REVISTA *THESIS JURIS*

ELEMENTOS DE GESTÃO DE SEGREDOS EMPRESARIAIS PARA A INOVAÇÃO

ELEMENTS OF TRADE SECRETS MANAGEMENT FOR INNOVATION

Juliano Scherner Rossi

Procurador Federal da Advocacia-Geral da União; Doutorando em Direito (UFSC); Mestre em Direito (UFSC); Especialista em Direito Público (UnB)

Submissão: 13/03/16.
Aprovação: 06/07/17.

Resumo

Este artigo propõe políticas empresariais para a proteção e transferência de conhecimentos e inovação colaborativa, com ênfase em *know-how* tecnológico, e informa sobre certas deficiências em estruturas jurídicas existentes para a proteção de segredos empresariais. São apresentados elementos teóricos de gestão do conhecimento para incorporação às rotinas das empresas de processos de proteção de segredos. As empresas devem desenvolver uma política de gestão de riscos relativa ao segredo empresarial e integrá-lo no código de conduta da empresa. Convergência da legislação de segredo empresarial entre jurisdições incrementa a segurança jurídica ao permitir o tratamento mais eficaz a apropriação indébita. A pesquisa adota o método monográfico e a técnica de pesquisa bibliográfica, em abordagem indutiva. O foco não está em resultados, mas em modelos teóricos que enderecem a questão.

Palavras-chaves: Inovação. Segredo empresarial. Gestão de risco.

Abstract: This paper proposes corporate policies for the protection and transfer of knowledge and collaborative innovation with an emphasis on technological know-how, and reports on certain shortcomings in existing legal frameworks for the protection of trade secrets. It presents a theoretical framework of knowledge management that incorporates trade secrets protection processes into companies' routines. Companies should develop a risk management policy with respect to trade secret and integrate it into the company's code of conduct. Convergence of trade secret law between jurisdictions increases legal certainty to prevent more effectively theft. This survey adopts the monographic method and an inductive approach. The focus is not on results but rather on theoretical models that address the issue.

Keywords: Innovation. Trade secret. Risk management.

1 Introdução

Abordagens modernas de inovação colaborativa requerem amplo compartilhamento de informações empresariais confidenciais. A proteção de segredos empresariais pode facilitar a partilha entre os parceiros, permitindo sua recuperação quando um terceiro apropriar-se indevidamente de informações valiosas. Fosse a proteção ausente, quarenta por cento das empresas europeias provavelmente reteriam informações estritamente para evitar a perda de controle sobre elas (UNIÃO EUROPEIA, 2013). De um ponto de vista prático, os regimes de segredos empresariais existentes são ineficazes devido aos baixos níveis de proteção jurídica, a fragmentação jurídica entre e no interior dos países e regiões e *enforcement* inadequado. A insegurança jurídica resultante é particularmente problemática à luz do atual ambiente de negócios, que é caracterizado pela PD&I globalmente dispersa, a mobilidade da mão de obra e dependência de Tecnologias de Informação e Comunicação (TICs).

O valor da informação segue a diretriz econômica da escassez: quanto menos concorrentes souberem, maior o benefício decorrente da vantagem que a informação proporcione; se apenas uma empresa conhecê-la, tanto melhor para ela. A colaboração para a inovação exige o compartilhamento de informação com funcionários, fornecedores, licenciados e outros parceiros. Se não houver algum tipo de garantia jurídica que a informação não seja utilizada indevidamente, o que significa dizer, fora das condições que o conhecedor do segredo estipular, essa informação provavelmente nem teria sido compartilhada em primeiro lugar.

Do ponto de vista da gestão do conhecimento, as rotinas das empresas devem incorporar elementos de segurança da informação, não apenas para retenção dos segredos empresariais, mas igualmente para permitir os fluxos de informação necessários à inovação. Buscam-se aqui elementos teóricos para, a partir da proteção jurídica dos segredos empresariais, estabelecer processos que permitam proteção do conhecimento sem interromper o fluxo de informações necessários aos negócios das empresas.

A primeira seção estabelece o quadro jurídico da proteção dos segredos empresariais e justificar economicamente a tutela jurídica, permitindo o fluxo de conhecimento e a inovação de modo a tomar em conta os riscos envolvidos. A segunda seção apresenta um modelo schumpeteriano de inovação, no qual o funcionamento das empresas é orgânico, não se assemelhando a mercados, mas a partir de rotinas e capacidades dinâmicas. A partir da noção de rotinas, a terceira seção apresenta elementos teóricos de gestão do conhecimento para incorporação às rotinas das empresas de processos de gestão de risco. A última seção retrata os desafios das empresas na salvaguarda de seus segredos. Não apenas dos riscos de perda de informações, como o furto ou a destruição acidental, mas igualmente dos riscos jurídicos

representados por sistemas legais incapazes de remediar as eventuais perdas.

A pesquisa adota o método monográfico e a técnica de pesquisa bibliográfica, em abordagem indutiva. O foco não está em resultados, mas em modelos teóricos que enderecem a questão.

2 O quadro jurídico e econômico dos segredos empresariais

Uma vez que a informação é produzida, é socialmente um desperdício criar a situação na qual outras empresas tenham um incentivo a produzir novamente aquela informação, a menos que a produção seja menos custosa que a transmissão (KITCH, 1980). A política que incentive patentes ou segredos empresariais lida com esse tipo de problema econômico da duplicação dos esforços.

O segredo empresarial cria ao seu detentor uma capacidade de produção industrial nova, fator que torna a informação valiosa e o estabelece como bem econômico, passível de transferência. O valor econômico do segredo empresarial, por outro lado, não se dá exclusivamente pela oportunidade empresarial que ele proporciona, mas igualmente pelo custo de sua aquisição, aqui também considerados os investimentos em inovação própria. O segredo empresarial tem valor econômico apenas enquanto inacessível ou pouco acessível. Seu valor decorrerá da capacidade de o seu detentor manter a informação ao largo do escrutínio público. Uma das justificativas ao regime de patentes está na sua eficiência econômica, em comparação com o regime dos segredos, pois a circulação da informação é severamente restringida neste (LANDES; POSNER, 2003; POSNER, 2005).

Segredos empresariais incluem qualquer informação protegida — técnica, financeira ou estratégica — que não seja geralmente conhecida e que proporcione uma vantagem competitiva para o proprietário. As definições de segredo empresarial são semelhantes entre as jurisdições, geralmente correspondente aos critérios articulados no artigo 39 do Acordo TRIPS (SCHULTZ; LIPPOLDT, 2014): (i) não ser do conhecimento geral ou de fácil acesso; (ii) ter valor comercial por ser secreto; e (iii) o proprietário ter tomado medidas razoáveis para mantê-lo em segredo. Essa disposição, inclusive o terceiro requisito, reproduz o *1985 Uniform Trade Secret Act* (*UTSA*) norte-americano, o qual acabou sendo adotado na Rodada Uruguai para o Acordo TRIPS. O mesmo modelo foi adotado posteriormente na Proposta de Diretiva do Parlamento Europeu e do Conselho Relativa à Proteção de *Know-how* e Informações Comerciais Confidenciais (Segredos Comerciais) contra a sua Aquisição, Utilização e Divulgação Ilegais.

O terceiro requisito relacionado acima, ou seja, as precauções de sigilo razoáveis por parte do titular, é de importância central, pois a obrigação de realizar não mais do que "precauções razoáveis" para manter a confidencialidade corresponde a uma justificação econômica fundamental. Na ausência de proteção legal, o montante gasto pelos proprietários e compradores poderia escalar sem que isso promova qualquer benefício social (LANDES; POSNER, 2003; RISCH, 2007). Em *E.I. DuPont v. Christopher*, um caso de apropriação indevida bem conhecido nos EUA, um tribunal condenou os réus que tinham tirado fotografias aéreas de uma instalação industrial que produzia segundo um processo de produção secreto enquanto ela estava em construção e, portanto, expostos à vista de cima. Os juízes consideraram os custos associados com a colocação de uma cobertura temporária sobre o local durante todo o período de construção como excessivamente elevados, portanto além da precaução razoável, ao mesmo tempo que enfatizou a conduta moralmente repreensível da parte dos perpetradores.[1] O que é "razoável" pode variar de acordo com as circunstâncias. Uma empresa que executa todas as suas operações dentro de um único edifício pode enfrentar adequadamente os riscos através de acordos de apropriação indevida de funcionários básicas e precauções visitante. No entanto, se espera de uma empresa globalmente interconectada que implemente tecnologias sofisticadas para detectar e impedir o *cyber*-furto, o que acarretaria custos potencialmente substanciais.

A conceituação mais acima é compatível com o âmbito da tutela da Lei de Patentes (Lei n. 9.279/96), lei que trata dos segredos empresariais: "[...] 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 [...]." (art. 195, XI). Esse fragmento não é extraído de uma definição legal, mas do tipo penal que define o crime de concorrência desleal, que prevê a proibição da revelação dessa categoria de conhecimento, informação ou dado confidencial sem permissão do detentor. Como se percebe, não há menção ao terceiro fator, as "precauções razoáveis".

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

[1] E.I. du Pont de Nemours & Co. v. Rolfe Christopher, 431 F.2d 1012 (5th Cir. 1970).

[2] O julgamento disse respeito ao prazo de validade das patentes, 20 anos, segundo o Acordo TRIPS, mas 15 anos,

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.

Tal como acontece com o conceito básico e definição de segredos empresariais, há um consenso sobre que ações constituem apropriação indébita, embora a cobertura do direito possa variar de país a país. Em situações em que a informação foi compartilhada sob obrigação contratual de confidencialidade e uso limitado, qualquer divulgação ou uso não autorizado é geralmente considerado ilegal (SCHULTZ; LIPPOLDT, 2014). Segundo regime do Acordo TRIPS, há responsabilidade igualmente para a aquisição das informações em uma "maneira contrária a práticas empresariais honestas" ou qualquer uso ou divulgação por alguém que obtém a informação com o conhecimento de sua aquisição indevida, situação que engloba a espionagem industrial. Muitas jurisdições reproduzem essa prescrição (SCHULTZ; LIPPOLDT, 2014). A lei brasileira o estabelece no art. 195, XII, da Lei n. 9.279/96, ao vedar a

nos termos da Lei n. 5.772/71, antiga lei brasileira de patentes e anterior ao TRIPS. Estava em julgamento a possibilidade de estender o prazo das patentes então vigentes por mais 5 anos. A despeito de o Resp n. 642.213 afirmar que o Acordo TRIPS não é lei uniforme, ele o fez *obiter dictum*, pois as razões de decidir foram efetivamente disposições do próprio tratado, o Art. 70(1), uma regra de direito intertemporal que previu que "Este Acordo não gera obrigações relativas a atos ocorridos antes de sua data de aplicação para o respectivo Membro", o qual foi fixada em 01.01.2000, por aplicação do Art. 65(2).

divulgação, a exploração ou o uso dos segredos indevidamente adquiridos.

Ao contrário das patentes, o alcance de segredos empresariais é virtualmente ilimitado. Os segredos empresariais estendem-se a essas diversas categorias como fórmulas, dados, conhecimento, termos de um contrato, listas de clientes, estratégias de *marketing*, finanças ou de informação, informações sobre fornecedores, concorrentes e outros participantes da indústria, assim como o trabalho experimental não comercializado e produtos ou estratégias inéditas. Além disso, pode abranger combinações de elementos que estejam no domínio público. O critério último é o valor da informação e não a sua utilização efetiva, de modo que segredos empresariais podem até mesmo proteger "*know-how* negativo", como abordagens de pesquisa equivocadas ou resultados negativos de experiências (JORDA, 2007).

Em termos jurídicos, a tutela dos segredos empresariais fundamenta-se na proteção de um poder de não divulgar uma informação que se possua. Se o compartilhamento do segredo é feito sob condições, sem as quais não se faria qualquer compartilhamento, tutela-se (i) a faculdade de estipular condições para o compartilhamento e (ii) contra a violação das condições previamente acordadas, ou seja, contra o inadimplemento de uma obrigação. A engenharia reversa e a descoberta independente naturalmente não se enquadram em nenhumas dessas condições, de modo que são lícitas.

Segredos empresariais e proteção de patentes são complementares e as empresas tendem a usar essas ferramentas em combinação, a fim de gerir de forma mais eficaz seus ativos intelectuais. Todas as invenções patenteáveis começam como segredos empresariais. Existem, contudo, importantes diferenças na lógica e na operação prática desses métodos de proteção. Os segredos empresariais, ao contrário das patentes, não necessitam de registro e, portanto, não há taxas governamentais ou outras formalidades na maioria das jurisdições (SCHULTZ; LIPPOLDT, 2014). Eles existem desde o momento da criação, pelo simples fato do seu valor comercial potencial e de o segredo ser bem guardado. Enquanto segredos empresariais podem consistir de qualquer informação útil, o objeto de uma patente é sempre técnico e deve cumprir critérios de patenteabilidade, como novidade e não-obviedade.

É possível questionar se a proteção das invenções sem a sua divulgação, sob a forma de segredo empresarial, é uma boa política pública. Mais especificamente, as sistemáticas aparentemente opostas de segredos empresariais e patentes podem levantar a questão de saber se os primeiros podem comprometer a difusão do conhecimento proporcionado por este último. No entanto, na prática, os dois sistemas podem coexistir razoavelmente bem. A existência de leis protegendo o segredo empresarial incentiva a difusão de tecnologia por meio de

licenciamento. Há sobreposição entre segredo empresarial e direito econômico no que e como o licenciamento não ocorre, situação que também não deve ser desprezada.

Na prática, segredos empresariais efetivamente complementam o sistema de patentes. Os segredos empresariais são particularmente úteis para proteger o conhecimento tácito ou não-codificável, ou seja, as informações necessárias para a implementação de uma invenção patenteada. Com efeito, a transferência de tecnologia frequentemente envolve licenciamento de ambas as patentes e segredos empresariais. Assim, a proteção do segredo empresarial permite às empresas compartilhar os conhecimentos complementares necessários para implementar, mas também para comercializar e aperfeiçoar tecnologias patenteadas. Em certos setores, segredos empresariais podem constituir a parte mais valiosa de um acordo de transferência de tecnologia quando uma licença de patente sozinha não permita a plena implantação de uma tecnologia proprietária (JAGER, 2002). A implantação combinada de segredos empresariais e patentes fornece exclusividade para o inovador sem deixar de promover a transferência de tecnologia através do licenciamento e outras transações (JORDA, 2007).

Do ponto de vista regulatório, as proteções jurídicas previstas ao segredo empresarial podem servir como substitutos para medidas físicas e contratuais. Por exemplo, quando da contratação de funcionários, um empregador pode se concentrar em habilidades e adequação dos candidatos para funções específicas, em vez de escolher as pessoas exclusivamente a partir de dentro de um círculo de confiança. Por outro lado, as empresas podem impor acordos de confidencialidade muito restritivos em relação às habilidades aprendidas no emprego, restringindo a mobilidade da mão de obra. As leis de proteção dos segredos empresariais deve fornecer desincentivos adequados para a apropriação indevida e equilibrar a mobilidade e desenvolvimento pessoal dos funcionários, por um lado, e os interesses legítimos das empresas em garantir a confidencialidade de suas informações, por outro lado.

A proteção do segredo empresarial pode facilitar os fluxos de conhecimento, tornando-se menos arriscado para as empresas a compartilhá-lo. Como as patentes, segredos empresariais fornecem uma solução parcial para o Paradoxo da Informação de Arrow (LANDES; POSNER, 2003), relacionado com as dificuldades de um inventor ao compartilhar uma ideia potencialmente valiosa, mas secreta, a fim de explorá-la comercialmente. Sem garantias adequadas, uma vez que o conhecimento seja trocado entre as partes, há poucos desincentivos ao receptor contra usar esse conhecimento para o benefício comercial. Assim, os potenciais parceiros podem reter informações por temor da criação de um novo concorrente. No entanto, a cooperação externa é um recurso cada vez mais importante dentre as estratégias de inovação

das empresas, permitindo-lhes combinar as competências e recursos e, assim, acelerar o desenvolvimento tecnológico e a comercialização.

O *know-how* nem sempre será patenteável, mas parte dele poderia vir a sê-lo, desde que o inventor fizesse o pedido de patente. Considerando que existe um regime jurídico que estabelece um direito exclusivo, algo que o segredo empresarial não é capaz de conferir, pode ser questionada a racionalidade da decisão do inventor que, podendo, não patenteia. O próprio processo judicial que serviria a protegê-lo representa um risco para o segredo, pois a prova exige sua divulgação, ainda que o acesso às provas fique restrito apenas às partes ou aos seus advogados. Cohen, Nelson e Walsh (2000), por outro lado, sugerem o contrário, que as empresas – no estudo, as americanas – utilizam-se mais do segredo industrial do que de patentes para proteger suas inovações. Os contextos de rotinas e cultura empresarial afetam a opção por patentear ou manter segredo. Segundo González-Álvarez e Nieto-Antolín (2007), as empresas onde o conhecimento tácito predomina optam por usar o segredo industrial, ao passo que as grandes empresas optam por usar as patentes como mecanismo de proteção.

Em uma resposta rápida, os inventores racionais escolhem proteção de segredos empresariais quando creem que a proteção de patentes é muito cara em relação ao valor ou lucratividade de sua invenção (fator em parte influenciado pelo tempo que os concorrentes levariam para reinventá-la) ou porque o âmbito da proteção de patentes, incluído o tempo, são insuficientes. Se o segredo empresarial fosse a única maneira de impedir a apropriação de classes significativas de informação com valor comercial, ou seja, se a obtenção de uma patente nunca foi uma alternativa, haveria custos pesados decorrentes das medidas necessárias para manter e decifrar segredos empresariais. A atividade inventiva seria excessivamente tendenciosa em favor de projetos que pudessem ser mantidos secretos e as transferências de tecnologia em todos os setores seriam inibidas (LANDES; POSNER, 2003).

Existem ao menos quatro situações em que a decisão de não patentear é racional economicamente. A primeira, quando as despesas da proteção por patentes, que podem ser substanciais, superarem o ganho que se tem com sua proteção. A segunda, a divulgação exigida pelo direito das patentes tornaria sem valor a invenção – ou ao menos a desvalorizaria a ponto de não ser vantajoso o patenteamento. A terceira, o inventor tem uma invenção patenteável que acredita que ninguém a reinventará no prazo de proteção de uma patente. A quarta, a invenção tem patenteabilidade duvidosa – ou seja, há um risco de negativa do pedido por falta de utilidade, novidade ou atividade inventiva – e o inventor crê que aos concorrentes demandaria tempo para a reinvenção suficiente a que obtivesse retorno substancial enquanto mantivesse em segredo a invenção.

Além de maior custo e requisitos administrativos adicionais, os atrasos consideráveis associados à obtenção de patentes pode torná-las menos eficazes para as empresas de setores dinâmicos ou para as empresas com menos recursos. No Brasil, 67% das patentes concedidas em 2014 o foram após dez anos (INPI, 2015). Com respeito os custos, nos Estados Unidos, por exemplo, litígios envolvendo *enforcement* de patentes podem custar três vezes mais do que os de segredos empresariais, com uma média de US$ 5 milhões para cada lado em despesas processuais para grandes litígios (AIPLA, 2013).

A proteção de segredos empresariais pode ser uma ferramenta especialmente atraente para pequenas e médias empresas (PMEs) tecnologicamente inovadoras, que tendem a ter menos recursos, conhecimentos e capacidade limitados de gestão de ativos intelectuais usando direitos de propriedade intelectual formais. Os segredos empresariais podem ser aplicadas a uma gama de abordagens utilizadas pelas PMEs para capturar o valor de suas inovações, reforçando estratégias como *lead-time*, a complexidade do produto e relações com os clientes. Patentes, para uma PME, seriam úteis para garantir proteção sobre os principais aspectos das suas invenções onde a engenharia reversa é relativamente fácil e, portanto, a exclusividade propicia maior proteção.

3 Um modelo schmpeteriano de inovação

As empresas não são agentes de maximização do lucro escolhendo a partir de um conjunto bem definido dado de escolhas, mas são, em vez disso, agentes em um ambiente incerto, que aprendem através da adaptação imperfeita e descoberta por meio da tentativa e erro. Os horizontes de uma empresa são determinados pelas suas experiências passadas (investimentos passados e rotinas). Se há muitos parâmetros atuando simultaneamente, limitações cognitivas confundem o processo de escolha (TEECE; PISANO, 1994). Inovação significa procurar algo novo sem saber se o novo será alcançado, vendido ou rentável. A incerteza é, portanto, um elemento-chave do processo de inovação. No processo de inovação, o aprendizado, o conhecimento, a forma como ele é internalizado pelas empresas e sua disseminação na sociedade têm um papel destacado. Fluxos de novos conhecimentos tornam a inovação um processo interativo de aprendizagem social. Só quando o novo conhecimento é criado pode florescer inovação. Conforme a teoria da firma, as firmas não se organizam em um modo assemelhado a mercados – no qual o sistema de preços coordena as atividades, ou seja, preços sinalizam no uso de recursos escassos.

Schumpeter utilizou uma abordagem original para identificação de padrões de atividade inovadora e, a partir dos padrões, a construção de modelos analíticos. Dois padrões foram identificados. Um primeiro, centrado na firma e no empresário, caracterizou-se pela "destruição criativa", na qual firmas entrantes têm novas ideias e inovações, lançam novos produtos e que desafiam as firmas estabelecidas e continuamente perturbam as formas existentes de produção, organização e distribuição, de modo a debelar as quase rendas (*quasi rents*) associadas às inovações anteriores (SCHUMPETER, 2011). Esse padrão tem por pressuposto a facilidade tecnológica de entrada no mercado e enfatiza o papel do empresário. Um segundo padrão é caracterizado pela "acumulação criativa", na qual há prevalência de grandes firmas e a presença de barreiras relevantes à entrada de novos competidores (SCHUMPETER, 2003). Esse padrão enfatiza os setores de PD&I e geração endógena de inovações. Esses dois padrões ocorrem simultaneamente na economia.

Os padrões de atividade inovadora são uma primeira aproximação à descrição do funcionamento das firmas, mas eles são limitados em modelar o fenômeno. O primeiro passo é modelar analiticamente os padrões de criação e disseminação de conhecimento nas empresas, fatores que são fortemente dependentes de como as empresas aprendem. Segundo o modelo de Teece e Pisano (1994), aprender é um processo pelo qual a repetição e a experimentação permitem que tarefas sejam executadas melhor e mais rápido e novas oportunidades de produção sejam identificadas. O aprendizado envolve habilidades individuais e organizacionais. O conhecimento organizacional aprendido é estabelecido em novas rotinas (novos padrões de interação que representam soluções bem-sucedidas para problemas particulares) ou lógicas de organização.

O conhecimento aqui contém duas dimensões: uma pública, tomando a forma de informação codificada em patentes, modelos, livros, e um tácito, incorporado em rotinas, capacidades, competências e práticas específicas (NELSON; WINTER, 1982; POLANYI 1967). O conhecimento tácito baseia o desempenho competente de atividade da qual a pessoa não é completamente consciente e acha difícil ou impossível de articular uma descrição completa de todos os seus detalhes. Muito do conhecimento permanece tácito porque não pode ser articulado rápido o suficiente ou em razão das limitações da comunicação por meio de uma linguagem simbólica (NELSON; WINTER, 1982). O conhecimento público é caro para criar, mas com baixo ou nenhum custo para ser transferido uma vez criado. Por outro lado, o conhecimento tácito não é tão facilmente transferido, sendo o resultado de diferentes processos de aprendizagem: aprendizado pela prática (*learning by doing*), pela pesquisa, por imitação,

pela interação, pela cooperação.

Nelson e Winter (1982) propuseram um modelo em que as habilidades organizacionais de uma empresa são expressas por rotinas, qualquer padrão de comportamento regular e previsível de firmas, que funcionam como memória organizacional, em analogia a como indivíduos lembram-se de habilidades ao exercê-las, que permitem o funcionamento competente de uma organização.

Teece e Pisano (1994) não negam a importância do conceito de rotinas e conhecimento tácito que ela congloba, mas, para eles, esse modelo não é analítico o suficiente. A dimensão estratégica da firma é expressa em função de capacidades dinâmicas (de adaptação ao ambiente e aos competidores), conforme (i) processos de gestão e organização, (ii) posição atual e (iii) caminhos disponíveis, que formam a dimensão estratégica da empresa. Processos e posições das firmas englobam coletivamente suas capacidades ou competências. Os processos gerenciais e organizacionais referem-se à forma como as coisas são feitas na empresa ou o que pode ser referido como suas rotinas ou padrões correntes de prática e aprendizagem. Posição atual diz respeito a sua dotação atual de tecnologia e propriedade intelectual, bem como a sua base de clientes e as relações com os fornecedores a montante. Caminhos são as alternativas estratégicas disponíveis para a empresa e a atratividade das oportunidades. A abordagem das capacidades dinâmicas vê a competição em termos schumpeterianos, o que significa que as firmas competem em projeto e qualidade de produto, eficiência de processos, entre outros aspectos. A competição envolve desenvolver novas competências, melhorar as existentes ou imitar os competidores mais qualificados.

A geração de inovação, nesse sentido, pode ser endógena, a partir da rotinização dos processos que favorecem a inovação. As capacidades das firmas em melhorar suas competências distintivas ou em desenvolver novos domínios de competência distintivas são críticas no longo prazo.

Há estrita relação entre crescimento econômico e progresso técnico, mas a relação entre eles é controversa. Inovações trazem grande retorno econômico e dependem de fatores de mercado (variação de preços relativo, rendimentos) e da força do progresso técnico. São, por outro lado, complexas incertas, em certos aspectos caóticas e sujeitas a mudanças de diversas ordens. Inovação é também difícil de medir e demanda coordenação de conhecimento técnico adequado e boas avaliações do mercado. O processo de inovação deve ser visto como uma série de mudanças em um sistema completo não apenas de capital físico, mas de ambiente de mercado, plantas de produção e conhecimento e os contextos de organização da inovação.

Os primeiros modelos de inovação eram lineares. A inovação dava-se segundo etapas sequenciais e unidirecionais mais ou menos estanques de pesquisa, desenvolvimento, produção e mercado. Segundo esse modelo, o que induz a inovação é ciência aplicada. Os modelos lineares, independentemente da abordagem, falham ao não considerar o *feed back* (retroalimentação) entre as etapas. Igualmente falha ao determinar que o processo central de inovação é a ciência, quando o projeto (*design*) é que cria a demanda por ciência. É possível, inovar mesmo na ausência ou inadequação de ciência.

Uma proposta para solução é o de paradigmas tecnológicos e trajetórias tecnológicas, conforme Dosi (1982). Há provável similaridade entre os procedimentos e a natureza das tecnologias e das das ciências. Paradigma tecnológico é um modelo e um padrão de solução de problemas tecnológicos selecionados, baseados em princípios selecionados derivados das ciências naturais e em material tecnológico selecionado. Trajetória tecnológica é o padrão da atividade "normal" de solução de problemas (ou seja, progresso) a partir de um paradigma tecnológico. Nesse sentido, paradigmas tecnológicos cumprem a mesma função de paradigmas científicos ou programas de pesquisa, analogamente aos modelos propostos por Kuhn (1987) e Lakatos (1978).

Dosi (1982) buscou uma teoria que que explicasse melhor a relação entre as influências do mercado e do progresso tecnológico no processo de inovação. Ele propõe que trajetórias tecnológicas determinam o processo de inovação de forma relativamente autônoma em relação aos fatores de mercado, funcionando como uma instância mediata entre fatores de mercado e inovação: os fatores de mercado influenciam as trajetórias, que influenciam o processo de inovação, mas não diretamente aqueles em relação a este. Haveria uma diferença entre a seleção de novos paradigmas tecnológicos (inovação radical) e progresso técnico em uma determinada trajetória (inovação incremental), endógeno ao mecanismo econômico "normal". Essa distinção corresponde historicamente às etapas de emergência, em função da tentativa e erro nas instituições com conhecimento acumulado e multiplicidade de atores que corram riscos e da maturidade das empresas, especialmente as oligopolistas, nas quais a produção, exploração e difusão de inovações são menos divorciados e o progresso técnico torna-se parte do padrão de concorrência monopolística.

Uma vez que o caminho tenha sido selecionado e estabelecido, ele tem um *momentum* próprio que contribui para definir as direções da atividade de solução de problemas. Observou-se que algumas trajetórias são mais fortes que outras e que trajetórias podem ser complementares. Na fronteira tecnológica está o nível tecnológico e econômico mais alto em

uma trajetória tecnológica e o progresso em uma trajetória provavelmente implica retenção de alguns aspectos cumulativos: a maior chance de sucesso no futuro depende da posição atual da firma da fronteira tecnológica. Quanto mais forte a trajetória, mas difícil de mover para uma trajetória alternativa, em razão da complexidade e incerteza. Somente *ex post* é possível analisar a superioridade de uma trajetória sobre a outra. O lado da oferta determina o universo de modalidades possíveis pelas quais as necessidades genéricas dos consumidores ou requisitos técnicos são satisfeitas. Há uma interação entre as condições econômicas com o processo de seleção de novas tecnologias, seu desenvolvimento, obsolescência e substituição (*feedback*).

Os modelos interativos também buscaram suprir as falhas dos modelos lineares, ao enfatizar a incerteza, os processos de *feedback*, de uso de conhecimento disponível e integrando a influência das trajetórias tecnológicas. Kline e Rosenberg (1986) propuseram o que ficou conhecido como modelo de elos em cadeia (*chain-linked model*), amplamente aceito, que previu um caminho central de inovação e os *feedbacks* entre as etapas, com recurso à pesquisa, quando necessário, mas de resultado incerto.

4 O segredo empresarial e a gestão do conhecimento

Até este momento não se definiu conhecimento, apesar de ser ter mencionado que pode ser codificado ou tácito. Geralmente é apontado que dados, informações e conhecimento são diferentes. Do ponto de vista de definições, é certo que se pode estabelecer diferenças e os dicionários cuidarão disso. A questão, entretanto, é que os modelos de gestão da inovação modelarão diferentemente os processos dentro da empresa a partir dessa diferenciação. Mais do que isso, a distinção entre informação, dado e conhecimento será relevante porque a proteção jurídica depende dessas categorias. Já foi visto acima que o conhecimento tácito é de mais difícil transmissibilidade, mas não definiu o que seja o conteúdo do conhecimento. Acima foi estabelecido que os conhecimentos formam dinamicamente as capacidades das empresas. Nesse sentido o conhecimento não é algo estático, mas relações que geram capacidades. Conhecimento envolve abstração e processamento com a finalidade de orientar a ação (ARÍS, 2007; DAVENPORT, 1998a).

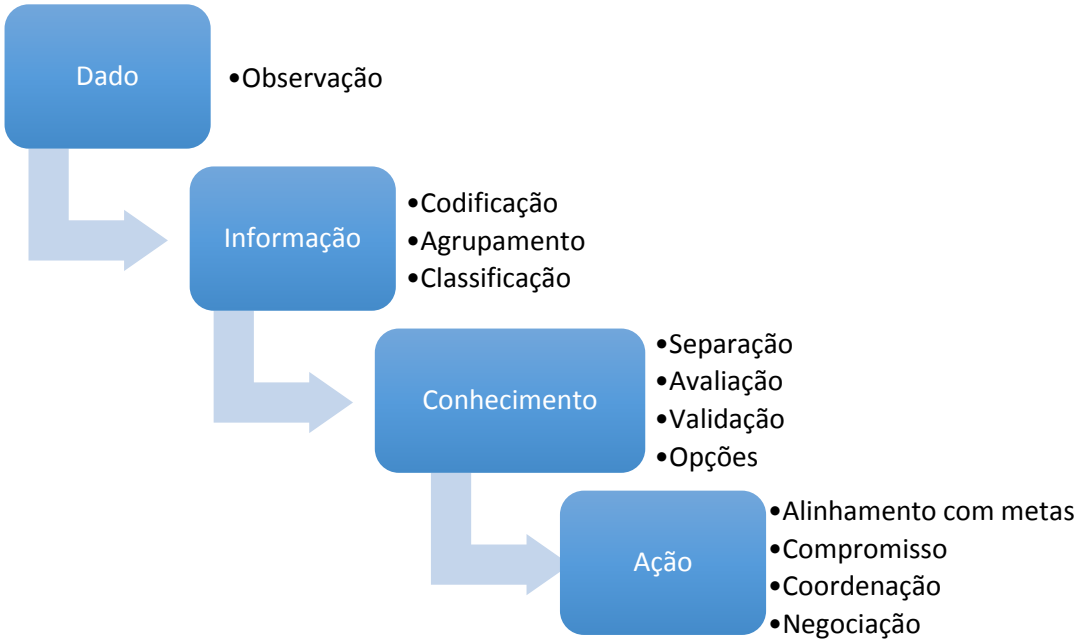
Um quadro ilustrativo das diferenças entre dado, informação e conhecimento e a cadeia de transformação da informação podem ser visto em

Dado	**Informação**	**Conhecimento**
Simples observações sobre o estado do mundo.	Dados dotados de relevância e propósito.	Informação valiosa da mente humana.
- Facilmente estruturado. - Facilmente obtido por máquinas. - Frequentemente quantificado. - Facilmente transferível	- Requer unidade de análise. - Exige consenso em relação ao significado. - Exige necessariamente a mediação humana.	- Inclui reflexão, síntese e contexto. - De difícil estruturação. - De difícil captura em máquinas. - Frequentemente tácito. - De difícil transferência.

e Quadro *2*.

Dado	**Informação**	**Conhecimento**
Simples observações sobre o estado do mundo.	Dados dotados de relevância e propósito.	Informação valiosa da mente humana.
- Facilmente estruturado. - Facilmente obtido por máquinas. - Frequentemente quantificado. - Facilmente transferível	- Requer unidade de análise. - Exige consenso em relação ao significado. - Exige necessariamente a mediação humana.	- Inclui reflexão, síntese e contexto. - De difícil estruturação. - De difícil captura em máquinas. - Frequentemente tácito. - De difícil transferência.

Quadro 1: Diferenças entre dados, informação e conhecimento.
Fonte: Davenport, 1998a.



Quadro 2: Cadeia de transformação da informação
Fonte: Elaboração própria, a partir de Aris (2007).

O caráter social do conhecimento é ressaltado por Davenport, De Long e Beers (1998b, p. 56; tradução nossa): "Ao contrário dos dados, o conhecimento é criado de forma invisível no

cérebro humano e só o clima organizacional correto pode convencer as pessoas a criar, revelar, compartilhar e usar o conhecimento". Segundo Santos (2016), o crescente volume de dados e de informações implica a necessidade de um bom planejamento e controle sobre as operações por meio de decisões efetivas baseadas no fluxo e atualização da informação.

Os segredos empresariais podem englobar quaisquer das categorias de dado, informação ou conhecimento, pois se enquadram nas definições do Acordo TRIPS e da Lei de Patentes, mas cada um possui fontes diversas de ameaças, principalmente relacionadas ao elemento de tacitude. Quanto maior a codificação do dado, informação ou conhecimento, maiores os riscos de perda relacionados ao conhecimento incorporado ao meio. Os principais fluxos de conhecimento dão-se a partir de interação entre empresas; entre empresas, universidades e laboratórios públicos de pesquisa; de difusão de conhecimento e tecnologia para firmas e de movimento de mão de obra (OCDE, 1997). A esses, devem ser somados os fluxos por meios ilícios, como a espionagem industrial, quebra de patentes ou de acordos de sigilo. A proteção do conhecimento deve ser vista não somente sobre a questão de proteção do patrimônio, pois existe o caráter estratégico do conhecimento. Aqui não se trata apenas da capacidade de produção de conhecimento, mas também da capacidade de compartilhá-lo corretamente e protegê-lo quando necessário. Conhecimento estruturado, atualizado, corretamente aplicado e protegido é uma grande vantagem competitiva. As rotinas das empresas devem ser estruturadas de modo a que o ciclo criação, difusão e proteção estejam contemplados.

A condição essencial para a gestão do conhecimento é identificar o conhecimento considerado valioso. Diferentes formas de atribuição de valores para o conhecimento influenciam na alocação de recursos para gerenciá-los.

Gold, Malhotra e Seagars (2001) abordam a gestão do conhecimento duas capacidades relacionadas à eficácia organizacional: a) a capacidade de infraestrutura de conhecimento, que detalha aspectos da tecnologia, da estrutura e da cultura, e b) capacidade de processos de conhecimento, que aborda aspectos da aquisição, da conversão, da aplicação e da proteção.

A capacidade da infraestrutura de conhecimento é composta pela *tecnologia,* que é a responsável pela criação de novos conhecimentos por meio da integração dos fluxos de informação e conhecimento; a *estrutura*, que diz respeito a presença de normas e mecanismos de confiança que permitem o compartilhamento do conhecimento no ambiente interno da organização; e a *cultura,* essencial para o processo de inovação porque possibilita a interação entre as pessoas. A capacidade dos processos de conhecimento é a essencial para gerir o conhecimento dentro da organização. O processo *aquisição* é responsável pela obtenção e acúmulo do conhecimento; o processo *conversão* por fazer o conhecimento existente utilizável;

o processo *aplicação* pelo uso do conhecimento atual; e o processo de *proteção* é o responsável pela proteção contra o uso ilegal ou inapropriado do conhecimento na organização, garantindo o ciclo de vida do conhecimento.

Quanto ao processo *proteção*, a partir da abordagem de Gold, Malhotra e Seagars (2001), dez tipos de processos de proteção devem ser equacionados na empresa: (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.

Além da abordagem acima, é possível associar a proteção dos segredos empresariais à gestão do risco. A capacidade de identificar e gerenciar riscos é considerada de vital importância na inovação, pois o lançamento de novos produtos mais rapidamente e com sucesso exige assumir riscos.

O termo risco é geralmente usado para significar a medida da probabilidade de um resultado, o tamanho do resultado ou uma combinação de ambos (ANSELL; WHARTON, 1992). A qualificação do resultado, se positivo ou negativo, neste caso uma ameaça, também é associado ao termo. Uma distinção entre incerteza e risco também às vezes também observada. A norma ISO 31000:2009, que estabelece padrões para a avaliação de risco, por outro lado, não as distingue, definindo risco como o efeito da incerteza sobre objetivos (ABNT, 2009). A incerteza surge a partir desses fatores internos e externos e influências que ele não controla completamente, mas que pode causar a organização a deixar de atingir os seus objetivos ou pode causar atraso. A definição da ISO 31000:2009 de risco muda a ênfase de preocupações anteriores com a possibilidade de um evento (algo acontece) para a possibilidade de um efeito e, em particular, um efeito sobre os objetivos. Quando o risco é definido dessa forma, ele revela mais claramente que a gestão de risco é um processo de otimização da consecução de objetivos. É por isso que a gestão de risco é um aspecto indissociável da gestão da mudança e outras formas de tomada de decisão.

A gestão de riscos é, conforme a norma, "o conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos." (ABNT, 2009, p. 2). Este processo envolve (i) comprometimento da alta direção da empresa, que deve liderar e sustentar o

processo; (ii) compreender o contexto interno e externo da organização (incluindo histórico de ocorrências, mudanças ocorridas ou previstas, etc.), estabelecer uma política de gestão de riscos, definir responsabilidades e autoridades, integrar a gestão de risco nos processos organizacionais, alocar recursos apropriados, estabelecer mecanismos de comunicação e relato internos e externos; (iii) estabelecer e cumprir um plano de gestão de riscos, baseado em uma estratégia e politica de gestão de riscos; (iv) uso de indicadores de desempenho, análise periódica e relato e tomada de decisões sobre risco e a própria estrutura; e (v) melhoria contínua da estrutura, por meio do aprendizado e da melhoria na cultura para gestão de riscos.

Existem alguns requisitos de desempenho claros que, se seguidos, asseguram que os riscos são geridos tanto eficaz e eficiente. Os princípios de gestão de risco eficaz, conforme a ISO 31000:2009 são: (i) criar e proteger o valor; (ii) ser uma parte integrante de todos os processos organizacionais; (iii) ser parte da tomada de decisões; (iv) abordar explicitamente a incerteza; (v) ser sistemático, estruturado e oportuno; (vi) ser baseado na melhor informação disponível; (vii) ser projetado sob medida; (viii) leve em conta fatores humanos e culturais; (ix) ser transparente e inclusivo; (x) ser dinâmico, interativo, e responsivo à mudança; e (xi) facilitar a melhoria contínua da organização (ABNT, 2009).

Segundo a ISO 31000:2009, existem dois elementos do processo que pode ser considerado como atuando continuamente, a comunicação e consulta com as partes interessadas e o monitoramento e avaliação. A coluna central da gestão de riscos trata da preparação e a avaliação de riscos. O processo começa pela definição do que a organização pretende atingir e os fatores internos e externos que podem influenciar o sucesso em alcançar aqueles objetivos. Este passo é chamado de estabelecimento do contexto. A identificação de riscos requer a aplicação de um processo sistemático para entender o que pode acontecer, como, quando e porquê.

A ISO 31000:2009 estabelece uma série de opções gerais a serem considerados quando o risco é tratado (a ordem da lista reflete preferência: (a) evitar os riscos ao decidir não iniciar ou continuar com a atividade que dá origem ao risco; (b) tomada ou aumento o risco, a fim de aproveitar uma oportunidade; (c) remover a fonte de risco; (d) alterar a probabilidade; (e) alterar as consequências; (f) partilhar o risco com a outra parte ou partes (incluindo contratos e financiamentos de risco); (g) retenção do risco pela decisão informada.

5 Desafios para as empresas na salvaguarda de segredos empresariais

Segredos empresariais representam fração considerável dos ativos das empresas. Segundo Forrester (2010), englobam dois terços do valor dos ativos intelectuais das empresas. Em uma pesquisa, empresas americanas avaliaram tecnologia proprietária como uma das principais fontes de vantagem competitiva e a grande maioria dos inquiridos (oitenta e oito por cento) citou habilidades e conhecimento como os ativos intelectuais mais importantes (IPOA, 2003).

As empresas estão cada vez mais vulneráveis ao roubo de informações confidenciais, quer devido ao mau comportamento de funcionários e ex-funcionários, espionagem empresarial ou *hacking*. As implicações do furto de segredos empresariais para as empresas incluem a perda de vantagem competitiva, das tecnologias de *core business*, de reputação corporativa e diminuição de desempenho e rentabilidade. Nos EUA, casos de furto de segredos empresariais duplicaram entre 1995 e 2004 e devem dobrar novamente até 2017 (ALMELING et. al., 2010, 2011). Em uma pesquisa recente nos países da UE, cerca de vinte por cento das empresas entrevistadas relataram ter sofrido pelo menos uma tentativa ou ato de apropriação indébita ao longo dos últimos dez anos, enquanto cerca de quarenta por cento afirmou que o risco aumentou durante esse período (MARTINIS; GAUDINO; RESPESS III, 2013). De acordo com um estudo japonês, mais de trinta e cinco por cento das empresas industriais sofreram algum tipo de perda de tecnologia (ONCIX, 2011). No Reino Unido, as empresas sofrem perdas de até £ 21 bilhões por ano devido a furto de propriedade intelectual e espionagem industrial (THE COST OF CYBERCRIME, 2011).

Uma série de fatores pode ter levado ao aumento do furto de segredos empresariais, como a globalização das cadeias de fornecimento, rápidos avanços em TICs, a crescente utilização de instalações de armazenamento digital e processamento externo de dados, inclusive em nuvem, a crescente importância do *know-how* como fonte de vantagem competitiva e uma maior mobilidade profissional. Tais fatores, a despeito de representarem potencial ganho, incrementam vulnerabilidades que devem ser endereçadas apropriadamente. Mais ampla disponibilidade de tecnologias mais sofisticadas e acesso a dados têm facilitado a intrusão em redes corporativas e a aquisição de dados sensíveis pelos funcionários, empreiteiros, consultores, fornecedores e vendedores. O armazenamento e processamento de informações digitais em servidores externos permite furtos iniciados a partir de qualquer lugar do mundo. Esses, por sua vez, obrigam as empresas a buscar os infratores onde ocorre a apropriação indébita, muitas vezes em jurisdições que oferecem uma proteção pouco eficaz pouca ou mesmo

nenhuma.

Além do furto, empresas enfrentam riscos de apropriação indébita ao fornecer às autoridades informações confidenciais em procedimentos para garantir o acesso ao mercado, como no caso de produtos farmacêuticos (art. 229-C, Lei n. 9.279/96). Se a informação não estiver devidamente armazenada e gerenciada por funcionários do governo ou for por eles revelada, segredos empresariais podem tornar-se do conhecimento público, perdendo o seu valor. Do ponto de vista de uma empresa, é fundamental que tais informações permaneçam confidenciais. Requisições do governo devem ser redigidos estritamente e, na medida do possível, excluir informações sobre segredo empresarial e as empresas devem estar preparadas para questionar, na tramitação dos pedidos de patentes, requisições que possam por em risco segredos empresariais.

Litígios envolvendo segredos empresariais geralmente se apresentam em três conjuntos básicos de circunstâncias: inteligência competitiva, transações entre empresas e funcionários que deixam a empresa (ALMELING, 2010; ALMELING et. al., 2011).

Nas cadeias de fornecimento globais, as empresas recorrem a três diferentes formas de transações de fornecimento baseados no conhecimento: fornecimento cativo (*captive sourcing*); terceirização (*third-party sourcing*) e de *joint-venture* (*joint-venture sourcing*) (TRADE SECRET THEFT, 2012). Enquanto o fornecimento cativo, ou seja, a criação ou aquisição de suas próprias instalações operacionais, permite às empresas manter um máximo de controle sobre seus ativos intelectuais, envolve, por outro lado, tempos de implementação longos e altos investimentos. Mesmo o fornecimento cativo apresenta riscos de segurança, por exemplo, quando os concorrentes contratam funcionários para a construção de estruturas longe das instalações principais da empresa. A terceirização (ou seja, o uso de fornecedores externos) oferece uma implementação rápida e de baixo custo, bem como uma maior flexibilidade em termos de capacidade de produção; no entanto, pode reduzir o controle da empresa sobre as operações, em especial sobre as informações confidenciais. Em uma *joint-venture*, forma intermediária de terceirização, as empresas estrangeiras e entidades locais se envolvem em parcerias, reduzindo assim os custos iniciais e compartilhando riscos; no entanto, *joint-ventures* envolvem questões estruturais e operacionais mais complicadas, especialmente no que respeita ao regime jurídico em jurisdição estrangeira.

A maior mobilidade da mão de obra é uma tendência global que afeta proteção de segredos empresariais, pois aumenta o risco de que os funcionários usem segredos empresariais de seu antigo empregador no emprego subsequente. Em 2008, cerca de sessenta por cento dos

acusados de apropriação indébita de informações confidenciais de empresas nos Estados Unidos da América (EUA) eram empregados ou ex-empregados (ALMELING, 2010; ALMELING et. al., 2011). Os controles mais utilizados consistem em acordos de confidencialidade com funcionários e de atribuição de titularidade de invenção ao empregador, juntamente com o monitoramento cuidadoso da atividade competitiva pós relação de emprego. Acordos de não concorrência podem ser usados, dependendo da jurisdição, para ajudar a controlar o risco de apropriação indevida indetectável por ex-empregados. No entanto, em litígio, os tribunais, por vezes, se recusam a reconhecer os acordos que pareçam excessivos na matéria ou na cobertura geográfica. Além disso, as leis de alguns países proíbem restrições à mobilidade da mão de obra e o uso de informações aprendidas no trabalho sob o fundamento do *restraint of trade*. Essa variação na regulação entre os países pode complicar a gestão de pesquisa, desenvolvimento e inovação (PD&I) globalizada ou geograficamente distribuída. No Brasil, não há regra específica sobre acordos de não concorrência, mas tal cláusula é geralmente considerada válida pelos tribunais, dependendo da presença de três requisitos: (a) compensação financeira (indenização compensatória), (b) estipulação no momento da contratação do emprego ou função, e (c) delimitação objetiva da abstenção de trabalho (geográfica, funcional e temporal) (MALLET, 2005; NOVO, 2007; TRT2, 2004).

Existe uma grande variação entre os regimes proteção do segredo empresarial entre jurisdições diferentes, mesmo dentro de países e regiões economicamente integradas, como a União Europeia (EU) (SCHULTZ; LIPPOLDT, 2014), o que proporciona diferentes graus de proteção e cria insegurança jurídica. Países como o Brasil, a China, a Alemanha, Polônia e o Japão protegem o segredo empresarial a título de tutela contra a concorrência desleal. Em certos países de direito comum (*common law*), como a Índia, há foco na violação de dever (*breach of duty*), em vez de apropriação indébita. (U. S. CHAMBER INSTITUTE FOR LEGAL REFORM, 2013). Nesses locais, a proteção de segredos empresariais pode ser limitado a casos abrangidos pelo contrato e relações laborais, fazendo reivindicações de apropriação indébita mais difícil, por exemplo, quando afirmado contra uma empresa subcontratada ou outro ator com quem o proprietário do segredo empresarial não tem qualquer relação contratual. O proprietário deve prestar muita atenção à elaboração do contrato, exigindo dos empreiteiros e contratados acordos de confidencialidade com subcontratados, além de limitar a partilha de segredos empresariais para somente aqueles com quem o proprietário tem uma relação direta.

Dentre as principais deficiências de regimes de proteção jurídica são (SCHULTZ; LIPPOLDT, 2014): (a) remédios civis ou penais inadequados para deter os infratores; (b)

medidas cautelares inadequadas ou inexistência de previsão de medidas *inaldita altera parte*; (c) incapacidade de proteger a confidencialidade de segredos empresariais durante o processo judicial; (d) *enforcement* inadequado e (e) ausência de mecanismos de cooperação processual. Tais aspectos devem ser tomados em consideração quando houver o estabelecimento de PD&I globalizada ou geograficamente distribuída, de modo a que os riscos jurídicos sejam corretamente apreciados.

Em geral, as jurisdições não adotam disposições que rejam a interação entre agências governamentais em caso de violação de segredos empresariais. Ao mesmo tempo, a falta de assistência jurídica mútua internacional complica proteção e *enforcement* além das fronteiras. Mesmo em países com regimes relativamente bem desenvolvidos para proteger segredos empresariais, a fragmentação pode ser um problema. Por exemplo, nos EUA, leis de proteção ao segredo empresarial não são totalmente unificados no nível estadual. Com o furto de segredos empresariais pode cruzar cada vez mais fronteiras estaduais e nacionais, as empresas têm expressado frustração com a incapacidade de os tribunais estaduais americanos responder eficazmente à apropriação indébita, uma vez que eles não têm jurisdição nacional (ao contrário do Brasil, por exemplo).

Internacionalmente, a proteção aos segredos empresariais permanece extremamente fragmentada, em parte porque o Acordo TRIPS (*Agreement on Trade-Related Aspects of Intellectual Property Rights*) não detalha a implementação das obrigações que impõe quanto a segredos empresariais.

6 Considerações finais

Garantir que as informações confidenciais da empresa sejam adequadamente protegidas da apropriação indébita implica uma ação em nível da empresa, em primeiro lugar. As empresas devem desenvolver uma política de segredo empresarial e integrá-lo no código de conduta da empresa. Eles devem pôr em prática medidas de segurança física e digitais apropriados para proteger segredos empresariais, rotineiramente marcando informações relevantes como "confidencial" e considerar abrigar as informações mais sensíveis em jurisdições com regimes de segredo empresarial mais robustas. É fundamental que as empresas eduquem os funcionários sobre as suas obrigações de confidencialidade, durante a vigência do emprego e após, explicitamente relacionadas em contratos de trabalho. As empresas devem limitar informações empresariais fornecidas a terceiros e devem exigir de parceiros externos, como fornecedores, restringir, monitorar e registrar o acesso de empregados e subcontratados

às suas informações confidenciais. No que diz respeito aos funcionários e parceiros externos, da mesma forma é importante que as empresas tomem medidas adequadas para após a relação comercial ter terminado.

Além de suas próprias ações, a capacidade de a empresa manter o controle sobre seus dados confidenciais e recuperá-los sem se expor a risco adicional dependerá, em grande parte, das estruturas jurídicas em jurisdições relevantes. A fragmentação das estruturas de proteção de segredo empresarial cria grandes desafios, dada a natureza globalizada de fazer negócios e a prevalência de inovação aberta. Convergência da legislação de segredo empresarial entre jurisdições poderia proporcionar segurança jurídica e permitir que os proprietários de segredos empresariais tratem de forma mais eficaz a apropriação indébita. Isto, por sua vez, pode aumentar os fluxos de conhecimento e investimentos transfronteiriços em PD&I.

Entidades governamentais e empresariais podem considerar o fornecimento de treinamento para as PMEs, de modo a orientá-las no uso de segredos empresariais, bem como sobre estratégias de gestão de ativos intelectuais. Em comparação com as grandes empresas, as PMEs têm níveis relativamente mais baixos de experiência e menos recursos para se dedicar à gestão de DPI. PMEs inovadoras podem se beneficiar de treinamento sobre ações apropriadas para proteger informações empresariais confidenciais, a fim de serem capazes de gerenciá-las e fazer valer os seus direitos perante os tribunais em caso de apropriação indébita.

Referências

ALMELING, David S.; SNYDER, Darin W.; SAPOZNIKOW, Michael; MCCOLLUM, Whitney E.; WEADER, Jill. A Statistical Analysis of Trade Secret Litigation in Federal Courts. **Gonzaga Law Review**, n. 45, p. 291-334, 2010.

ALMELING, David S.; SNYDER, Darin W.; SAPOZNIKOW, Michael; MCCOLLUM, Whitney E.; WEADER, Jill. A Statistical Analysis of Trade Secret Litigation in State Courts. **Gonzaga Law Review**, n. 46, p. 57-101, 2011.

AMERICAN INTELLECTUAL PROPERTY LAW ASSOCIATION (AIPLA). **Report of Economic Survey**. Arlington (VA) : AIPLA, 2013.

ANSELL, Jake; WHARTON, Frank. **Risk-analysis, assessment and management**. Sussex : Wiley, 1992.

ARÍS, Enrique Paniagua (Org.) **La gestión tecnológica del conocimento**. Murcia: Editum, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de risco – princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

BRASIL. Lei n. 9.279, de 14 de maio de 1996b. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9279.htm>. Acesso em: 14 out. 2012.

COHEN, Wesley M.; NELSON, Richard R.; WALSH, John P. **Protecting their intellectual assets**: Appropriability conditions and why U.S. manufacturing firms patent (or not). Cambridge (MA) : National Bureau of Economic Research, 2000.

DAVENPORT, Thomas H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998a.

DAVENPORT, Thomas H.; DE LONG, David W.; BEERS, Michael C. Successful Knowledge Management Projects. **Sloan Management Review**, p. 43-57, inv. 1998b.

DOSI, Giovani Technological Paradigms and Technological Trajectories: a suggested interpretation of the determinants and directions of technical change. **Research Policy**, vol. 11, n. 3, p. 147-62, 1982.

FORRESTER CONSULTING. **The value of corporate secrets**: how compliance and collaboration affect enterprise perceptions of risk. Disponivel em: https://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf. Acesso em: 3 dez. 2015.

GOLD, Andrew H.; MALHOTRA, Arvind; SEGARS, Albert H. Knowledge management: An organizational capabilities perspective. **Journal of Management Information Systems**, v. 18, n. 1, p. 185-214, verão 2001.

GONZÁLEZ-ÁLVAREZ, Nuria; NIETO-ANTOLÍN, Mariano. Appropriability of innovation results: An empirical study in Spanish manufacturing firms. **Technovation**, v. 27, n. 5, p. 280–295, maio 2007.

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL (INPI). **Agenda Prioritária 2014**: relatório de *status* (dezembro/2014) atualizado em 13 de março de 2015. [s. n. : s. l.], 2015. Disponível em: http://www.inpi.gov.br/sobre/arquivos/130315_status_agenda_prioritaria_dez_14_executivo_v2.pdf. Acesso em: 3 dez. 2015.

INTELLECTUAL PROPERTY OWNERS ASSOCIATION (IPOA). **Survey results from the 2003 Intellectual Property Owners Association survey on strategic management of intellectual property**. [s. l. : s. n.], 2003. Disponível em: http://www.ipo.org/wp-content/uploads/2013/04/survey_results_revised.pdf. Acesso em: 3 dez. 2015.

JAGER, M. The Critical Role of Trade Secret Law in Protecting Intellectual Property Assets. In: GOLDSCHNEIDER, R. (Ed.) **The LESI Guide to Licensing Best Practices**. Hoboken: Wiley, 2002.

JORDA, K. F. Trade Secrets and Trade-Secret Licensing. In: KRATTIGER, A.; KITCH, Edmund W. The law and economics of rights in valuable information. **Journal of. Legal Studies**, v. 9, p. 683-724, 1980.

KLINE, Stephen J.; ROSENBERG, Nathan. An overview of innovation".In: LANDAU, R.; ROSENBERG, N. (eds.). **The Positive Sum Strategy**: Harnessing Technology for Economic Growth. Washington : National Academy Press, 1986. p. 275–305.

KUHN, Thomas S. **A estrutura das revoluções científicas**. São Paulo: Perspectiva, 1987.

LAKATOS, Imre. **The methodology of scientific research programmes**. Philosophical Papers Cambridge : Cambridge University, 1978. v.1

LANDES, William M.; POSNER, Richard A. **The economic structure of intellectual property law**. Cambridge: Harvard University Press, 2003. Edição Kindle (ebook).

MAHONEY, R. T.; NELSEN, L. (Ed.). **Intellectual Property Management in Health and Agricultural Innovation**: A Handbook of Best Practices. Oxford: MIHR, 2007.

MALLET, Estêvão. Cláusula de não-concorrência em contrato individual de trabalho. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 100, p. 121-146, 2005.

MARTINIS, Lorenzo de; GAUDINO, Francesca; RESPESS III, Thomas S. **Study on Trade Secrets and Confidential Business Information in the Internal Market**. Prepared for the European Commission. [s. l. : s. n.], 2013. Disponível em: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf . Acesso em: 3 dez. 2015.

NELSON, Richard R.; WINTER, Sidney G. **An evolutionary theory of economic change**. Cambridge (MA) : Harvard University Press, 1982.

NOVO, Catia Guimarães Raposo. **Da cláusula de não-concorrência no contrato individual de trabalho**. 2007. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, Faculdade de Direito. Orientador: Renato Rua de Almeida.

OFFICE OF THE NATIONAL COUNTER INTELLIGENCE EXECUTIVE (ONCIX). **Foreign Spies Stealing US Economic Secrets in Cyberspace**. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. Washington : Office of the National Counterintelligence Executive, 2011. Disponível em: http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. Acesso em: 5 dez. 2015.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. **Manual de Oslo**: diretrizes para coleta e interpretação de dados sobre inovação. Tradução Flávia Gouveia. 3. ed. [S. l.] : FINEP, [1997].

POLANYI, Michel. **The tacit dimension**. London: Routledge & Kegan Paul, 1967.

POSNER, Richard A. Intellectual Property: The Law and Economics Approach**. Journal of Economic Perspectives**, v. 19, n. 2, p. 57-73, primavera 2005.

RISCH, M. Why Do We Have Trade Secrets? **Marquette Intellectual Property Law Review**, v. 11, p. 1-76, 2007.

SANTOS, Maria Isabel Araújo Silva dos. **A segurança do segredo**: proposta de *framework* de aplicação dos instrumentos de proteção do segredo no ambiente de inovação da base industrial de defesa. 2016. Tese (Doutorado em Engenharia e Gestão do Conhecimento) – Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis.

SCHULTZ, Mark F.; LIPPOLDT, Douglas C. **Approaches to Protection of Undisclosed Information (Trade Secrets)**. Paris: OECD, 2014. Trade Policy Paper 162.

SCHUMPETER, Joseph A. **Capitalism, socialism and democracy**. London : Taylor & Francis, 2003. ISBN 0-203-26611-0.

SCHUMPETER, Joseph A. **The Theory of Economic Development**: An Inquiry Into Profits, Capital, Credit, Interest, And The Business Cycle. Piscataway: Transaction Publishers, 2011. E-book.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). Recurso Especial n. 642.213, E I Du Pont De Memours and Company v. Instituto Nacional de Propriedade Industrial – INPI, rel. João Otávio de Noronha, Brasília, 28 abr. 2010. **Diário de Justiça Eletrônico**, Brasília, 2 ago. 2010. Disponível em: <https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=200400038267&dt_publicacao=02/08/2010>. Acesso em 18 out. 2013.

SUPREMO TRIBUNAL FEDERAL (STF). Agravo Regimental em Carta Rogatória n. 8.279 - República Argentina, Coagulantes Argentinos S/A, Rel. Celso de Mello, Brasília, 17 jun. 1998. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=324396>. Acesso em: 17 out. 2013.

SUPREMO TRIBUNAL FEDERAL (STF). Medida Cautelar na Ação Direta de Inconstitucionalidade n. 1.480, Confederação Nacional do Transporte – CNT e Confederação nacional da Indústria – CNI *v.* Presidente da República e Congresso Nacional, Rel. Celso de Mello, Brasília, 4 set. 1997. **Revista Trimestral de Jurisprudência**, Brasília, v. 179, n. 2, p. 493-563, jan./mar. 2002.

TEECE, David; PISANO Gary. **The dynamic capabilities of firms**: an introduction. laxenbourg : international institute for applied systems analysis, 1994.

THE COST OF CYBERCRIME. **A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office**. [s. l. : s. n.], 2011. Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf. Acesso em: 4 dez. 2015.

TRADE SECRET THEFT: Managing the growing threat in supply chains. Washington : CREATe, 2012. White Paper. Disponível em: http://dev.create.org/sites/default/files/CREATe_White-Paper_Trade-Secret-Theft_Final-e.pdf. Acesso em: 4 dez. 2015.

TRIBUNAL REGIONAL DO TRABALHO DA 2.ª REGIÃO (TRT2). **Recurso Ordinário n. 02243.2000.381.02.00-9**, José Carlos Cerqueira de Souza, Dinap S/A Distribuidora Nacional

de Publicações, São Paulo, 18 maio 2004. Disponível em: <http://www.trt2.jus.br/cons-acordaos-turmas>. Acesso em: 3 abr. 2014.

U.S. CHAMBER INSTITUTE FOR LEGAL REFORM. **International Comparisons of Litigation Costs**: Canada, Europe, Japan, and the United States. Washington : U.S. Chamber Institute for Legal Reform, 2013.

UNIÃO EUROPEIA (UE). Comissão Europeia. **Assessment accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure**. [s. n.] : Brussels, 2013. Commission Staff Working Document.