brasileira optou-se por tratar do segredo empresarial na Lei de Propriedade Industrial (LPI), em seu artigo 195, como repressão à concorrência desleal. Depreende-se do texto legal que o termo "segredo" não é indicado, mas sim os termos "conhecimentos, informações ou dados confidenciais", sendo que esses dados podem ser da indústria, comércio ou prestação de serviços, exceto aqueles de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato. Dessa forma, para a legislação brasileira:

Tabela 1: O que é protegido pelo segredo empresarial na legislação brasileira




Fonte: elaborado pelos autores.

Inexiste na legislação supramencionada orientações como aquelas vistas na legislação americana: a) a necessidade de esforços razoáveis para manter a informação em segredo; e b) que a informação seja valiosa e dê vantagem competitiva para o titular ou seu detentor.

Contudo, o TRIPS[10], ao qual o Brasil aderiu em 1994, em seu artigo 39, orienta que

[10] TRIPS - Trade-Related Aspects of Intellectual Property Rights. Promulgada no Brasil pelo Decreto 1355 de 30 de dezembro de 1994. "SEÇÃO 7: PROTEÇÃO DE INFORMAÇÃO CONFIDENCIAL. ARTIGO 39. 1. Ao

as informações serão protegidas desde que cumpram alguns requisitos: seja secreta, tenha valor comercial por ser secreta e tenha se submetido a medidas razoáveis de proteção desse segredo. (TRIPS, 1994).

Segundo Rossi (2014), as diferenças entre as definições trazidas pela LPI e pelo TRIPS residem no fato de que a noção de segredo abrange a existência de meios e intenção de manter a informação sigilosa por meio de condutas exteriorizadas, e ainda que os tratados internacionais tenham aplicação direta quando aderidos pelo Brasil, no caso do TRIPS, nos termos da jurisprudência do STJ (Resp nº 642.213), a adesão não se aplica diretamente aos cidadãos. Isso quer dizer que, os requisitos excedentes previstos pelo TRIPS não seriam exigíveis aos casos brasileiros. Contudo, Rossi desenvolve esse raciocínio (2018, p. 29):

> Ainda que os tratados internacionais tenham, no Brasil, a princípio, aplicação direta, conforme a jurisprudência do Supremo Tribunal Federal (STF) (ADI-MC n. 1.480 e ArCR n. 8.279) (STF, 1998, 2002), o Acordo TRIPS, nos termos da jurisprudência do Superior Tribunal de Justiça – STJ (Resp n. 642.213) não constitui uma Lei Uniforme e não vincula diretamente os cidadãos (apesar de o alcance dessa afirmação não ter ficado claro).2 O Acordo TRIPS 39(2)(c), por outro lado, ao definir segredo empresarial, não cria obrigações, mas simplesmente estabelece um conceito de forma incondicionada e suficientemente precisa, sem que qualquer outra medida legislativa seja necessária a que tenha aplicação pelos tribunais e sem que pudesse ser implementada de outro modo sem que isso violasse disposição do tratado. A jurisprudência do STF ressalva a possibilidade de dar aplicação a norma produzida pela legislatura em conflito com disposição de tratado, segundo o critério do lex specialis ou lex posterior (vide ADI-MC n. 1.480 e ArCR n. 8.279). Pode-se argumentar que o Acordo TRIPS, por ser anterior à Lei de Patentes, seria derrogado por esta e o terceiro requisito ou teste não seria exigível para caracterização do segredo empresarial, no Brasil. Não parece ser esse o caso, pois a lei brasileira não define precisamente segredo empresarial. O conceito se infere de uma conduta penalmente proibida, mais restrita — especial, portanto — em relação à definição geral do Acordo TRIPS. Se uma conduta é penalmente proibida, é certamente civilmente ilícita, considerado o art. 927, do Código Civil, mas uma conduta civilmente ilícita não se torna penalmente proibida pelo simples fato, considerado o art. 5.º, XXXIX, da Constituição. Os âmbitos de aplicação das normas são diversos, de modo que a antinomia é apenas aparente. A seguir-se a lógica dos precedentes indicados, deve ser considerado então legislação aplicável no Brasil e serve de guia à identificação objetiva de informações confidenciais, mesmo na ausência de obrigações expressamente consentidas. Não há, entretanto, precedentes nos tribunais brasileiros sobre a questão.

Dias, Sant´Anna e Santos (2016, p. 5), ao tratarem sobre os diferentes aspectos do

assegurar proteção efetiva contra competição desleal, como disposto no ARTIGO 10bis da Convenção de Paris (1967), os Membros protegerão informação confidencial de acordo com o parágrafo 2 abaixo, e informação submetida a Governos ou a Agências Governamentais, de acordo com o parágrafo 3 abaixo. 2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação: a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes; b) tenha valor comercial por ser secreta; e c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.

*trade secret* e do know-how, salientam o fato da presença do elemento "segredo" e da exigência das evidências da condução de esforços para manter a informação sigilosa no caso da proteção pelo segredo empresarial:

> Os segredos empresariais possuem ainda um elemento distintivo, que é o recurso de sigilo em um sentido objetivo. Essa característica determina a exigência do titular de evidenciar uma conduta ativa e razoável para manter o conhecimento sigiloso a terceiros não autorizados. Nessa questão, surge outra diferença: enquanto o know-how tem por finalidade permitir o uso e a exploração da tecnologia ou a realização de uma tarefa específica de forma eficiente, o segredo comercial busca manter a informação fora do alcance de pessoas não autorizadas e concorrentes indesejáveis. (tradução livre)[11]

Portanto, vê-se que o uso dos requisitos previstos no TRIPS também é usado para interpretação da diferenciação entre institutos, o que fortalece o indicativo de que a legislação é aplicável em âmbito nacional.

Assim, por meio das conceituações legais trazidas somado a análise do tratado internacional aderido pelo país (TRIPS), é possível concluir que no Brasil, o segredo empresarial protege as informações (sejam conhecimentos, dados ou outros) que tenham por característica o segredo (sejam secretas); por serem secretas, concedam ao titular alguma vantagem competitiva; que essas informações tenham sido objeto de esforços para se manterem em segredo; que sejam informações fora do domínio público (conhecimento geral); que a informação não seja evidente (facilmente determinável); e que o acesso a ela não tenha se dado por meios adequados.

Tabela 2: Definição de segredo empresarial aplicável

| **SEGREDO EMPRESARIAL**<br>(informação, conhecimento, dados; em conjunto apenas "informação") | |
|---|---|
| **REQUISITOS DE PROTEÇÃO** | **NÃO PROTEGIDO** |
| Ser confidencial | Conhecimento geral (domínio público) |
| Concedam vantagem competitiva | Seja evidente – facilmente determinável |
| Sejam eivados esforços para manter a informação, conhecimento e/ou dados em | Acessado por meios adequados – lícitos (ex: relação de trabalho, engenharia reversa, |

[11] Trade secrets hold further a distinguishing element, which is the secrecy feature in an objective sense. This characteristic determines the requirement of the holder to evidence an active and reasonable conduct to keep knowledge undisclosed to unauthorized third parties. In this matter, another difference arises: while the purpose of know-how is to permit the use and exploitation of the technology or the undertaking of a specific task efficiently, trade secret seeks to maintain the information out of reach of unauthorized parties and undesirable competitors.

| | |
|---|---|
| segredo | observação de uso, obtido por meio da literatura etc.) |

Fonte: elaborado pelos autores.

A delimitação do conceito do segredo empresarial fornece os critérios que precisam ser avaliados internamente no âmbito empresarial para identificação dos ativos intangíveis protegidos pelo instituto. É com base nessa delimitação, portanto, que os mecanismos de proteção podem ser desenvolvidos.

### 4.1 Mecanismos de proteção do segredo empresarial

O conceito de segredo empresarial indica o que pode estar protegido e o que está excluído da proteção conferida pelo instituto. Ainda, dá conta de indicar os elementos que precisam estar presentes em complementaridade à informação protegida, por exemplo, a informação relacionada à indústria pode estar protegida desde que seja confidencial, dê vantagem competitiva, e tenham sido eivados esforços para mantê-la em segredo.

Para John G. Sprankling e Thomas G. Sprankling (2020), a proteção do segredo empresarial pode ser efetivada através da criação de medidas de segurança físicas (exemplos: senhas, criptografia de dados, cofres para os documentos, barreiras, guardas, protocolos de lixo, vigilância por vídeo) e procedimentos de confidencialidade (exemplos: acordos de confidencialidade, marcas em documentos, manuais para os empregados, orientações para os empregados desligados, políticas internas, restrições de acesso a documentos).

Além disso, ao tratarem sobre as características do segredo empresarial, especificamente sobre a necessidade de não ser de conhecimento geral, os autores indicam meios de se provar que a informação não está no domínio público. Dentre essas medidas, está a comprovação do investimento financeiro no desenvolvimento da informação, de forma que manter esses dados registrados pode ser considerado um mecanismo de proteção. (SPRANKLING; SPRANKLING, 2020).

John G. Sprankling e Thomas G. Sprankling (2020), apontam um estudo que demonstra que 77% (setenta e sete por cento) dos casos de apropriação indevida de segredo empresarial ocorre em virtude da relação de trabalho. Por essa razão, os autores propõem que as empresas devem concentrar seus esforços na criação de mecanismos de proteção do segredo em torno dessa relação empregado – empregador. Dentre os meios de se proteger, a sugestão

dos autores é de que o detentor do segredo empresarial deve se valer dos seguintes contratos (acordos): i) acordo de não divulgação (confidencialidade); ii) acordo de não competição (não concorrência); iii) acordo de não solicitação.

No acordo de não divulgação (i) o colaborador concorda em não divulgar e não usar informações confidenciais. Nesse documento é essencial esclarecer o escopo da informação protegida; relembrar os empregados dos seus deveres de sigilo; estabelecer quem é o dono da informação; evidenciar os esforços de manter o segredo. (SPRANKLING; SPRANKLING, 2020).

No acordo de não competição (ii) é previsto que o colaborador é proibido de trabalhar em competidores ou por si competir com o empregador ou ex-empregador; esse tipo de contrato, implicitamente, evita a comunicação de informações confidenciais. Nesses casos, as cortes estadunidenses têm entendido que o prazo de duração razoável da não competição é de 1(um) a 2(dois) anos; que deve haver uma limitação geográfica, com a exceção de casos em que a empresa opera pela internet; deve ser relacionado no documento as funções que o empregado exerce(exercia) e as que estão proibidas. (SPRANKLING; SPRANKLING, 2020).

No acordo de não solicitação (iii) haverá previsão de impedimento do funcionário (ex-funcionário) de buscar negócios com os clientes do empregador, aliciar funcionários (convidar funcionários para se juntar a ele), ou ambos. Nesse caso, as regras aplicáveis são as mesmas que no acordo de não competição. (SPRANKLING; SPRANKLING, 2020).

Para James Pooley (2015), criar mecanismos para proteger o segredo empresarial tem dois objetivos: i) prevenir problemas; ii) demonstrar os esforços realizados para a proteção do segredo. Assim, para o Autor a proteção vai além dos contratos, termos e autorizações, a orientação é criar um plano de proteção da informação, o qual deve seguir os seguintes princípios: i) a informação deve estar acessível apenas para quem precisa ter acesso à ela; ii) o plano de proteção precisa ser simples, principalmente ao categorizar a informação (privada, sensível, confidencial etc), pois sistemas complexos tendem a ser ignorados pelas pessoas; iii) é preciso se ter em mente que não é possível manter tudo em segredo o tempo todo, de forma que o importante é saber os procedimentos a serem adotados quando a informação for revelada e ter flexibilidade no plano implantado; iv) os maiores riscos são internos e não externos, o grande problema enfrentado pelas companhias está relacionado com seus empregados e não com ataques externos; v) a segurança da informação é apenas um mecanismo de gerenciamento de risco, de forma que o gerenciamento deve ser feito diretamente com as pessoas, por alguém encarregado dessa tarefa, competente para analisar e gerir riscos; vi) o programa deve ser

sempre reconsiderado a partir de três pontos: valor, risco e custo.

Com fulcro nessas bases, o plano de proteção deverá especificar: i) premissas de segurança; ii) classificação da informação; iii) processos de segurança; iv) contratos necessários; v) educação; vi) regras; vii) responsabilidades; viii) revisões constantes.

Seguindo os ensinamentos de Pooley (2015), para um modelo básico de proteção do segredo deve-se indicar uma pessoa que irá gerenciar o planejamento e identificar qual é o segredo – o que a empresa tem que é sensível e de valor? Além disso, o plano deve conter orientações sobre a segurança das instalações (visitantes devem ser identificados e não podem entrar portando câmeras; o acesso a áreas sensíveis deve ser controlado; dispositivos com dados importantes e documentos sensíveis devem estar em espaços privados e seguros); conter a classificação da informação e que quem poderá acessá-la; prever um processo de segurança em relação a senhas, atualização de sistemas, criptografia de dados; prever os contratos que precisam ser assinados, sendo indispensável que empregados assinem acordos de confidencialidade, assim como visitantes ou terceiros que tenham acesso a informações, também deverão assinar documentos de confidencialidade; criar planos de educação, ou seja, todos os colaboradores, incluindo sócios, devem ter treinamentos sobre segurança da informação.

Após a implantação adequada e efetiva do plano básico, a empresa deve evoluir para a criação de regras e políticas específicas sobre a segurança da informação, lembrando que elas devem ser claras e simples; deve delegar tarefas e responsáveis pelo gerenciamento das informações, que responderão ao responsável principal (indicado no plano inicial); deve tornar a segurança da informação parte de um plano específico de continuidade de negócios e resposta a emergências; deve estabelecer e implementar revisões no planejamento (POOLEY, 2015).

No caso de empresas maiores ou com risco mais elevado em relação a suas informações, James Pooley (2015) adiciona a necessidade de um plano de segurança mais robusto, incluindo políticas de uso de e-mails e redes sociais; gerenciamento de termos de confidencialidade e *due-dilligence* de terceiros que irão se relacionar com a empresa; educação mais intensiva dos colaboradores, criando uma cultura interna de proteção aos segredos.

Assim como John G. Sprankling e Thomas G. Sprankling (2020), Pooley (2015) também insiste que a proteção deve estar fortemente focada na questão dos empregados. No entanto, o autor trabalha as duas pontas do contrato: a visão dos empregadores e o ponto de vista dos empregados.

No tocante aos empregadores, a proteção do segredo empresarial se dá por acordos

de não competição e outras restrições, além dos acordos de confidencialidade. A respeito da não competição, o Autor ressalta que o empregador deve tomar alguns cuidados vez que as cláusulas não são absolutas, isso quer dizer, podem depender de alguns requisitos para serem válidas assim como podem gerar grandes indenizações em determinados estados onde a limitação da concorrência é mais restritiva, como na Califórnia, onde é proibido infringir o livre exercício da profissão. (POOLEY, 2015).

Além disso, Pooley (2015) indica algumas cláusulas que são utilizadas pelo empregador nesses tipos de acordo: a) cláusula "holdover clause", utilizada para indicar que toda invenção que seja desenvolvida pelo empregado após a sua rescisão contratual, será atribuída a titularidade à empregadora; b) cláusula "garden leave", utilizada para indicar que o empregado, após a rescisão contratual, permanecerá recebendo o seu salário integral sem contraprestação de serviço, por determinado período de tempo, apenas para não se relacionar com o(s) concorrente(s); c) cláusula "consulting contract", utilizada para indicar que empregado, após a rescisão contratual, exercerá um papel de consultor para a empresa, durante determinado período de tempo, sem acesso a atualização das informações, apenas para não se relacionar com o(s) concorrente(s).

No tocante a visão dos empregados, ou seja, o que deve ser observado para que não corram o risco de violação de algum segredo empresarial, as orientação são: a) revisar todos os contratos e documentos assinados durante o contrato de trabalho, buscando por obrigações e restrições relacionadas as informações da empresa; b) se tiver dúvidas, consultar um profissional da área; c) não concorrer enquanto estiver na empresa, pois existe um dever de lealdade para com a organização; d) ao se desvincular da empresa, questionar: o que está autorizado a ser levado pelo empregado? (exemplos: toda informação relacionada aos termos da relação de emprego; cópias pessoais de documentos não secretos; tudo que o empregador permitir que o empregado leve) e o que não pode ser levado com o empregado? (exemplos: tudo que o empregador pagou por ou forneceu para o empregado; tudo que tenha sido produzido para o empregador; tudo que possa ser reivindicado como um segredo empresarial do empregador). (POOLEY, 2015).

Para R. Mark Halligan e Richard F. Weyand (2016), uma vez que o segredo empresarial só é validado judicialmente, ou seja, não existe um registro de propriedade como em outros bens intelectuais, a melhor forma de protegê-lo é tomar ações que possam ser utilizadas como prova no judiciário. Para tanto, os autores indicam um sistema chamado EONA, sigla em inglês para *existence, ownership, notice, access* (existência, titularidade, aviso e

acesso). Isso quer dizer que a existência, titularidade, o aviso e o acesso devem ser demonstrados em casos de violação de segredo, de forma que as empresas devem se organizar em torno desses requisitos.

A prova da existência do segredo se dá por meio da compreensão da definição legal do instituto, ou seja, a informação se qualifica como um segredo? Como já visto, nesse sentido, os autores se utilizam da UTSA, que exige: que a informação que tenha valor econômico independente; não seja de conhecimento geral (para outras pessoas que possam obter valor econômico com sua divulgação ou uso); não seja verificável por meios próprios; tenha sido razoavelmente protegida. Além do conceito trazido pela UTSA, os autores referenciam outra legislação dos estados unidos, Restatement of Torts, que apesar de não apresentar uma definição exata do segredo empresarial, indica os fatores que precisam ser considerados para entender se a informação é ou não considera um segredo. Segundo R. Mark Halligan e Richard F. Weyand (2016), referidos fatores são:

i. o quanto a informação é conhecida fora do negócio (quanto mais extensivamente a informação for conhecida fora da empresa, menos provável é que seja um segredo protegido);
ii. até que ponto as informações são conhecidas pelos funcionários e outros envolvidos na empresa. (quanto maior o número de funcionários que conhecem a informação, menos provável é que seja um segredo protegido).;
iii. as medidas tomadas para guardar a informação (quanto maiores as medidas de segurança tomadas pela empresa para manter a informação em segredo, maior a probabilidade de que a informação seja um segredo protegido.);
iv. o valor da informação para a empresa e para seus concorrentes (quanto maior o valor da informação para a empresa e seus concorrentes, maior a probabilidade de que seja um segredo comercial protegido);
v. os gastos da empresa (tempo, esforço, dinheiro) no desenvolvimento da informação (quanto mais tempo, esforço e dinheiro forem gastos no desenvolvimento da informação, mais provável é que seja um segredo protegido);
vi. a facilidade ou dificuldade com que as informações podem ser adquiridas ou duplicadas adequadamente por outros (quanto mais fácil for adquirir ou duplicar as informações, menos provável que seja um segredo comercial protegido).

O Conselho Administrativo de Defesa Econômica (2015), ao tratar sobre atos de

concentração, elenca algumas informações consideradas sensíveis comercialmente, cujo potencial de proteção por segredo empresarial é alto. Portanto, devem ser considerados quando do processo de identificação da informação que dá vantagem econômica. A saber:

a) custos da empresa;

b) nível de capacidade e planos de expansão;

c) estratégias de marketing;

d) precificação de produtos (preços e descontos);

e) principais clientes e descontos assegurados;

f) salários de funcionários;

g) principais fornecedores e termos de contratos com eles celebrados;

h) informações não públicas sobre marcas e patentes e Pesquisa e Desenvolvimento (P&D);

i) planos de aquisições futuras;

j) estratégias competitivas.

No tocante a prova da titularidade (a quem pertence a informação), ela se dá por meio de contratos, termos e acordos escritos. No terceiro aspecto, o aviso de confidencialidade acerca da informação deve ter sido noticiado a outra parte pelo titular, e isso pode ocorrer, por exemplo, ao gravar os documentos com os termos "confidencial" ou "proprietário", possuir uma lista das informações que são consideradas secretas etc. Já o acesso, significa a demonstração de que a informação não foi obtida de forma independente, ou seja, ela foi acessada pela parte infratora. (HALLIGAN; WEYAND, 2016).

Por outro lado, a proteção também se dá através do reforço da segurança da empresa, tanto externa quanto interna. A segurança das informações em face de terceiros de fora da empresa é evitada por meio de processos de educação interna, isso quer dizer que todos os colaboradores, sócios, acionistas, dentre outros, precisam identificar, compreender e saber como agir em relação a informação protegida. Os exemplos trazidos pelos autores são: i) divulgação descuidada ou inadvertida, em feiras, conferências, chamadas de vendas, entrevistas; ii) divulgações desprotegidas para clientes em potencial, funcionários contratados, empregadores em potencial; iii) discussão de informações proprietárias entre colaboradores em locais públicos; iv) erros na transmissão de informações proprietárias nos e-mails e pela internet; v) descarte descuidado de documentos de registros da empresa, computadores e mídia de armazenamento. (HALLIGAN; WEYAND, 2016).

Em complementariedade, entender como os segredos são perdidos é um caminho

importante para a criação de estratégias e soluções, de forma que a fuga não mais ocorra. Para os autores (HALLIGAN; WEYAND, 2016), as seguintes perguntas devem ser objeto de reflexão:

i. Quais são as maneiras mais óbvias de coletar informações confidenciais de fora da empresa?
ii. A empresa implementa um crachá ou outro procedimento de identificação e aplica rigorosamente esses procedimentos de identificação para funcionários e convidados?
iii. Os convidados são sempre acompanhados nas instalações da empresa?
iv. As câmeras, inclusive as de celulares, relógios e outros aparelhos eletrônicos, são proibidas nas instalações da empresa?
v. A empresa possui lixeiras para descarte de documentos e trituração de documentos no local?
vi. As senhas são obrigatórias para acesso a todos os computadores da empresa e existe um processo em vigor para garantir que sejam alteradas regularmente?
vii. Os funcionários são proibidos de usar computadores externos, como seus próprios laptops ou computadores domésticos, para lidar com informações proprietárias da empresa?

A existência, titularidade, o aviso e o acesso são elementos que devem ser trabalhados dentro de políticas internas de proteção dos segredos da empresa. Para R. Mark Halligan (WIPO, 2022c) quatro etapas, exatamente nessa ordem, devem ser seguidas na elaboração da política de proteção: 1) Identificação; 2) Classificação; 3) Proteção; e 4) Valoração. Para ele, o grande erro das empresas é iniciar seu planejamento pelo item 3, ou seja, tentar proteger aquilo que elas ainda desconhecem, o que pode ser fatal na hipótese de o sistema falhar.

Seguindo Halligan e Weyand (2016), o processo de identificação se inicia com um inventário de tudo aquilo que pode ser considerado um segredo pela empresa, sendo que o levantamento pode ser feito pelos próprios empregados e revisado por um responsável geral. Referido inventário deve seguir três passos: (a) providenciar treinamento para os colaboradores sobre o que é o segredo para que eles possam distinguir esses bens de outros tipos de informação; (b) coletar com os colaboradores uma lista de potenciais conhecimentos que devem ser mantidos em segredo; (c) passar por um processo de revisão (HALLIGAN; WEYAND, 2016).

Após a identificação dos bens protegidos por segredo, eles precisam ser classificados, ou seja, é necessária uma indicação da sensibilidade daquela informação que guiará suas formas de tratamento e níveis de proteção. Pooley (2015), Halligan e Weyand (2016) recomendam que os níveis de proteção não sejam complexos e não tenham muitas variações, o ideal é que a classificação aplicada especificamente aos segredos seja de três níveis, sendo que os mais frequentemente utilizados são "confidencial", "secreto" e "ultra secreto", de modo que para cada nível deve haver uma estrutura de medidas de segurança, regras de distribuição, de compartilhamento, transporte, transmissão, além de controles de acesso e monitoramento/rastreamento das informações. Após a classificação dos segredos, a empresa deverá criar seus mecanismos de proteção, a depender do seu negócio e dos riscos envolvidos.

Somados aos itens previamente abordados, Halligan e Weyand (2016) investigam alguns cenários do mundo real e convidam as empresas para algumas reflexões quando da elaboração de suas políticas internas:

> a) No primeiro cenário, são consideradas as apresentações de produtos e serviços para um atual ou potencial consumidor: os profissionais que farão a apresentação estão instruídos sobre os limites das informações que poderão ser discutidas? Foi definido pela empresa quais as informações podem se tornar públicas? Ou eles estão autorizados a compartilhar qualquer tipo de conhecimento para impressionar os consumidores?
>
> b) No segundo cenário, são consideradas apresentações em conferências, simpósios, dentre outros, direcionados ao público da mesma atividade da empresa, para fins de pesquisa e desenvolvimento: as pessoas que farão a apresentação em nome da empresa estão instruídas sobre as informações que não podem ser compartilhadas? Essas pessoas assinaram acordos de confidencialidade? As apresentações foram revisadas por responsáveis pelo gerenciamento das informações sigilosas? Ou eles estão autorizados a compartilhar qualquer tipo de informação?
>
> c) No terceiro cenário, a equipe de vendas diretas ao consumidor é levada em consideração: o quanto a equipe conhece sobre informações confidenciais? Há instrução clara sobre o compartilhamento dessas informações com os consumidores, ou qualquer ação pode ser compartilhada desde que a venda seja efetivada? Caso exista o compartilhamento de informações, ela ocorre apenas após a assinatura de um termo de confidencialidade?

d) O quarto cenário é somado ao terceiro, a hipótese de visita do cliente na empresa: a entrada do cliente foi registrada e pode ser rastreada? Existem informações sigilosas nos ambientes que o cliente visitará? Os funcionários foram orientados sobre os procedimentos a serem adotados durante as visitas? Fotos e publicações em redes sociais são permitidas?

e) O quinto cenário é a entrevista de emprego: o que é compartilhado e apresentado ao candidato? As responsabilidades da vaga podem ser integramente compartilhadas? A equipe que entrevistará o candidato está devidamente instruída sobre o compartilhamento de informações sensíveis? Sempre lembrar que após a entrevista, o candidato poderá retornar ou ir para um competidor.

Os cenários representados acima são ilustrativos de situações cotidianas que podem levar uma empresa a dissipar um conhecimento que lhe gera vantagem competitiva. No entanto, especialmente na contemporaneidade, em modelos de negócios digitais, extraterritoriais, baseado em usos de sistemas e em colaboração, uma especial atenção deve ser direcionada para determinadas características, como o uso de dispositivos eletrônicos interna e externamente (quais sistemas de segurança estão implantados nesses dispositivos?); a existência de senhas pessoais para acesso aos sistemas, bem como sua atualização constante (é possível implantar um sistema de dupla autenticação? É possível implantar o uso de biometria?); o uso de dispositivos pessoais (laptops, smartphones etc.) deve ser evitado ao máximo (POOLEY, 2015).

Da mesma forma que Halligan, o autor Juliano Rossi (2018) entende ser condição essencial a identificação inicial do conhecimento considerado valioso. Essa necessidade é inerente a efetiva gestão do conhecimento relacionada a eficácia organizacional, a qual é dividida em: a) a capacidade de infraestrutura de conhecimento (tecnologia, estrutura e cultura); b) a capacidade de processos de conhecimentos (aquisição, conversão, aplicação e proteção). Sob a perspectiva de Gold, Malhotra e Seagars (2001 apud ROSSI, 2018, p. 40), no campo da proteção, a empresa deve se estruturar contra o uso ilegal ou inapropriado do conhecimento da organização, mantendo alguns processos:

> (a) contra o uso inadequado dentro da organização; (b) contra o uso inadequado fora da organização; (c) contra o furto originário da organização; (d) contra o furto originário de fora da organização; (e) encorajamento de proteção do conhecimento; (f) restrição de acesso a algumas fontes de conhecimento; (g) políticas e procedimentos para proteger os segredos empresariais; (h) valorização da proteção do conhecimento incorporado nos indivíduos; (i) identificação clara do conhecimento restrito; e (j) comunicação clara sobre a importância da proteção do conhecimento.

Outros diversos tópicos podem surgir na busca pela proteção do conhecimento empresarial, tal como destacado previamente, por trata-se de um processo particular e peculiar para a empresa e seu negócio. No entanto, um item que deve ser destacado no planejamento, para qualquer tipo de companhia, é o treinamento de seus colaboradores. Isso porque, a maioria dos casos de vazamento de informações acontece de dentro da empresa, e eles ocorrem por conta de negligência e não dolo (intenção de violar) (POOLEY, 2015), o que pode ser evitado com educação e mudança de cultura. Para tanto, é preciso que o processo seja inclusivo, ou seja, todas as pessoas da companhia devem participar do treinamento, não apenas aqueles que terão acesso a informações sensíveis; o processo de treinamento precisa ser interessante e o treinamento não pode ser pontual, mas um processo contínuo, seguido, por exemplo, de dicas em e-mails, histórias, lembranças etc. (POOLEY, 2015).

Assim, criar um plano de proteção e como consequência instrumentalizar esse plano em orientações/políticas internas e contratos/acordos entre as partes, são mecanismos que indicam os esforços razoáveis da empresa para proteger o segredo, indicam o próprio segredo que se protege, além de possibilitar a criação de condutas a serem tomadas em caso de violação.

Segundo os autores analisados, a proteção do segredo empresarial pode se dar por diversas medidas, mas todas elas são preventivas. As providências indicam a criação de mecanismos internos de identificação do segredo empresarial, realização de acordos, termos e contratos específicos, desenvolvimento de planos de proteção interna e externa da informação e promoção de educação em torno do tema.

Apesar da convergência nas indicações analisadas, a legislação brasileira não aponta de forma específica como os segredos empresariais são protegidos em âmbito nacional. Como visto, o art. 195 da LPI dispõe sobre as consequências da violação de um segredo, por meio do qual é possível identificar o que é protegido e o que não é protegido pela lei nacional. Com essa compreensão, os mecanismos de proteção podem ser desenvolvidos tendo por base o próprio conceito auferido sobre o instituto, exposto previamente.

Assim sendo e considerando que a proteção do segredo empresarial nacional tem uma amplitude quando comparada com as legislações trazidas pelos autores analisados, e que essencialmente consideram as mesmas características para identificar o que está fora da proteção legal, as orientações identificadas podem ser consideradas dentro do ambiente brasileiro, com limitações específicas relacionadas as peculiaridades legais do sistema nacional em cada recomendação, especialmente relacionadas aos contratos/acordos. Isso porque, para

não incorrer em cláusulas nulas, abusivas ou que gerem indenizações, os contratos, termos e acordos devem ser desenvolvidos seguindo outras legislações nacionais para além das regras do segredo.

## 5 CONCLUSÃO

Como visto no presente estudo, sobreviver no mercado competidor tem exigido um comportamento empresarial de produção inovadora e veloz, o que culmina em estratégias de criação e fortalecimento dos ativos intangíveis. O conhecimento de valor resultado desses investimentos em sua grande parcela é protegido pelas ferramentas de propriedade intelectual, cuja compreensão dicotômica (propriedade industrial e direito autoral) é ampliada para assumir características de proteção dos elementos oriundos da criatividade que possam gerar competitividade no âmbito empresarial, mas cuja exclusividade não é garantida ou oportunizada pelas ferramentas tradicionais.

Dentro desta perspectiva, compreendeu-se que as informações dotadas de valor competitivo num determinado mercado encontram proteção no ordenamento jurídico não como direito de exclusiva (exclusividades que recaem sobre um bem intelectual em decorrência de lei), mas por expressarem situações de fato em que a empresa que detém oportunidade recairá a tutela de uma posição jurídica por meio da concorrência. Dentre as modalidades de proteção por meio da repressão a concorrência desleal está o segredo empresarial, termo utilizado na presente pesquisa que inclui segredo de negócio, industrial e de comércio, alicerçado no artigo 195 da LPI.

A pesquisa identificou que o uso do segredo empresarial como mecanismo de proteção de ativos intangíveis tem se intensificado no mundo por ser uma ferramenta atrativa para empresas no nível prático, uma vez que protege praticamente qualquer tipo de informação, não tem prazo, pode ser invocado sempre que previsto em contratos e medidas internas de segurança, além do que, para empresas que adotam modelos de inovação colaborativa e estão presentes em redes globais, o segredo empresarial, além de ser rápido e simples por não depender de instituições específicas, não é territorial. Contudo, a adoção do segredo empresarial é desafiadora e arriscada na medida em que evitar a fuga do conhecimento é cada vez mais difícil na era digital e exige medidas preventivas pela empresa que optar por essa escolha e comprometimento com ferramentas de monitoramento e educação sobre a proteção da

informação.

Compreendeu-se que o segredo empresarial se refere a informação, conhecimento e/ou dados (“informação”), da indústria, do negócio ou do comércio, cuja proteção existe, desde que: a) seja confidencial; b) conceda vantagem competitiva; c) sejam eivados esforços por parte do titular para manter a informação em segredo. Assim, não estão protegidos por segredo empresarial as informações de conhecimento geral (domínio público), aquelas que sejam evidentes e/ou facilmente determináveis, ou a informação cujo acesso se deu por meios adequados. Com base na delimitação do conceito de segredo empresarial é que as empresas possuem os elementos que devem ser avaliados para identificação dos ativos intangíveis protegidos pelo instituto e poderão criar seus mecanismos de proteção.

## REFERÊNCIAS


ARRABAL, A. K. **Propriedade Intelectual, inovação e complexidade**. Rio de Janeiro: Lumen Juris, 2017.

BARBOSA, D.B. **Uma Introdução à Propriedade Intelectual**. 2.ed. Cidade: Lumen Juris, 2010. Disponível em <https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf>.

_____. **Tratado da Propriedade Intelectual**: Tomo IV. 2 ed. Rio de Janeiro: Lumen Juris, 2017.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm Acesso em: 12 out. 2021.

_____. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm Acesso em: 12 out. 2021.

_____. **Lei nº 9.609, de 19 de Fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9609.htm> Acesso em: 20 jun. 2019.

_____. **Lei nº 10.973, de 2 de Dezembro de 2004**. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm>. Acesso em: 18 jun. 2019.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia para análise da consumação prévia de atos de concentração econômica**. 2015. Disponível em

https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/gun-jumping-versao-final.pdf. Acesso em: 23 dez. 2022.

CIURIAK, D.; PTASHKINA, M. **Quantifying Trade Secret Theft: Policy Implications** (April 9, 2021). CIGI Paper 253. Waterloo: Centre for International Governance Innovation. Disponível em https://ssrn.com/abstract=3706511 or http://dx.doi.org/10.2139/ssrn.3706511. Acesso em: 24 maio 2022.

DINIZ, D. M. **Propriedade Industrial e segredo em comércio**. Belo Horizonte: Del Rey, 2003.

European Union Intellectual Property Office (EUIPO). **The baseline of trade secrets litigation in the EU member states**. doi: 10.2814/19869. 2018.

GANDELMAN, M. **Poder e conhecimento na economia global**. Rio de Janeiro: Civilização Brasileira, 2004.

HALLIGAN, R. M.; WEYAND, R.F. **Trade Secret Asset Management 2016**: A Guide to Information Asset Management Including the Defend Trade Secrets Act of 2016. Bloomington, Indiana, USA: Weyand Associates, Inc., 2016.

LEONARDOS, G. **A Lei de Inovação (Lei 10.973/2004) e as Patentes Originadas no Brasil**. In: PAIVA, R. B. (Org.). Temas contemporâneos de propriedade intelectual. Brasília: OAB, Conselho Federal, 2017.

POOLEY, J. **Secrets:** Managing Information Assets in the Age of Cyberespionage. Califórnia, EUA: Verus Press, 2015.

ROSSI, J. S. **Elementos de gestão de segredos empresariais para a inovação**. Revista Thesis Juris, São Paulo, v. 7, n. 1, p. 25-50, jan./jun. 2018.

_____. **Análise econômica do Know-how**. Direito e economia I [Recurso eletrônico on-line]. Org. CONPEDI/UFPB; Coord. Hertha Urquiza Baracho, Gina Vidal Marcílio Pompeu, Everton das Neves Gonçalves. Florianópolis: CONPEDI, 2014.

SANTOS, D. A. **O Direito, a Propriedade Intelectual e a Inovação Tecnológica para o Desenvolvimento do Brasil**. Piracicaba, Cadernos de Direito, v. 4, n. 7, p.81-105, jul./dez. 2004.

SEGADE, J. A. G. **El secreto industrial (know-how);** concepto e proteccion. Madrid: Technos, 1974.

SPRANKLING, J.G.; SPRANKLING, T. G. **Understanding trade secret law**. Durham, North Carolina: Carolina Academic Press, LLC, 2020.

SVEIBY, K. E. **A nova riqueza das organizações**. Trad. Luiz Euclydes Trindade Frazão Filho. Rio de Janeiro: Campus, 1998.

**Uniform Trade Secrets Act** (UTSA). Disponível em https://www.law.cornell.edu/wex/trade_secret#:~:text=Overview,Columbia%20have%20adopted%20the%20UTSA. Acesso em: 23 maio 2022.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). **WIPO Symposium on Trade Secrets and Innovation**. Geneva, 2019. Disponível em https://www.wipo.int/edocs/mdocs/patent_policy/en/wipo_inn_ge_19/wipo_inn_ge_19_inf_3.pdf Acesso em: 19 maio 2022.

_____. **WIPO Symposium on Trade Secrets and Innovation 2022**. Geneva, 2022a. Disponível em: https://c.connectedviews.com/05/SitePlayer/wipo?session=115459. Acesso em: 23 maio 2022.

_____. **WIPO Symposium on Trade Secrets and Innovation 2022**. Geneva, 2022b. Disponível em: https://c.connectedviews.com/05/SitePlayer/wipo?session=115461.

Acesso em: 23 maio 2022.

_____. **WIPO Symposium on Trade Secrets and Innovation 2022**. Geneva, 2022c. Disponível em: https://c.connectedviews.com/05/SitePlayer/wipo?session=115482. Acesso em: 24 maio 2022.

_____. **WIPO Symposium on Trade Secrets and Innovation 2022**. Geneva, 2022d. Disponível em: https://c.connectedviews.com/05/SitePlayer/wipo?session=115486. Acesso em: 24 maio 2022.

_____. **Act on the Protection of Trade Secrets (TS Act).** Disponível em: http://www.wipo.int/edocs/lexdocs/laws/en/se/se005en.pdf. Acesso em: 06 jun. 2022.

WORLD TRADE ORGANIZATION (WTO). **Agreement on Trade Related Intellectual Property Rights – TRIPS**. Marraqueche, 15 de abril de 1994. Disponível em https://www.wto.org/english/tratop_e/trips_e/ta_docs_e/1_tripsagreement_e.pdf. Acesso em: 20 jan. 2021.