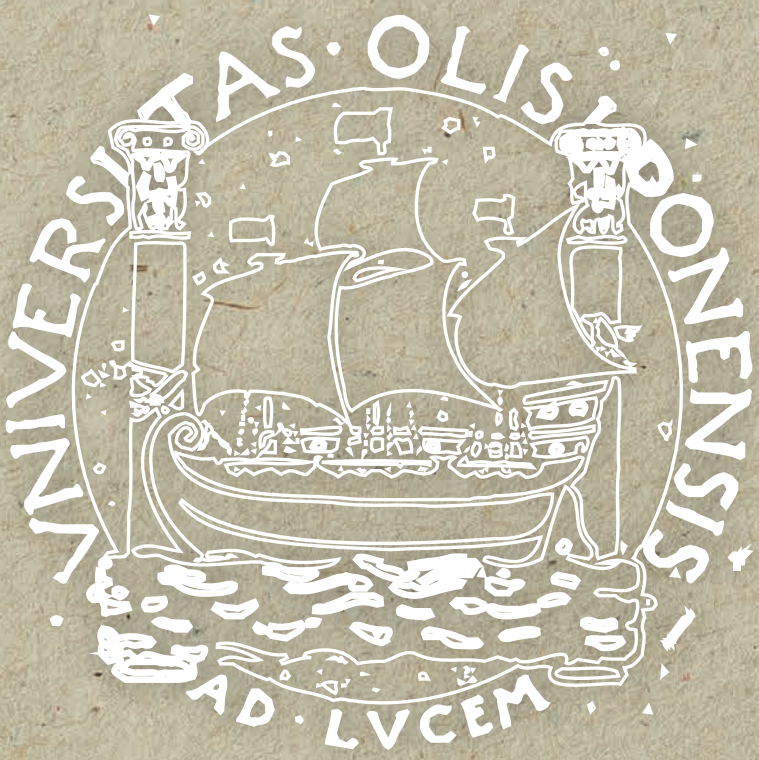
REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

LISBON LAW REVIEW



Número Temático: Tecnologia e Direito

ANO LXIII 2022 NÚMEROS 1 E 2

REVISTA DA FACULDADE DE DIREITO
DA UNIVERSIDADE DE LISBOA
Periodicidade Semestral
Vol. LXIII (2022) 1 e 2

LISBON LAW REVIEW

PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade – 1649-014 Lisboa – Portugal

EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO
LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

ISSN 0870-3116 Depósito Legal n.º 75611/95

Data: Outubro, 2022

ÍNDICE 2022

LIVROS & ARTIGOS

Sobre a proteção jurídica dos segredos comerciais no espaço digital*

On the Legal Protection of Trade Secrets in the Digital Space

João de Oliveira Geraldes**

Resumo: Este estudo trata da proteção dos segredos comerciais, evidenciando alguns dos novos desafios e problemas jurídicos originados pelo espaço digital. Partindo, na primeira parte, do enquadramento jurídico geral, segue-se uma segunda parte na qual se procede à análise da divulgação de segredos comerciais no espaço digital e do dever de adotar diligências razoáveis para manter a informação secreta.

Palavras-chave: segredos comerciais, espaço digital, concorrência desleal, propriedade intelectual.

Abstract: This study deals with the protection of trade secrets, highlighting some of the new challenges and legal problems arising in the digital space. Starting, in the first part, from the general legal framework, a second part follows in which it is analysed the disclosure of trade secrets in the digital space, as well as the duty to take reasonable measures to keep the information secret.

Keywords: trade secrets, social digital space, unfair competition, intellectual property.

* Abreviaturas – AcP: Archiv für die civilistische Praxis; BGH: Bundesgerichtshof; CPI: Código da Propriedade Industrial; DTSA: Defend Trade Secret Act (EUA/2016); GeschGeh: Gesetz zum Schutz von Geschäftsgeheimnissen (Alemanha/2019); GRUR: Gewerblicher Rechtsschutz und Urheberrecht Zeitschrift der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht; Id.: Idem; LPI: Lei da Propriedade Industrial do Brasil (1996); NStZ-RR: Neue Zeitschrift für Strafrecht Rechtsprechungsreport; OLG: Oberlandesgericht; RDI: Revista de Direito Intelectual; ROA: Revista da Ordem dos Advogados; UTSA: Uniform Trade Secrets Act (EUA/1979); UWG: Gesetz gegen den unlauteren Wettbewerb.

** Professor Auxiliar da Faculdade de Direito da Universidade de Lisboa. O texto que se publica corresponde, com desenvolvimento, à intervenção no curso de pós-graduação "*Propriedade Intelectual no Direito Comercial e no Direito Internacional Privado",* FDUL/FDUSP (Lisboa, 29 de junho de 2022), agradecendo-se o convite do Professor Doutor Dário Moura Vicente para nele participar. São ainda devidos agradecimentos, pelas observações e sugestões, aos Revisores anónimos e a André Salgado de Matos, Gonçalo Leite de Campos, Gregor Albers, José António Veloso, Luís Faustino, Nuno Guimarães e Nuno Sousa e Silva.

I. Introdução

§1. Razão de ordem

1. O desenvolvimento tecnológico, no contexto transformador da globalização e da afirmação pós-moderna da sociedade da informação, tem proporcionado inequívocos benefícios económicos e sociais. Tal como no aforismo atribuído a Heráclito, nada é permanente, exceto a mudança. Porém, com a revolução provocada pela expansão do espaço digital surgem também novos desafios jurídicos[1], especialmente quando se verifica que as informações que circulam no espaço digital podem corresponder a segredos comerciais. Tem, portanto, pleno cabimento

[1] T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* De Gruyter, Berlin/Boston, 2021, p. 3.

enfatizar a perigosidade do espaço digital para os segredos comerciais[2], atendendo à circunstância de várias atividades industriais e comerciais estarem hoje dependentes das redes de *Intranet, Extranet* e *Internet*[3]. Sem a colocação de informação nestas redes e sem a utilização de programas informáticos que com elas se relacionam, as referidas atividades industriais e comerciais tornar-se-iam frequentemente ineficientes ou até mesmo impossíveis de desenvolver. Convirá ainda ter presente que o espaço digital, por ser tendencialmente público, potencia ainda mais o risco de divulgação de segredos comerciais[4]. Deste modo, também a própria natureza do espaço digital incrementa a dificuldade na proteção dos segredos comerciais, facilitando a sua destruição e a produção de danos de grande escala[5].

2. A relação que se acaba de estabelecer é tanto mais relevante se pensarmos que, para que haja tutela jurídica de segredos comerciais, será necessário dar como preenchidos vários requisitos legais não isentos de ambiguidade semântico-jurídica[6/7]. O recurso a conceitos jurídicos vagos e indeterminados na configuração de enunciados normativos[8] – "informação facilmente acessível", "informação geralmente conhecida",

---

[2] Como refere Cundiff, o espaço digital – *digital space* – não é favorável à proteção dos segredos comerciais: V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, IDEA–The Intellectual Property Law Review, v. 49, 2009, pp. 359 ss., p. 363.

[3] A *Internet* é de acesso universal, enquanto que uma *Intranet* é um espaço digital de acesso privado. Uma *Extranet* é uma combinação tanto da *Internet* como de uma *Intranet*, funcionado como uma *Intranet* que permite acesso a determinadas pessoas ou empresas externas.

[4] J. Brammsen/S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft. I, 2022, p. 3

[5] Brammsen e Apel apontam para danos anuais, na Alemanha, estimados conservadoramente entre quinze a vinte cinco mil milhões de euros: J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p. 19: "Der für die bundesrepublikanische Wirtschaft bezifferte Maximalschaden von 55Mrd. EUR erscheint selbst bei zehnfacher Dunkelziffer deutlich zu hoch gegriffen, insbesondere wenn der Fokus einmal stärker auf den Mittelstand gerichtet wird. (...) Es ist daher angemessen, unter Einbeziehung einer gleichanteilig hohen Schadenssumme für nachrichtendienstliche Industriespionage die alljährliche Gesamtschadenssumme auf 15-25 Mrd. EUR zu reduzieren".

[6] Constituindo pano de fundo do presente estudo, convém relembrar a necessidade de equilíbrio entre a proteção da privacidade comercial e a garantia da liberdade de iniciativa económica e concorrencial. Sobre a perspetiva jurídica da informação como objeto de direitos, acentuando que a informação deve "considerar-se submetida a um *princípio de liberdade*": D. Moura Vicente, *A informação como objecto de direitos,* Propriedade Intelectual – Estudos Vários, AAFDL, Lisboa, 2018, pp. 7 ss., p. 22.

[7] Sobre a aplicação judicial do Direito, sublinhando a distinção central entre *aplicação* e *criação* do Direito: J. Lamego, *Elementos de Metodologia Jurídica,* Almedina, Coimbra, 2018, pp. 155 ss.

[8] Sobre a utilização de conceitos indeterminados na regulação de práticas comerciais desleais: A. Ohly, *Richterrecht und Generalklausel im Recht des unlauteren Wettbewerbs – ein Methodenvergleich*

"pessoas que lidam habitualmente com este tipo de informação", "objeto de medidas razoáveis" – introduz considerável incerteza na concretização do conceito de segredo comercial, o que, aliás, ocorre também em outros ordenamentos jurídicos[9]. Sem prejuízo de ulteriores observações sobre este ponto, note-se que a proteção do segredo comercial exige que a informação seja secreta (313.º/1/a, CPI), tenha valor comercial por ser secreta (313.º/1/b, CPI) e tenha sido objeto de diligências razoáveis no sentido de a manter secreta (313.º/1/c, CPI). Não é difícil de antever a dificuldade de concretizar os elementos presentes neste enunciado normativo. Mais ainda: especialmente quanto às *diligências razoáveis* para a manutenção do segredo comercial, cumpre salientar que este requisito se esteia em longo lastro histórico que, para sua boa compreensão, deve ser conhecido. Com efeito, a exigência de *diligências razoáveis* surgiu no sistema norte-americano, quando neste se associava a tutela do segredo comercial à teoria da *property*: o controlo possessório era assumido como requisito necessário para a existência de *property rights*[10]. Não surpreende, portanto, que a consagração do dever de adotar *diligências razoáveis*, depois da erosão da teoria da *property* ou em sistemas de *civil law* que nunca consagraram esta teoria, dê azo a complexos problemas na determinação do seu sentido normativo[11].

3. Em termos gerais, o desenvolvimento do conceito jurídico de segredo comercial tem registado longo percurso, pautado por flutuantes ponderações de política económica e por instabilidade na determinação dos seus elementos constituintes. O segredo comercial nem sempre surge legalmente definido ou, quando surge, a sua noção definitória é introduzida com traço muito largo: é o que sucedeu no direito português. Sublinhe-se, porém, que o direito português não é caso

---

des englischen und des deutschen Rechts, Schriftenereihe zum Gewerblichen Rechtsschutz, 100), Carl Heymanns, Köln, 1997, p. 197 ss, p. 253 e p. 365 ss.; *id., Generalklausel und Richterrecht,* AcP, Bd. 20, 2001, pp. 1 e ss. Criticamente, no plano da análise da teoria que associa as cláusulas gerais à *função de delegação normativa*, Hedemann acentua o problema dos *espaços legais abertos*: J. W. Hedemann, *Die Flucht in die Generalklauseln: eine Gefahr für Recht und Staat*, Mohr, Tübingen, 1933, pp. 58 ss. Sublinhando a especificidade da *realidade jurídica*, J. P. Charters Marchante, *Das lacunas da lei, no Direito português – maxime, do disposto no art. 203.º da CRP ("Os tribunais [...] apenas estão sujeitos à lei.")*, diss., Lisboa, 2017, pp. 265 ss.

[9] Acentuando que a proteção de segredos comerciais requer segredos com qualidades (jurídicas) especiais: Y. Rody, *Der Begriff und die Rechtsnatur von Geschäfts- und Betriebsgeheimnissen unter Berücksichtigung der Geheimnisschutz-Richtlinie,* Nomos, 2019, pp. 50 ss.

[10] R. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* The Law and Theory of Trade Secrecy, Edward Elgar Publishing, 2011, p. 8.

[11] R. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* cit., pp. 46 ss.

isolado. Muito pelo contrário: veja-se, por exemplo, o caso do direito brasileiro, em que a ambiguidade do artigo 195.º da LPI não oferece ao seu aplicador guiada precisão no que toca ao conceito de segredo comercial[12], impulsionando a doutrina brasileira, nomeadamente Krueger Pela[13], a formular propostas de revisão legal. Neste mesmo contexto, registe-se a símil situação do direito alemão: até 2019, a legislação alemã – §17 UWG[14], preceito com origem em 1896[15] – não oferecia uma definição de segredo comercial (*Betriebsgeheimnisse* ou *Geschäftsgeheimnisse*), o que determinou ambiguidade jurídica na sua concretização. Coube, deste modo, aos tribunais alemães a missão de identificar – no plano de uma designada função de delegação (*Delegationfsunktion*)[16] na substanciação de conceitos indeterminados[17]

---

[12] Lei nº 9.279, de 14 de Maio de 1996 (LPI, Regula direitos e obrigações relativos à propriedade industrial), Artigo 195.º – 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.

[13] Analisando a situação atual e futura da proteção dos segredos comerciais no direito brasileiro: J. Krueger Pela, *The Brazilian Regulation of Trade Secrets. A proposal for its review*, GRUR, 06/2018, pp. 546-550.

[14] O §17 UWG abrangia três tipos de atos: (i) a divulgação não autorizada de segredos comerciais por parte de funcionários/empregados, (ii) a aquisição não autorizada de segredos comerciais (a) através de meios técnicos, (b) através de cópia, (c) e através de furto, bem como (iii) a utilização de segredo comercial obtido de um funcionário/empregado nos termos anteriores. (Versão revogada em 2019 do § 17 UWG: (...) (2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, 1. sich ein Geschäfts- oder Betriebsgeheimnis durch a) Anwendung technischer Mittel, b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert).

[15] K. Natelski, *Der Schutz des Betriebsgeheimnisses*, GRUR, 1957, p. 2; T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 13.

[16] Sobre a *função de delegação* e a substanciação de conceitos indeterminados: J. W. Hedemann, *Die Flucht in die Generalklauseln: eine Gefahr für Recht und Staat*, cit., pp. 58 ss., P. Heck, *Grundriß des Schuldrechts*, Mohr-Siebeck, Tübingen, 1929, pp. 11 ss., A. Ohly, *Generalklausel und Richterrecht,* cit., pp. 5 ss., F. Bydlinski, *Rechtsdogmatik und praktische Vernunft*, Symposion zum 80. Geburtstag von Franz Wieacker (org. Okko Behrends/Malte Diebelhorst/Ralf Dreier), Vandenhoeck & Ruprecht, Göttingen, 1990, pp. 189 ss. Para a importância do "grupo de casos", da ideia de sistema flexível e dos seus elementos concretizadores, tem também interesse ter presente a influência de Wilburg e do *Bewegliche System*: W. Wilburg, *Entwicklung eines beweglichen Systems im bürgerlichen Recht*, Kienreich, Graz, 1950, pp. 12 ss.

[17] Entre nós, referindo *conceitos de delegação* e *normas de delegação*: A. Menezes Cordeiro, *Da boa fé no direito civil,* Almedina, Coimbra, 1997 (reimp.), p. 361 e p. 1191.

– quais os pressupostos necessários para adjudicar a proteção jurídica de segredo comercial a uma informação. Foi assim que, nos casos *Möbelpaste* (1955)[18], *Präzisionsmessgeräte* (2002)[19] e *Kundendatenprogramm* (2006)[20], o BGH desenvolveu judicialmente o conceito jurídico de segredo comercial para efeito do §17 UWG. Destas decisões do BGH resultou que o conceito de segredo comercial dependeria então do preenchimento dos seguintes pressupostos: a informação *(i)* deveria ser respeitante a uma empresa ou ao comércio e *(ii)* não ser geralmente conhecida ou acessível, *(iii)* cujo titular tivesse vontade de a proteger e, por último, *(iv)* desde que essa informação se relacionasse com um interesse comercial legítimo[21].

4. A dificuldade na concretização dos pressupostos da proteção jurídica dos segredos comerciais não é, no entanto, uma particularidade dos sistemas de *civil law.* A comprová-lo, averiguando a situação nos sistemas de *common law*, tem interesse apontar a ambiguidade identificável nas decisões dos tribunais norte-americanos quando chamados a determinar o conceito de *trade secret*, nomeadamente para averiguar se o segredo comercial subsiste depois de ser exposto na *Internet*. Neste contexto, merece especial destaque o recente caso *Compulife Software, Inc. v. Newman* (2020)[22]. Em termos sintéticos, refira-se que a *Compulife Software* é uma empresa que fornece acesso pago à sua base de dados *Transformative,* contendo uma compilação de dados sobre as propostas de várias empresas seguradoras organizada através de *software* computacional especial ("*life insurance quoting software*"), apenas do conhecimento da *Compulife Software*. Uma empresa concorrente conseguiu reproduzir parcialmente a base de dados *Transformative*, iniciando sequentemente a sua comercialização. Para obter a reprodução parcial da base de dados *Transformative,* foi utilizado um *bot*[23], durante quatro dias, que executou o método de *scraping*[24], assim recolhendo quarenta e três milhões de propostas de individuais de seguro, sem que

[18] BGH, 15.03.1955, *Möbelpaste*, GRUR, 1955, p. 424.
[19] BGH, 07.11.2002, *Präzisionsmessgeräte*, GRUR, 2003, pp. 356 a 358.
[20] BGH, 27.4.2006, *Kundendatenprogramm* (acesso: *juris.bundesgerichtshof.de*).
[21] H. Piper/A. Ohly/O. Sosnitza, *UWG Kommentar*, C. H. Beck, 2016 (7ª), § 17 (*Verrat von Geschäfts- und Betriebsgeheimnissen*), pp. 1084 ss.
[22] *Compulife Software Inc. v. Newman*, No. 18-12004 (11th Cir. 2020) (acesso: *lawjustitia.com*).
[23] Programa de computador que executa tarefas repetitivas tipicamente na *Internet.*
[24] Técnica computacional mediante a utilização de um programa que extrai dados estruturados da *web* de uma forma automatizada. Durante quatro dias, o *bot* solicitou informação à base de dados *Transformative,* a um ritmo impossível de alcançar por humanos, conseguindo uma quantidade volumosa de dados, permitindo, por força desse volume, mimetizar parcialmente a (função da) base de dados.

a *Compulife Software* tivesse tomado qualquer medida de prevenção quanto à recolha de dados no seu *sítio* na *Internet* através do método de *scraping*. Perante esta factualidade, o *District Court* da *Florida* (2017)[25] – referindo que "nada há de fácil neste caso; os factos são complicados e o direito vigente é ambíguo", bem como que o caso "fica muito denso e difícil rapidamente"[26] – decidiu que, apesar de a própria base de dados *Transformative* poder ser perspetivada, *per se,* como um segredo comercial, as propostas individuais de seguro, devido à sua natureza "pública", por estarem disponíveis em plataforma aberta ao exterior, não poderiam ser consideradas como tal, escapando à proteção contra a apropriação indevida de segredos comerciais. Assim, decidiu aquela instância norte-americana não haver violação de segredo comercial dada a natureza "pública" das propostas de seguro contidas naquela base de dados.

Por seu turno, a instância de recurso – *Court of Appeal* do *Eleventh Circuit* (2020)[27] – emitiu decisão em sentido contrário, considerando que o problema não residia na facilidade de aceder às propostas de seguro individuais por estarem disponíveis ao público através de uma plataforma digital, mas antes na quantidade de propostas individuais de seguro obtidas através do método de *scraping*, o que permitiu reproduzir e mimetizar parcialmente a base de dados *Transformative* e a sua funcionalidade. Para a instância de recurso, houve violação de segredo comercial, salientando-se ainda que, de outro modo, as bases de dados deste tipo perderiam substancialmente o seu valor comercial.

5. Ainda que muito perfunctoriamente, os elementos até aqui aduzidos permitem indiciar a multiplicidade de novos desafios e problemas jurídicos com os quais a proteção dos segredos comerciais se confronta no espaço digital. Um desses problemas é precisamente o de discernir que tipo de efeito ocorre depois de se verificar a divulgação (*disclosure*) de um segredo comercial na *Internet*: estará em causa um efeito extintivo *ipso facto*? Como deve reagir o titular de um segredo comercial para o preservar depois de este ser divulgado na *Internet*?

Com este pano de fundo, o primeiro objetivo deste estudo é o de fornecer sinteticamente o quadro geral do direito nacional vigente quanto à tutela do segredo

---

[25] *Compulife Software Inc. v. Newman* (Southern Florida District Court, 9:16-cv-81942-BER/2017) (acesso: *lawjustitia.com*).

[26] *Compulife Software Inc. v. Newman* (Southern Florida District Court, 9:16-cv-81942-BER/2017) (acesso: *lawjustitia.com*): "There's nothing easy about this case. The facts are complicated, and the governing law is tangled. At its essence, it's a case about high-tech corporate espionage." (...) Warning: This gets pretty dense (and difficult) pretty quickly".

[27] *Compulife Software Inc. v. Newman*, No. 18-12004 (11th Cir. 2020) (acesso: *lawjustitia.com*).

comercial, proporcionando uma visão geral do sistema. Depois, na parte especial, o estudo concentra-se nos problemas específicos causados pelo espaço digital. Primeiramente, serão enunciadas breves referências históricas que permitem identificar a crescente regulamentação e subsequente autonomização da proteção dos segredos comerciais. Seguidamente, será dada nota sobre os processos de harmonização europeia e norte-americana: indicar-se-ão as linhas gerais da diretiva 2016/943, de 8 de junho de 2016[28], bem como do *Defend Trade Secret Act* (DTSA), de 11 de maio de 2016[29]. Prosseguindo e aproveitando elementos dos sistemas inglês, norte-americano e alemão, analisar-se-á a transposição da referida diretiva europeia, em 2018, para o direito português. Por último, serão então analisados novos problemas originados pelo espaço digital e enunciadas pistas para densificar os critérios de decisão que lhes podem ser aplicáveis.

§2. Nota sobre as origens da proteção do segredo comercial

1. Desde a Antiguidade, a par do desenvolvimento da produção e comercialização de bens, emergiu a necessidade de proteger, por meio de segredo, o modo como eram desenvolvidas as atividades industriais e comerciais. São múltiplas as indicações históricas revelando a existência de indícios de segredos relativos à técnica de irrigação, à apicultura, à coloração do vidro e à atividade metalúrgica, assim como de casos de furtos de segredos comerciais[30].

Dada a necessidade de preservar determinados modos especiais de produzir bens e de os comercializar, não pode surpreender que uma das primitivas medidas preventivas de guarda de segredo tenha sido a utilização de cifragem ou até mesmo, preventivamente, a sua não redução à forma de escrito, privilegiando-se a sua transmissão por via oral. Pelo seu simbolismo histórico, merece também especial referência o cuidado na divulgação de segredos em *círculos subjetivos* de âmbito muito restrito na Antiguidade. Precisamente, tem sido apontada, como primeira manifestação da proteção de segredos, uma tábua do ano 2000 a.c., do monarca faraó egípcio Mentuhotep[31],

---

[28] Jornal Oficial da União Europeia (PT), 15/6/2016, Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais, pp. L.157/1–L.157/18.

[29] *Defend Trade Secrets Act of 2016*, Public Law, 114th Congress, 11/5/2016, pp. 114-153.

[30] Relatando casos de furto de segredos comerciais na antiguidade: J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., rn 1, p. 3.

[31] Esta tábua está em exposição no Louvre; reprodução em: M. Collin, *Driving Innovation: Intellectual Property Strategies for a Dynamic World,* Cambridge University Press, Cambridge, 2008, p. 27.

vedando o acesso a segredos comerciais e industriais na sua posse, com a exceção do seu primogénito[32].

2. A propósito da origem da proteção jurídica do segredo comercial assume identicamente especial significado a querela entre romanistas quanto ao âmbito de aplicação da *actio servi corrupti*[33]. Por meio desta *actio*, identificável em D. 11.3.1[34], contra aquele que tivesse dado guarida a um escravo de outrem, com a intenção fraudulenta de que o escravo fizesse algo que o tornasse menos valioso, poderia ser pedida a sua condenação no pagamento do dobro da consequente perda de valor. Porém, têm sido enunciadas sérias dúvidas quanto ao âmbito concreto desta compensação devido à ambiguidade da seguinte parte do referido fragmento[35]: "*...in eum quanti ea res erit in duplum iudicium dabo*". Neste contexto, contestando a ideia de que Roma não interferia nas práticas competitivas e na privacidade empresarial, Schiller veio propor uma releitura da *actio servi corrupti*[36], sustentando que nesta *actio* estava também contemplada a tutela jurídica face à utilização desleal de marcas ou firmas por parte de competidores, bem como perante a utilização de escravos de outrem visando a divulgação dos seus segredos[37]: a obtenção de fórmulas secretas, listas de clientes e estado financeiro do seu proprietário. Nestas circunstâncias, o instigador do escravo seria, segundo Schiller, abrangido pelo âmbito de aplicação da *actio servi corrupti*, que deste modo permitiria também a compensação por violação de segredos comerciais[38].

No entanto, esta interpretação de Schiller tem sido objeto de refutação[39]. Encabeçando as críticas, Watson veio sublinhar precisamente o caráter dubitativo de "*...in eum quanti ea res erit in duplum iudicium dabo*" ("contra ele darei uma

---

[32] J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., Rn. 1, p. 3.

[33] Para o enquadramento geral: B. Albanese, *Actio servi corrupti,* Seminario giuridico: Annali, Università di Palermo, Montaina, 1959.

[34] D. 11.3.1 *Ulpianus libro 23 ad edictum: pr. Ait praetor: "Qui servum servam alienum alienam recepisse persuasisseve quid ei dicetur dolo malo, quo eum eam deteriorem faceret, in eum quanti ea res erit in duplum iudicium dabo".*

[35] Referindo-se precisamente a esta muito questionável e ambígua exceção: J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p. 3: "der äußerst umstrittenen spätrömischen *actio servi corrupti".*

[36] A. Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti,* Columbia Law Review, v. 30, n.º 6, 1930, pp. 837 ss., p. 839.

[37] A. Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti,* cit., p. 845.

[38] A. Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti,* cit., p. 845.

[39] J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p. 4; J. Drescher, *Industrie- und Wirtschaftsspionage in Deutschland: Phänomenologie – materielles Recht – prozessuale Durchsetzung: Bestandsaufnahme und Perspektiven*, Lit, 2019, p. 26.

ação pelo dobro da quantia envolvida")[40], considerando que a interpretação que lhe é dada por Schiller não passa de uma *ópera bufa*[41]. De acordo com Watson, não existem quaisquer indícios que permitam afirmar que a *actio servi corrupti* tenha sido pensada ou utilizada para proteger segredos industriais ou comerciais. Pelo contrário, para Watson, na *actio servi corrupti* estaria essencialmente em causa o valor do escravo, cuja depreciação, por via de má conduta, deveria ser compensada, em dobro, pelo instigador dessa má conduta[42], mas sem qualquer relação direta com a violação de segredos comerciais.

3. Independentemente de ser possível traçar conclusões quanto ao âmbito de aplicação da *actio servi corrupti*, bem como quanto à emergência do segredo comercial como *conceito jurídico*, seguindo-se aqui os ensinamentos de Brammsen/Apel[43], reveste-se de interesse enquadrador o facto de que a Europa medieval se organizou através de corporações de ofícios. Estas corporações de ofícios controlavam a produção de bens, regulavam o modo de os comercializar e ordenavam as relações entre os membros das respetivas corporações. Providenciou-se, desta forma, uma proteção institucional orgânica aos segredos dos vários ofícios. Mais do que um direito subjetivo ao segredo comercial, emergiu, neste contexto, um dever estatutário de confidencialidade que beneficiava, por via de externalidade, os membros das corporações de ofícios. Ora, por força da erosão e subsequente abolição da estrutura feudal corporativa e da afirmação da liberdade, no plano industrial e comercial, ganhou corpo a necessidade de tutelar o segredo industrial.

Perante a sobredita erosão da proteção estatutária e orgânica associada às antigas estruturas corporativas, que já se tinha começado a verificar a partir do século XV[44],

---

[40] A. Watson, *Trade Secrets and Roman Law: The Myth Exploded,* Tulane Law Review, v. 11, 1995, pp.19 ss.

[41] A. Watson, *Trade Secrets and Roman Law: The Myth Exploded,* cit., p. 19: "I am not writing to show weaknesses in Schiller's Roman law analysis. What you will see in this Section is the long prologue to a brief *opera buffa* in two Acts".

[42] A. Watson, *Trade Secrets and Roman Law: The Myth Exploded,* cit., pp. 19 ss.

[43] J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p 4.

[44] J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p 4: "Es waren die berufsständischen Vorgaben der Zünfte und Gilden, die mit Wander- und Auswanderverboten für bestimmte Handwerkszweige, Abwerbeverboten und Geboten, Arbeitsgeräte, Werkzeuge und Rohmaterialien nicht Orts- oder Zunftfremden zugänglich zu machen, die seinerzeit dominierende vornehmlich regionale Versorgungswirtschaft abzusichern suchten. Dieser Trend fand mit dem Niedergang des spätmittelalterlichen Personenverbandsstaats und dem Verlust der politischen Macht der Zünfte seit dem 15. Jahrhundert sein langsames Ende: Zunehmend eingeengt durch kaiserliche Edikte, Reichsabschiede, Reichspolizeiverordnungen und das Privilegienwesen verloren

não parece ser muito difícil captar a razão para que, depois da Revolução Francesa, tenha surgido a necessidade de estabelecer novas formas de ordenação de condutas na atividade industrial e comercial. Assim, o Código Penal francês de 1810, no artigo 418.º[45], passou a prever que os gerentes e empregados de fábrica que comunicassem segredos de fábrica – *secrets de fabrique* – a estrangeiros ou a franceses residentes no estrangeiro seriam punidos com pena de prisão e com multa de quinhentos a vinte mil francos; caso o segredo fosse comunicado a franceses residentes em França, a pena de prisão e a multa seriam menores[46]. Na esteira desta inovadora previsão legal francesa, em muitos outros sistemas avançou-se para a expressa consagração da tutela do segredo comercial (mas ainda sem a moderna configuração autónoma). Em Portugal, por exemplo, no dealbar do século XX, no artigo 462.º do Código Penal de 1852 e, depois, no artigo 462.º do Código Penal de 1896[47], passou a incriminar-se a revelação de segredos de fábrica por parte de empregados, operários ou encarregados da administração ou da direção, seguindo-se assim, bem de perto, o legado francês iniciado com o Código Penal francês de 1810[48].

---

ihre wettbewerbsregelnden Satzungen beständig an Wirkung und waren schließlich seit dem dreißigjährigen Krieg kaum noch von verhaltenssteuernder Kraft".

[45] J. L. Capdeville, *Le délit de violation du secret de fabrique*, AJ (Actualité Juridique) Pénal, n° 10, 2011, pp. 459 ss.

[46] Código Penal Francês (1810) – Artigo 418: Tout directeur, commis, ouvrier de fabrique, qui aura communiqué ou tenté de communiquer à des étrangers ou à des Français résidant en pays étrangers des secrets de la fabrique où il est employé, sera puni d'un emprisonnement de deux ans à cinq ans et d'une amende de 1800 F à 120000 F. Il pourra, en outre, être privé des droits mentionnés en l'article 42 du présent Code, pendant cinq ans au moins et dix ans au plus à compter du jour où il aura subi sa peine. Si ces secrets ont été communiqués à des Français résidant en France, la peine sera d'un emprisonnement de trois mois à deux ans et d'une amende de 500 F à 15000 F. Le maximum de la peine prononcée par les paragraphes 1er et 3 du présent article sera nécessairement appliqué s'il s'agit de secrets de fabrique d'armes et munitions de guerre appartenant à l'Etat.

[47] Para mais indicações sobre a evolução histórica da proteção de segredos comerciais no direito português, sobretudo no plano da proteção penal, cfr. M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* Propriedade Intelectual, Contratação e Sociedade da Informação – Estudos Jurídicos em Homenagem a Manuel Oehen Mendes, Col. Estudos de Direito Intelectual, Tomo VI, APDI/Almedina, Coimbra, 2022, pp. 363-364.

[48] Por outro lado e complementarmente, no n.º 8 do artigo 201.º da Lei n.º 21 de maio de 1896, no contexto da identificação de práticas de concorrência desleal, qualificou-se como ilícita a conduta do industrial que, por via de suborno, espionagem, compra de empregados ou operários, ou por outro meio criminoso, conseguisse obter a divulgação de um segredo de fábrica, usando-o depois em seu benefício. Sobre o conceito de *segredo de fábrica*, no contexto geral da *vagueza normativa* da concorrência desleal, Lobo d'Ávila deixou conselho para que "ninguém procure limites precisos na concorrência desleal": J. Lobo d´Ávila, *Da concorrencia desleal*, Imprensa da Universidade,

§3. Segredos comerciais, concorrência desleal e direitos privativos de propriedade industrial

1. O fundamento em que assenta a proteção dos segredos comerciais tem sido objeto de teorização variada[49]. Não obstante a sua proximidade com a concorrência desleal e com os direitos privativos de propriedade industrial, os segredos comerciais apresentam características *sui generis*, sendo disputada a sua qualificação jurídica[50]. Independentemente de ter sido encerrada esta disputa, importa salientar que, no plano puramente empírico, os segredos comerciais têm sido um meio privilegiado pelos agentes de inovação para a proteção dos seus ativos informativos mais valiosos.

A experiência comprova, tal como descrito em vários estudos empíricos – considerando os dados provenientes da União Europeia, Reino Unido, Suíça e Estados Unidos da América –, que os agentes de inovação industrial e comercial têm optado, em percentagem muito significativa, por proteger as suas inovações mais valiosas por via da técnica do segredo comercial[51]. A despeito de poderem ser identificadas razões subjetivas e particulares para justificar essa opção, é asseverável que os segredos comerciais, apesar da sua dúbia configuração jurídica, oferecem vantagens objetivas que têm sido perspetivadas positivamente pelos agentes de inovação[52].

2. Desde logo, a proteção dos segredos comerciais não necessita de submissão a incertos processos administrativos nem aos seus custos, tal como sucede com a proteção das invenções através do procedimento de concessão de patentes. Note-se, aliás, que o espaço digital pode tornar menos eficazes muitas das técnicas de proteção da inovação baseadas em estruturas nacionais ou organismos cuja soberania/jurisdição/competência esteja territorialmente delimitada. A que se aduz ainda a problemática decorrente da divulgação de segredo num determinado território

---

Coimbra, 1910, p. 166.

[49] Tito Rendas, *O segredo dos segredos comerciais: breves reflexões acerca da justificação para a atribuição de proteção à luz da Diretiva (UE) 2016/943*, Os segredos no Direito: Actas de Conferências / coordenação de Carla Amado Gomes, Ana F. Neves, Pedro Lomba, AAFDL Editora, Lisboa, 2019, pp. 273 ss.

[50] Referindo-se aos segredos comerciais como *realidade jurídica híbrida* e "objeto de quase exclusivos", D. Moura Vicente, anotação ao artigo 313.º, *CPI Anotado*, Almedina, 2021, p. 1186.

[51] T. Ocaña, *The Notion of Secrecy, A Balanced Approach in the Light of the Trade Secrets Directive,* Nomos, 2021, p. 55.

[52] D. S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important,* Berkeley Technology Law Journal, v. 27, n.º 2, 2012, p. 1108.

soberano e consequentes efeitos no território de outro estado soberano[53], exponenciada pela natureza transnacional do espaço digital. Muitos dos métodos clássicos de proteção da inovação apresentam problemas de eficiência económico-jurídica, como sucede precisamente no caso do *software*[54].

Por outro lado, o recurso à via dos segredos comerciais assegura, por natureza, um nível muito elevado de proteção real, uma vez que não é necessária qualquer exposição do conteúdo do segredo, ao contrário do que sucede no procedimento de concessão de patentes, em que se exige a divulgação do segredo na descrição da patente.

3. Por último, mas não com menor relevância, a proteção da inovação através de segredos comerciais não está sujeita a um prazo legalmente fixado. Assim, a via do segredo comercial permite que a defesa da inovação se dilate por períodos mais longos do que os da proteção obtida pelos direitos de propriedade industrial[55], nomeadamente pelo prazo que delimita a proteção conferida pelo direito das patentes. Exemplos clássicos da proteção de inovação através de segredos comerciais, extravasando temporalmente a duração das patentes, são a fórmula secreta da *Coca-Cola*[56] – o segredo da *Coca-Cola* está submetido à forma escrita, é guardado num cofre e é conhecido apenas por duas pessoas, sendo proibida a sua digitalização ou inserção no espaço digital[57] – e a receita *onze ervas e especiarias* (*11 Herbs &*

---

[53] Veja-se a decisão *Franchi v. Franchi* (1967), do *High Court of Justice of England and Wales*, Reports of Patent, Design and Trade Mark Cases, v. 84, n.º 5, 1967, pp. 149 a 153, defendendo que a publicação de segredo na descrição de uma patente, mesmo que ocorra na Bélgica, faz cessar o segredo comercial também na Inglaterra. Em sentido não similar, a decisão *Kieselsäure,* do BGH (1962), sustentando que a publicação de segredo na descrição de uma patente nos Estados Unidos da América não invalida automática e necessariamente anteriores acordos celebrados, nos termos do direito alemão, que tenham por objeto esse segredo comercial: BGH, 16.10.1962 – KZR 11/61, GRUR 1963, p. 207.

[54] Como refere Ohly, embora os programas de computadores possam ser protegidos por direitos de autor e por patentes, os segredos comerciais manifestam-se, no entanto, decisivos no campo do *software*: cfr. A. Ohly, *Harmonising the Protection of Trade Secrets: Challenges and Perspectives,* La protection des secrets d'affaires, The Protection of Trade Secrets (A. Jazairy, A. Ohly, J. Passa, R. Schlosser, S. Turner, J. de Werra), Schulthess, Genève/Zurich/Bâle, 2013, p. 26.

[55] Admitindo a existência de limitações temporais mesmo nas situações de segredo comercial: T. Ocaña, *The Notion of Secrecy, A Balanced Approach in the Light of the Trade Secrets Directive,* cit., pp. 552 e ss.

[56] *Coca-Cola Bottling Co. of Shreveport, Inc. v. the Coca-Cola Co*., 107 F.R.D. 288 (D. Del. 1985) 227 U.S.P.Q. (BNA) 18 (acesso: *lawjustitia.com*).

[57] O acesso ao cofre onde é mantido o segredo da Coca-Cola depende de prévia autorização do seu conselho de administração. No caso *Coca-Cola Bottling Co. of Shreveport, Inc. v. the Coca-Cola Co*.

Spices) da empresa *KFC*, também conhecida como receita do *Coronel Harlan Sander,* que envolve um método de produção com separação empresarial[58].

4. No que respeita à relação da concorrência desleal com os segredos comerciais, sobressai o seguinte elemento: quando a tutela do segredo comercial é absorvida pelo regime da concorrência desleal, ocorre uma limitação subjetiva do seu âmbito de aplicação[59]. Com efeito, a tutela da concorrência desleal assenta, primordialmente, na definição do conteúdo da *relação subjetiva* de concorrência entre empresas do mesmo setor de atividade. A existência de relação subjetiva de concorrência é, portanto, um pressuposto constitutivo da situação de concorrência desleal. Esta limitação subjetiva do âmbito de aplicação, ainda que possa também surgir na tutela dos segredos comerciais, não é, no entanto, um pressuposto necessário deste tipo de tutela. Como se verá, a evolução da tutela jurídica dos segredos comerciais, a par da tutela penal, caminhou no sentido da sua autonomização, ainda que com alguma variação e fragmentação se comparados os vários sistemas jurídicos que

---

(1985), o *District Court* do Delaware decidiu que as fórmulas da *Coca-Cola*, *New Coca-Cola* e *Diet Coke*, deviam ser revelados à *Cola Bottling Co. of Shreveport, Inc.*, porque esta cumpriu o seu ónus probatório de demonstrar ter uma necessidade da fórmula maior do que a necessidade da *Coca-Cola Co*. para a proteção dos seus segredos. Porém, a referida instância sublinhou que dada a natureza *proprietária* da informação, justificava-se uma ordem judicial de proteção mais rigorosa do que a usual para impedir a divulgação pública das fórmulas, nomeadamente para limitar a divulgação das fórmulas apenas ao advogado do julgamento e a peritos independentes. Cfr. *Coca-Cola Bottling Co. of Shreveport, Inc. v. the Coca-Cola Co*., cit.: "It has been held that defendant must disclose its complete formulae, including secret ingredients, for diet Coke, old Coke, new Coke, caffeine free Coke, and certain experimental low calorie colas, but not the formulae for TAB and caffeine free diet Coke. In addition, it has been held that defendant must disclose certain taste test results. Given the proprietary nature of the formula information, however, a more stringent protective order than the one currently in effect is warranted to prevent public disclosure of the formulae. For example, it may be advisable to limit the disclosure of the formulae to plaintiffs' trial counsel and independent experts. Because the parties have not addressed what additional protective measures would be satisfactory, the Court will not enter a new protective order at this time. Instead, the parties shall negotiate a protective order that both allows access to information and prevents disclosure of trade secrets. The parties shall submit that order within twenty days".

[58] O seu processo de fabrico envolve empresas separadas. A mistura das especiarias não é executada apenas por uma empresa; para a manter em segredo, metade dos ingredientes são misturados pelos Laboratórios *Griffith* e depois a mistura é enviada para a empresa *McCormick*, onde a outra metade é adicionada. Sobre a sua proteção como *trade secret*, cfr. *KFC Corp. v. Marion-Kay Co., Inc.,* (620 F. Supp. 1160, S.D. Ind. 1985, US District Court for the Southern District of Indiana – 620 F. Supp. 1160 (S.D. Ind. 1985) (acesso: *law.justia.com*).

[59] D. Moura Vicente, anotação ao artigo 313.º, *Código da Propriedade Industrial Anotado*, Almedina, 2021, p. 1186.

acolheram a proteção autónoma dos segredos comerciais, libertando-a do pressuposto da *relação subjetiva concorrencial.*

II. Coordenadas gerais

§1. Situação anterior à diretiva europeia de 2016

1. Para assegurar uma proteção efetiva contra a concorrência desleal, seguindo o curso iniciado no artigo 10.º *bis* da Convenção de Paris (1967)[60], no artigo 39.º do TRIPS (1994)[61] foi inscrita a finalidade de proteger certo tipo de *informações*

---

[60] Decreto n.º 22/75, Diário da República n.º 18. Série, I, 22 de janeiro de 975: Convenção de Paris para a Protecção da Propriedade Industrial, de 20 de Março de 1883, revista em Bruxelas a 14 de Dezembro de 1900, em Washington a 2 de Junho de 1911, na Haia a 6 de Novembro de 1925, em Londres a 2 de Junho de 1934, em Lisboa a 31 de Outubro de 1958 e em Estocolmo a 14 de Julho de 1967. Artigo 10.º-*bis*– 1) Os países da União obrigam-se a assegurar aos nacionais dos países da União protecção efectiva contra a concorrência desleal. 2) Constitui acto de concorrência desleal qualquer acto de concorrência contrário aos usos honestos em matéria industrial ou comercial. 3) Deverão proibir-se especialmente: 1.º Todos os actos susceptíveis de, por qualquer meio, estabelecer confusão com o estabelecimento, os produtos ou a actividade industrial ou comercial de um concorrente; 2.º As falsas afirmações no exercício do comércio, susceptíveis de desacreditar o estabelecimento, os produtos ou a actividade industrial ou comercial de um concorrente; 3.º As indicações ou afirmações cuja utilização no exercício do comércio seja susceptível de induzir o público em erro sobre a natureza, modo de fabrico, características, possibilidades de utilização ou quantidade das mercadorias.

[61] O Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio (1994), Parte II – Normas relativas à existência, âmbito e exercício dos direitos de propriedade intelectual

Artigo 39.º 1 – Ao assegurar uma protecção efectiva contra a concorrência desleal, conforme previsto no artigo 10.º bis da Convenção de Paris (1967), os Membros protegerão as informações não divulgadas em conformida: de com o disposto no n.º 2 e os dados comunicados aos poderes públicos ou organismos públicos em conformidade com o disposto no n.º 3; 2 – As pessoas singulares e colectivas terão a possibilidade de impedir que informações legalmente sob o seu controlo sejam divulgadas, adquiridas ou utilizadas por terceiros sem o seu consentimento de uma forma contrária às práticas comerciais leais (*), desde que essas informações: a) Sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exactas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; b) Tenham valor comercial pelo facto de serem secretas; e c) Tenham sido objecto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secreta; (...) (*) *Para efeitos da presente disposição, a expressão «de uma forma contrária às práticas comerciais leais» designará pelo menos práticas como a ruptura de contrato, o abuso de confiança e a incitação à infracção, incluindo a aquisição de informações não divulgadas por parte de terceiros que tinham conhecimento de que a referida aquisição envolvia tais práticas ou que demonstraram grave negligência ao ignorá-lo.*

não divulgadas[62]. Para esse efeito, procurando harmonizar conceitos, ficou previsto, para que sejam protegidas como segredo comercial, que as informações devem: *(i)* ser secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; *(ii)* possuir valor comercial pelo facto de serem secretas; *(iii)* ter sido objeto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas[63].

2. Com maior ou menor proximidade em relação ao TRIPS (1994)[64], tomando agora a situação europeia como caso de estudo, verifica-se uma variação muito significativa na forma de tutelar as *informações não divulgadas*. A análise sistemática dos vários modelos de proteção dos segredos comerciais, existentes na União Europeia antes de 2016, foi levada a cabo por Ohly[65], postulando este Autor que os segredos comerciais surgem frequentemente como a *cinderela* ou o *órfão* do direito da propriedade intelectual.

O estudo de Ohly parte da análise do relatório elaborado em 2011, a pedido da Comissão Europeia, pela sociedade de advogados *Hogan Lovells*[66], nele se identificando, naquela data, seis grandes modelos de proteção jurídica de segredos comerciais no contexto europeu: *(i)* o primeiro modelo corresponde ao sistema sueco, neste sendo possível encontrar uma previsão específica de *tutela autónoma* dos segredos comerciais desde 1990[67]; *(ii)* o segundo modelo, designado como *modelo propriedade intelectual*, corresponde ao sistema consagrado no Código da Propriedade Intelectual italiano de 2005[68] e traduz a inclusão dos segredos comerciais na categoria de direitos de propriedade intelectual; *(iii)* o terceiro modelo corresponde ao *modelo híbrido francês*[69], no qual se opera uma distinção entre segredos de fábrica (perspetivados como direitos de propriedade

---

[62] T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 37, N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, Kluwer Law International, 2008, pp. 200 ss.

[63] M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., pp. 363 ss.

[64] N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, cit., pp. 189 ss., pp. 224 ss.

[65] A. Ohly, *Harmonising the Protection of Trade Secrets: Challenges and Perspectives,* cit., p. 25.

[66] *Study on Trade Secrets and Parasitic Copying (Look-alikes)*, *Report on Trade Secrets for the European Commission*, Hogan Lovells International, LLP, 2011(acesso: *https://op.europa.eu/en/publication-detail/-/publication/068c999d-06d2-4c8e-a681-a4ee2eb0e116*).

[67] *Study on Trade Secrets and Parasitic Copying (Look-alikes)*, cit., p. 32.

[68] *Study on Trade Secrets and Parasitic Copying (Look-alikes)*, cit., p. 21.

[69] *Study on Trade Secrets and Parasitic Copying (Look-alikes)*, cit., p. 17.

intelectual) e segredos comerciais (beneficiando da proteção pelo regime da concorrência desleal e do direito delitual civil e penal); *(iv)* o quarto modelo, como sucede em Espanha[70], associa a proteção dos segredos comerciais à *tutela geral da concorrência desleal*; *(v)* o quinto modelo, identificável na Alemanha[71], Áustria[72] e Polónia[73], promove o desenvolvimento jurídico da proteção dos segredos comerciais com base na *incriminação penal* da concorrência desleal associada à tutela civil; *(vi)* por último, o sexto modelo, presente no Reino Unido[74] e na Irlanda[75], perante a ausência de regime legal específico, ainda assim permite a proteção dos segredos comerciais por via da *breach of confidence*.

3. Apesar da existência de diversos modelos de regulação, Ohly realçou que os segredos comerciais não fomentaram, no contexto europeu, significativo interesse e tratamento científico jurídico. Nas suas palavras: "em comparação com outras áreas da propriedade intelectual, como o direito de patentes ou o direito de autor, há menos decisões judiciais, há surpreendentemente poucos escritos académicos, e mesmo conceitos chave como a definição de segredo comercial, os meios de apropriação indevida e a noção de *unfairness* (deslealdade) ainda não foram completamente esclarecidos"[76]. Ohly teve então ocasião de referir que "salvo a exceção do artigo 39.º do TRIPS, não houve qualquer harmonização do direito europeu (...) e não existem acórdãos do Tribunal de Justiça da União Europeia que possam atrair a atenção de praticantes e estudiosos"[77].

Porém, os estudos empíricos revelam que a técnica do segredo comercial tem sido historicamente assumida pelos agentes de inovação como um meio privilegiado para acautelar as suas inovações industriais e comerciais. Com este pano de fundo, a crescente integração política e económica do bloco europeu ditou a necessidade de harmonizar a proteção dos segredos comerciais na União Europeia. Consonantemente, em 2013, a Comissão Europeia apresentou, pela primeira vez, uma proposta de diretiva europeia relativa à *proteção dos segredos comerciais*[78]: a fragmentação jurídica

---

[70] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 20.
[71] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 18.
[72] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 10.
[73] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 24.
[74] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 33.
[75] *Study on Trade Secrets and Parasitic Copying (Look-alikes),* cit., p. 20.
[76] A. Ohly, *Harmonising the Protection of Trade Secrets: Challenges and Perspectives,* cit., p. 25.
[77] A. Ohly, *Harmonising the Protection of Trade Secrets: Challenges and Perspectives,* cit., p. 26.
[78] Entre nós, sobre esta proposta de diretiva, oferecendo panorama geral e perspetivas quando à fundamentação/justificação teórica do regime: N. Sousa e Silva, *A proposta de diretiva em matéria de segredos comerciais – estado e perspectivas,* R.D.I., n.º 2, 2014, pp. 285-319.

no bloco europeu introduzia, segundo as autoridades europeias, uma indesejável desarmonia jurídica no espaço europeu. Daqui resultou a aprovação da diretiva 2016/943, de 8 de junho de 2016[79/80].

§2. A uniformização europeia da proteção dos segredos comerciais

2.1. A diretiva 2016/943 relativa à proteção de *know-how* e de informações comerciais confidenciais – segredos comerciais – contra a sua aquisição, utilização e divulgação ilegais

1. Com este enquadramento e relevando devidamente a especial perigosidade do espaço digital, o ponto 4. dos considerandos da diretiva 2016/943, de 8 de junho de 2016, espelha a preocupação das autoridades europeias quanto à necessidade de harmonizar a proteção dos segredos comerciais. O Parlamento Europeu e o Conselho da União Europeia sublinharam precisamente que as "empresas inovadoras (...) estão cada vez mais expostas a práticas desonestas que visam a apropriação indevida de segredos comerciais, como o roubo, a cópia não autorizada, a espionagem económica ou a violação de requisitos de confidencialidade, quer dentro, quer fora da União", acentuando ainda que essa exposição é agravada por novos elementos como "a globalização (...) e o uso acrescido de *tecnologias da informação e comunicação*" (*itálico nosso*), pois esses novos elementos "contribuem para o aumento do risco destas práticas".

Foi precisamente neste contexto que as autoridades europeias decidiram criar "meios jurídicos eficazes" para proteger os segredos comerciais na União Europeia[81], dado que a "aquisição, utilização ou divulgação ilegais de um segredo comercial comprometem a capacidade de o titular legítimo do segredo comercial obter retornos de pioneiro decorrentes dos seus esforços relacionados com a inovação"[82].

2. Foi assim que, na diretiva europeia, o segredo comercial surgiu conceitualmente como correspondendo às informações que cumulativamente tenham as seguintes

---

[79] Jornal Oficial da União Europeia (PT), 15/6/2016, pp. L.157/1–L.157/18, Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais.

[80] T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 14.

[81] T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 15.

[82] Jornal Oficial da União Europeia (PT), 15/6/2016, p. L.157/2.

características[83]: *(i)* serem secretas, no sentido de não serem geralmente conhecidas pelas pessoas dos círculos que lidam normalmente com o tipo de informações em questão, ou não serem facilmente acessíveis a essas pessoas; *(ii)* terem valor comercial pelo facto de serem secretas; *(iii)* e terem sido objeto de diligências razoáveis, atendendo às circunstâncias, para serem mantidas secretas pela pessoa que exerce legalmente o seu controlo[84/85].

No escopo da diretiva europeia de 2016 há alguns requisitos fundamentais a considerar. Uma primeira premissa é a de que, para que haja segredo comercial, a informação não pode ser do *conhecimento geral* e/ou não pode ser *facilmente acessível*: este elemento é particularmente relevante no plano da sociedade digital, tendo em consideração o problema da divulgação (*disclosure*) de segredos comerciais na *Internet*. Em segundo lugar, é ainda necessário que a informação tenha valor comercial por ser secreta. Por último e tão importantemente, a diretiva veio estabelecer o padrão de conduta exigível ao titular do segredo comercial – este tem o dever de adotar *diligências razoáveis* para a manutenção da informação secreta.

---

[83] Artigo 2º da Diretiva 2016/943, de 8 de junho de 2016 – Definições: Para efeitos da presente diretiva, entende-se por: 1) «Segredo comercial», as informações que cumprem cumulativamente os requisitos seguintes: a) serem secretas, no sentido de, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, não serem geralmente conhecidas pelas pessoas dos círculos que lidam normalmente com o tipo de informações em questão, ou não serem facilmente acessíveis a essas pessoas; b)terem valor comercial pelo facto de serem secretas; c) terem sido objeto de diligências razoáveis, atendendo às circunstâncias, para serem mantidas secretas pela pessoa que exerce legalmente o seu controlo; 2) «Titular do segredo comercial», a pessoa singular ou coletiva que exerce legalmente o controlo de um segredo comercial; 3) «Infrator», a pessoa singular ou coletiva que tenha adquirido, utilizado ou divulgado ilegalmente um segredo comercial.
4) «Mercadorias em infração», mercadorias cuja conceção, características, funcionamento, processo de produção ou comercialização beneficiam significativamente de segredos comerciais adquiridos, utilizados ou divulgados ilegalmente.

[84] Por outro lado, no contexto da diretiva, a aquisição de um segredo comercial sem o consentimento do titular do segredo comercial é tida como ilegal sempre que tal resulte de: *i)* acesso, apropriação ou cópia não autorizados de documentos, objetos, materiais, substâncias ou *ficheiros eletrónicos*, legalmente sob controlo do titular do segredo comercial, que contenham o segredo comercial ou a partir dos quais seja possível deduzir o segredo comercial; *ii*) outras c*ondutas* que, nas circunstâncias específicas, sejam *consideradas contrárias às práticas comerciais honestas.* Tendo sido *ilegalmente adquirido,* a utilização ou divulgação de um segredo comercial é também considerada ilegal sem o consentimento do titular do segredo comercial.

[85] Verifica-se, portanto, que na diretiva europeia relativa à proteção de segredos comerciais foi acolhido um conceito jurídico de segredo comercial composto pelos três elementos que de modo similar já constavam do artigo 39.º do TRIPS (1994): T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 14.

Contanto que estes requisitos não se tenham dado como verificados, tal impede a aplicação do regime de proteção jurídica do segredo comercial. Explicite-se ainda que o último requisito apontado – *diligências razoáveis* – é de todo significado no contexto da sociedade digital, uma vez que confronta os agentes de inovação com a necessidade de adotar permanentemente uma conduta preventiva – e, por vezes, reativa – para assegurar a manutenção do segredo comercial no quadro da dinâmica do espaço digital. Haverá ocasião, mais adiante, para enunciar pistas de concretização desta importante exigência de adotar *diligências razoáveis*.

2.2. A harmonização europeia no contexto global: o regime norte-americano

1. No seguimento dos pontos anteriores, cumpre sublinhar que tanto o TRIPS (1994) como a diretiva europeia (2016) devem ser contextualizados pela evolução da proteção dos segredos comerciais no sistema norte-americano. Com efeito, do sistema norte-americano resultaram geneticamente os elementos que determinaram o desenho final do artigo 39.º do TRIPS (1994) e que conformaram também os atuais sistemas europeus[86]. Assim, a importância do elemento histórico comparado conduz-nos a analisar a evolução do sistema norte-americano, elemento determinante para a explicitação do sentido normativo do artigo 2.º da diretiva europeia de 2016, bem como do artigo 313.º CPI (2018).

Posto isto, saliente-se que, nos Estados Unidos da América, a tutela dos segredos comerciais desenvolveu-se judicialmente a partir de princípios jurídicos, percorrendo um longo curso até à sua etapa mais recente com a aprovação do *Defense Trade Secret Act* (2016)[87]. Tradicionalmente, é apontada a decisão judicial de 1868, no caso *Joseph Peabody & others, executors v. John R. Norfolk & another*[88], do *Supreme*

---

[86] Como já foi possível identificar anteriormente, a proteção dos segredos comerciais convoca, em muitos casos, a necessidade de concretizar cláusulas gerais e/ou conceitos indeterminados. Nessa medida, tem muita relevância, atender ao que vem sendo concretizado pela jurisprudência norte-americana, que é confrontada frequentemente com casos que espelham bem a dificuldade da proteção de segredos comerciais na era digital: recorde-se o exemplo, acima mencionada, do recente caso *Compulife Software, Inc. v. Newman,* com decisões divergentes por parte do *District Court* da Florida (United States District Southern Florida District Court, caso 9:16-cv-81942-BER (2017), e do *Court of Appeal* (Atlanta/Georgia) United States Court of Appeals (11th Circuit), D.C. Docket No. 9:16-cv-8 0808-RLR (2020), relativo à utilização de *bots* para desenvolver a atividade de *data scraping* de portais comerciais disponíveis na *Internet.*

[87] Public Law, 114th Congress, Defend Trade Secrets Act of 2016, 11/5/2016, pp. 114-153.

[88] *Massachusetts Supreme Judicial Court: Joseph Peabody & others, executors, v. John R. Norfolk & another*, Massachusetts Supreme Judicial Court Reports, volume 98, p. 452 ss. Sinteticamente: P., tendo construído uma fábrica, equipando-a com maquinaria secretamente inventada por ele mesmo

Court de *Massachusetts*, como a decisão judicial pioneira quanto à proteção de *trade secrets*. No caso que espoletou esta histórica decisão, a instância norte-americana decidiu que "aquele que inventa ou descobre, e mantém em segredo, um processo de fabrico, próprio de uma patente ou não, tem sobre ele *propriedade*, propriedade esta que um tribunal protegerá contra aquele que, em violação do contrato e quebra de confiança, se compromete a aplicá-la ao seu próprio uso ou a revelá-la a terceiros" (*itálico nosso*), sublinhando ainda que "um segredo de comércio ou fabrico não perde o seu carácter ao ser revelado confidencialmente a agentes ou empregados"[89].

2. Para compreender a evolução do sistema norte-americano, são muito valiosos os ensinamentos de Robert Bone[90]. Na sua lição, partindo da decisão de 1868 do *Supreme Court* de *Massachusetts*, a evolução do sistema norte-americano teve várias fases até se alcançar a codificação federal em 2016. Em primeiro lugar, numa primeira fase que se expandiu até 1920, os segredos comerciais foram essencialmente perspetivados como *forma de propriedade*[91] ("The Dominance of the Property Theory")[92]. Seguiu-se uma fase que durou até cerca de 1940, verificando-se

---

para fabricar tecidos de juta por um processo secreto também de sua invenção, fez um contrato escrito com N., que havia adquirido conhecimento confidencial dessas invenções enquanto estava envolvido com P. na assistência nas experiências e na construção das máquinas para a referida fábrica. Por este contrato, N. concordou em "servir" P., como engenheiro da fábrica, obrigando-se a "considerar todas as referidas máquinas como sagradas, para serem usadas apenas em benefício de P. ou seus cessionários" e "por todos os meios ao seu alcance impedir que outras pessoas obtenham tal que lhes permita usá-lo". P. concordou em pagar a N. um salário "pelos serviços descritos acima", "desde que N. preste seus serviços aceitáveis a P., e P. ou seus cessionários ou agentes continuem os negócios na referida fábrica ou em outro lugar." O tribunal considerou que o salário acordado a ser pago por P. a N. era suficiente *consideration* (causa) para a promessa de N. de manter em segredo as invenções de P., bem como para a promessa de servir como engenheiro na fábrica de N.

[89] *Massachusetts Supreme Judicial Court: Joseph Peabody & others, executors, v. John R. Norfolk & another,* cit., p. 461.

[90] R. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, California Law Review, v. 86, n.º 2, 1998, pp. 241-313; *id, Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* The Law and Theory of Trade Secrecy, Edward Elgar Publishing, 2011, pp. 46 e ss; *id., The (Still) Shaky Foundations of Trade Secret Law*,Texas Law Review, v. 92, n.º 7, 2014, pp. 1803-1838.

[91] Este dado histórico é decisivo, porquanto explicita a razão de no sistema norte-americano ter emergido a necessidade de tomar *reasonable measures* para manter o segredo comercial: estas medidas eram enquadradas como conduta possessória relevante. Adiante retomar-se-á este ponto, pela sua extrema relevância, quando for analisado mais detalhadamente o requisito das *medidas razoáveis,* hoje previsto na alínea c) do n.º 1 do artigo 313.º CPI de 2018.

[92] R. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* cit., p. 49.

tendencial e paulatinamente o afastamento judicial da teoria da propriedade e a aproximação dos tribunais norte-americanos à tutela dos segredos comerciais como *ato de concorrência desleal* ("The Decline of the Property Theory and the Rise of Unfair Competition Theory"[93]). Essa aproximação tendencial passou a ser dominante a partir de 1940 e até 1979, período em que os segredos comerciais surgiram intrinsecamente relacionados com o desenvolvimento judicial da *teoria da concorrência desleal* ("The Dominance of the Unfair Competition Theory"[94]). Por seu turno, o ano de 1979 data historicamente um dos momentos mais decisivos para a evolução da proteção jurídica dos segredos comerciais: dá-se a aprovação do *Uniform Trade Secrets Act* (UTSA/1979), por parte da *Uniform Law Commission*, no seguimento de uma recomendação formulada pela *American Bar Association*, promovendo-se a autonomização da tutela dos segredos comerciais.

3. O UTSA (1979) foi aprovado por ser necessário harmonizar o nível de proteção dos segredos comerciais, uma vez que essa proteção apresentava significativa variação nos vários estados norte-americanos[95]. Dada a natureza não vinculativa do UTSA (1979), o seu propósito foi o de servir ordenadoramente como modelo de uniformização normativa, registando, a esse nível, significativo êxito, pois foi transposto por quase todos os estados norte-americanos, corporizando assim a primeira grande uniformização no que respeita aos segredos comerciais[96]. Pela sua

---

[93] R. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* cit., p. 51.

[94] R. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions,* cit., p. 53.

[95] Em particular, sentia-se a necessidade de traçar com mais rigor e de forma harmonizada o conceito jurídico de *trade secret* e os seus elementos constituintes, dada a porosidade conceitual detetada nas leis estaduais e em várias decisões judiciais.

[96] Uniform Trade Secrets Act (National Conference of Commissioners on Uniform State Laws) 1979 (rev. 1985): §1. Definitions: As used in this Act, unless the context requires otherwise: (1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means. (2) "Misappropriation " means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired

evidente relevância, assinale-se como, no §1.4. do UTSA (1979), o conceito de *trade secret* surgiu definido como *informação – fórmulas, padrões, compilações, programas, aparelhos/instrumentos, métodos, técnicas* e *processos* – da qual resulte valor económico, atual ou potencial, por não ser geralmente conhecida e por não ser facilmente acessível por meios adequados por parte de pessoas que possam obter ganhos económicos com a sua divulgação ou utilização. Por outro lado, como requisito herdado da *Property Theory*, essa informação, para ser protegida, teria de ter sido objeto de *esforços razoáveis – reasonable efforts* – para manter a sua natureza secreta.

4. Posteriormente, no contexto da crescente globalização e da expansão do espaço digital, o Congresso dos Estados Unidos da América aprovou, em 1996, o *Economic Espionage Act*, visando proteger as empresas inovadoras perante a crescente ameaça da espionagem industrial. Porém, a variação conceitual quanto à noção de segredo comercial persistiu também neste instrumento normativo, gerando diferentes e conflituantes perspetivas estaduais. Por essa razão, o Senado norte-americano promoveu a revisão do *Economic Espionage Act* através do não menos histórico *Defend Trade Secret Act* (DTSA), aprovado em 2016.

De acordo com o §1839 do DTSA (2016)[97], o conceito de segredo comercial passou a abranger todas as formas de informação financeira, comercial, científica,

---

by accident or mistake. (3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity. (4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from no being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

[97] §18 U.S. Code § 1839 (*Defense do Trade Secret Act,* 2016) – As used in this chapter: (...) (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if– (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information; (4) the term "owner", with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed; (5) the term "misappropriation" means– (A) acquisition of a trade secret of another by a person who

técnica e económica – nas quais se incluem: "padrões, planos, compilações, programas, dispositivos de programas, fórmulas, designs, protótipos, métodos, técnicas, processo, procedimentos, códigos, tangíveis ou intangíveis, e independentemente de como foram arquivados, guardados compilados, seja através de forma física, eletrónica, gráfica, fotográfica ou escrita". Por outro lado, para que estas informações sejam juridicamente protegidas, na mesma seção §1839 do DTSA (2016), exige-se ainda que o proprietário dessas informações tenha tomado "as *medidas razoáveis* para manter essa informação secreta" (*itálico nosso*) e que desta informação "resulte valor económico autónomo, atual ou potencial, pela razão de não ser geralmente conhecida e por não ser facilmente acessível por meios adequados por parte de outra pessoa que possa obter ganhos económicos com a sua divulgação ou utilização"[98].

No DTSA (2016) passaram assim a estar consagrados, a nível federal, os principais elementos normativos que geneticamente se filiam no UTSA (1979) – e que, de modo similar, foram depois posteriormente adotados no artigo 39.º do TRIPS (1994) por influência da delegação norte-americana[99]. Estava assim proporcionada, no direito norte-americano, a via para que o conceito de segredo comercial passasse a ter expressa e legalmente uma dimensão jurídica objetiva

---

knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who– (i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was– (I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii)before a material change of the position of the person, knew or had reason to know that– (I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake; (6) the term "improper means"– (A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition.

[98] J. D´ÁVILA, *Da concorrencia desleal*, cit., pp. 252 ss.

[99] Consegue-se assim identificar a origem da necessidade de adotar uma conduta que seja suficiente para preencher o critério de razoabilidade – *reasonable efforts* – no que respeita às medidas tomadas para a manutenção do segredo comercial. Para a *história legislativa* do 39.2 do TRIPS (1994), cfr. N. PIRES CARVALHO, *The TRIPS Regime of Antitrust and Undisclosed Information*, cit., pp. 207 ss., em particular quanto ao requisito da diligência razoável, a proposta americana exigia o seguinte: "to maintain legal protection, the owner of a trade secret may be required to *make efforts reasonable under the circumstances* to maintain such secrecy but need not show that no one else possesses the trade secret. Without losing the requisite secrecy, the owner may communicate a trade secret to employees involved in its use, communicate a trade secret to others pledged to secrecy or make any other communications required by law or as a condition for marketing".

estática (o tipo de informação, sua natureza secreta e o seu valor) e uma dimensão jurídica subjetiva dinâmica (necessidade de adotar um comportamento razoavelmente diligente para preservar o secretismo da informação não divulgada).

III. Segredos comerciais no Código da Propriedade Industrial de 2018

§1. Breve nota sobre a evolução legislativa até 2018

1. No ordenamento jurídico português, a par da incriminação legal prevista no artigo 462.º do Código Penal de 1852 e no artigo 462.º do Código Penal de 1896, a proteção dos segredos comerciais surge historicamente relacionada com o regime da concorrência desleal. Saliente-se como o n.º 8 do artigo 201.º, da Carta de Lei de 21 de maio de 1896, qualificava como ato de concorrência desleal os casos "em que o industrial, por suborno, espionagem, compra de empregados ou operários, ou por outro qualquer meio criminoso, consegue a divulgação de um segredo de fábrica e o utiliza"[100].

Pode assim ser observado que a tutela de informações secretas, sem prejuízo da existência de tutela penal autónoma (ainda que insuficiente)[101], associou-se ao regime da proteção contra a concorrência desleal, neste ficando delimitada tanto no plano subjetivo (agentes industriais) como no plano objetivo (segredos de *fábrica*)[102]. Posteriormente, no n.º 9 do artigo 212.º, do CPI (1940), a violação de segredos da indústria ou comércio continuou a ser considerada como hipótese normativa de concorrência desleal, considerando-se como ilícita a "apropriação, utilização ou divulgação dos segredos da indústria ou comércio de outrem (...)"[103/104].

---

[100] A primeira lei portuguesa a consagrar a proteção da propriedade industrial (apenas relativamente a invenções) data de 16 de janeiro de 1837, seguindo-se várias outras leis nesta matéria até à aprovação da Carta de Lei de 21 de maio de 1896, considerada como o primeiro Código Português da Propriedade Industrial: "*Artigo 201.° São considerados casos de concorrencia desleal, e como taes puniveis: (...) 8.° Aquelles em que o industrial, por suborno, espionagem, compra de empregados ou operarios, ou por outro qualquer meio criminoso, consegue a divulgação de um segredo de fábrica e o utilisa*".

[101] M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., p. 367.

[102] Sobre conceito de *segredo de fábrica,* para efeito do n.º 8 do artigo 201.º, da Carta de Lei de 21 de maio de 1896, cfr. J. d´Ávila, *Da concorrencia desleal*, cit., pp. 252 ss.

[103] Nos termos deste preceito, "todo o operário ou empregado em fábrica ou estabelecimento industrial, ou encarregado da sua administração ou direção, que com prejuízo do seu proprietário descobrir os segredos da sua indústria, será punido com prisão de três meses a dois anos e multa correspondente".

[104] A tutela penal autónoma dos segredos persistiu, depois, no artigo 184.º do Código Penal de 1982 e no artigo 196.º do Código Penal de 1995, cfr. M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., pp. 364-367.

2. Em momento ulterior, na alínea i) do artigo 260.º, com a formulação resultante do posterior CPI (1995), continuou a manter-se a violação dos segredos comerciais no regime da concorrência desleal, prevendo-se que "quem, com intenção de causar prejuízo a outrem ou de alcançar para si ou para terceiro um benefício ilegítimo, praticar qualquer *acto de concorrência* contrário às normas e usos honestos de qualquer ramo de atividade, nomeadamente: (...) a ilícita apropriação, utilização ou divulgação dos segredos da indústria ou comércio de outrem" (*itálico nosso*) deveria ser punido "com pena de prisão até 3 anos ou com pena de multa até 360 dias"[105].

No CPI de 2003, visando adaptar o direito português ao TRIPS (1994)[106], a proteção dos segredos comerciais foi formalmente autonomizada. Contudo, continuou integrada no regime da concorrência desleal[107], através de uma relação de remissão normativa entre os artigos 317.º e 318.º, do CPI de 2003[108]. A despeito da sua qualidade legística[109], no artigo 318.º do CPI (2003), preceito legal relativo à proteção de informações não divulgadas, considerava-se como ato ilícito a divulgação, a aquisição ou a utilização de segredos comerciais de um *concorrente*, sem o consentimento do mesmo, desde que essas informações fossem secretas, tivessem valor comercial e tivessem sido objeto de diligências consideráveis no sentido de as manter secretas. Note-se que a proibição de concorrência desleal através da proteção das informações não divulgadas apenas abrangia subjetivamente os *concorrentes*. Neste contexto, no CPI de 2003, a proteção dos segredos comerciais foi inserida na delimitação do conteúdo da relação subjetiva de concorrência.

3. Por tudo isto, o segredo comercial foi sendo protegido no CPI, pelo menos até 2018, como uma espécie do género normativo da proibição de concorrência

---

[105] Criticamente: J. Cruz, *Sugestões para a revisão do Código da Propriedade Industrial*, Viseu, 1996, p. 13.

[106] No preâmbulo do Decreto-Lei DL n.º 36/2003, de 05 de Março, pode ler-se: "sublinhe-se, ainda, a integração de regras decorrentes do Acordo sobre Aspectos dos Direitos de Propriedade Industrial relacionados com o Comércio (ADPIC), celebrado no âmbito da Organização Mundial do Comércio, da qual Portugal é Estado membro, de pleno direito, desde Janeiro de 1996".

[107] J. Oliveira Ascensão, *Concorrência desleal,* Almedina, Coimbra, 2002, p. 468, Patrício Paúl, *Concorrência desleal de segredos de negócio*, Direito Industrial, II, Almedina, Coimbra, 2002, pp. 139 ss.

[108] Defendendo que a integração da tutela dos segredos comerciais na concorrência desleal é historicamente anacrónica, J. Oliveira Ascensão, *Parecer sobre a proposta de alteração ao Código da Propriedade Industrial*, RFDUL, v. XLI, n.º 1, 2000, p. 333.

[109] Sinalizando má técnica legislativa: J. Patrício Paúl, *Breve análise do regime da concorrência desleal no novo Código da Propriedade Industrial,* R.O.A., ano 63, v. I/II, 2003, p. 339.

desleal[110]. Finalmente, transpondo a diretiva europeia 2016/943, de 8 de junho de 2016, o que sucedeu através do Decreto-Lei n.º 110/2018, de 10 de Dezembro, a tutela dos segredos comerciais no CPI (2018) sofreu uma mudança de paradigma: tornou-se substancialmente autónoma face ao regime da concorrência desleal, preterindo-se a necessidade de relação subjetiva concorrencial[111]. Esta modificação de paradigma ocorrida em 2018, no quadro da sociedade moderna e da expansão do espaço digital, é profundamente relevante, uma vez que, por esta via, o CPI passou a permitir uma proteção transversal do segredo comercial[112/113].

§2. A proteção dos segredos comerciais na doutrina portuguesa

1. Na doutrina portuguesa, têm surgido vários estudos analisando a evolução da proteção jurídica dos segredos comerciais[114], concedendo especial atenção à sua

---

[110] D. Moura Vicente, anotação ao artigo 313.º, *Código da Propriedade Industrial Anotado*, Almedina, 2021, p. 1186.

[111] Defendendo, já anteriormente, a autonomização da tutela dos segredos comerciais: L. Bigotte Chorão, *Notas sobre o âmbito da concorrência desleal*, R.O.A., ano 55.º, v. III, 1995, p. 741.

[112] Como refere Moura Vicente: "diferentemente do que sucedia com o CPI de 2003, o atual Código (*de 2018*) não se limita a sujeitar os segredos comerciais ao regime da concorrência desleal (...) uma vez que não requer (...) uma relação de concorrência": D. Moura Vicente, anotação ao artigo 313.º, *C Anotado*, Almedina, 2021, p. 1186.

[113] Quanto à sua configuração concreta, no artigo 313.º do CPI (2018), os segredos comerciais surgem concretizados como *informações* que reúnam cumulativamente os seguintes requisitos: *(i)* sejam *secretas*, no sentido de *não serem geralmente conhecidas ou facilmente acessíveis,* na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; *(ii)* tenham *valor comercial* pelo facto de serem secretas; *(iii)* tenham sido objeto de *diligências razoáveis* por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas.

[114] D. Moura Vicente, *Proteção do know-how, segredo comercial e direito intelectual,* R.D.I., n.º 2, 2018, pp. 91-118, A. Azevedo Amorim, *A protecção dos segredos comerciais num contexto de mobilidade dos trabalhadores"*, AA.VV., Atas do IX Congresso Internacional de Ciências Jurídico Empresariais, Leiria, Instituto Politécnico de Leiria, 2017, pp. 166-187; *id., O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* Revista Electrónica de Direito, v.19, Junho, 2019*,* pp. 11 ss.; M. Lopes Rocha, *Breve nota sobre a Proposta de Directiva relativa à protecção do know-how não divulgado e ao segredo comercial*, Revista de Direito Intelectual, n.º 1, 2016, pp. 111-118; N. Sousa e Silva, *Um retrato do regime português dos segredos comerciais*, R.O.A., ano 75, I/II, janeiro/junho 2015, pp. 223-257; *id., A nova disciplina dos segredos de negócio, análise e sugestões,* Homenagem ao Professor Doutor Germano Marques da Silva, II, UCP Editora, 2020, pp. 2175 ss.; Tito Rendas, *O segredo dos segredos comerciais: breves reflexões acerca da justificação para a atribuição de proteção à luz da Diretiva (UE) 2016/943*, Os segredos no Direito: Actas de Conferências / coordenação de Carla Amado Gomes, Ana F. Neves, Pedro Lomba, AAFDL Editora, Lisboa, 2019, pp. 273 ss.; Evaristo Mendes, *Segredos comerciais e liberdade profissional*, Revista de Direito Comercial, 2021,

recente autonomização. A este propósito, relevam, no principal, as observações de Moura Vicente, pretextuadas pela revisão do CPI em 2018, defendendo que se verificou uma "clara ampliação do âmbito de aplicação do regime legal do segredo comercial", e concluindo que os segredos comerciais passaram a ter "um estatuto híbrido". Segundo a lição de Moura Vicente, os segredos comerciais, "sem serem objeto de direitos de exclusivo, beneficiam de um regime muito próximo dos direitos de propriedade industrial", sendo, nesta medida, "o objeto de quase exclusivos"[115]. Similarmente, Azevedo de Amorim veio também enfatizar que "a necessidade de *alargar o âmbito de aplicação* da proteção dos segredos comerciais ao nível europeu esteve na origem da aprovação da Diretiva" (*itálico nosso*), bem como que, "contrariando o disposto anteriormente no CPI de 2003 (...) o novo diploma estendeu o regime jurídico a terceiros", deixando de "estar em causa necessariamente uma relação de concorrência"[116]. Assim, ainda de acordo com Azevedo de Amorim, "podem agora ser qualificados como infratores, por exemplo, os jornalistas que divulguem ilicitamente informação protegida, sem fundamento no interesse público"[117].

Reportando-nos agora ao ponto que mais interessa a este estudo – a proteção do segredo comercial no *espaço digital* – importa recensear criticamente, embora com traço muito largo e de modo genérico, o vem sendo afirmado quanto à atual formulação do enunciado normativo constante do artigo 313.º do CPI (2018). Mais concretamente quanto: *a)* ao *tipo de informação* juridicamente relevante para o conceito de segredo comercial; *b)* à sua *natureza secreta*; *c)* ao seu *valor económico*; *d)* e à necessidade de realizar *diligências razoáveis* para a manutenção do segredo. É necessário apreender perfunctoriamente este quadro geral para depois, na especialidade, o concretizar criticamente no plano do espaço digital.

a) Tipo de informação

2. O primeiro elemento que sobressai quando analisado o conceito jurídico de segredo comercial, nos termos do n.º 1 do artigo 313.º do CPI (2018), é a sua

---

pp. 743-848; M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* Propriedade Intelectual, Contratação e Sociedade da Informação – Estudos Jurídicos em Homenagem a Manuel Oehen Mendes, Col. Estudos de Direito Intelectual, Tomo VI, APDI/Almedina, Coimbra, 2022, pp. 363 ss.

[115] D. Moura Vicente, anotação ao artigo 313.º, *CPI Anotado*, cit., p. 1186.

[116] A. Azevedo de Amorim, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* cit., p. 18.

[117] A. Azevedo de Amorim, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* cit., p. 18.

associação ao conceito de *informação*. Esta, a informação, tem sido concretizada na doutrina portuguesa, tal como sucede com Sousa e Silva, como correspondendo a um "conjunto de dados organizados/estruturados"[118]. Por seu turno, Moura Vicente propõe que o conceito de informação deve ser interpretado de forma a nele ser possível compreender todos "os conhecimentos e experiências de natureza técnica, comercial, administrativa, financeira ou outra, aplicáveis na prática para a explicação de uma empresa ou o exercício de uma profissão"[119]. Moura Vicente anota relevantemente que aquele preceito legal abrange não apenas a informação confidencial "relativa à atividade empresarial"[120] como também "o *know how*, as informações empresariais e as informações tecnológicas"[121].

b) Natureza secreta da informação

3. Relativamente à natureza *secreta* da informação, tomando em consideração o previsto na alínea a) do artigo 313.º do CPI (2018), estabelece-se que essa natureza secreta resultará do facto de as informações *não serem geralmente conhecidas* ou *facilmente acessíveis*, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão. É de recordar que é necessário um requisito objetivo – *informações não conhecidas geralmente ou não facilmente acessíveis* –, depois delimitado por um círculo legal subjetivo – *pelas pessoas que lidam com esse tipo de informação*. Em momento expositivo superveniente, mais integrada será a compreensão deste aspeto.

Porém, desde já, tem interesse registar a observação de Sousa e Silva a propósito da natureza secreta da informação. Refere este Autor que "*a partir do momento* em que a informação *seja publicada,* o segredo *perde-se*" (*itálico nosso*)[122]. Esta posição do referido Autor – que não persuade plenamente se tomada como postulado absoluto, pelas razões que sobrevirão no texto – é particularmente relevante no

[118] N. Sousa e Silva, *A nova disciplina dos segredos de negócio, análise e sugestões,* cit., p. 2182.
[119] D. Moura Vicente, anotação ao artigo 313.º, *CPI Anotado*, cit., p. 1185.
[120] D. Moura Vicente, anotação ao artigo 313.º, *CPI Anotado*, cit., p. 1185.
[121] Para Moura Vicente, tem pertinência salientar que, no direito português vigente, o conceito de segredo comercial, quanto ao elemento *informação,* compreende assim, de forma ampla, tanto o *(i) segredo industrial* – informação secreta patenteável ou não relativa a métodos ou técnicas de produção e aos próprios produtos industriais – como o *(ii) segredo comercial em sentido estrito* – informação secreta relativa à atividade das empresas: D. Moura Vicente, anotação ao artigo 313.º, *CPI Anotado*, cit., p. 1185.
[122] N. Sousa e Silva, *A nova disciplina dos segredos de negócio, análise e sugestões,* cit., p. 2182.

contexto do espaço digital. Como já foi sublinhado, o espaço digital corresponde a um aumento do espaço real, representando, nessa medida e proporcionalmente, uma expansão da potencialidade de danos resultantes da divulgação de informação secreta na *Internet*. A pergunta que se impõe formular, ao examinar-se este requisito, é a seguinte: a publicação ou divulgação de um segredo comercial na *Internet* implica *ipso facto*, como postulado absoluto e de um modo quase axiomático, que a informação deixe de ser considerada juridicamente como segredo comercial?

Note-se que a divulgação, para ser relevante, tem de atingir o *círculo legal subjetivo*, que é, nos termos legais nacionais, composto apenas pelas pessoas que lidam normalmente com o tipo de informação que esteja concretamente em causa. Um enunciado de resposta à pergunta agora formulada integrará a parte especial deste estudo, quando se analisar o problema da divulgação (*disclosure*) de segredos comerciais no espaço digital. Para já, é advertência bastante a de que se impõe alguma cautela metodológica, pois cominar *ipso facto* toda e qualquer publicação com a cessação do estatuto de segredo comercial parece ser passo maior do que o possível, atendendo aos dados legais vigentes.

c) Valor comercial da informação

4. Relativamente ao valor comercial da informação protegida, na alínea b) do artigo 313.º do CPI (2018), prescreve-se que essas informações devem ter *valor comercial* precisamente pelo facto de serem secretas. Como ponto dubitativo surge o momento em que deve ser avaliado o valor comercial, podendo ser apenas considerado o valor comercial atual ou também o valor potencial. Na doutrina portuguesa, Sousa e Silva defende que o valor atual "parece ser a melhor" concretização do conceito de valor comercial[123]. Em estudo anterior, Sousa e Silva havia afirmado esta posição, invocando então que "entendemos que o valor potencial não tem real significado: tudo o que existe tem valor potencial"[124]. Não operando, porém, a lei portuguesa qualquer distinção, também não persuade a invocada justificação metodológica para o afinamento conceitual proposto pelo Autor, podendo, de resto, conduzir a uma restrição do âmbito de danos indemnizáveis. Tal como ensina Ohly[125], respeitando-se o espírito da diretiva europeia, que é sempre elemento com

[123] N. Sousa e Silva, *A nova disciplina dos segredos de negócio, análise e sugestões,* cit., p. 2182.
[124] N. Sousa e Silva, *Um retrato do regime português dos segredos comerciais*, cit., p. 240 (nota 96).
[125] A. Ohly, *Das neue Geschäftsgeheimnisgesetz im Überblick,* GRUR, 5/19, p. 443, sublinhando que "Auch unter § 2 Nr. 1 Buchst. a GeschGehG ist das Kriterium des „wirtschaftlichen Werts" weit zu verstehen, wie ein Blick auf Erwägungsgrund 14 der GeschGeh-RL zeigt", bem como que

relevância na atividade interpretativa, é de valorizar que, no considerando n.º 14 da referida diretiva, o conceito de valor comercial surja precisamente, de forma ampla, como valor comercial real ou potencial[126]. E não parece tratar-se de uma questão irrelevante: a inclusão da expressão potencial foi discutida durante das negociações da diretiva europeia[127]. A sua adoção permite proteger também as "laboratory zones" das empresas inovadoras[128/129]. Inclusivamente, esta perspetiva ampla quanto ao conceito de valor comercial nem sequer representa qualquer originalidade europeia, pois é oriunda do sistema norte-americano, mais propriamente do §1839 UTSA (1979) – "independent economic value*, actual or potential*" (*itálico nosso*) –[130], sendo depois mantida no DTSA (2016).

Assente este ponto, o que mais releva quanto ao valor comercial é que este esteja relacionado causalmente com a natureza secreta da informação: é um valor derivado do secretismo. Daqui se seguindo que, caso não seja provada a existência de valor comercial associado à referida informação porque esta é secreta, não existe verdadeiramente uma violação de segredo comercial. No entanto, para lá deste aspeto, não se julga possível introduzir mais qualquer elemento que restrinja, direta ou indiretamente, o âmbito do dano indemnizável.

d) Diligências razoáveis para manutenção do segredo comercial

5. Como último requisito, na alínea c) do artigo 313.º do CPI (2018), estabelece-se como condição necessária de proteção jurídica que as informações secretas

---

"Ausreichend sollte wie schon bisher *ein potenzieller Wert* sein", considerando, neste plano, a diretiva europeia: "Erwägungsgrund 14 der GeschGehRL stellt unter anderem auf das *wissenschaftliche oder technische Potenzial ab*" (*itálico nosso*).

[126] Jornal Oficial da União Europeia (PT), 15/6/2016, p. L.157/4.

[127] T. Ocaña*, The Notion of Secrecy, A Balanced Approach in the Light of the Trade Secrets Directive,* cit., p. 310.

[128] T. Ocaña*, The Notion of Secrecy, A Balanced Approach in the Light of the Trade Secrets Directive,* cit., p. 46.

[129] Referindo-se ainda a valor comercial por via de *perspetiva negativa*: *Uniform Trade Secret Act*, *with Prefatory Note and Comments approved by the American Bar Association,* National Conference of Commissioners on Uniform State Law, Baltimore, Maryland, 1986, p. 6: "The broader definition in the proposed Act extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put a trade secret to use. The definition includes information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor".

[130] Sobre a relevância da expressão "*potential*" tanto no UTSA 1969 como no DTSA 2016: C. A. Hrdy & M. A. Lemley, *Abandoning Trade Secrets,* Stanford Law Review, 73.º, 2021, pp. 36 ss.

tenham sido objeto de *diligências razoáveis* para a manutenção da sua natureza secreta por parte da pessoa que detém legalmente o seu controlo. Quanto a este ponto, na doutrina portuguesa, tome-se novamente em conta o posicionamento de Sousa e Silva, no sentido de que a diligência razoável "implica apenas um *mínimo de exigência*, apoiando-se numa noção de *voluntariedade de proteção* e impondo um cuidado adequado, concretizando a ideia de proporcionalidade e funcionando como critério de repartição entre tutela privada e tutela pública"[131] (*itálico nosso*).

Esta proposição normativa de Sousa e Silva é considerada como *não tradicional* por Azevedo de Amorim, ao referir que " ao contrário do que parece resultar de um entendimento tradicional, alguns autores (*citando precisamente a posição de Sousa e Silva*) têm vindo a defender a necessidade de um *mero cuidado* razoável do titular na manutenção do secretismo, de acordo com o valor das informações, com fundamento no princípio da proporcionalidade" (*itálico nosso*)[132].

6. Parecem justificar-se as considerações de Azevedo de Amorim, como adiante se demonstrará, uma vez que o critério de razoabilidade como concretização do princípio da proporcionalidade não se traduz numa *obrigação de mínimo*, devendo ser, isso sim, perfilado como um critério de decisão jurídica relativo e dinâmico, levando em conta a granularidade da casuística. Esta é a posição esmagadora, por exemplo, da doutrina e da jurisprudência dos sistemas alemão e norte-americano.

Sem prejuízo de referência sobrevinda mais detalhada, concite-se, apenas título de exemplo, como o OLG de *Hamm* (2020)[133], concretizando o conceito de segredo comercial previsto no §2 da *GeschGehG* (2019), enfatizou precisamente que as medidas tomadas pelo proprietário do segredo comercial devem ser *razoáveis* e concretizou que a razoabilidade não pressupõe uma proteção ótima ou máxima. Mas o referido tribunal alemão, seguindo de perto a doutrina alemã[134], explicitou expressamente que a não exigência de uma proteção ótima não significa a aceitação de uma obrigação mínima. Não é, portanto, suficiente para preencher o critério da razoabilidade a adoção de uma conduta que revele – para evitar custos elevados e um maior esforço organizacional – a adoção do *mínimo* de medidas de proteção para a manutenção do segredo.

---

[131] N. Sousa e Silva, *A nova disciplina dos segredos de negócio, análise e sugestões,* cit., p. 2185.
[132] A. Azevedo de Amorim, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* cit., p. 23.
[133] OLG de Hamm, 15.09.2020, ref. 4 U 177/19 (acesso: *openjur.de*).
[134] Por todos: A. Ohly, *Das neue Geschäftsgeheimnisgesetz im Überblick,* cit., p. 444.

IV. Segredos comerciais e espaço digital

§1. Sequência

1. Apresentadas, perfunctoriamente, as coordenadas gerais que condicionam normativamente a proteção de segredos comerciais, é de avançar para mais detalhada análise de aspetos particulares que resultam da inserção e exposição dos segredos comerciais no espaço digital[135]. Em termos gerais, é útil ter presente que se está a lidar com problemas causados pelo *movimento de disrupção digital,* que também tem impacto no método da ciência jurídica[136], justificando-se, em congruência, uma aproximação geral de tipo analógico aos referidos problemas, valorizando-se a especificidade do *espaço digital*[137].

Uma breve síntese da parte geral deste estudo permitiu já concluir que a proteção dos segredos comerciais pode ser decomposta num plano jurídico estático, que corresponde aos elementos normativos objetivos da informação juridicamente relevante, e num plano jurídico dinâmico, corporizado pela necessidade de adotar diligências razoáveis para manter a informação secreta. Veremos, seguidamente, como têm sido concretizados estes dois planos que integram o conceito jurídico de segredo comercial.

2. Assim, com o enquadramento metodológico acima mencionado e tentando sistematizar alguns problemas que apresentam elevada dispersão temática, serão

---

[135] J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p. 11: "Neue zukunftsträchtige Industrien und die inzwischen nahezu überall einzusetzenden Informationstechnologien formen ein unerschöpfliches Gefahrenbündel, dessen Gefährdungspotenzial durch die Themenbereiche „Big Data" und „Industrie 4.0" auf eine höhere Stufe gehoben wird".

[136] Sobre os novos problemas e ciência jurídica: W. Hoffmann-Rien, *Digitale Disruption und Transformation. Herausforderungen für Recht und Rechtswissenschaf*, Digitale Disruption und Recht (Workshop zu Ehren des 80. Geburtstags von Wolfgang Hoffmann-Riem/org. M. Eifert), Nomos, 82, Baden-Baden, 2020, pp. 143 ss.

[137] Com muito interesse, note-se como Zech sustenta que, por vezes, uma abordagem analógica estrutural entre *facto* clássico/natural previsto no enunciado normativo e esse mesmo facto quando digitalizado pode ter de ser corrigida através de redução teleológica. Cfr. H. zech, *Digitalisierung – Potential und Grenzen der Analogie zum Analogen,* Digitale Disruption und Recht (Workshop zu Ehren des 80. Geburtstags von Wolfgang Hoffmann-Riem/org. M. Eifert), Nomos, 82, Baden-Baden, 2020, pp. 29 ss., p. 43: "Als Ausblick soll darauf hingewiesen werden, dass sich aus dem Vergleich von digitalen und analogen Sachverhalten nicht nur Analogieschlüsse, sondern auch teleologische Reduktionen rechtfertigen lassen. Normen, die für analoge Sachverhalte geschaffen wurden und nach deren Digitalisierung zu funktionswidrigen Ergebnissen führen, können entsprechend teleologisch reduziert werden".

analisados, de modo particular, os seguintes pontos: *(i)* a divulgação de segredos na *Internet* e seus efeitos no próprio conceito de segredo comercial (sua manutenção como tal); *(ii)* a divulgação de segredos na *Intranet*, particularmente a transferência (*upload*) de informação para serviços de nuvem (*cloud*), *(iii)* a concretização do conceito de *diligência razoável* para a manutenção do segredo comercial, primeiramente em termos gerais e depois de modo especial no contexto do espaço digital[138].

§2. Divulgação de segredo comercial na *Internet*

1. Como referido *supra*, o primeiro propósito especial deste estudo é o de apurar que tipo de efeito jurídico se verifica com a divulgação de segredos no espaço digital, nomeadamente se com a divulgação *online* de segredos comerciais ocorre *ipso facto* a cessação da sua proteção jurídica como tal. O que naturalmente não deixa de relevar, também, para o decretamento de medidas processuais cautelares e inibitórias que permitam salvaguardar os segredos comerciais. Caso tenha cessado o segredo comercial, a tutela processual cautelar e inibitória deixa de ser possível, dada a inexistência da pretensão principal.

Iniciando o caminho que nos permita retirar coordenadas mais aproximadas para identificar critérios de decisão, é determinante o recurso à jurisprudência de alguns dos sistemas jurídicos com os quais o direito nacional apresenta estreita conexão nesta área. Com efeito, tem sido precisamente ao nível da granularidade de situações críticas que tem sido possível dar mais passos na concretização dos vários elementos normativos que permitem delinear a configuração da proteção jurídica do segredo comercial. Com a rápida disseminação do espaço digital, evidentemente, logo começaram a surgir os primeiros litígios judiciais que conduziram os tribunais a sindicar se a divulgação (*disclosure*) de um segredo comercial na *Internet* faz cessar a sua proteção jurídica como tal. Assim, na riqueza da casuística será possível recolher vários elementos que permitem aprofundar o tema que é objeto deste estudo.

2. Neste ensejo, ainda nos primórdios da expansão da *Internet*, tem oportunidade salientar o caso *Religious Technology Center v. Arnaldo Pagliarina Lerma/Washington*

---

[138] Como chamam à atenção Brammsen/Apel, "são sobretudo as indústrias (...) informática e das telecomunicações que dominam atualmente e em absoluto o mercado da espionagem (...) os programas informáticos, *microchips*, testes de diagnóstico, métodos de codificação, etc., representam agora (...) o setor mais importante de espionagem": J. Brammsen / S. Apel, *GeschGehG: Geschäftsgeheimnisgesetz Kommentar*, cit., p. 12.

Post (1995): um antigo membro da igreja da cientologia, no decurso dos dias 31 de julho e 1 de agosto de 1995, publicou na *Internet* várias informações obtidas através do *Digital Gateway Systems*. Na sequência, o antigo membro daquela organização enviou as mesmas informações para o jornal *Washington Post*, que depois as publicou no dia 19 de agosto de 1995, sob o título "*Church in Cyberspace: Its Sacred Writ is on the Net. Its Lawyers are on the Case*"[139]. Reagindo, a igreja da cientologia, entre outras causas de pedir, invocou judicialmente ter ocorrido a violação de segredos comerciais por parte do *Washington Post*. Porém, como a informação havia sido publicada previamente na *Internet* pelo seu antigo membro, o *District Court* da *Virginia* decidiu que o pedido da organização seria improcedente, dado que o segredo havia cessado juridicamente por via da sua prévia divulgação *online*[140]. Igual desfecho teve também a tentativa de obter tutela inibitória através de uma *restraining order* contra o seu antigo membro, tendo aqui o tribunal norte-americano considerado que, depois de decorridos dez dias sobre a publicação *online* daquela informação, o segredo comercial tornou-se geralmente conhecido – "remained potentially available to the millions of *Internet* users around the world"[141] –, nada mais havendo a preservar nesse plano: "once a trade secret is posted on the *Internet*, it is effectively part of the public domain, impossible to retrieve"[142].

---

[139] H. Poole/L. Lambert/C. Woodford *The Internet: A Historical Encyclopedia*, v. II, Abc-clio, California, 2005, p. 126.

[140] *Religious Technology Center* v. *Arnaldo Pagliarina Lerma* (Civ. A. No. 95-1107-A – 1995): "As other courts who have dealt with similar issues have observed, "posting works to the *Internet* makes them `generally known'" at least to the relevant people interested in the news group. Religious Technology Center v. Netcom On-Line Communications Services, Inc., No. C. 95-20091 RMW (N.D.Cal.) Slip Opinion entered 9/22/95 at 30. Once a trade secret is posted on the *Internet*, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the *Internet* may be liable for trade secret misappropriation, the party who merely down loads *Internet* information cannot be liable for misappropriation because there is no misconduct involved in interacting with the *Internet*", (acesso: *law.justia.com*).

[141] *Religious Technology Center* v. *Arnaldo Pagliarina Lerma* (Civ. A. No. 95-1107-A – 1995), (acesso: *law.justia.com*): "Of even more significance is the undisputed fact that these documents were posted on the *Internet* on July 31 and August 1, 1995. (Lerma Affidavit). On August 11, 1995, this Court entered a Temporary Restraining Order among other orders which directed Lerma to stop disseminating the AT documents. However, that was more than ten days after the documents were posted on the *Internet*, where they remained potentially available to the millions of *Internet* users around the world".

[142] *Religious Technology Center* v. *Arnaldo Pagliarina Lerma* (Civ. A. No. 95-1107-A – 1995), (acesso: *law.justia.com*).

3. Outra situação que justifica particular atenção verificou-se no caso *DVD Copy Control Ass'n Inc. v. Bunner* (2004)[143]. No caso que foi apreciado, *Bunner*, um utilizador do sistema operativo *Linux*, decidiu que o *DeCSS*[144], um programa de computador alegadamente contendo segredos comerciais da empresa *DVD Copy Control Ass'n, Inc.*, seria útil para os demais utilizadores do sistema *Linux*, tendo então colocado o referido programa de computador na *Internet*. Em sua defesa, *Bunner* alegou que quando colocou a informação no seu sítio na *Internet* não tinha na sua posse quaisquer informações que sugerissem que o *DeCSS* continha segredos comerciais ou que envolvia, de algum modo, a apropriação indevida de segredos comerciais. No entanto, acusando *Bunner* de divulgar informações comerciais secretas através da *Internet*, a *DVD Copy Control Ass'n, Inc.*, reagiu judicialmente, ao abrigo da Lei de Segredos Comerciais da Califórnia – que correspondia, grosso modo, ao UTSA (1979) –, solicitando, e com sucesso, o decretamento de medidas cautelares. Não se conformando, *Bunner* recorreu para o *Court of Appeal* da *California*, que determinou que as provas constantes dos autos não justificavam as medidas cautelares decretadas pelo tribunal recorrido, pois não existiam indícios de que *Bunner* tinha colocado a informação sobre o *DeCSS* pela primeira vez na *Internet* e de que a informação era um segredo comercial quando foi colocada na *Internet*. Pelo contrário, havia sim abundante prova que demonstrava que a informação havia sido já tão amplamente divulgada na *Internet* que, por essa razão, tinha perdido o seu estatuto jurídico de segredo comercial. Por conseguinte, as medidas cautelares decretadas pelo *District Court* foram revogadas pelo *Court of Appeal* da *California*, considerando-as como restrição ilegal do direito de liberdade de expressão[145].

---

[143] Anotando esta decisão: A. Eaton-Salners, *DVD Copy Control Association v. Bunner: Freedom of Speech and Trade Secrets*, Berkeley Technology Law Journal, vol. 19, 2004, pp. 269 ss., concluindo de forma crítica que o tribunal "created an unresolved tension between trade secret jurisprudence and the First Amendment" (p. 288).

[144] O sistema de decodificação de conteúdo (*DeCSS*) é um *software* que permite descriptografar o conteúdo de discos de vídeo em formato *DVD*.

[145] *DVD Copy Control Ass'n Inc.* v. *Bunner* (116 CAL. APP. 4TH 241, 10 CAL. RPTR. 3D 185/2004): "We conclude that evidence in the limited record before us does not justify the issuance of an injunction under the UTSA. DVD CCA presented no evidence as to when Bunner first posted DeCSS and no evidence to support the inference that the CSS technology was still a secret when he did so. Further, there is a great deal of evidence to show that by the time DVD CCA sought the preliminary injunction prohibiting disclosure of the DeCSS program, DeCSS had been so widely distributed that the CSS technology may have lost its trade secret status.", (acesso: *casetext.com*).

4. É ainda de atentar no caso *United States of America v. Genovese* (2005)[146]: nesta situação, partes do código fonte (*source code*)[147] da *Microsoft Corporation* para dois dos seus sistemas operativos informáticos, o *Windows* NT 4.0 e o *Windows* 2000, foram divulgados na *Internet*[148]. Por esse motivo, *Genovese* foi acusado pela prática de *download*, cópia, venda e tentativa de venda do código fonte da *Microsoft* sem autorização desta. Especificamente, o governo americano afirmou que, no dia 12 de fevereiro de 2004, *Genovese* publicou uma mensagem no seu *sítio* na *Internet* promovendo a venda do referido *código fonte*. Depois de a *Microsoft* apresentar queixa junto das autoridades norte-americanas, em julho de 2004, um agente infiltrado do *FBI* contactou *Genovese* e adquiriu, por seu intermédio, o código fonte da *Microsoft*. Em sua defesa, *Genovese* invocou em tribunal que a legislação de proteção de segredos comerciais era ambígua e, por outro lado, argumentou ainda que não tinha como conhecer: *(i)* se o código fonte da *Microsoft* não era já geralmente conhecido quando o encontrou na *Internet* – "Genovese maintains that he had every reason to believe the code had become publicly available when he found it on the *Internet*"[149] –; *(ii)* e se a *Microsoft* tinha tomado as medidas razoáveis para o proteger como segredo comercial.

O tribunal norte-americano acabou por decidir que um *trade secret* não perde o seu estatuto nem a sua proteção jurídica quando "temporariamente, acidentalmente ou ilicitamente é divulgado publicamente, desde que não se torne geralmente conhecido"[150]. Neste significativo aresto, o tribunal enunciou claramente que a divulgação de um segredo comercial na *Internet* não extingue *ipso facto* a sua proteção jurídica, sendo necessário demonstrar que, por via dessa divulgação, o segredo se tornou geralmente conhecido[151].

---

[146] *United States of America v. Genovese* (409 F. Supp. 2d 253, S.D.N.Y./2005), (acesso: *casetext.com*).
[147] O código fonte (*source code*) é o código legível por humanos usado por programadores de *software* para escrever programas.
[148] Um *sistema operacional* é o *software* que controla a atribuição e utilização de recursos de *hardware,* tais como memória, tempo da unidade central de processamento (CPU), espaço em disco, e dispositivos periféricos.
[149] *United States of America v. Genovese* (409 F. Supp. 2d 253, S.D.N.Y./2005), (acesso: *casetext.com*).
[150] *United States of America v. Genovese* (409 F. Supp. 2d 253, S.D.N.Y./2005), (acesso: *casetext.com*).
[151] Ainda no que respeita ao sistema norte-americano, recorde-se o já referido caso Compulife Software, Inc. v. Newman (2020): o District Court da Florida (United States District Southern Florida District Court, caso 9:16-cv-81942-BER – 2017) considerou que a propostas individuais de seguro contidas numa base de dados da Compulife Software inc., devido à sua natureza pública, não poderiam ser consideradas como objeto da proteção contra a apropriação indevida de segredos comerciais, o *Court of Appeals* (United States Court of Appeals (11th Circuit), D.C. Docket No. 9:16-cv-8 0808-RLR – 2020). Seguindo caminho diverso e sustentou que o problema não residiria

5. Também os tribunais britânicos se confrontaram com casos similares, permitindo dar novos passos na concretização dos efeitos da divulgação de um segredo comercial na *Internet*. Examine-se, por exemplo, a situação que corresponde ao caso *Barclays Bank Plc v. Guardian News and Media Ltd* (2009)[152], decidido pelo *High Court* de *England & Wales*. Na situação apreciada pela instância britânica, um funcionário do *Barclays* entregou ao jornal *Guardian* vários documentos secretos contendo informações sobre as técnicas de planeamento fiscal desenvolvidas pelo *Barclays*. O *Guardian* decidiu publicar a referida informação no seu *sítio* na *Internet*, seguindo-se a imediata reação por parte do *Barclays*, que solicitou judicialmente o decretamento de medidas cautelares, visando a remoção das informações do *sítio* do *Guardian.* A instância judicial britânica considerou procedente a pretensão do *Barclays*, justificando-se, para tanto, com a importância de as informações terem estado *online* apenas durante quatro horas até ser analisado o pedido formulado pelo *Barclays*. A razão pela qual foi concedida procedência ao pedido residiu precisamente na circunstância de a divulgação na *Internet* da informação ser muito recente – apenas quatro horas – e também ter ocorrido de forma incompleta, uma vez os documentos foram publicados parcialmente, com recurso ao modo de censura voluntária (*redacted*). Assim, considerou-se que o segredo comercial do *Barclays* não perdeu a sua natureza jurídica mesmo depois de ter sido divulgado no *sítio* na *Internet* do *Guardian*, valorizando-se o tempo e o modo de exposição e divulgação do referido segredo[153]. O que, assim, permitiu decretar medidas cautelares para *salvaguardar* o segredo *divulgado*.

---

na facilidade de aceder às propostas de seguro individuais por estarem disponíveis ao público, mas antes e de forma mais apropriada na quantidade de propostas individuais de seguro, obtidas através do scraping, que permitiu reproduzir/mimetizar parcialmente a base de dados "Transformative Database": concluindo que, neste caso, houve violação de segredo comercial.

[152] *Barclays Bank Plc v Guardian News and Media Ltd.*, High Court of Justice, Queen's Bench Division, 19 de março de 2009, EWHC 591 (QB) 2009 WL 648829 (acesso: *ucpi.org.uk*).

[153] *Barclays Bank Plc v Guardian News and Media Ltd.*, High Court of Justice, Queen's Bench Division, 19 de março de 2009, EWHC 591 (QB) 2009 WL 648829 (acesso: *ucpi.org.uk*): "I conclude that, applying the question of probability as to the prospects at trial, that the claimant has a sufficient realistic chance, as the evidence stands today, of persuading the trial court that the dissemination to date has not destroyed the confidentiality of the material contained in the documents so as to characterise this as now being freely available. I am influenced in this conclusion also by the consideration that such further availability of the complete unredacted documents as there may be in this case may well have been only as a result of the brief period that the documents were available to the public at large on the Guardian's web site. It is therefore somewhat unattractive for the defendant to rely upon publication by others if that publication was caused by their wrongful publication on their own web site in the first place."

6. Por seu turno e ainda antes da aprovação em 2019 da lei de proteção de segredos comerciais alemã, também os tribunais alemães analisaram situações de divulgação de segredos na *Internet,* obrigando-os a concretizar os elementos constitutivos da proteção jurídica dos segredos comerciais. Elucidativa a tal respeito foi a decisão do BGH, em 2012, no caso *Movicol*[154]. De modo sintético: um antigo funcionário da *Movicol* não foi condenado por utilizar segredos comerciais desta quando já trabalhava numa outra empresa concorrente, dado que, segundo o BGH, a informação utilizada por esse funcionário já estava disponível na *Internet*, afastando, desse modo, a possibilidade de a qualificar juridicamente como segredo comercial para efeito do §17 UWG[155]. Mais recentemente, o OLG[156] de *Karlsruhe*, em 2016, decidiu que, apesar de o segredo comercial já estar acessível na *Internet*, mediante a utilização de um sistema informático de descodificação – sistema de *unlock* –, ainda assim devia ser condenada a utilização do segredo comercial sem ter sido obtida a devida autorização do respetivo titular[157]. Ou seja, da divulgação da informação na *Internet* (informação que consubstanciava um segredo comercial), de acordo com o tribunal superior de *Karlsruhe*, não resultou *ipso facto* a cessação do estatuto de segredo comercial.

2.1. Divulgação do segredo comercial e círculos subjetivos relevantes

1. No ponto anterior, os efeitos da divulgação na *Internet* de segredos comerciais foram referenciados considerando-se a necessidade de que, para a sua preservação como tal, é necessário que a informação secreta não se torne geralmente conhecida ou facilmente acessível. Pôde apurar-se, assim, que a publicação de informação secreta na *Internet* constitui um elemento decisivo para averiguar se ocorreu divulgação de segredo comercial. No entanto, o problema da divulgação de segredo comercial obriga a que se faça mais demorado caminho, sobretudo quando considerado especialmente o plano do espaço digital. Com efeito, tanto no sistema norte-americano como nos sistemas europeus – em especial, no direito português, nos termos do artigo 313.º/1/a) do CPI (2018) –, o facto que corresponde à divulgação, permitindo que a informação seja geralmente conhecida ou que seja facilmente acessível, tem

[154] BGH, *Movicol,* 23/2/12, I ZR 136/10, GRUR, 10/2012, pp. 1048-1049.
[155] Sobre o problema da divulgação associada à mobilidade dos trabalhadores, referindo o caso *Movicol*: M. Kolasa, *Trade Secrets and Employee Mobility,* vol. 44, Cambridge University Press, 2018, p. 46.
[156] Tribunal superior regional.
[157] NStZ-RR, 8/2016, p. 248: OLG de Karlsruhe, 29.01.2016 – 2 (6) Ss 318/15 – AK 99/15.

de ser juridicamente perspetivado à luz dos *círculos subjetivos* legalmente exigidos para que a divulgação dos segredos seja juridicamente relevante. Ou seja: determinante é sindicar se ocorreu divulgação junto das pessoas que integram os círculos subjetivos delimitados legalmente. Sem surpreender, diagnostica-se significativa variação quanto à concretização dos *círculos subjetivos* relevantes.

2. Com efeito, nos termos do § 1839 do *U.S. Code* (DTSA 2016), a informação continuará a ser qualificada como informação secreta enquanto esta mantiver o seu valor comercial por não ser geralmente conhecida ou facilmente acessível através de meios adequados *por parte de qualquer pessoa que possa beneficiar economicamente com a sua divulgação ou utilização*. Nestes termos, o círculo subjetivo legalmente relevante é delimitado pelo benefício económico: "who can obtain economic value from the disclosure or use"[158]. De outro lado, seguindo o que já resultava do artigo 39.º TRIPS (1994) – "pessoas dos círculos que lidam normalmente com o tipo de informações em questão"[159] –, no artigo 2º da Diretiva 2016/943, de 8 de junho de 2016, a informação será secreta enquanto não seja *geralmente conhecida* pelas *pessoas dos círculos que lidam normalmente com o tipo de informações em questão* ou enquanto não seja *facilmente acessível* ao mesmo tipo de pessoas.

Como se acaba de verificar, na diretiva europeia, a delimitação subjetiva do círculo de pessoas legalmente relevante não surge diretamente associada ao benefício económico, mas antes com a pertença a um grupo que tenha uma relação de habitualidade e familiaridade com aquele tipo de informação. O mesmo, aliás, sucede com o direito português vigente: a alínea a) do n.º 1 do artigo 313.º do CPI (2018) exige que as informações sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis para *pessoas dos círculos que lidam normalmente com o tipo de informações em questão*. Assim, tanto no TRIPS (1994) como na diretiva europeia (2016) e na alínea a) do n.º 1 do artigo 313.º CPI (2018), os círculos subjetivos relevantes correspondem às pessoas que *lidam normalmente* com o tipo de informações em questão.

3. Desta forma, tanto no sistema norte-americano como nos sistemas europeus, a divulgação de informação apenas será relevante se for considerada no contexto

---

[158] §18 U.S. *Code* § 1839, 3, (B), *Defense do Trade Secret Act,* 2016: "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can *obtain economic value* from the disclosure or use of the information".

[159] N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, cit., p. 233.

destes *círculos subjetivos especiais*: terá de abranger *(i)* quaisquer pessoas que possam obter benefício económico (*sistema norte-americano*); ou *(ii)* quaisquer pessoas que lidem normalmente com o tipo de informações em questão (*sistemas europeus/TRIPS*). Tem-se por imprescindível que se verifique, então, se uma publicação na *Internet* atingiu o círculo subjetivo relevante. Assim, a publicação de um segredo na *Internet* não implica automaticamente, *ipso facto*, a cessação da proteção dessa informação como segredo comercial. Por outro lado, a divulgação na *Internet* de determinada informação será suficiente para fazer cessar a proteção do segredo comercial mesmo que não seja do conhecimento do público em geral, bastando que seja do conhecimento do círculo subjetivo normativamente delimitado. A concretização destes círculos subjetivos, como seria expetável, é missão jurídica que exige apurado afinamento.

4. Precisamente quanto a este ponto, insista-se novamente, tem sido a partir da granularidade dos casos concretos que têm vindo a ser traçados mais aproximadamente também os contornos do conceito jurídico de segredo comercial, nomeadamente quanto aos círculos subjetivos acima referidos. A este propósito, tem cabimento apontar o caminho pioneiro trilhado pelos tribunais norte-americanos. Por exemplo, no caso *Ruckelhaus v. Monsanto* (1984), quanto à delimitação dos círculos subjetivos relevantes, o *Supreme Court* norte-americano sublinhou a importância de considerar que esses círculos integram os "membros de uma indústria"[160/161]. No entanto, a concretização do que seja a divulgação de segredo comercial

---

[160] *Ruckelshaus v. Monsanto Co*. (467 U.S. 986/1984), (acesso: *supreme.justitia.com*): "*Information (...) that is generally known in an industry cannot be a trade secret*".

[161] Mais referindo aquele tribunal superior que quando a informação que seja segredo comercial for divulgada, o titular do segredo perde o *interesse jurídico* nessa informação. Mesmo que a informação continue a ser muito útil para o seu titular mesmo depois da sua divulgação, tal será irrelevante para avaliar o impacto económico da divulgação, uma vez que o valor económico da titularidade reside na vantagem competitiva sobre terceiros pelo acesso exclusivo a essa informação e que a sua divulgação ou utilização por terceiros destruiria posição dessa vantagem; cfr. "*Ruckelshaus v. Monsanto Co*. (467 U.S. 986/1984), (acesso: *supreme.justitia.com*): "once the data that constitute a trade secret are disclosed to others, or others are allowed to use those data, the holder of the trade secret has lost his property interest in the data. That the data retain usefulness for Monsanto even after they are disclosed – for example, as bases from which to develop new products or refine old products, as marketing and advertising tools, or as information necessary to obtain registration in foreign countries – is irrelevant to the determination of the economic impact of the EPA action on Monsanto's property right. The economic value of that property right lies in the competitive advantage over others that Monsanto enjoys by virtue of its exclusive access to the data, and disclosure or use by others of the data would destroy that competitive edge".

junto dos *membros de uma indústria* continua a oferecer significativas dificuldades e tem merecido abordagens variadas, comprova-o a análise das decisões judiciais norte-americanas. Assim, por exemplo e privilegiando uma perspetiva quantitativa – usando o *critério da maioria* dos membros da indústria –, no caso *TGC Corp. v. Htm Sports* (1995)[162], foi decidido que não existe segredo comercial quando a informação respeitante a esse segredo é do conhecimento da *maioria dos membros* da respetiva indústria[163]. Esta decisão afastou-se de anteriores decisões que optaram por uma perspetiva *maximalista* no que respeita à proteção do segredo comercial – por exemplo, no caso *Wilson v. Barton & Ludwig* (1982)[164], foi decidido que existirá proteção do segredo comercial até ao momento em que *todos os membros* da respetiva indústria dele tenham conhecimento[165/166].

5. Procurando também concretizar judicialmente o círculo subjetivo legalmente relevante para efeito da perda da proteção de segredo comercial na sequência da sua divulgação, a jurisprudência e a doutrina alemãs têm avançado com critérios de delimitação. Neste plano, nos casos *Möbelpaste* (1955)[167] e *Petromax* II (1963)[168], o BGH sustentou que a proteção dos segredos depende da sua manutenção num

---

[162] *TGC Corp. v. Htm Sports*, *US District Court for the Eastern District of Tennessee* (896 F. Supp. 751, E.D. Tenn./1995), (acesso: *law.justia.com*).

[163] *TGC Corp. v. Htm Sports*, *US District Court for the Eastern District of Tennessee* (896 F. Supp. 751, E.D. Tenn./1995): "The seamless-palm feature of the TGC glove is clearly not a trade secret. It is disclosed in both of TGC's working-hand glove patents (...). In fact, a seamless-palm glove which uses a five-piece pattern nearly identical to that of TGC's glove was patented by one (...) Additionally, seamless-palm gloves in this design have been made for many years by C.D. Genter and by others as work, garden, and driving gloves. TGC claims, however, that it was the first to use the seamless-palm design in a golf glove or a racquetball glove. Viewing the evidence most favorably to TGC, this is true. This, however, does not make the seamless palm a trade secret. Both of TGC's patents claim that the TGC design may be used on the "sports field," including a "golf course." (...) The application to golf and sports gloves of public information regarding the fashioning of seamless-palm, gunn-cut-designed gloves is not a trade secret".

[164] *Wilson v. Barton & Ludwig*, *Court of Appeals of Georgia* (163 Ga. App. 721, 296 S.E.2d 747/1982), (acesso: *law.justia.com*).

[165] Em sentido similar quanto ao artigo 39.º TRIPS: N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, Kluwer Law International, 2008, p. 233.

[166] Como ensina Unikel, entendeu-se assim, neste último caso, que há "direito à proteção do segredo comercial, desde que a informação proporcione ao seu proprietário uma vantagem sobre um único concorrente que não a possua": R. Unikel, *Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets,* Loyola University Chicago Law Journal, vol. 29/4, 1998, p. 841 ss., p. 860.

[167] BGH, *Möbelpaste,* 15.3.1955, GRUR, 1955, pp. 424-425.

[168] BGH, *Petromax II,* 17.7.1963, GRUR, 1964, pp. 31-32.

círculo subjetivo muito restrito. No caso Petromax II (1963), o BGH explicitou que "o facto a ser mantido em segredo só pode ser conhecido por um grupo de pessoas *estritamente definido*"[169] (*itálico nosso*). O BGH amparou-se, portanto, numa perspetiva essencialmente *quantitativa*, apesar de a não concretizar especificamente (em termos de percentagens). Mais recentemente, o BGH manteve o *critério quantitativo* no caso *Kundendatenprogramm* (2006)[170], referindo que "um segredo comercial é qualquer facto relacionado com um negócio que não é do conhecimento público, mas conhecido apenas por um *grupo restrito de pessoas* e que se destina a ser mantido em segredo de acordo com a intenção declarada do proprietário do negócio com base em interesses económicos" (*itálico nosso*). Este *critério quantitativo* da instância superior alemã, ao longo dos tempos, tem vindo a ser objeto de variadas críticas por parte da doutrina alemã, uma vez que o critério quantitativo – *grupo restrito de pessoas* – é vago e ambíguo, causando significativa indeterminação.

6. Por essa razão, têm surgido novos caminhos para tentar delimitar os círculos subjetivos relevantes. Evidencie-se assim, desde já, a *teoria do controlo*, identificada por Kalbfus[171], nos termos da qual o segredo comercial subsistiria enquanto o seu titular tivesse controlo efetivo sobre o círculo subjetivo relevante, nomeadamente através de acordos de confidencialidade. Explorando outra via, Kalfbus apontou ainda outra possibilidade: a *teoria do interesse comum*, segundo a qual o segredo comercial manteria a sua proteção desde que os seus titulares e terceiros que tenham tido acesso ao segredo mantivessem um interesse comum na sua preservação como segredo. Para esta teoria, persistiria ainda segredo comercial, mesmo quando divulgado, desde que os membros do círculo subjetivo relevante que tenham tido acesso ao segredo continuassem a ter um interesse na manutenção da sua natureza secreta. Por seu turno, Reimann[172], mas antes da diretiva de 2016 e da atual lei

---

[169] BGH, *Petromax II,* 17.7.1963, GRUR, 1964, p. 32 "In solchen Fällen kann der Geheimnisschutz nach § 17 UWG überdies schon an dem objektiven Schützeriordernis scheitern, daß die geheimzuhaltende Tatsache nur einem eng begrenzten Personenkreise bekannt sein darf".

[170] BGH, *Kundendatenprogramm*, I ZR 126/03, 27.4.2006, (acesso: *juris.bundesgerichtshof.de*): "Ein Geschäfts- oder Betriebsgeheimnis ist jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll".

[171] B. Kalbfus, *Know-how-Schutz in Deutschland zwischen Strafrecht und Zivilrecht – welcher Reformbedarf besteht?,* Carl Heymanns, 2011, p. 86.

[172] T. Reimann, *Einige Überlegungen zur Offenkundigkeit im Rahmen von §§ 17 ff. UWG und von § 3 PatG,* GRUR, 3, 1998 pp. 298 ss.

alemã de proteção de segredos comerciais de 2019, defendeu a *teoria concorrencial*: o círculo subjetivo relevante devia ser tido como compreendendo os concorrentes do titular do segredo. Porém, em face da evolução legislativa alemã ocorrida em 2019, a teoria concorrencial perdeu terreno. Estas considerações, *mutatis mutandis*, aplicam-se, de igual modo, à *teoria do interesse comum* que acima foi enunciada.

7. Tudo quanto antecede neste estudo suporta a ilação de que a divulgação de segredo comercial, mesmo ocorrendo na *Internet*, não implica necessariamente, *ipso facto,* o não preenchimento de todos os pressupostos normativos que são condição necessária para a concessão de proteção jurídica a determinadas informações. A concretização dos círculos subjetivos é determinante para apurar se com a publicação de uma informação ocorreu verdadeiramente uma divulgação do segredo comercial em termos de fazer cessar a sua existência como tal. Como se demonstrou, a este propósito existe elevada variação na concretização dos *círculos subjetivos* relevantes nos vários sistemas jurídicos analisados – e até mesmo no quadro do TRIPS[173]. Nessa medida, analisar os efeitos de uma mera divulgação na *Internet* exige redobrada cautela metodológica. Aliás, neste contexto, é de salientar o importante contributo trazido pela *teoria da preservação sequencial*, a qual pretende demonstrar como é necessário densificar critérios que permitam imputar à divulgação o efeito extintivo da proteção que recai sobre a informação que constitua segredo comercial.

2.2. Divulgação do segredo comercial e teoria da preservação sequencial

1. Como se disse nas linhas imediatamente sobrescritas, visando apurar em que casos a divulgação na *Internet* faz cessar o segredo comercial[174], assume especial

---

[173] Defendendo uma interpretação *maximalista*: N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, Kluwer Law International, 2008, p. 233: "Secrecy, under subparagraph (a), remains *until the last competitor (or the last person within the circle that normally deals with that information) obtains the desired information*. If there are ten firms competing in a certain market, and nine of them know (secretly) about a process whereas the tenth does not know it, nor has it access to the information, that information is a trade secret as far as the tenth company is concerned. The important aspect is that information be not readily available to that tenth company (for example, as a result of its having been published in a scientific magazine, of which that company is not aware). In this regard, there is profound similarity between novelty for the purposes of patents and novelty for the purposes of trade secrets. Of course, patent law acknowledges certain exceptions to novelty (like priority and the grace period) that trade secret law does not accept".

[174] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* Wake Forest Law Review, 42, 1, 2007, p. 3.: "Although trade secret owners have always

interesse a teoria da preservação sequencial enunciada por Rowe[175]. Ainda que tenha sido desenvolvida no plano do sistema norte-americano, esta teoria tem relevância transversal.

Partindo da análise de alguns casos norte-americanos já anteriormente referidos – *Religious Technology Center v. Lerma*; *DVD Copy Control Assoc. v. Bunner*; *United States of America v. Genovese* –, Rowe propugnou ser necessário averiguar o tipo concreto de divulgação *online* que se verificou[176]. Com efeito, existem vários e diferentes tipos de divulgação de segredo da *Internet* e nem todos correspondem ao tipo que pode ter relevância jurídica.

Assim, segundo Rowe, há que atender a três fatores essenciais: *(i)* o tempo da exposição do segredo e a reação do respetivo titular (*time and action*)[177]; *(ii)* a extensão da divulgação (*extent of disclosure*)[178]: e, por último, *(iii)* situação do(s) destinatário(s) da divulgação no que respeita ao conhecimento da natureza da informação (*recipient's reason to know the information was trade secret*)[179]. O primeiro fator a considerar tem em conta o intervalo de tempo de exposição ao segredo comercial e se o proprietário foi suficientemente rápido em agir para salvar o segredo comercial depois ter descoberto a divulgação. O segundo fator analisa se o segredo comercial entrou no *domínio público* como resultado da divulgação na *Internet*. Por último, para Rowe, deve considerar-se um terceiro fator que se traduz na análise da posição do(s) destinatário(s) da divulgação da informação. Veremos, de seguida, estes pontos com maior detalhe.

---

risked disclosure of their highly sensitive and confidential information, today the *Internet* magnifies that risk exponentially. It facilitates complete destruction of a trade secret in an instant, and the law strips the trade secret owner's power to control or contain the damage. Even when the party posting the information may not have intended to cause harm to the trade secret owner, the injury can be no less devastating".

175 E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., pp. 1 ss.

176 E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 6: "My objective is to articulate a workable test that courts can use when deciding whether a trade secret that has been disclosed on the *Internet* can still be preserved as secret, regardless of whether there is or is not a First Amendment defense in the case".

177 E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 32.

178 E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 33.

179 E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 34.

a) O tempo de exposição do segredo comercial e a reação do seu titular

2. Centre-se agora a nossa atenção primeira no hiato temporal entre o momento em que o segredo comercial foi colocado na *Internet* e a reação por parte do seu titular. Segundo este padrão de avaliação avançado por Rowe, as situações em que a informação foi afixada durante um período muito curto de tempo e o seu proprietário ou titular tomou imediatamente medidas para que seja removida devem ser perspetivadas de forma favorável à manutenção do segredo[180]. Da célere reação do titular da informação secreta resulta, deste modo, um índicio de não destruição do segredo comercial. No entanto, é de ter presente que a relação entre o tempo de exposição do segredo comercial e a prontidão da reação do seu titular dependerá de uma avaliação granular e casuística. Ainda assim, pode estabelecer-se o seguinte: o ritmo a que a informação circula na *Internet* obriga a que, por regra, haja uma reação rápida– judicial ou de outra natureza – para evitar a cessação do segredo comercial. Nesta medida, uma informação respeitante a um segredo comercial que tenha sido afixada "há mais de vinte e quatro horas"[181] determinará muito provavelmente que esse segredo tenha cessado porque a informação se tornou "geralmente conhecida"[182]. O titular do segredo comercial deve reagir prontamente e tomar medidas de forma imediata – por exemplo: recurso a instâncias judiciais, contactos imediatos com o fornecedor de *Internet* para que a informação seja removida, bem como o envio de uma carta de cessação e desistência (*cease and desist letter*) ao infrator (se conhecido) que promoveu a divulgação[183].

b) A extensão da divulgação da informação relativa ao segredo comercial

3. Outro ponto decisivo no que à teoria da preservação sequencial – muito relevante no já mencionado caso *Barclays v. Guardian* – prende-se com a *extensão* da divulgação do segredo comercial[184]. Neste ponto, valoriza-se não o *tempo* de

---

[180] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit, p. 32.
[181] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 32.
[182] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 32.
[183] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 32.
[184] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 33.

exposição, mas antes a *forma* ou o *modo* como a divulgação e exposição do segredo comercial na *Internet* se verificou. Donde, a publicação de informação relativa a um segredo comercial na *Internet* não é *ipso facto* suficiente para destruir o segredo se a publicação for obscura ou transitória ou de outra forma limitada de modo a que não se torne geralmente conhecida pelas pessoas dos círculos subjetivos delimitados legalmente[185].

Neste plano, deve ser avaliado o *locus* no espaço digital onde foi divulgada a informação relativa ao segredo comercial: importa sobremaneira apurar se foi numa simples página pessoal (por exemplo: um *blogue*, mais ou menos privado e com uma dezena de leitores), se foi numa rede social com centenas de milhões utilizadores (por exemplo: *facebook, instagram, twitter, linkedin, tiktok, twitch, wechat* ou *reddit*) ou no *sítio* na *Internet* de uma *empresa tradicional* de informação (normalmente, também com centenas de milhões de utilizadores). Em face do *local* no espaço digital, a probabilidade de cessação do segredo comercial poderá ser maior ou menor, o que obrigará respetivamente a uma reação mais ou menos rápida por parte do seu titular.

Importará ainda analisar, neste contexto, se no grupo de utilizadores e leitores do local do espaço digital se encontram pessoas que integram o círculo subjetivo relevante para efeitos legais. Este ponto pode ser particularmente relevante em face da existência de redes que admitem a existência de grupos fechados ou de acesso restrito. Nestes casos, terá de ser avaliado se desses grupos constam pessoas que integram o círculo subjetivo legalmente relevante.

4. Defende igualmente Rowe, para lá do *local* no espaço digital, ser ainda de atribuir significado jurídico à *quantidade* da informação revelada (proteção parcial do segredo)[186]: em circunstâncias em que apenas partes do segredo comercial foram reveladas, tem cabimento defender que as partes não reveladas continuam a beneficiar do estatuto jurídico de informação protegida por segredo comercial, permitindo todos os meios de reação contra a divulgação, acesso e utilização não autorizados por parte do seu titular. Esta situação, para melhor se explicitar o que acaba de ser referido, pode suceder paradigmaticamente nos casos de segredos compostos por vários elementos, bem como em situações em que a informação é publicada de forma parcial ou com censura voluntária (modo *redacted*). Pode ainda

[185] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 33.
[186] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 34.

suceder que, mesmo com a divulgação parcial, o segredo comercial se mantenha integralmente e não apenas quanto às partes não divulgadas, nomeadamente em situações em que o segredo comercial se traduz numa *função* que é o resultado final da composição de vários elementos, ineficientes de forma isolada, mas funcionais quando dispostos conjugadamente e de forma integrada[187].

c) A razão do destinatário para saber que a informação era segredo comercial

5. Um outro elemento a considerar quando se analisa o efeito da divulgação sobre a manutenção a proteção do segredo comercial, segundo Rowe, prende-se com a situação do destinatário da divulgação: "recipient's reason to know the information was trade secret"[188]. Para o Autor, este elemento compõe também uma parte importante da definição de apropriação indevida de segredos comerciais e que se relaciona diretamente com a sua preservação. Por exemplo, se o proprietário do segredo comercial notificou em tempo útil o(s) destinatário(s) da divulgação de que a informação era um segredo comercial, essa reação pode ser benéfica na defesa sua pretensão de preservação do segredo, pois será um indício de que adotou medidas razoáveis para a sua manutenção. Segundo a lição de Rowe, ao notificar o(s) terceiro(s) destinatário(s) da divulgação, informando-o(s) da situação de ilicitude com a qual tomar(am) contacto, tal poderá ser valorizado judicialmente como sinal de medida que preenche o critério de razoabilidade, como adiante melhor se explicitará. Neste contexto, para Rowe, tem particular significado avaliar se o(s) destinatário(s) da divulgação conhecia(m) ou não devia(m) desconhecer a natureza jurídica especial da informação divulgada[189].

---

[187] Note-se como na alínea a), do n.º 1 do artigo 313.º CPI (2018), surge também o seguinte: "entende-se por segredo comercial e são como tais protegidas as informações que reúnem cumulativamente os seguintes requisitos: a) sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, *na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos* (...)" (*itálico nosso*).

[188] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 34.

[189] Entre nós, este ponto tem conexão com o atual n.º 3 do artigo 314.º, do CPI de 2018: "Constitui ainda ato ilícito a obtenção, utilização ou divulgação de um segredo comercial sempre que uma pessoa, no momento da obtenção, utilização ou divulgação, *tivesse ou devesse ter tido conhecimento*, nas circunstâncias específicas em que se encontrava, que o segredo comercial tinha sido obtido direta ou indiretamente de outra pessoa que o estava a utilizar ou divulgar ilegalmente nos termos do número anterior".

d) Síntese: a aplicação da teoria da preservação sequencial

6. A *teoria da preservação sequencial* corporiza, deste modo, uma tentativa de constituir uma *lista de testes* que permita aos tribunais verificar se determinada divulgação de informação na *Internet* ocorreu de modo a fazer cessar o seu estatuto de segredo comercial. Rowe alerta que deve ser evitada a imediata associação da divulgação do segredo comercial com a perda desse estatuto. Segundo a teoria da preservação sequencial, o tribunal deve seguir um caminho faseado, respondendo progressivamente às seguintes perguntas: a informação divulgada beneficiava do estatuto de segredo comercial antes de ser publicada na *Internet*? Se a resposta for negativa, cessa a aplicação da teoria da preservação sequencial. Em caso afirmativo, o tribunal deve prosseguir, respondendo à seguinte questão: as informações mantiveram o seu estatuto de segredo comercial apesar de ter ocorrido a sua publicação na *Internet*?

Para responder a esta pergunta, o tribunal deve então aplicar os critérios acima referidos – tempo de divulgação/reação do titular, extensão da divulgação e situação do destinatário da divulgação. Depois de cumpridas estas etapas, caso todas as perguntas tenham merecido resposta afirmativa, tal significa que ainda existe segredo comercial[190]. Se assim for deveras, poderá ser solicitado o decretamento das medidas judiciais consideradas adequadas para a preservação do referido segredo. De forma exemplificativa, o tribunal pode ordenar a remoção da informação da *Internet* e ainda determinar, no plano inibitório, que não seja utilizada a informação divulgada, pois tal utilização é ainda considerada um ato ilícito – assim se mantendo o segredo comercial.

§3. Divulgação do segredo comercial na nuvem (*cloud*)

1. Foi já analisada a divulgação de informação secreta na *Internet* por terceiros não titulares do segredo comercial, mas esta divulgação poderá ocorrer, no contexto do espaço digital, por ação do titular do segredo de forma não intencional. Com efeito, as informações com relevância comercial e industrial – *os cadernos e ficheiros de laboratório de uma empresa, os resultados de testes, os processos de fabrico, os planos estratégicos a longo e curto prazo, os planos de marketing, as propostas enviadas a clientes, dossiers de contratos, relatórios de crédito, análises financeiras, listas de pessoal,*

[190] E. Rowe, *Saving Trade Secret Disclosures on the Internet on the Internet Through Sequential Preservation,* cit., p. 34.

etc. – são elementos que tradicionalmente seriam arquivados fisicamente. Porém, o arquivo físico é cada vez mais um anacronismo. Razões de praticabilidade, a relação entre custo e benefício, bem a possibilidade de acesso remoto num contexto de mobilidade laboral, justificam modernamente que o arquivamento de informação empresarial seja processado através de serviços de nuvem (*cloud*). Deste modo, com muita frequência, os titulares de segredos comerciais transferem os seus ativos informativos para os referidos serviços de nuvem (*cloud computing*)[191].

2. Numa caracterização elementar, o *serviço de nuvem* pode ser descrito como uma tecnologia que permite hospedar diversos programas e informações, facilitando que determinado usuário possa utilizá-los multifuncionalmente através vários meios e a partir de vários locais. Por essa via, é possível diminuir substancialmente os custos associados à aquisição e à manutenção de *hardware* e *software*. Do mesmo modo, verifica-se um ganho com a significativa redução da necessidade de espaço físico, permitindo ainda que a atividade fique organizada através de um sistema central. Como vantagem adicional, com um razoável nível de segurança, há ainda a apontar a facilitação do trabalho remoto, bem como a possibilidade de criar uma plataforma que suporte a interação contínua com terceiros (por exemplo: fornecedores, clientes e colaboradores internos e externos)[192].

Em termos de modalidades dos serviços de *cloud computing*, são divisáveis três grandes níveis: público, privado e duplo/híbrido. No primeiro caso, na situação de nuvem pública, toda a informação e todos os programas estão disponíveis para todos os usuários. Pelo contrário, na nuvem privada, a empresa tem o controlo da infraestrutura e o acesso a esta é condicionado, permitindo-se esse acesso apenas a usuários específicos. Estes dois modelos, a nuvem privada e a nuvem pública, podem

---

[191] S. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, Virginia Journal of Law and Technology, v. 19, 2014 (Sandeen, Sharon K., Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection (*ssrn.com/abstract=2490671*), pp. 1 ss.

[192] R. B. Milligan/D. J. Salinas, *A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media,* NYBSA (One on One), New York Bar Association, 2012, v. 33, n.º 2, pp. 22 ss.: "Cloud computing involves three general service models. The simplest model is Infrastructure as a Service (IaaS). This involves basic storage and data hosting. The second model is Software as a Service (SaaS). In this model, the cloud provider provides the software to access, manage, and utilize the data. This is commonly seen with email (e.g., Gmail, Yahoo mail, Hotmail) and social media sites (e.g., Facebook, LinkedIn, Twitter). The third model is Platform as a Service. This model provides an operating system in which the company can develop and build its own applications. For example, Facebook allows third parties to build and distribute applications within its service. The main factor distinguishing the three models is the level of control the subscriber retains over its data".

ser combinados – modelo híbrido – com recurso a partições: alguns dos recursos seguem um modelo de acesso privado e outros são de acesso livre e público.

3. No que respeita ao segredo comercial, importa, portanto, aferir se a mera *transferência* de ativos informativos para um sistema de *cloud computing* implica que a informação tenha passado a ser *geralmente conhecida* ou *facilmente acessível*. Daqui resulta a necessidade de aferir se é possível traçar uma linha divisória entre *transferência* de informação e *divulgação* de informação. Respondendo positivamente, especial menção merece o estudo por Sandeen[193], pois este Autor densificou os deveres de conduta dos titulares de segredos comerciais quando estes recorrem aos serviços de nuvem ou *cloud computing*. Neste contexto, Sandeen defende também o recurso a uma *lista de testes*, procurando apurar em que casos verdadeiramente se pode considerar que houve relevante divulgação do segredo comercial quando o seu titular utiliza os serviços de nuvem. Repisando o já anteriormente afirmado, a transferência de informação não pode ser confundida *ipso facto* com a sua divulgação, pelo que deve ser rejeitada liminarmente a associação automática entre a ação de transferência de informação secreta para um serviço de nuvem e a ação de divulgação de segredo comercial. Neste contexto, é importante destrinçar entre a transferência de informação para uma *nuvem privada*, com acesso condicionado, ou para uma *nuvem pública*, em que não existe um acesso condicionado à informação. Apenas no primeiro caso – acesso condicionado em nuvem privada – será possível defender que não ocorreu divulgação do segredo comercial.

4. Continuando a acompanhar o pensamento de Sandeen, outro ponto que deve ser analisado diz respeito ao *controlo do acesso* à informação transferida para os serviços de nuvem por parte dos funcionários da empresa que presta esse serviço. Este elemento está também associado à expetativa do utilizador dos serviços de nuvem: ou seja, se o titular do segredo, quando faz a transferência da informação, tem ou não tem uma expetativa de que esta informação será mantida em situação que permite manter o segredo comercial que a integra.

Relacionando-se com este ponto, Sandeen sublinha ainda a relevância de os serviços nuvem serem automatizados ou necessitarem de intervenção humana[194]. Neste último caso (*necessidade de intervenção humana*), a proteção do segredo

[193] S. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, cit., pp. 1 ss.
[194] S. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, cit., pp. 1 ss.

comercial determina a necessidade de adoção de medidas especiais de confidencialidade, enquanto que no primeiro caso (*serviço de nuvem automatizado*) tais medidas são menos relevantes, desde que o sistema esteja protegido em termos de *hardware* e *software*. Não pode igualmente deixar de ser analisado o tipo de função que o serviço de nuvem pode executar, nomeadamente se o prestador do serviço de nuvem pode aceder e processar a informação transferida para os seus servidores, caso em que se justificam também medidas especiais de confidencialidade. Por último, é ainda útil considerar a dimensão concreta da relação entre o segredo comercial e o prestador do serviço de nuvem: ou seja, se o último acedeu efetivamente à informação transferida para os seus servidores, mesmo sem autorização[195].

§4. Facilidade de acesso e espaço digital

1. Nova dimensão problemática da proteção de segredos comerciais no espaço digital prende-se com o outro conceito vago e indeterminado que passou a constar da alínea a) do n.º 1 do artigo 313.º, do CPI (2018): a informação não pode ser *facilmente acessível*. Este segundo critério, que surge como alternativa ao critério de a informação não poder ser *geralmente conhecida*, encontra-se também geneticamente relacionado com o sistema norte-americano, nomeadamente com previsto no UTSA (1979) e no DTSA (2016).

Sem prejuízo de no sistema norte-americano surgir, hoje em dia, a expressão *ascertainable by proper means* (verificável/determinável por meios apropriados)[196] e no sistema europeu se recorra a *facilmente acessível*, é possível encontrar proximidade semântico-jurídica entre os dois conceitos, e, também, comunhão quanto à sua difícil concretização. Não obstante o auxílio proporcionado pelos *comments* da *National Conference of Commissioners on Uniform State Law* relativos ao texto do UTSA (1979)[197], é patente a dificuldade perante este conceito indeterminado. Nem do TRIPS (1994), nem da diretiva europeia de 2016, nem do artigo 313.º

---

[195] S. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, cit., pp. 1 ss.

[196] §18 U.S. *Code* § 1839, 3, (B): "(...) not being *readily ascertainable* through proper means (...)".

[197] *Uniform Trade Secret Act*, *with Prefatory Note and Comments approved by the American Bar Association,* National Conference of Commissioners on Uniform State Law, Baltimore, Maryland, 1986, p. 6: "Information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market. On the other hand, if reverse engineering is lengthy and expensive, a person who discovers the trade secret through reverse engineering can have a trade secret in the information obtained from reverse engineering" (acesso: *uniformlaws.org*).

do CPI (2018), constam elementos normativos que permitam captar de forma aproximada o sentido normativo de *facilmente acessível*. A estas dificuldades interpretativas acresce ainda a circunstância de o *espaço digital* ser naturalmente caracterizado precisamente pela *facilidade* de acesso.

2. Impõe-se a este propósito uma contextualização explicitadora: o requisito da *facilidade de acesso* surge como a outra face do previsto na alínea b) do artigo 315.º[198] do CPI (2018), no que respeita à engenharia reversa/inversa. Com efeito, há certas circunstâncias em que a informação é apenas acessível (*licitamente*) por via de engenharia reversa/inversa (*nos casos de acesso não fácil*), uma vez que o seu titular a organizou de forma *não facilmente acessível*[199]. Feita esta observação, o sentido normativo a atribuir ao que resulta conjugadamente da alínea a) do n.º 1 do artigo 313.º e da alínea b) do artigo 315.º, do CPI (2018), traduz-se na proteção de informação que, para ser obtida ou entendida, exija significativo tempo, recursos, conhecimentos especializados e investimento. Nestes casos, o *mero acesso* não é suficiente para *entender* o sentido da informação, pelo que da possibilidade de *mero acesso* não resulta a *facilidade de acesso.* No que tange a este requisito, o *acesso simples* não é assim relevante *per se*: não basta ser *acessível*. O que releva é o *grau de dificuldade* para que haja *verdadeiro* acesso à informação (no sentido do seu entendimento), o que justifica a utilização, no enunciado normativo, do advérbio de modo *facilmente.*

Esta linha de pensamento foi seguida pelo BGH no caso *Movicol*, em 2012[200], afirmando esta instância superior alemã que, para apurar se a informação é *facilmente acessível*, "o fator decisivo é se a documentação divulgada/publicada requer um *grande dispêndio* de tempo ou dinheiro" (*itálico nosso*). Esta decisão, aliás, vem na sequência de anteriores decisões do BGH, nomeadamente no caso *Schweißmodulgenerator* (2007)[201], tendo então o BGH decidido que a "proteção como segredo comercial

---

[198] CPI de 2018, Artigo 315.º –Aquisição, utilização e divulgação lícitas de segredos comerciais; A obtenção de um segredo comercial constitui um ato lícito quando resulte de: (...) b) Observação, estudo, desmontagem ou teste de um produto ou objeto que tenha sido disponibilizado ao público ou que esteja legalmente na posse do adquirente da informação, não estando este sujeito a qualquer dever legalmente válido de limitar a obtenção do segredo comercial.

[199] T. Ocaña, *The Notion of Secrecy, A Balanced Approach in the Light of the Trade Secrets Directive,* cit., p. 320.

[200] BGH, *Movicol*, 23.2.12, I ZR 136/10, GRUR, 10/2012, pp. 1048-1049.

[201] BGH, 13.2.07, I ZR 71/05 (acesso:*bundesgerichtshof.de*): "Für den Schutz als Betriebsgeheimnis kommt es darauf an, ob die fragliche Information allgemein, d.h. ohne großen Zeit- und Kostenaufwand, zugänglich ist. Der Stand der Technik umfasst dagegen eine Fülle von unaufbereiteten Informationen, die nur mit großem Aufwand ausfindig und zugänglich gemacht werden können".

depende se as informações em questão são geralmente acessíveis, ou seja, *sem grandes gastos de tempo e dinheiro*. O estado da arte, por outro lado, compreende uma riqueza de informações não processadas que só podem ser encontradas e tornadas acessíveis com *grande esforço e despesa*" (*itálico nosso*).

§5. Medidas razoáveis para a manutenção do segredo comercial no espaço digital

1. Prosseguindo o nosso estudo, cumpre agora fazer notar que assiste à proteção da informação através da técnica jurídica do segredo comercial, como já explicitado anteriormente, uma dimensão *objetiva* e *estática* e uma dimensão *subjetiva* e *dinâmica*. Com efeito, a mera existência *objetiva* de informação secreta não é judicamente suficiente para que essa informação possa beneficiar de proteção jurídica como segredo comercial. É ainda necessário que o seu titular/possuidor assuma *subjetivamente* um comportamento ativo e dinâmico no sentido de preservar a sua natureza secreta. Caso não sejam tomadas *medidas razoáveis* para evitar que a informação seja facilmente acessível ou que se torne geralmente conhecida, desta conduta passiva resultará a impossibilidade jurídica de proteção dessa informação como segredo comercial.

Este ponto é particularmente relevante pois nem sempre foi exigida a adoção de medidas razoáveis para tutelar a informação secreta, bastando, por vezes, apenas a sua qualidade objetiva de segredo comercial para que fosse protegida como tal. Por exemplo, no sistema britânico, em termos gerais, não era exigido que o titular do segredo tomasse *medidas razoáveis* para proteger o segredo. Bastava, no plano da *breach of confidence*, que a informação tivesse natureza confidencial, que fosse violada uma obrigação de confidencialidade e que ocorresse uma utilização não autorizada da mesma com prejuízo para o seu titular originário: estes três elementos, sem exigências adicionais no plano dinâmico, surgem claramente, por exemplo, na decisão *Coco v. A N Clark (Engineers) Ltd* (1969)[202].

2. Porém, em sentido contrário, no sistema norte-americano, pelo menos a partir do UTSA (1979), o conceito de *trade secret* passou a exigir expressamente o

[202] *Coco* v. *A N Clark (Engineers) Ltd*, Reports of Patent, Design and Trade Mark Cases, v. 86/ 2, 1969, pp. 41 ss.: "First, the information must be of a confidential nature. (...) "*something which is public property and public knowledge*" cannot *per se* provide any foundation for proceedings for breach of confidence. (...) The second requirement is that the information must have been communicated in circumstances importing an obligation of confidence. (...). Thirdly, there must be an unauthorised use of the information to the detriment of the person communicating it".

preenchimento de um requisito sujetivo associado à conduta do titular do segredo comercial – o dever de adotar as *medidas razoáveis*, atendendo às circunstâncias, para manter a informação secreta – cumulativamente com os demais requisitos legais.

Como ensina Bone[203], o requisito subjetivo é anacrónico e anómalo, mas tem uma explicação histórica. Com efeito, inicialmente, o dever de tomar medidas razoáveis surgiu no contexto da perspetiva do segredo comercial pelo prisma dos direitos de propriedade e da respetiva exigência de *controlo possessório* no contexto dos *property rights* do sistema norte-americano do século XIX. Assim, as medidas razoáveis relacionam-se historicamente com a teoria do direito de propriedade, num período em que, no pensamento norte-americano, o direito natural dominou a teoria sobre a propriedade – em finais do século XIX – e com repercussão no plano da exigência de controlo possessório. Por essa razão, a teoria do direito de propriedade colocou o requisito das medidas razoáveis no eixo central do conceito jurídico de segredo comercial. O proprietário de um segredo comercial que não tomasse as medidas "possessórias" razoáveis para preservar o seu segredo não estaria a exercer o controlo ou domínio sobre a informação secreta e, portanto, já não possuía verdadeiramente a informação secreta, ditando a cessação de *property rights* sobre a mesma.

3. Como explicita Bone, esta exigência de medidas *possessórias* razoáveis remonta ao final do século XIX e início do século XX, tendo um lado funcional e outro formal. Quanto ao *lado funcional*, as medidas razoáveis teriam de cumprir as seguintes funções: informar terceiros sobre o dever de manter a confidencialidade do segredo comercial e assegurar que a informação secreta não era divulgada/tornada acessível. Do lado formal, as medidas razoáveis teriam de corporizar o exercício formal de controlo do segredo, ou seja, teriam de representar formalmente a própria existência e continuidade do direito de propriedade sobre o segredo comercial[204].

Ora, com o desaparecimento desta teoria, a tutela do segredo comercial foi progressivamente absorvida pela teoria da concorrência desleal, que deslocou o foco do plano da propriedade para o plano *ilicitude da apropriação* do segredo por violação da *fair competition*. Não obstante esta mutação substantiva, no UTSA (1979), a necessidade de adotar *medidas razoáveis* emergiu expressamente como requisito legal. Para Bone, tomando posição crítica quanto à sua manutenção e

[203] R. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions,* cit., pp. 46 ss.
[204] R. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions,* cit., pp. 46 ss.

propondo mesmo a sua abolição, o requisito das *medidas razoáveis* introduz elementos de grande perturbação heurística, deixando o intérprete sem base para conseguir identificar um padrão decisório rigoroso, dado o elevado nível de variação na delimitação das medidas razoáveis[205].

4. A história associada a este requisito revela ainda um outro dado importante para compreender os sistemas europeus e o sistema português em especial. Por influência da delegação norte-americana[206], o requisito das medidas razoáveis foi consagrado no artigo 39.º do TRIPS (1994), passando a prever-se, muito similarmente ao previsto no UTSA (1979), que a proteção das informações depende também de terem sido "objeto de *diligências consideráveis*, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secreta" (*itálico nosso*). No sistema europeu continental, este requisito dinâmico, pelo menos de forma autónoma e expressamente, não era exigido e era até desconhecido na generalidade dos ordenamentos jurídicos. Por exemplo, na Alemanha, o §17 UWG não o exigia, o mesmo sucedendo em Portugal, nas várias versões do CPI até à revisão de 2003[207]. No entanto, no plano europeu, no artigo

---

[205] R. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions,* cit., pp. 46 e ss., chegando a advogar a sua abolição: "The doctrine's original rationale is not persuasive now that the property theory has been rejected; conventional justifications based on notice and evidence all have serious shortcomings, and the standard policies cited to justify trade secret law seem to offer little support. This strongly suggests that the RSP requirement should be eliminated, and I am inclined to support this reform. Before implementing it, however, we must be sure we understand all the social benefits of the doctrine. Toward that end, this Section describes in a general way three potential benefits that have been largely overlooked and that need more careful study. Two have to do with minimizing enforcement costs, and the third has to do with using precautions as a signal to channel innovation in efficient ways".

[206] Para a *história legislativa* do 39.2 do TRIPS (1994), sublinhando o conteúdo da proposta norte-americana, cfr. N. Pires Carvalho, *The TRIPS Regime of Antitrust and Undisclosed Information*, cit., pp. 207 ss.: "to maintain legal protection, the owner of a trade secret may be required to *make efforts reasonable under the circumstances* to maintain such secrecy but need not show that no one else possesses the trade secret. Without losing the requisite secrecy, the owner may communicate a trade secret to employees involved in its use, communicate a trade secret to others pledged to secrecy or make any other communications required by law or as a condition for marketing".

[207] CPI (2013), Artigo 318.º [*revogado – Decreto-Lei n.º 110/2018, de 10 de Dezembro*]: Nos termos do artigo anterior, constitui acto ilícito, nomeadamente, a divulgação, a aquisição ou a utilização de segredos comerciaiss de um concorrente, sem o consentimento do mesmo, desde que essas informações: a) Sejam secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exactas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; b) Tenham valor comercial pelo facto de serem secretas; c) *Tenham sido objecto de diligências consideráveis*,

2º da Diretiva 2016/943, que se poderá qualificar como um transplante jurídico, o conceito de segredo comercial passou a exigir que as informações devem ter sido "*objeto de diligências razoáveis*, atendendo às circunstâncias, para serem mantidas secretas *pela pessoa que exerce legalmente o seu controlo*" (*itálico nosso*).

5. Com este pano de fundo, tanto Portugal como a Alemanha, entre outros países, procederam à alteração dos seus ordenamentos jurídicos. Assim, em Portugal, em 2018 (seguindo linha similar à do CPI de 2013, que resultava da incorporação do artigo 39.º do TRIPS), o artigo 313.º, do CPI (2018), passou a prever o seguinte: para que sejam protegidas, que as informações "tenham sido objeto de *diligências razoáveis*, para a manutenção do segredo, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas" (*itálico nosso*).

No ano seguinte, em 2019[208], a Alemanha aprovou a lei de proteção de segredos comerciais, nela passando a exigir-se que: a informação seja objeto de *medidas de sigilo razoáveis* pelo seu legítimo titular – "die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist"[209]. Deste modo, por força do TRIPS (1994) e da transposição da diretiva europeia de 2016 quanto aos segredos comerciais, foi adotado, em vários sistemas europeus, como é o caso do direito nacional e do direito alemão, o requisito que se traduz na necessidade de demonstrar que o titular do segredo comercial promoveu a adoção de diligências razoáveis para manter a informação secreta.

6. Este requisito *subjetivo* e *dinâmico* assume significado particular para o estudo em curso, uma vez que é necessário densificar o tipo de conduta que o titular legítimo do segredo comercial deve adotar, considerando especialmente a perigosidade do espaço digital. Como certeiramente foi enfatizado por Cundiff,

---

atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas.

208 T. Hoeren / R. Münker, *GeschGehG: Gesetz zum Schutz von Geschäftsgeheimnissen – De Gruyter Kommentar,* cit., p. 28.

209 GeschGehG (BGBl. I S. 466): § 2 Begriffsbestimmungen: 1. Geschäftsgeheimnis eine Information: a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und; b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht".

"o mundo digital não é amigável para os segredos comerciais"[210], pelo que "o titular do segredo deve ser *vigilante na identificação de novas ameaças e na identificação de novos meios digitais para as combater*"[211] (*itálico nosso*). A não adoção de medidas e/ou a tomada de decisões empresariais informadas que considerem também as novas tecnologias tem uma consequência jurídica inevitável: a informação não poderá ser juridicamente protegida como segredo comercial por não terem sido levadas a cabo as necessárias medidas razoáveis[212], tendo em consideração precisamente o especial contexto do mundo digital e o mundo das novas tecnologias[213].

a) O critério de razoabilidade no sistema norte-americano

6. Tal como explicitado, o critério de razoabilidade surge historicamente associado à perspetiva norte-americana do segredo comercial como *property right*. Não obstante essa perspetiva ter sido paulatinamente superada, o conceito de segredo comercial, tal como previsto no UTSA (1979), passou a integrar nos seus elementos constituintes a exigência de esforços razoáveis, do titular do segredo comercial, para manter a informação secreta.

Este critério, como salientado por Bone[214], pela sua abertura semântica, permite significativa variação quando se procede à sua densificação perante a casuística. Como ponto prévio e em termos gerais, impõe-se referir que do critério de razoabilidade não resulta um dever genérico de conduta que imponha a adoção de todas as medidas possíveis: é nesse sentido que Cundiff enfatiza precisamente a necessidade de equilíbrio ("balance"[215]) entre a finalidade última, a proteção do segredo, e as medidas que devem ser adotadas. Mas se é possível estabelecer uma não obrigação de comportamento máximo, o mesmo já não é possível afirmar quanto à suficiência de um comportamento mínimo para preencher a necessidade

---

[210] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, IDEA – The Intellectual Property Law Review, v. 49, 2009, pp. 359 ss., p. 363, p. 361.
[211] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 363.
[212] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 364: "New technologies present new reasons–and new ways–to implement these time-honored rules. Trade secret owners who do not make informed decisions to adapt their practices to take new technologies into account have failed to take reasonable measures to protect their secrets".
[213] Referindo "*digital safeguards in digital environment*": V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 365.
[214] R. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions,* cit., p. 46, defendendo a sua abolição.
[215] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 363.

legal de tomar as medidas razoáveis. Com este enquadramento e procurando precisamente traçar coordenadas mais aproximadas ao núcleo do critério de razoabilidade, é, novamente, incontornável o labor da jurisprudência norte-americana.

7. Pela sua significância, é de apontar, desde logo, o caso *E.I. duPont deNemours & Co. v. Christopher* (1970), julgado pelo *Fifth Circuit* do *Court of Appeal*[216], ilustrativo da concretização do critério de razoabilidade. Este caso traduz uma situação típica de espionagem industrial: *Rolfe* e *Gary Christopher* foram contratados por terceiros para tirar fotografias aéreas de novas construções na fábrica de *Beaumont de E. I. DuPont deNemours & Company, Inc*.[217]. Entre outros aspetos, estava em causa apreciar se a *DuPont* tomou as medidas razoáveis para preservar o segredo comercial que invocou. Na construção de uma fábrica, que decorreu ao ar livre, cumpria determinar se era exigível que os elementos que pudessem expor o segredo foram devidamente resguardados durante o processo de construção da nova fábrica. Analisando a situação, o tribunal norte-americano afirmou não ser juridicamente exigível que uma pessoa, singular ou coletiva, tome precauções "não razoáveis" para evitar que outra pessoa faça o que não deveria fazer em primeiro lugar. No entanto, segundo aquela instância, é possível exigir precauções "razoáveis" contra

---

[216] *E.I. du Pont de Nemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970) (acesso: *law.justia.com*).

[217] Os empregados da *DuPont* detetaram a presença de uma aeronave utilizada para esse efeito e logo trataram de aferir a causa do sobrevoo. Tendo descoberto a razão, a *DuPon*t entrou em contacto com os *Christophers* pedindo-lhes que revelassem o nome da pessoa ou empresa que solicitou as fotografias. Este pedido foi recusado pelos *Christophers*, contrapondo como razão o desejo do cliente de permanecer anónimo. Perante esta recusa, a *DuPont* apresentou posteriormente um processo contra os *Christophers*, alegando que os *Christophers* tinham obtido indevidamente fotografias que revelavam os segredos comerciais da *DuPont,* as quais depois venderam a terceiros não revelados. A *DuPont* alegou que tinha desenvolvido um processo altamente secreto, mas não patenteado, de produção de metanol, um processo que deu à *DuPont* uma vantagem competitiva sobre outros produtores. Neste contexto, a *DuPont* alegou que o processo era um segredo comercial desenvolvido após uma investigação muito dispendiosa e demorada e que se tratava de segredo que a empresa tinha tomado precauções especiais para salvaguardar. Na área fotografada pelos *Christophers* estava precisamente a fábrica concebida para produzir metanol através deste processo secreto, e porque a fábrica ainda estava em construção, partes do processo foram expostas à vista diretamente de cima da área de construção. As fotografias dessa área, deste modo, permitiriam a uma pessoa competente deduzir o processo secreto para a produção de metanol. A *DuPont* argumentou assim que os *Christophers* se tinham apropriado indevidamente do segredo comercial da *DuPont*, tirando as fotografias e entregando-as a terceiros. No seu processo, a *DuPont* pediu uma indemnização para cobrir o prejuízo já sofrido em resultado da revelação indevida do segredo comercial e requereu providências judiciais proibindo qualquer outra circulação das fotografias já tiradas e proibindo qualquer outra fotografia adicional da fábrica de metanol.

a curiosidade de terceiros predadores. No caso concreto, o tribunal acabou por decidir que exigir a construção de uma *fortaleza impenetrável* seria uma *exigência não razoável*, não sendo equilibrado sobrecarregar os inventores industriais com tal dever para proteger os frutos dos seus esforços de inovação[218].

8. Também no caso *Innovative Construction Systems, Inc.* (1986), julgado pelo *Court of Appeal* do *Seventh Circuit*[219], foi necessário densificar o critério de razoabilidade no que respeita às medidas adotadas pelo titular do segredo[220]. A *Innovative Construction Systems, Inc. ("Innovative"),* processou judicialmente a *Bowen Supply, Inc. ("Bowen Supply"),* e a *Sunbelt Brick Company, Inc. ("Sunbelt")*, alegando ter ocorrido uma violação de segredo comercial relativo ao processo de fabrico de painéis de tijolo para a indústria da construção de casas. Estava em causa analisar se foram tomadas as medidas adequadas e razoáveis no que respeita à proteção da informação quanto ao processo de fabrico dos tijolos.

Um antigo funcionário da *Innovative*, que era gerente de fábrica e por essa razão teve acesso aos segredos desta empresa, desvinculou-se e fundou a *Sunbelt*

---

[218] *E.I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970) (acesso: *law.justia.com*)

[219] *Innovative Construction Systems, Inc., debtor-appellant, 793 F.2d 875 (*7th Cir. 1986) (acesso: *law.justia.com*). A *Innovative Construction Systems, Inc*. ("Innovative") processou a *Bowen Supply*, *Inc.* ("*Bowen Supply*") e a *Sunbelt Brick Company*, *Inc.* ("Sunbelt"), estando em causa o processo de simulação de painéis de tijolo para a indústria da construção de casas. O método que desenvolveram exigia a aplicação de três camadas, compostas de agregado de escória, cimento, agente de colagem e chorume, a um painel de suporte de quatro por oito pés: o produto resultante foi chamado "Panl Brick". Para promover o seu produto, a *Innovative* celebrou um acordo de distribuição com a *Bowen Supply*, que se tornou na sua única distribuidora nacional. A *Innovative* tinha como gerente de fábrica o funcionário *Strand*, que estava frequentemente em comunicação com *a Bowen Supply.* Devido à vários contactos entre a *Strand* e a *Bowen Supply,* aquele acabou por notificar a *Innovative* que iria fazer cessar a relação entre ambos. Nesta altura, *Strand* sabia que em breve assumiria uma posição na *Bowen Supply* e que se ajudasse a *Bowen Supply* a estabelecer uma fábrica, utilizando os seus conhecimentos, a *Innovative* perderia o seu único cliente. No entanto, *Strand* não referiu que iria trabalhar com a *Bowen Supply*. Pouco depois, foi fundada a *Sunbelt*, por *Harrold Bowen* e *Strand* em Maio de 1981, e iniciou-se a produção de painéis de tijolo. Durante o julgamento, a *Bowen Supply* admitiu que utilizou praticamente as mesmas técnicas de fabrico que *Innovative* tinha desenvolvido para a produção de *Panl Brick*. No entanto, modificou as fórmulas que a *Strand* tinha adquirido enquanto empregado pela *Innovative*. Estas modificações foram necessárias devido às diferenças climáticas entre *Wisconsin* e a *Georgia*, bem como pela disponibilidade de agregados de escória. Por seu turno, a *Innovative* testemunhou que o tempo que a *Bowen Supply* precisou para desenvolver variações viáveis nas suas fórmulas era insignificante em comparação com o esforço que tinha despendido no desenvolvimento das fórmulas originais, alegando, por isso, violação de segredo comercial.

[220] Sobre este caso: P. Philips, *The Concept of Reasonableness in the Protection of Trade Secrets,* The Business Lawyer, v. 42, n. 4 (8/1987), pp. 1045 ss.

com um dos sócios da *Bowen Supply*, que era a única distribuidora contratada pela Innovative para colocar o seu produto. Volvido pouco tempo, a *Sunbelt,* com a especial participação do antigo funcionário da *Innovative* e agora sócio da *Sunbelt,* passou a fabricar tijolos usando uma técnica decalcada da que fora desenvolvida pela *Innovative*. Por esse motivo, a *Innovative* invocou a violação de segredo comercial. Porém, a *Innovative* não exigia que os seus empregados assinassem acordos de não divulgação (NDA) e, por outro lado, as diretrizes afixadas na área de produção industrial não mencionavam a natureza confidencial das fórmulas utilizadas pelos seus funcionários. Foi por este motivo que a *Bowen Supply* sustentou que a *Innovative* não tomou as medidas necessárias para manter as suas fórmulas em segredo.

Este caso é particularmente relevante pois ilustra bem a *porosidade* conceitual do critério de razoabilidade através da divergência entre o *District Court* do *Wisconsin* e o *Court of Appeal*. O *District Court* do *Wisconsin* decidiu que a conclusão de que a *Innovative* adotou medidas razoavelmente adequadas para proteger o sigilo das suas fórmulas não estava suficiente apoiada pelas provas apresentadas. Por seu turno, o *Court of Appeal*, decidindo reavaliar esta questão, considerou, em sentido contrário, que existiam provas suficientes para considerar como *razoáveis* os esforços desenvolvidos para informar/vincular os seus empregados quanto à necessidade de manter as fórmulas em segredo – mesmo sem acordos escritos de confidencialidade[221] –, bem como para restringir o acesso de não empregados às suas fórmulas secretas e para as salvaguardar nas negociações com terceiros[222].

---

[221] Sobre este ponto e em sentido mais restritivo, em *M.C. Dean, Inc. v. City of Miami Beach* (Fla., 199 F. Supp. 3d 1349, 1356/S.D. Fla. 2016), por exemplo, o tribunal norte-americano deu relevância ao facto de o titular do segredo não ter tomado quaisquer medidas para manter o segredo, concluindo que, por essa razão, não existia qualquer segredo comercial tutelado juridicamente. O tribunal sublinhou que não foi implementado qualquer acordo de confidencialidade nem qualquer outro meio de proteção, nomeadamente a rotulagem de segredos comerciais. Em sentido similar, no caso *McKee v. James* (n.º 09 CVS 3031, 2013 NCBC 38 LEXIS 33, N.C. Super. Ct./July 24, 2013), considerou-se que não existia segredo comercial porque o titular do segredo não apresentou quaisquer medidas razoáveis tomadas para o manter o segredo (acesso: *law.justia.com*).

[222] Com efeito, o *Court of Appeal* veio a decidir em sentido contrário, considerado que a não realização de "entrevistas de exit" e a não exigência de acordos escritos de não divulgação (NDA) não implica necessariamente que um empregador não tenha tomado medidas razoavelmente adequadas para vincular os seus empregados quanto à natureza secreta da informação em questão. O que estava em causa, em sentido geral, era se, dadas as circunstâncias, as medidas adotadas foram razoáveis. Para a instância superior, ao perguntar se os esforços particulares foram razoavelmente adequados dadas as circunstâncias, o júri é chamado a exercer o seu julgamento de bom senso para determinar se eram necessárias medidas adicionais para guardar o segredo das fórmulas. No essencial, isto requer uma avaliação da dimensão e natureza do negócio, do custo de medidas de proteção adicionais

9. Um outro ponto que tem sido objeto de reflexão é o da real efetividade das medidas adotadas. Em casos em que estavam em vigor medidas de proteção, mas o titular do segredo não as seguiu ou cumpriu, os tribunais norte-americanos têm decidido que tal comportamento não é suficiente para preencher o critério de razoabilidade. A adoção de medidas, mais do que a sua mera enunciação programática, deve corresponder à materialização das mesmas. Neste sentido, no caso *Call One,*

(custo do NDA), e do grau em que tais medidas diminuiriam o risco de divulgação. Segundo o tribunal norte-americano, o que podem ser medidas razoáveis num contexto podem não o ser necessariamente num outro contexto. No caso, o *Court of Appeal*, considerou que seria suficiente que os funcionários tenham sido informados sobre a natureza secreta das fórmulas e concordado em manter essa informação confidencial (não sendo necessário um acordo escrito). Por outro lado, foi ainda analisada a necessidade de contratar pessoal de segurança, para efeito do preenchimento do conceito de segredo comercial. A *Innovative* não tinha ao seu serviço pessoal de segurança e a fábrica não estava fechada durante o horário de trabalho. Deste modo, aos fornecedores, candidatos a emprego, amigos pessoais dos empregados, entre outros, não era negada a entrada na área de fabrico. Por essa razão, a *Bowen Supply* novamente invocou que a *Innovative n*ão tomou medidas razoavelmente adequadas para guardar o sigilo das suas fórmulas. A *Innovative* alegou que, devido ao cimento húmido gerado na produção de *Panl Brick,* os não empregados não entrariam na área de fabrico, o que asseguraria naturalmente o secretismo do processo de fabrico de tijolos. Neste plano, argumentou ainda que não foi feita prova de qualquer indicação ou qualquer registo sobre a quantidade de tempo permitida a esses não empregados para estarem na fábrica e esse tempo foi substancial, não havendo razão para pensar que estavam em condições de recolher as informações contidas nas fórmulas a partir da observação distante e casual do processo de fabrico dos tijolos. Neste contexto, o *Court of Appeals* considerou existirem provas suficientes para apoiar a inferência de que as medidas adotadas pela *Innovative* para guardar o segredo das suas fórmulas de não empregados eram razoavelmente adequadas. Finalmente, a *Bowen Supply* invocou que a *Innovative* tomou medidas inadequadas para guardar o sigilo das suas fórmulas ao discutir a possível venda do seu negócio a outros. Várias empresas, incluindo a *Bowen Supply*, tinham manifestado interesse em adquirir a *Innovative.* Representantes de algumas destas empresas inspecionaram a fábrica de fabrico e a *Innovative* não exigiu que nem as empresas nem os seus representantes assinassem acordos de não divulgação. Quanto a este ponto, a *Innovative* invocou que os acordos escritos de não divulgação (NDA) não eram normalmente utilizados na indústria, pelo menos durante as fases negociais preliminares de aquisição. Por outro lado, apresentou ainda prova de que obteve garantias orais de confidencialidade das partes interessadas e, em alguns casos, não divulgou informações confidenciais. Com efeito, durante o julgamento, ficou provado que, para efeito das negociações preliminares de aquisição, a *Innovative* preparou um relatório que continha uma descrição geral do *Panl Brick*, mas nesse relatório não estavam as proporções exatas das matérias-primas utilizadas para produzir o *Panl Brick*. Após um exame minucioso deste documento e das fórmulas de *Panl Brick,* o *Court of Appeal* concluiu que *Innovative* não comprometeu o segredo dessas fórmulas enviando o relatório para *Bowen Supply*. Além disso, considerou que as provas como um todo, juntamente com todas as inferências razoáveis delas retiradas, permitiam concluir que a *Innovative* tomou medidas razoavelmente adequadas para assegurar o sigilo das suas fórmulas secretas.

Inc. v. Anzine (2018)[223], o titular do segredo comercial não assinalou a natureza confidencial nos documentos relativos ao segredo, apesar de ter sido estabelecido internamente que tal identificação fazia parte da *política da empresa*; por essa razão, por causa da não materialização da sua política interna, foi decidido que não havia segredo comercial a proteger.

Também no caso *GTAT Corp. v. Fero* (2017)[224], o titular do segredo tinha estabelecido medidas para salvaguardar o segredo, mas não as aplicou de forma consistente: com esse fundamento, o tribunal também rejeitou decretar medidas cautelares para proteger o alegado segredo comercial.

10. Ainda neste contexto, procurando delimitar o critério de razoabilidade com base num critério de *eficiência,* pode verificar-se que, no caso *United States v. Tien Shiah* (2008)[225], o *District Court* considerou que o titular do segredo satisfez[226] o critério de razoabilidade com as medidas tomadas, sublinhando, porém, que devia ter sido *mais claro* na identificação concreta de qual informação correspondia a segredo comercial.

Em sentido mais rigoroso, no caso *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC* (2018)[227], o *Court of Appeal* concluiu que os esforços de segurança do titular do segredo não eram razoáveis por serem *ineficientes*, uma vez que o seu titular confiou que os seus funcionários soubessem que a informação correspondia a um segredo comercial, baseando-se para tanto apenas em entendimentos implícitos e declarações ou avisos verbais e não em acordos escritos: seria exigível, para este tribunal norte-americano, o recurso à forma escrita[228].

---

[223] *Call One, Inc. v. Anzine* (n.º 18 C 124, 2018 U.S. Dist. LEXIS 96169, 25/N.D. Ill. June 7, 2018), (acesso: *govinfo.gov*).

[224] *GTAT Corp. v. Fero* (n.º 17-55-M-DWM, 2017 U.S. Dist. LEXIS 80511, 9-10/D. Mont. May 25, 2017).

[225] *United States* v. *Tien Shiah*, *(*SA CR 06-92 DOC (C.D. Cal. Feb. 19, 2008), (acesso: *court.cacd.uscourts.gov*).

[226] *United States* v. *Tien Shiah*, SA CR 06-92 DOC (C.D. Cal. Feb. 19, 2008), (acesso: *court.cacd.uscourts.gov*): "Nonetheless, the Court finds that the deficiencies in Broadcom's measures were not so extensive to qualify as unreasonable; Broadcom barely satisfies the standard of reasonableness".

[227] *Yellowfin Yachts, Inc. v. Barker Boatworks* (*LLC,* 898 F.3d 1279, 11th Cir. 2018), (acesso: *law.justia.com*).

[228] *Yellowfin Yachts, Inc. v. Barker Boatworks* (*LLC,* 898 F.3d 1279,11th Cir. 2018), (acesso: *law.justia.com*): "with mere verbal statements that the Customer Information should not be given to outsiders, Yellowfin relinquished the information to Barker, who refused to sign a confidentiality agreement, with no instruction to him as to how to secure the information on his cellphone or personal laptop. In doing so, Yellowfin effectively abandoned all oversight in the security of the

b) O critério de razoabilidade no sistema alemão

11. Na Alemanha, a concretização do critério de razoabilidade tem também sido objeto de várias decisões judiciais e estudos doutrinais. Ohly enfatiza, inclusivamente, que o novo requisito da diligência razoável, previsto no §2 da GeschGehG (2019), tem causado algum "nervosismo"[229] na comunidade empresarial alemã.

Com este enquadramento, tem especial interesse atentar na decisão do OLG de *Hamm* (2020)[230], pois este tribunal alemão, chamado a decidir um caso sobre a proteção de segredo comercial relativo a processos de tamponamento industrial, teve de averiguar se o conceito de segredo comercial previsto no §2 da *GeschGehG* (2019) foi preenchido tanto no *plano estático* como no *plano dinâmico*. Na sua fundamentação, a instância alemã acentuou, nesse ensejo, que as medidas tomadas pelo titular do segredo deviam ser razoáveis – "Angemessene Geheimhaltungsmaßnahmen" – e que a razoabilidade é um *critério flexível* e *aberto,* que segue a ideia de *proporcionalidade jurídica*. Decorre ainda da decisão do OLG de *Hamm* que o critério da razoabilidade não é *absoluto* e *estático*, mas sim *relativo* e *dinâmico*. Com muita relevância, este tribunal alemão frisou ainda que um *comportamento mínimo* de proteção do segredo comercial não preenche o critério de razoabilidade. Esta orientação jurisprudencial tem o apoio de significativa parte da doutrina alameã. Tal como ensina Ohly[231], a razoabilidade não pressupõe uma proteção ótima ou máxima, pois caso contrário o conceito de segredo seria juridicamente demasiado restritivo, quebrando-se o equilíbrio imposto pela proporcionalidade. Não é assim necessário que sejam adotadas as melhores e mais eficazes medidas para proteger as suas informações confidenciais, mas também não é suficiente um comportamento que represente a adoção do *mínimo* de medidas para proteção do segredo comercial. Como também é defendido por Köhler/Bornkamm/Feddersen[232], não é assim suficiente uma conduta que revele,

---

Customer Information. Accordingly, the District Court did not err in determining that no reasonable jury could find that Yellowfin employed reasonable efforts to secure the information".

[229] A. Ohly, *Das neue Geschäftsgeheimnisgesetz im Überblick,* cit., p. 443: "Für Nervosität in der Wirtschaft sorgt § 2 Nr. 1 Buchst. b GeschGehG, dem zufolge die Information „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber" sein muss".

[230] OLG de Hamm, 15.09.2020, ref. 4 U 177/19 (acesso: *openjur.de*).

[231] A. Ohly, *Das neue Geschäftsgeheimnisgesetz im Überblick,* cit.: "Daher verlangt die Vorschrift zu Recht „angemessene", nicht jedoch absolut wirksame oder unumgehbar Schutzmaßnahmen". Do mesmo modo: S. Maassen, *„Angemessene Geheimhaltungsmaßnahmen" für Geschäftsgeheimnisse,* GRUR 4/2019, 2019, pp. 352 ss., p. 358.

[232] H. Köhler/J. Bornkamm/H. Feddersen, *Gesetz gegen den unlauteren Wettbewerb: UWG, GeschGehG, PAngV, UKlaG, DL-InfoV*, *P2B-VO*, C.H. Beck, 2022, p. 1962 ss., pp. 2037 ss. (§6).

nomeadamente para evitar custos elevados e um maior esforço organizacional, a adoção de um *comportamento mínimo* de proteção da informação.

12. Confrontando-se, depois e diretamente, com a necessidade de identificar elementos que possibilitem uma maior concretização da conduta normativamente exigível, foi ainda enunciado, pela acima referida instância alemã, que o juízo de razoabilidade deve ter em conta a perspetiva de um *observador objetivo* dos círculos profissionais que normalmente lidam com este tipo de informação.

Para os juízes alemães, vários critérios de avaliação devem ser ponderados. Desde logo, é destacada a *natureza* e o *valor económico* do segredo: tal significa que os custos das medidas para preservar o segredo devem ser *proporcionais* ao valor do segredo comercial, não sendo possível estabelecer previamente uma relação fixa entre o valor do custo das medidas e o valor do segredo comercial. Para este tribunal alemão, deve, no entanto, considerar-se como irracional a exigência de medidas cujo custo exceda o valor do segredo comercial. Deve ainda ser considerada a dimensão da empresa: uma empresa multinacional com grandes recursos deve tomar medidas especiais e mais dispendiosas quando comparadas com as exigíveis a uma empresa regional de pequena dimensão e com recursos bastante inferiores. Ademais, é relevante ponderar o setor económico em que a empresa opera, uma vez que as normas típicas de regulação e de segurança desse setor poderão servir como referentes para estabelecer o padrão normativo de razoabilidade.

13. Ainda no plano da densificação do critério de razoabilidade, é também de notar a importante decisão do OLG de *Stuttgart* (2021)[233]. Neste aresto, cumpria aferir se houve violação de um alegado segredo comercial relativo a sistemas de espuma de poliuretano e adesivos. Neste ensejo, o tribunal alemão teve de verificar novamente se estava ou não preenchido o critério da razoabilidade e, para tanto, foi necessário especificá-lo atendendo às circunstâncias do caso concreto: estava em causa a tomada de *medidas razoáveis* na *partilha da informação* com funcionários. Foi então decidido que, como padrão mínimo, exige-se que a informação relevante só possa ser partilhada com pessoas que potencialmente necessitem da informação para desempenhar a sua tarefa (*need to know basis*) e que estejam vinculadas ao sigilo. Qualquer partilha, física ou digital, que escape a este *princípio de necessidade* pode fazer perigar o preenchimento do requisito da razoabilidade das medidas de proteção do segredo. Para além do *princípio de*

[233] OLG de Stuttgart, 19.11.2020, ref. 2 U 575/19 (acesso: *openjur.de*).

necessidade, as pessoas com acesso à informação devem ainda estar conscientes da *obrigação de confidencialidade*: daqui resultam deveres de informação e/ou de celebração acordos de confidencialidade (na fase pós-laboral). Mas o tribunal superior de *Stuttgart* foi ainda mais longe na densificação do critério de razoabilidade, determinando que as medidas devem ser tomadas de acordo com as circunstâncias: por exemplo, em caso de fuga de dados (*data leak*) pode chegar-se à conclusão de que não foram tomadas as medidas razoáveis quando o titular do segredo tenha permitido aos seus funcionários guardar ficheiros em suportes de dados privados sem a proteção de senha/*password*[234].

Para os mesmos efeitos de análise, vale ainda a pena convocar a decisão do OLG de *Düsseldorf* (2021)[235]: neste recente caso, envolvendo a possível violação de segredo comercial relativo a centrífugas totalmente automáticas, o tribunal alemão afirmou que as medidas de proteção adequadas ao caso individual são determinadas tendo em conta que a lei não exige uma *proteção ótima* ou *segurança extrema*, devendo ser respeitada a proporcionalidade. Deste modo, devem ser tidos em conta: 1) o tipo de segredo; 2) o seu valor e os custos associados ao seu desenvolvimento; 3) a natureza da informação; 4) a importância do segredo para a empresa; 5) a dimensão da empresa; 6) as medidas de sigilo habituais no setor; 7) o tipo de rotulagem da informação; e 8) as disposições contratuais acordadas com terceiros, nomeadamente funcionários e parceiros comerciais[236].

---

[234] OLG de Stuttgart, 19.11.2020, ref. 2 U 575/19 (acesso: *openjur.de*).

[235] OLG de Düsseldorf, 11.03.202, ref. 15 U 6/20 (acesso: *openjur.de*). O caso *sub judice* teve ainda uma dimensão temporal que teve de ser resolvida: sublinhando precisamente que a *GeschGehG* veio introduzir uma obrigação nova ou adicional do titular do segredo comercial em comparação com o §17/2 da antiga versão da UWG, que ainda não tinha sido estabelecida em 2017 (data dos factos), foi decido que a proteção das expectativas legítimas e a proibição da retroatividade das leis exigem que sejam tomadas medidas de sigilo adequadas apenas a partir da entrada em vigor da *GeschGehG*. Deste modo, no caso dos autos, as medidas deviam, portanto, ter estado em vigor continuamente apenas desde 26 de abril de 2019.

[236] OLG de Düsseldorf, 11.03.202, ref. 15 U 6/20 (acesso: *openjur.de*). O caso *sub judice* teve ainda uma dimensão temporal que teve de ser resolvida: sublinhando precisamente que a *GeschGehG* veio introduzir uma obrigação nova ou adicional do titular do segredo comercial em comparação com o §17/2 da antiga versão da UWG, que ainda não tinha sido estabelecida em 2017 (data dos factos), foi decido que a proteção das expectativas legítimas e a proibição da retroatividade das leis exigem que sejam tomadas medidas de sigilo adequadas apenas a partir da entrada em vigor da *GeschGehG*. Deste modo, no caso dos autos, as medidas deviam, portanto, ter estado em vigor continuamente apenas desde 26 de abril de 2019.

§5. Em especial: o critério de razoabilidade no espaço digital

1. Da análise enunciada quanto aos sistemas norte-americano e alemão resultam ponderosos elementos, no plano do direito nacional, para a concretização do critério de razoabilidade e que agora se procurarão aplicar ao espaço digital. De forma sintética, é possível estabelecer que não é razoável exigir que se adotem *todas as medidas* de proteção informática para proteger o segredo comercial no espaço digital. Está afastada, portanto, a exigência normativa de uma conduta de *cuidado máximo* que possa prevenir todas as potenciais ameaças ao segredo comercial no espaço digital. Por outro lado, o que consta da alínea c) do n.º 1 do artigo 313.º, do CPI (2018), não traduz uma *obrigação de resultado*: basta apenas demonstrar que o titular do segredo agiu de forma razoavelmente diligente na manutenção do segredo comercial e não que tenha tido êxito, apesar da exigência de eficiência das medidas adotadas.

2. A diligência exigível ao titular do segredo comercial relaciona-se concreta e circunstancialmente com vários elementos, nomeadamente com o valor do segredo comercial, o perigo da sua divulgação e os custos das medidas de proteção, tudo no quadro da proporcionalidade. As medidas básicas a tomar, seguindo o ensinamento de Cundiff, traduzem-se nos deveres de controlar o acesso ao segredo, de não divulgar o segredo mais amplamente do que o necessário, de não partilhar genericamente o segredo com pessoas que não têm obrigação de o manter, de estabelecer e atualizar orientações de segurança e o dever de adotar uma conduta vigilante no plano do espaço digital[237].

Ora, é precisamente neste contexto que o mundo das novas tecnologias exige que sejam tomadas novas medidas para proteger razoavelmente o segredo de acordo com o critério de diligência previsto na alínea c) do n.º 1 do artigo 313.º, do CPI (2018). Como igualmente refere Cundiff, "o titular do segredo deve ser vigilante na identificação de novas ameaças e na identificação de novos meios digitais para as combater"[238]. Porque a não adoção proativa de medidas e/ou a não tomada de decisões empresariais informadas que considerem também as novas tecnologias desprotegerá juridicamente a informação enquanto segredo comercial[239],

---

[237] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., pp. 363 e 364.
[238] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 363.
[239] V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 364: "New technologies present new reasons–and new ways–to implement these time-honored rules.

tendo em conta precisamente a importância do espaço digital e das novas tecnologias[240].

a) O acesso ao segredo

3. Concretizando o padrão de conduta normativamente exigível ao titular do segredo comercial, um primeiro elemento a ter em mente é o da limitação do acesso a segredos comerciais apenas às pessoas, grupos ou departamentos com base no *princípio da necessidade* de acesso[241]. O acesso à informação é particularmente relevante no tempo presente, nomeadamente quando muitas empresas têm de recorrer ao serviço de trabalho remoto, usando para tanto as plataformas digitais, ou quando a relação com fornecedores e clientes é feita também com recurso, cada vez mais frequente, a esse tipo de plataformas digitais. Assim, no plano do espaço digital, o cumprimento do *princípio da necessidade* (*need to know basis*)[242] pode resultar da adoção de medidas de restrição de acesso a sistemas, bases de dados ou programas informáticos específicos, permitindo o acesso apenas às pessoas que dele necessitem para o cumprimento da sua prestação/função[243]. Neste contexto, tem todo o cabimento regressar novamente à casuística judicial norte-americana, nela procurando identificar densificações do padrão de comportamento no contexto digital.

4. Por exemplo, no caso *First Fin. Bank, N.A. v. Bauknecht* (2014)[244], estava em causa determinar se uma lista de clientes seria ou não um segredo comercial, analisando especialmente se e de que forma foi acautelado o acesso a essa lista de clientes, nomeadamente se um dos seus funcionários (*Bauknecht*) acedeu e utilizou ilicitamente essa informação. O titular do segredo, neste contexto, apresentou

---

Trade secret owners who do not make informed decisions to adapt their practices to take new technologies into account have failed to take reasonable measures to protect their secrets".

[240] Referindo medidas de *defesa digital*: "digital safeguards in digital environment", V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., p. 365

[241] Neste sentido, OLG de Stuttgart, 19.11.2020, ref. 2 U 575/19 (acesso: *openjur.de*).

[242] M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., p. 388.

[243] A. Ohly, *Das neue Geschäftsgeheimnisgesetz im Überblick,* cit., p.444: "Drittens sollten nach dem „*Need to know*"-Prinzip Mitarbeiter nur Zugang zu denjenigen vertraulichen Informationen erhalten, die sie für ihre Arbeit benötigen. Viertens können technische Schutzmaßnahmen erforderlich sein, die von einem einfachen Passwortschutz über *Firewalls* bis hin zu komplexen Sicherheitssystemen reichen können".

[244] *First Fin. Bank, N.A. v. Bauknecht,* (71 F. Supp. 3d 819/C.D. Ill. 2014) (acesso: *lawjustitia.com*).

provas de que os seus colaboradores precisavam de códigos especiais de segurança para aceder ao seu sistema informático e apresentou provas de que foram também instruídos em como remover informações confidenciais dos seus *iPads* pessoais. Tal foi suficiente para que o tribunal norte-americano considerasse que foram adotadas as medidas razoáveis para manter a informação secreta.

Por seu turno, no caso *Stampede Tool Warehouse, Inc. v. May* (1995)[245], considerou-se que determinada lista de clientes da empresa era confidencial porque, entre outras coisas, a empresa limitava o *acesso ao computador* apenas a duas pessoas e fornecia informações de clientes com base no *princípio da necessidade* de conhecimento. Ainda quanto a este ponto, tome-se boa nota como, no caso *Cumulus Radio Corp. v. Olson* (2015)[246], o *District Court* do *Illinois* considerou que não tinham sido tomadas medidas razoáveis, não obstante terem sido celebrados acordos de confidencialidade com os seus empregados, porque a informação "secreta" empresarial era *livremente acessível* numa rede informática partilhada que podia ser consultada por qualquer pessoa que tivesse acesso ao referido sistema informático: não foram adotadas quaisquer medidas de segurança, nomeadamente o estabelecimento de códigos pessoais de acesso. Ou seja, uma vez que a *Cumulus Radio* não limitou o acesso dos funcionários de acordo com princípio da necessidade de acesso e não protegeu o acesso geral ao seu sistema informático, o tribunal norte-americano concluiu que não havia segredo comercial por não estar verificado o requisito dinâmico[247].

5. Em termos gerais, é de considerar como medida razoável a utilização de *firewalls* ou outro tipo de *software* de segurança análogo, criando desta forma uma

---

[245] *Stampede Tool Warehouse, Inc. v. May,* (272 Ill. App. 3d 580/Ill. App. Ct. 1995, 651 N.E.2d 209) (acesso: *lawjustitia.com*): "Stampede protects its customer list using reasonable efforts to maintain its secrecy and confidentiality. Its offices are locked, garbage is checked daily, special computer access codes are used, customer information is limited to persons on a need-to-know basis, hard copies of customer lists are kept locked in the office or in Kuhn's basement at home, salesmen's call books and customer cards are kept locked up and cannot be removed from the office, and security cameras are used. Moreover, both defendants signed employee confidentiality agreements that stated that the names of Stampede's customers could not be used or disclosed because they belonged to Stampede and were confidential. As a result, we conclude that Stampede's customer list is a trade secret that is protectable under the ITSA".

[246] *Cumulus Radio Corporation v. Olson et al*, (80 F. Supp. 3d 900/C.D. Ill. 2015) (acesso: *lawjustitia.com*): "Although nondisclosure agreements provide evidence that an employer has taken adequate steps, they are not sufficient to demonstrate that an employer has taken reasonable steps".

[247] Também neste sentido, na Alemanha, cfr. OLG de Düsseldorf, 11.03.2021, ref. 15 U 6/20 (acesso: *openjur.de*).

barreira digital entre a sua rede interna e as redes externas (como é caso da *Internet*)[248]. Com efeito, dadas as circunstâncias empresariais concretas, é entendível que os tribunais exijam algum tipo de *firewall*: as medidas de segurança terão de ser mais amplas quando estejam em causa empresas maiores, mais sofisticadas e sujeitas a ameaças informáticas mais frequentemente (há muitas empresas que sofrem ataques informáticos diariamente). Precisamente neste sentido, considerando que a adoção de *firewalls* corresponde à adoção de "medidas razoáveis" para proteger os segredos comerciais armazenados numa rede, no caso *United States of America v. Tien Shiah*[249], o *District Court* da *California* teve de analisar a conduta do titular de um segredo relativo a dados informáticos. Ora, verificando que este protegeu os seus dados através da sua equipa de tecnologia da informação, geriu um sistema de *firewalls*, adquiriu *software* de deteção de intrusão, estabeleceu palavras-passe para aceder à *Intranet*, criou uma camada de proteção entre a rede intranet e a rede de *Internet*, e estabeleceu um protoloco interno de armazenamento digital seletivo de ficheiros, a instância norte-americana considerou que foi preenchido o critério de razoabilidade, uma vez que o titular do segredo tomou em consideração o espaço digital na proteção dos seus segredos.

6. Outras medidas de segurança de rede que podem ser exigidas correspondem à aquisição de *software* de prevenção de perda de dados, bem como de segregação da rede, para evitar agregar segredos comerciais numa rede centralizada, e testes de *stress* concebidos para assegurar que todos os sistemas e medidas de segurança do sistema funcionam de forma apropriada. Bem assim, a encriptação de qualquer informação secreta de valor comercial particularmente elevado – a encriptação pode ser utilizada para determinados ficheiros, discos de computador, servidores, tráfego de correio eletrónico – é um indício forte de ter sido preenchido o critério de razoabilidade[250].

Por outro lado, especialmente em situações de trabalho ou acesso remoto, são vindicáveis medidas de segurança doméstica para as redes domésticas, incluindo

---

[248] M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., p. 389.

[249] *United States* v. *Tien Shiah*, SA CR 06-92 DOC (C.D. Cal. Feb. 19, 2008), (acesso: *court.cacd.uscourts.gov*).

[250] Os tribunais norte-americanos têm perfilado a encriptação como prova suficiente dos esforços razoáveis do titular de um segredo comercial para proteger os segredos comerciais, mas não aceitam conclusão contrária quando se prova a não utilização da encriptação, ou seja, a falta desta não é qualificada automaticamente como falha na tomada de medidas razoáveis. Deste modo, a encriptação é um indício positivo de razoabilidade, mas a sua não adoção não é um perspetivada automaticamente como um indício negativo de razoabilidade.

a proteção por senha de qualquer rede *wi-fi* e limitações subjetivas ao seu acesso[251]. É assim suscetível de preencher o critério de razoabilidade a prova de ter sido implementado *software* antivírus e *software* contra *malware* e de proteção contra ciberataques. Pode também contribuir para preencher o requisito legal que seja feita prova de que todos os dispositivos utilizados para aceder remotamente à rede do titular do segredo comercial são protegidos por *passwords* sofisticadas e alteradas periodicamente, e que os dispositivos utilizados no acesso remoto estão sujeitos a encriptação do disco rígido, sendo possível executar a limpeza de ficheiros remotamente, com permissões de acesso remoto, em caso de extravio. Novamente, é também de aplicar o princípio da necessidade, restringindo-se o acesso de cada funcionário à rede apenas aos locais ou segmentos da rede que o funcionário necessita de utilizar, com a segurança apropriada para esses locais. Ao que podem acrescer a imposição de credenciais para descarregar certos dados sensíveis e a proibição de realizar descarregamentos, inclusivamente com bloqueios informáticos. Tal foi precisamente o que sucedeu no caso *Diamond Power Int'l, Inc. v. Davidson* (2007)[252], tendo o tribunal considerado como significativo (para o não preenchimento do critério da razoabilidade) que o titular do segredo comercial tenha falhado ao prevenir que os seus funcionários transferissem, com liberdade, ficheiros informáticos para os seus dispositivos pessoais.

7. Seguindo a mesma filosofia, configura também um indício positivo de razoabilidade a utilização de filtros de *e-mail* para restringir as comunicações de e para locais potencialmente arriscados ou suspeitos, para impedir a transmissão de ficheiros particulares, e/ou para se proteger contra tentativas de *phishing* ou *malware* que possam constituir um risco para os segredos comerciais[253]. Tem igual pertinência restringir o uso dispositivos portáteis de arquivamento digital, bem como a proibição

---

[251] R. B. Milligan/D. J. Salinas, *A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media,* cit., p. 26.

[252] *Diamond Power Int'l, Inc. v. Davidson* (540 F. Supp. 2d 1322, 1333-35/N.D. Ga. 2007) (acesso: *lawjustitia.com*): "the Court concludes that Diamond Power has failed to demonstrate that it took reasonable efforts to maintain the secrecy of the PI Library, the FWI Library, and the PI Configurator. The record establishes that Diamond Power provided virtually *no guidance to its employees concerning the safe handling of this information,* despite its awareness that it was regularly communicated to customers and used at customer sites. Because the information at issue was widely distributed among its employees, and not restricted from exposure to its customers or others, Diamond Power's efforts do not suffice to afford these files trade secret protection".

[253] R. B. Milligan/D. J. Salinas, *A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media,* cit., p. 26.

do uso de tais dispositivos ou o bloqueio total das portas de conexão a esses dispositivos, a fim de proteger o roubo de segredos comerciais, *malware*, cópias e downloads não autorizados. No plano do acesso remoto e do uso de meios digitais de comunicação – *e-mail* e *apps* de mensagens instantâneas, como o *whatsapp, telegram, facetime, zoom, skype*, etc. –, devem privilegiar-se meios de comunicação que permitam encriptação ou sejam encriptados por configuração geral, pois a utilização deste tipo de meios pode ser demonstrativa de que foram adotadas medidas razoáveis quanto à proteção da circulação da informação secreta.

b) A divulgação do segredo

8. Nos casos em que seja cumprido o *princípio da necessidade* no acesso à informação, é sequentemente necessário acautelar que não se verifique uma divulgação do segredo por parte de quem a ele teve legítimo acesso, pois tal poderá significar o fim da tutela jurídica da informação que se pretende manter sob segredo. Nessa medida, controlar o acesso não significa necessariamente que foram tomadas todas as medidas razoáveis para evitar a sua divulgação.

É preciso estabelecer medidas razoáveis no contexto da partilha digital do segredo, nos vários momentos relevantes, ou seja, *ex ante*, durante e *ex post*. Neste enquadramento, previamente a fornecer o acesso a quaisquer segredos comerciais a funcionários e/ou terceiros, é de assinalar a relevância que pode resultar da inserção de *cláusulas de confidencialidade* nos contratos de trabalho – densificando[254] o dever de confidencialidade que resulta do artigo 128.º, alínea f), do Código do Trabalho[255] – bem como, em geral, nos contratos de prestação de serviços com entidades externas.

Por exemplo, os tribunais norte-americanos têm valorizado positivamente, para prova dos *esforços razoáveis* para a manutenção do segredo comercial, a inserção de

---

[254] Referindo-se a uma função de densificação do dever legal de confidencialidade: M. Nogueira Serens, *A tutela dos segredos comerciais no acordo TRIPS,* cit., p. 391.

[255] Embora sejam nulas as cláusulas de contrato de trabalho que, por qualquer forma, possam prejudicar o exercício da liberdade de trabalho, tal como resulta do n.º 1 do artigo 136.º do Código do Trabalho, não é de confundir o *pacto de não concorrência* – que visa acautelar, por certo tempo, o prejuízo decorrente do exercício de atividade concorrencial e o risco de indefinição entre as situações ilícitas de utilização de informação reservada ou confidencial e o normal exercício dos conhecimentos profissionais e técnicos adquiridos pelo desempenho e experiência, constitutivos estes do chamado património profissional do trabalhador –, com as *cláusulas de confidencialidade* – que visam apenas impedir a divulgação, no subsequente período pós-contratual, de factos que não fazem parte da experiência profissional do trabalhador, cfr. E. Mendes, *Segredos comerciais e liberdade profissional*, cit., pp. 743 ss.

cláusulas confidencialidade em contratos de trabalho e em contratos de prestação de serviços. De modo inverso, a não existência de cláusulas de confidencialidade – entre nós, sobretudo quando não seja aplicável o artigo 128.º, alínea f), do Código do Trabalho – pode introduzir dificuldade na prova da adoção de *diligências razoáveis*[256].

9. Por outro lado, depois de ter sido concedido o acesso à informação e permitido o seu arquivamento em computadores pessoais, especialmente nos casos em que há trabalho com acesso remoto ou utilização de plataformas digitais, é de precaver a situação que se verifica após a cessação da relação entre o titular do segredo e a pessoa a quem foi permitido o respetivo acesso[257]. Está em causa, nomeadamente, a realização de "entrevistas de *exit*", nas quais se solicita que sejam devolvidas ou apagadas todas as informações sobre segredos comerciais. Percebe-se a relevância particular deste aspeto quando se verifica que este tipo de medida costuma ser considerada pelos tribunais como uma medida razoável. Assim sucedeu no caso *Yellowfin Yachts, Inc. v. Barker Boatworks*, *LLC* (2018)[258], tendo o *Court of Appeal* enfatizando que o facto de titular do segredo comercial não ter solicitado que fossem eliminados ficheiros relativos ao segredo, depois de terminada a relação com terceiro a quem permitiu acesso ao mesmo, tal constitui um indício de não de adoção de medidas razoáveis, enfraquecendo a proteção jurídica da informação secreta[259].

10. Por outro lado, ainda no plano da concretização do critério de razoabilidade, requerem especial abordagem as situações em que se verifique a divulgação não

---

[256] Assim sucedeu em *M.C. Dean, Inc. v. City of Miami Beach* (M.C. Dean, Inc. v. City of Miami Beach, Fla., 199 F. Supp. 3d 1349, 1356 (S.D. Fla. 2016): o tribunal norte-americano sublinhou que não foi implementado qualquer acordo de confidencialidade nem qualquer outro meio de proteção. Entre nós, explorando múltiplas dimensões deste problema: E. Mendes, *Segredos comerciais e liberdade profissional*, cit., pp. 743 ss.

[257] R. B. Milligan/D. J. Salinas, *A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media,* cit., p. 26.

[258] *Yellowfin Yachts, Inc. v. Barker Boatworks,* LLC, No. 17-11176 (11th Cir. 2018) (acesso: *lawjustitia.com)*.

[259] *Yellowfin Yachts, Inc. v. Barker Boatworks,* LLC, No. 17-11176 (11th Cir. 2018) (acesso: *lawjustitia.com)*: "Yellowfin limiting employee access to the information and password-protecting the computer network on which the information resided were positive steps in securing the alleged trade secret. (...) But Yellowfin compromised the efficacy of these measures by encouraging Barker to keep the Customer Information on his cellphone and personal laptop. Indeed, Barker refused to sign an employment agreement which stated that he would, among other things, keep all Yellowfin trade secrets in confidence. Further, Yellowfin neither marked the Customer Information as confidential nor instructed Barker to secure the information on his personal devices. And when Barker left Yellowfin, the company did not request that Barker return or delete any of the information".

autorizada do segredo comercial. Com efeito, perante o conhecimento ou mera suspeita de qualquer revelação não autorizada de segredos comerciais, o seu titular deve tomar medidas imediatas – por exemplo: medidas judiciais cautelares a fim de proteger os seus segredos comerciais – para demonstrar que tomou "medidas razoáveis" para manter/preservar o segredo.

Note-se, como visto anteriormente, que a mera divulgação pode não ser suficiente para destruir o segredo comercial, pelo que o requisito das *diligências razoáveis* continua a ser aplicável mesmo depois do segredo comercial ter sido divulgado na *Internet*. Contextura na qual a inação, a passividade ou a delonga na adoção de medidas reativas podem ser consideradas judicialmente como uma falha quanto às "medidas razoáveis" para proteger segredos comerciais[260]. Por exemplo, no caso *HiRel Connectors, Inc. v. United States of America*, o *District Court* (2007)[261], uma vez que o titular do segredo aguardou mais de dois anos para reagir depois de ter tido conhecimento de que os seus segredos comerciais tinham sido publicados na *Internet*, o tribunal norte-americano concluiu que a informação tinha deixado de ser um segredo comercial por essa razão. Com igual interesse e precisamente

[260] Note-se que, caso esteja em causa a tomada de medidas judiciais, também é necessário agir com razoabilidade, suscitando ao tribunal que considere as informações objeto do litígio como confidenciais, nos termos do artigo 352.º CPI, sob pena de ser perdido o segredo no decurso do processo judicial. Sobre a proteção dos segredos no contexto processual: cfr. Acórdão do Tribunal da Relação de Guimarães, processo n.º 51/20.9T8VNF-B.G1 (3 de fevereiro de 2022): "Sendo solicitada a "exibição" de elementos da escrituração comercial de um terceiro, no âmbito de um processo, não é lícita a recusa com fundamento no disposto no artigo 42.º do CCom, que se aplica apenas à exibição judicial por inteiro, conforme artigo 435.º do CPC, caindo-se na alçada do artigo 417.º do CPC. Na apreciação de qualquer pedido de "exibição" parcial, devem conjugar-se os interesses em jogo, limitando-se a pretensão ao que for necessário e imprescindível para a prova pretendida, de acordo com critérios de adequação e proporcionalidade. Quem aceda a elementos relativos a segredo profissional (artigo 352.º do CPI) ou elementos sujeitos a confidencialidade (artigo 164.º do CPC), fica sujeito a ao dever de sigilo"; bem como o Acórdão do Tribunal da Relação de Lisboa, processo n.º 99/21.6YHLSB-A.L1-PICRS (10 de março de 2022): "(...) Importa assim reconhecer que (...) as dificuldades apontadas pelo Tribunal a quo no despacho recorrido, existem, na medida em que, por um lado, o acesso a informação técnica reservada, know-how, processos utilizados, programas de computador, dados comerciais sensíveis, como a identidade de clientes, trabalhadores, valores de facturação, preços praticados, é essencial para a procedência da pretensão da autora; mas por outro lado, a sua divulgação pode lesar gravemente os interesses da primeira ré, numa altura em que ainda não se apurou, e pode até nem vir a apurar-se, a existência da alegada violação de segredos comerciais. Porém, para solucionar tais dificuldades, o Tribunal deve ter em conta os dois interesses contrapostos, sem ir ao extremo de, para preservar a confidencialidade, denegar à autora o exercício dos poderes que o artigo 339.º do CPI lhe confere. Para esse efeito, o Tribunal deverá decretar as medidas adequadas, específicas e proporcionais à preservação dos segredos comerciais em processos judiciais, nos termos previstos pelo artigo 339.º n.º 3 e recorrendo se necessário ao artigo 352.º do CPI".

[261] *HiRel Connectors, Inc. v. United States of America*, o *District Court,* 540 F. Supp. 2d 1322 (N.D. Ga. 2007).

sobre este ponto, o facto de a informação ter sido publicada ou não na *Internet* foi determinante no caso *PQ Labs, Inc. v. Yang Qi* (2014)[262]: neste caso, o *District Court* considerou que esperar vinte meses para reagir judicialmente ainda era razoável, uma vez que os segredos comerciais não foram publicados na *Internet*. Assim, o local da divulgação da informação secreta foi a circunstância decisiva para apurar se foram tomadas as medidas razoáveis para a manutenção do segredo[263].

c) Planeamento dinâmico de segurança e vigilância

11. Por último, é apropriado revisitar o caso apreciado pelo OLG de *Hamm* (2020)[264]: tendo esta instância acentuado que as medidas de sigilo tomadas pelo

---

[262] *PQ Labs, Inc. v. Yang Qi*, No. 12-0450 CW (N.D. Cal. Jan. 29, 2014): "The district court cases that Defendants cite are likewise inapposite. In *Gemisys Corp. v. Phoenix America*, Inc., 186 F.R.D. 551 (N.D. Cal. 1999), this Court granted summary judgment to the defendant on a trade secret claim because the plaintiff failed to mark its alleged trade secrets as confidential. That marking requirement, however, is irrelevant here because, as outlined above, PQ Labs has presented evidence that it used other means to notify its employees and agents that its technological and customer information was confidential. Moreover, the trade secret claims in Gemisys were brought under Colorado's trade secret statute, not CUTSA, and the marking requirement was derived from Tenth Circuit case law. See id. at 558 (citing Jensen v. Redevelopment Agency of Sandy City, 998 F.2d 1550, 1557 (10th Cir. 1993)). Thus, Gemisys does not apply here. The Central District of California's decision in *HiRel Connectors, Inc. v. United States*, 2005 WL 4958547 (C.D. Cal.), also differs from the present case in important respects. There, the court granted partial summary judgment to the defendant because the plaintiff failed to act quickly to protect its trade secrets, even after it learned that the trade secrets had been published online. The court concluded that, because the plaintiff waited more than two years to protect its confidential information after it was disclosed publicly, the information ceased to be a trade secret. Here, in contrast, PQ Labs waited only twenty months to file this suit once it learned of Defendants' possible misappropriation. This period is comparable to the eighteen-month delay in filing suit that the court found permissible in HiRel.. More importantly, PQ Labs' alleged trade secrets were never disclosed in a public forum. As the HiRel court explained, once a plaintiff's trade secret has been publicly disclosed, "merely filing suit against the alleged wrongdoer does not constitute 'reasonable efforts' to protect the trade secrets against others who might be interested in obtaining those secrets." This rationale does not apply in the present case, where PQ Labs' trade secrets were never publicly disclosed".

[263] Note-se que no caso *HiRel Connectors, Inc. v. United States of America* o tribunal considerou que o titular do segredo não agiu rapidamente para proteger os seus segredos comerciais, mesmo depois de saber que os segredos comerciais *tinham sido publicados* na *Internet.* O tribunal concluiu que esperar mais de dois anos para proteger informações confidenciais após a sua divulgação na *Internet* faz cessar o segredo comercial. Na situação da *PQ Labs*, o titular do segredo demorou vinte meses para reagir judicialmente, mas alegou que os segredos comerciais nunca foram revelados *online*, circunstância que foi determinante.

[264] OLG de Hamm, 15.09.2020, ref. 4 U 177/19 (acesso: *openjur.de*).

titular do segredo comercial não pressupõem uma proteção ótima ou máxima, pois caso contrário haveria desvio quanto à necessidade de proporcionalidade jurídica, o tribunal superior de *Hamm* sublinhou que o critério da razoabilidade não é *absoluto* e *estático*, mas sim *relativo* e *dinâmico*.

Foram salientados, nos pontos anteriores, múltiplos elementos que assentam num *juízo relacional* na concretização do critério de razoabilidade. É o que sucede, por exemplo, quando se comparam os custos associados ao segredo e os custos da proteção. Porém, como sublinhado pela instância superior alemã, o critério de razoabilidade comporta uma *dimensão dinâmica*. Em termos técnico-jurídicos, pode afirmar-se que essa dimensão dinâmica, no ponto que agora se pretende enfatizar, traduz a necessidade de adotar uma *conduta vigilante*, bem como a necessidade de *atualização* perante o desenvolvimento tecnológico.

Ou seja, a proteção do segredo não é estática nem está cristalizada temporal e juridicamente. Um segredo que num certo período pode estar legalmente protegido, perante a inexistência de uma conduta vigilante e zelosa, poderá vir a perder proteção legal. Assim, existe uma necessidade de proteção permanente do segredo comercial, e esta característica da continuidade dinâmica integra o núcleo central do critério de razoabilidade das medidas exigíveis ao seu titular.

12. Uma das manifestações desse dever contínuo e dinâmico traduz-se, por exemplo, na necessidade desenvolver uma *cultura empresarial de proteção*, nomeadamente mediante a adoção de programas regulares de formação em matéria de segurança da informação, com especial atenção à identificação dos segredos comerciais e à forma como estes devem ser tratados. No contexto da atividade de formação, justifica-se que seja dada particular atenção a grupos particulares com acesso regular a informação mais sensível ou valiosa, bem como sobre como se comportar fora das instalações do titular do segredo, nomeadamente em viagens/deslocações. Por exemplo, regras sobre a proibição digitalização de documentos secretos, revelarão, com maior probabilidade, uma conduta que se traduz na adoção de medidas razoáveis para proteger o segredo[265].

A importância da *atividade de formação* no preenchimento do critério de razoabilidade verificou-se precisamente no caso *Avery Dennison Corporation v. Finkle* (2002)[266]: o tribunal norte-americano considerou ser significativa a circunstância

[265] Cundiff V. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, cit., pp. 364 ss.
[266] *Avery Dennison Corporation v. Finkle*, No. CV010757706, 2002 WL 241284 (Conn. Super. Ct. Feb. 1, 2002).

de o titular do segredo ter adotado um *programa de formação permanente*, com cursos anuais de formação em propriedade intelectual ("yearly refresher courses in intellectual property and trademarks"[267]). Já no caso *Diamond Power Int'l, Inc. v. Davidson* (2007)[268], em face de um comportamento passivo por parte do titular do segredo comercial, o tribunal norte-americano considerou que não foram tomadas medidas razoáveis, uma vez que o titular do segredo não forneceu formação e não transmitiu quaisquer orientações quanto à forma de lidar com a informação secreta – "provided virtually no guidance to its employees concerning the safe handling of this information" –[269], revelando assim uma conduta que não preencheu o requisito das *diligências razoáveis*.

13. Regressando novamente ao sistema alemão – por exemplo: nas decisões do Tribunal Regional Superior de *Dusseldorf* (2021)[270] e do Tribunal Regional Superior de *Hamm* (2020)[271] – tem sido confirmada a necessidade de adotar uma conduta que seja reveladora de *vigilância dinâmica*. Com efeito, as medidas a tomar pelo titular do segredo comercial devem corresponder a um *sistema de proteção em evolução*. Por exemplo, caso seja detetada uma *fragilidade potencial* do sistema informático (por via de um novo *vírus* informático que ameace várias empresas), ou uma *fragilidade real* porque já ocorreram violações no passado, é exigível uma conduta de *atualização* do sistema de proteção e/ou de reparação desses sistemas

---

[267] *Avery Dennison Corporation v. Finkle*, No. CV010757706, 2002 WL 241284 (Conn. Super. Ct. Feb. 1, 2002): "The court finds that Avery Dennison, by having employees such as Donald Finkle sign *non competition* provisions as contained in paragraph eight of their employment agreement, by having suppliers, where possible, sign nondisclosure agreements, by having workers keep logs as to the products on which they work, by giving employees yearly refresher courses in intellectual property and trademarks, by using "read only" files to prevent printing of the business plan and by having employees such as Donald Finkle sign the employee check out form when they end their employment, has used reasonable efforts under the circumstances to maintain the secrecy of its trade secret information".

[268] *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1336 (N.D. Ga. 2007).

[269] *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1336 (N.D. Ga. 2007): "Having reviewed this evidence, the Court concludes that Diamond Power has failed to demonstrate that it took reasonable efforts to maintain the secrecy of the PI Library, the FWI Library, and the PI Configurator. The record establishes that Diamond Power provided virtually no guidance to its employees concerning the safe handling of this information, despite its awareness that it was regularly communicated to customers and used at customer sites. Because the information at issue was widely distributed among its employees, and not restricted from exposure to its customers or others, Diamond Power's efforts do not suffice to afford these files trade secret protection".

[270] OLG de Düsseldorf, 11.03.2021, ref. 15 U 6/20 (acesso: *openjur.de*).

[271] OLG de Hamm, 15.09.2020, ref. 4 U 177/19 (acesso: *openjur.de*).

de proteção. A inação perante fragilidades potenciais ou reais coloca em risco o sistema de proteção do segredo comercial, podendo ser considerada como indiciária de não terem sido tomadas as medidas razoáveis para a manutenção do segredo. Por outro lado, tal como sublinhou o Tribunal Regional Superior de *Dusseldorf*[272], as medidas têm de ter sido adotadas *continuadamente*: assim, têm de ser aplicadas técnicas de vigilância eficazes e implementados os sistemas de controlo adequados para detetar fragilidades e potenciais ameaças. Evidentemente, todas estas exigências têm de ser calibradas pelo *princípio da proporcionalidade*, que integra o reduto nuclear do juízo sobre a razoabilidade das medidas adotadas pelo titular do segredo comercial.

§6. Síntese conclusiva

1. A montante, foi analisada a evolução histórica da proteção jurídica do segredo comercial, verificando-se que oscilou entre a *teoria da propriedade* e a *teoria da concorrência desleal*, emergindo modernamente de *modo autónomo*, nomeadamente nos sistemas europeus continentais e norte-americano. Como momento chave na construção da proteção dos segredos comerciais, destaca-se o UTSA (1979), que viria a marcar decisivamente o TRIPS (1994), influenciando este, por seu turno, vários ordenamentos jurídicos europeus, nomeadamente o direito português (CPI 2003). Dada a fragmentação jurídica europeia e norte-americana na tutela jurídica do segredo comercial, num plano de globalização e de afirmação do espaço digital, foram posteriormente aprovados dois instrumentos decisivos para a proteção dos segredos comerciais: o DTSA (2016) norte-americano e a diretiva europeia 2016/943 (2016), visando estabelecer um regime harmonizado para os blocos norte-americano e europeu. Neste contexto, Portugal procedeu à revisão do CPI (2018), autonomizando a tutela do segredo comercial, concluindo o caminho que havia sido iniciado com a reforma do CPI em 2003.

2. Assente o contexto geral e depois de perscrutado o conceito jurídico de segredo comercial – tipo de informação; natureza secreta; valor comercial; diligências razoáveis para manutenção do segredo comercial–, procedeu-se à explicitação das coordenadas gerais dos problemas que resultam especialmente do espaço digital, nomeadamente: *(i)* a divulgação de segredos na *Internet* e seus efeitos no próprio segredo; (*ii)* a divulgação e transferência de informação para serviços de nuvem;

[272] OLG de Düsseldorf, 11.03.2021, ref. 15 U 6/20 (acesso: *openjur.de*).

(*iii)* o conceito de *diligência razoável* para a manutenção da informação secreta no contexto do espaço digital.

3. Quanto a (*i),* pode concluir-se que, para efeito do artigo 313.º/1/a) do CPI (2018), a divulgação na *Internet* de segredos comerciais não importa *ipso facto* a cessação da sua tutela enquanto tal. Para apurar o efeito da divulgação, é necessário densificar critérios, avaliando a extensão da divulgação, o tempo de exposição do segredo comercial e o de reação do seu titular. Neste ponto em particular, referiu-se a importância da *teoria da preservação sequencial* desenvolvida por Rowe.

Quanto a (*ii),* verificou-se a necessidade de distinguir entre vários tipos de serviço de nuvem (privada, pública e híbrida). Seguindo-se o pensamento de Sandeen, sustentou-se que a utilização do serviço de nuvem privada é indiciadora de não ter ocorrido a divulgação da informação secreta, ao invés do que sucede quando se verifica o recurso ao serviço de nuvem pública. Por outro lado, rejeitou-se a associação automática entre *transferência (upload) de informação secreta* e *divulgação do segredo comercial*.

Quanto a (*iii),* identificou-se a origem histórica da *dimensão dinâmica* do conceito jurídico de segredo comercial – para efeito do artigo 313.º/1/c) do CPI (2018) –, enfatizando-se a necessidade de o titular do segredo comercial adotar uma *conduta positiva* que revele *diligência razoável* na manutenção do segredo comercial. Não é, pois, suficiente que a informação seja objetivamente secreta, exingido-se ainda que o seu titular adote um comportamento – *digilências razoáveis* – de proteção da informação. O critério de razoabilidade carece, portanto, de ser densificado através de vários subcritérios. Neste contexto, identificaram-se os deveres de controlo do acesso ao segredo, de prevenção e de reação perante a divulgação do segredo, de vigilância continuada e de atualização do sistema de proteção no quadro de um planeamento geral dinâmico de segurança. Enunciaram-se depois, para cada um destes deveres, medidas concretas a adotar no plano do espaço digital.