INSTITUTO
UNIVERSITÁRIO
DE LISBOA

A Proteção dos Segredos de Negócio em Ambientes de Inteligência Artificial: Abordagem ao Uso do ChatGPT

Joana Catarina Vaz da Costa Silva

Mestrado em Direito das Empresas e do Trabalho, com especialização em Direito das Empresas

Orientador:
Professor Doutor Luís Fernando Pimentel de Oliveira Vasconcelos Abreu - Professor Auxiliar, ISCTE - Instituto Universitário de Lisboa

Outubro, 2024

CIÊNCIAS SOCIAIS
E HUMANAS

Departamento de Economia Política

A Proteção dos Segredos de Negócio em ambientes de Inteligência Artificial: Abordagem ao Uso do ChatGPT

Joana Catarina Vaz da Costa Silva

Mestrado em Direito das Empresas e do Trabalho, com especialização em Direito das Empresas

Orientador:
Professor Doutor Luís Fernando Pimentel de Oliveira Vasconcelos Abreu - Professor Auxiliar, ISCTE - Instituto Universitário de Lisboa

Outubro, 2024

Agradecimentos

Primeiramente gostaria de expressar um sincero agradecimento ao Professor Doutor Luís Fernando Pimentel de Oliveira Vasconcelos Abreu, pela disponibilidade, compreensão, ajuda prestada e liberdade concedida para este processo.

À minha família, por toda a paciência, apoio e, especialmente, pela confiança que sempre depositam em mim.

Ao Martim, por me aturar nesta fase de ego menos brilhante e tornar este processo menos penoso, por toda a compreensão e carinho, tanto nesta fase, como no nosso dia a dia.

Ao Oliver, o melhor amigo que o ser humano pode ter, que me acompanhou nas longas horas da noite e que sempre me lembrou da importância de fazer pausas durante o processo criativo.

Aos meus amigos, que apesar da distância, estiveram sempre disponíveis para uma palavra de encorajamento, incentivo ou de ajuda.

Por último, quero agradecer a todos aqueles, que de alguma forma, ajudaram neste processo e contribuíram para a realização deste trabalho.

"If you want to be a grocer, or a general, or a politician, or a judge, you will invariably become it, that is your punishment. If you never know what you want to be, if you live what some might call the dynamic life but what I will call the artistic life, if each day you are unsure of who you are and what you know you will never become anything, and that is your reward."

— Oscar Wilde

Resumo

O presente trabalho pretende colocar em introspetiva a interação entre os segredos de negócio e o uso de sistemas de inteligência artificial, em especial o ChatGPT.

A Era Digital veio acompanhada da crescente preocupação em proteger informações confidenciais que comportam valor comercial e conferem vantagens competitivas aos seus titulares, pelo que surge a necessidade de equilibrar essa proteção com os benefícios que as tecnologias oferecem aos negócios.

Este paradigma vem exigir a adaptação dos modelos tradicionais de Direito, que muitas vezes se mostram inadequados diante das novas realidades sociais e empresariais, como também vem exigir a aplicação de mecanismos de prevenção de riscos junto das empresas.

Passando ainda pela abordagem do quadro jurídico constituído, sobretudo, mas não só, pela Diretiva Europeia 2016/943 e a sua transposição para Portugal pelo Código de Propriedade Industrial de 2018, como pelo recente contributo europeu do AI Act.

Por fim pretendemos compreender o instituto normativo dos segredos de negócio e perceber se existe efetiva tutela no ordenamento jurídico português, aquando da sua violação por meio do uso do ChatGPT, ou no mínimo, colocar em análise os desafios impostos e implicações teórico-legais desta hipótese.

Palavras-Chave: segredo comercial, inteligência artificial, chatgpt, proteção legal, propriedade industrial

Abstract

This work seeks to put into perspective the interaction between trade secrets and the use of artificial intelligence systems, in particular ChatGPT.

The digital era has been accompanied by a growing concern to protect confidential information that has commercial value and gives its owners competitive advantages, so there is a need to balance this protection with the benefits that technologies offer to business.

This paradigm requires the adaptation of traditional models of law, which are often inadequate in the context of new social and business realities, as well as the application of risk prevention mechanisms within companies.

We will also look at the legal framework consisting mainly, but not only, of European Directive 2016/943 and its transposition into Portugal by the 2018 Industrial Property Code, as well as the recent European contribution of the AI Act.

Finally, we intend to understand the normative institute of trade secrets and understand whether there is effective protection in the Portuguese legal system, when it is violated through the use of ChatGPT, or at the very least, to analyze the challenges imposed and the theoretical legal implications of this hypothesis.

Keywords: trade secret, artificial intelligence, chatgpt, legal protection, industrial property

Lista de Abreviaturas e Siglas

ADPIC/TRIPS - Acordo sobre os Direitos de Propriedade Intelectual relacionados com o Comércio / *Trade Related Aspects of Intellectual Property Right*

CC - Código Civil

CCTV - *Closed-Circuit Television*

ChatGPT/GPT - *Chat Generative Pre-Trained Transformer*

CPC – Código de Processo Civil

CPI - Código de Propriedade Intelectual

CT - Código do Trabalho

CUP - Convenção da União de Paris

Diretiva/Diretiva Europeia - Diretiva Europeia 2016/943, de 8 de Junho de 2016

DTSA - *Defend Trade Secrets Act*

GPDP - *Garante per la Protezione dei Dati Personali*

IA/AI - Inteligência Artificial / *Artificial Intelligence*

IBM - *International Business Machines Corporation*

OMC/WTC - Organização Mundial de Comércio / *World Trade Organization*

OMPI/WIPO - Organização Mundial da Propriedade Intelectual / *World Intellectual Property Organization*

PME - Pequenas e Médias Empresas

Regulamento/AI Act - Regulamento (UE) 2024/1689 de 13 de Junho

RGPD - Regulamento Geral sobre a Proteção de Dados

UE - União Europeia

UTSA - *Uniform Trade Secrets Act*

Índice

Introdução

Este trabalho procura refletir e analisar o regime jurídico do segredo comercial, explorando as várias implicações ditadas pelo desenvolvimento da inteligência artificial, e principalmente, a interação com o ChatGPT e o modo em que se justifica e opera a sua proteção legal.

A escolha deste tema deve-se sobretudo ao interesse pessoal em aumentar o conhecimento em temas que norteiam o grande ramo da Propriedade Intelectual, a par do interesse em abordar um tema emergente e inovador. Tomando facto, quando me foi proposta a elaboração de um pequeno artigo para o blogue jurídico da sociedade em que laborava, e deste modo, o pouco que me cruzou o entendimento sobre este tema, despertou interesse para maior aprofundamento. Pelo que do ponto de vista da necessidade de enquadramento com matéria que verse sobre o direito das empresas, pareceu-me uma combinação perfeita.

Ao longo deste estudo, recorremos a vários métodos de análise, nomeadamente, o método comparativo, o método histórico, o método teórico legal e, principalmente, o método dogmático legal. Pelo que procuramos abordar o tema pela abordagem legal do sistema jurídico nacional, europeu e norte-americano, compreender a evolução do instituto dos segredos de negócio ao longo do tempo, e a complementar, uma abordagem teórica e análise interpretativa do quadro legal vigente.

O rápido desenvolvimento tecnológico e digital ditou o reconhecimento de uma 4.ª Revolução Industrial, e com ela, a construção de um novo paradigma social. Por esta senda, não só se veem benefícios, como também se assistiu à eclosão de novos desafios jurídicos. Nomeadamente, quando pode estar em causa a violação de segredos de negócio pelo risco de divulgação no espaço digital. Pelo que se parte da ideia que o desenvolvimento tecnológico representa um perigo imenso para as informações confidenciais com valor comercial e económico que conferem vantagem competitiva para as empresas, que pela necessidade de atualização e adaptação ao mundo digital, carecem do uso de mecanismos informáticos para se manterem na vanguarda do mercado industrial e empresarial.

O que vamos constatar, é que houve um crescente interesse para regular o segredo comercial, contudo, cabe entender agora se as normas atuais, especialmente, o Regulamento Europeu 2016/943 e a sua transposição para o ordenamento jurídico nacional através do Código de Propriedade Industrial de 2018, sobrevivem ao teste do tempo e à mudança rápida de necessidades sociais pelos impactos inerentes à inteligência artificial.

E não será por acaso que a conceptualização de segredo comercial afigurou-se uma tarefa hercúlea. Muitas das dúvidas devem-se à ambiguidade semântico-jurídica, derivada da utilização de

conceitos indeterminados de difícil compreensão, que em quase tudo que norteia a concretização do termo e regime legal, gera dificuldades para depreender a aplicação da tutela legal.

No seguimento, os sistemas de inteligência artificial configuram um mecanismo de facilitação e complementaridade ao ser humano na mais variada execução de tarefas, a incluir, o seu uso no contexto laboral. Não ignorando as vantagens, não podemos deixar de fazer a ressalva das suas desvantagens, que passam, nomeadamente, pelo problema da potencial divulgação de segredos de negócio.

Pelo que o reconhecimento da necessidade de avaliação holística da inteligência artificial passou a constituir parte do quadro de prioridades dos últimos anos da Comissão Europeia e Parlamento Europeu. Concretizando-se o AI Act que configura uma forma de atribuir deveres e regular condutas que sustentam a relação ponderada de sistemas de inteligência artificial nos mais variados campos da sociedade e mercado único.

Por sua vez, a relação entre segredos de negócio e utilização de ferramentas de inteligência artificial pode não ser muito clara, contudo, quando colocamos em perspetiva que a transposição da informação confidencial para um sistema de IA, em especial, o ChatGPT, determina o armazenamento por parte do algoritmo da ferramenta, estará em causa a possível partilha em interações futuras com pessoas que não o titular.

Partindo da ideia que a sua conjugação pode ser entendida a três níveis: a primeira, pela transposição do segredo comercial para o ChatGPT; a segunda, pela possibilidade de essa informação ser partilhada com outro utilizador; a terceira, que a pessoa alheia que recebe esta informação a possa divulgar e/ou utilizar, tomando para si a vantagem económica e competitiva de titular concorrente.

Uma das questões que procuramos responder versa precisamente em compreender o instituto normativo dos segredos de negócio com o intuito de averiguar se existe efetiva tutela no ordenamento jurídico português, aquando da suposta violação por meio do uso do ChatGPT, e que efeitos se reproduzem após a divulgação do segredo, no sentido da extensão da tutela e as medidas que podem ser tomadas.

Para tal, construímos todo um caminho de análise, que podemos perspetivar pela seguinte estrutura:

O primeiro capítulo parte de um enquadramento jurídico do segredo comercial, desconstruindo a problemática da conceptualização do termo, tomando em consideração a proximidade com diferentes institutos, nomeadamente a concorrência desleal, a patente e o *know-how.* Em complemento pelo seu contexto histórico, desde a sua origem até à evolução como regime de proteção autónoma, passando por uma breve abordagem comparativa com o sistema jurídico norte-americano e exposição do ordenamento jurídico português, concretizando a análise interpretativa do

artigo 313.º do Código de Propriedade Intelectual e os requisitos necessários para a classificação do objeto – o segredo comercial.

No segundo capítulo, procuramos desmitificar o espaço digital, através do enquadramento do conceito de inteligência artificial e exposição evolutiva. Cabe também, enquadramento do ChatGPT, por abordagem das suas vantagens e desvantagens e ligação ao ambiente empresarial e laboral.

Com o terceiro capítulo, procurámos fazer um juízo dos desafios que existem pela relação dos segredos de negócio em conjugação com ambientes de inteligência artificial e uso do ChatGPT. Neste ponto é abordada a questão da relevância da divulgação para depreender a extinção, ou não, do regime jurídico de proteção do segredo comercial. Fazendo uso de diferentes perspetivas e tomando em consideração elementos como os círculos subjetivos relevantes e a teoria da preservação sequencial. Procura-se enquadrar os mesmos elementos na hipótese de transposição do segredo para o ChatGPT, pelo que se faz nova análise aos desafios ditados pela divulgação. É feito também um enquadramento do risco e formas de o mitigar em prol da preservação do segredo comercial.

No quarto, e último capítulo, damos destaque à tutela do segredo comercial, abordando as medidas razoáveis de diligência por parte do titular, a regulamentação da IA proposta pela Comissão Europeia, e terminamos com a proposta de uma hipótese prática que procura densificar o quadro legal português no sentido de perspetivar a aplicação da lei, a tutela conferida ao segredo comercial e o quadro de medidas preventivas e sancionatórias pela transposição de informação confidencial para o ChatGPT, o seu armazenamento, subsequente partilha com utilizador alheio e posterior uso deste para negócio próprio.

Neste sentido, a presente dissertação propõe investigar o impacto da divulgação do segredo comercial no meio digital de inteligência artificial emergente, em particular, pelo uso do ChatGPT, analisar os desafios inerentes à sua condição, determinando, pelos preceitos legais, se há lugar à proteção do segredo comercial e respetiva aplicação sancionatória.

(Tomamos nota, que para a elaboração deste estudo, o ChatGPT foi somente utilizado para confirmação de questões relacionadas com o seu funcionamento e auxílio semântico, pelo fornecimento de sinónimos)

CAPÍTULO 1

Segredos de Negócio

Cabe de ponto de partida deste estudo a apreensão da temática, observando o contexto evolutivo e determinação do enquadramento terminológico e jurídico daquilo que se entende vulgarmente como "a alma do negócio".

1.1 A Relevância dos Segredos de Negócio no Contexto Empresarial

O rápido desenvolvimento dos mercados gerou o consequente aumento da competitividade entre empresas que, cada vez mais, se procuram afirmar num mundo em constante mutação e crescentes necessidades. O *keep-up* ou a vontade de permanecer numa posição de vantagem afirmada leva a que aumentem os movimentos de criação e inovação. Não será de difícil entendimento que manter tais informações para si e para o negócio estabelece uma posição de vantagem competitiva e económica perante os demais participantes no mercado.

Os mercados atuais são cada vez mais exigentes e é incontornável a necessidade de novidade como um fator determinante para o sucesso de uma empresa ou indústria. Mas este aumento de competitividade aumenta também o risco de apropriação indevida ou maliciosa dos segredos de negócio alheios.

Por sua vez, a tutela destes segredos de negócio não pode deixar de seguir uma abordagem jurídica de grande importância e complexidade. A violação de um segredo de negócio pode comprometer a posição de uma empresa na perspetiva do mercado local ou mesmo no mercado global, gerando um prejuízo imenso para a entidade, comprometendo o futuro da mesma[1] ou constituir um risco para a sociedade, se for utilizada para práticas ilegais.

Ao longo dos anos tem vindo a crescer o interesse jurídico em segredos de negócio, devendo-se a variadíssimos fatores, dos mais relevantes: *(i)* a globalização de mercados e de pessoas, nomeadamente pelo aumento dos mercados a nível mundial, acompanhado pela crescente mobilidade de pessoas e aumento da concorrência transnacional; *(ii)* a não adequação do uso de proteção por direitos exclusivos, caso em que não se verificam preenchidos todos os requisitos para fazer valer esse direito; ou *(iii)* a preterição de mecanismos de proteção de direitos exclusivos, como a concessão de patentes, que pelas suas características não representam a tutela mais vantajosa e relevam uma menor adequação para a salvaguarda dos interesses em questão, pelo que, os titulares

[1] Deixando nota que o prejuízo monetário pode-se revelar maior nas empresas de maior dimensão, contudo, são as pequenas e médias empresas que encontram o futuro sucesso do seu negócio comprometido e por períodos de tempo mais prolongados.

acabam por optar pela via da proteção do segredo comercial; *(iv)* o aumento da rede de comunicação e arquivamento de dados que, com o consequente aumento da rede de transmissão, aumenta o risco de divulgação e consequente apropriação indesejada de informação sensível do ponto de vista negocial, e como destaque nesta exposição *(v)* o surgimento de sistemas artificiais que, nos dias de hoje, atuam como intervenientes acessórios ou complementares no mundo empresarial, adquirindo uma relevância semelhante ao ser humano no desenvolvimento das empresas.

A par das necessidades de proteção, a existência de uma rede de segurança proporciona uma sensação de confiança efetiva aos atores do mercado. A existência de tutela dos segredos comerciais influência a atuação dos titulares no mercado, passando a agir em função desse facto. Querendo isto traduzir-se no facto de que a proteção funciona como uma espécie de incentivo à procura e inovação, pelo desenvolvimento de novos modos de produção, novas estruturas, criação de mecanismos únicos que não são só para proveito da empresa em questão, como também de toda a sociedade.

Neste sentido, destaca-se a relevância dos segredos de negócio em setores de indústria farmacêutica, alimentar, biotecnológica, médica e até mesmo ambiental, que denotam claras vantagens no panorama comercial. Pense-se na quantidade de empresas farmacêuticas que mantêm para si fórmulas e métodos de produção de medicamentos. Destacando assim clara a importância e transversalidade dos segredos de negócio que não encontram limite nos setores económicos e empresariais que existem. Enquanto nós, pessoas e sociedade, observamos o surgimento de benefícios pela resposta a várias necessidades relacionadas com estes setores. Ao que por trabalharem num contexto em que lhes é permitido prosperar com possível permanência das descobertas em segredo, adquiriram o impulso para desenvolver novas criações.

1.2 Noção e o Problema da Conceptualização

Definir segredo de negócio não tem sido tarefa fácil, pelo que muita tinta já se fez correr ao longo do tempo e em várias jurisdições se procurou alcançar uma precisão terminológica que abarcasse todas as suas vertentes, ou pelo menos, as que compreendiam relevância jurídica.

Este fator de incerteza foi determinante para perceber a instabilidade estrutural e dificuldade de enquadramento de um instituto autónomo para a proteção dos segredos de negócio.

Tanto quanto, a sua evolução jurídica está intimamente ligada e quase de forma proporcional à perceção da palavra nos seus vários entendimentos e definições.

Vocábulos como segredo comercial, segredo industrial, *know-how,* informações secretas, informações sensíveis, informações reservadas, informações não patenteáveis, informações não

divulgadas, constituem conceitos indeterminados que comprometem a concretização inequívoca do conceito de segredo comercial.

A falta de uma conceptualização clara e concreta leva a que cada autoridade judiciária interprete e aplique o preceito de forma diferente em cada um dos seus países.

Houve uma constante procura pela clarificação e, em momento ulterior, a busca pela harmonização do conceito de segredos de negócio.

O *Trade Related Aspects of Intellectual Property Right* (doravante TRIPS) de 1994[2], refere no número 1 do artigo 39.º a terminologia de "*informações não divulgadas*" que tem por base a ideia de propriedade aplicada pela *common law*[3]. SOUSA E SILVA refere a preocupação que houve em adotar um termo neutro, pois de outro modo, *trade secrets* representaria muito o tradicionalismo norte-americano e a posição de constituir um tipo de propriedade[4]. No entanto, outras designações não seriam suficientemente amplas para comportar todas as vertentes que pretendemos mencionar ao falar de segredos de negócio.

Foi com o Código de Propriedade Intelectual (doravante CPI) de 2003, no seu artigo 318.º e o contributo do TRIPS que se acolheu o conceito mais abrangente de informações não divulgadas. Segundo COUTO GONÇALVES, "*Trata-se agora da proteção de "informações não divulgadas" ou, melhor dito, de "segredos comerciais" e já não apenas de "segredos de indústria ou comércio"*[5].

O legislador queria compreender a tutela a todas as informações que podiam corresponder aos elementos de segredo de negócio, não deixando de outro modo excluídas as informações que não fossem segredos de indústria e segredos comerciais. Passando a compreender informações relativas a: invenções, *know-how*, técnicas de *marketing*, protótipos, *softwares*, algoritmos, modelos e desenhos, técnicas de organização empresarial, fórmulas, ideias e outros conhecimentos[6].

Pois, o segredo comercial comporta tanto um sentido *strictu sensu*, como comporta o segredo industrial. O segredo comercial *strictu sensu* abrange todas as informações ou conhecimentos relativos ao setor comercial de uma empresa, enquanto os segredos industriais comportam uma

---

[2] Em português – Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio - ADPIC, de 15 de abril de 1994. Tratado internacional relevante para o nosso estudo e com especial destaque mais adiante, <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>

[3] Os países de *common law,* como é o caso dos Estados Unidos da América, associam os *"trade secrets"* à ideia de propriedade e de posse sobre um objeto. Neste caso, a posse seria do titular e o objeto seria o segredo. Pelo que limitar o termo a este sentido resulta na diminuição do seu âmbito de aplicação. Limitando-se a um tipo de proteção de direito exclusivo sobre informações e prevenção da concorrência desleal.

[4] SILVA, Nuno Sousa e, *Quando o segredo é a "alma do negócio" – definição de um conceito*, Revista da Associação Brasileira da Propriedade Intelectual, n.º 126, set/out 2013, p. 6.

[5] GONÇALVES, Luís Couto, *Manual de Direito Industrial, Propriedade industrial e Concorrência Desleal,* 7ª Edição, Revista e Atualizada, Almedina, Coimbra, 2017, *Op. cit* p. 403.

[6] De sentido semelhante ao que resulta do considerando 14 da Diretiva da União Europeia 2016/943, do Parlamento e Conselho Europeu, de 8 de junho de 2016, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0943> e Acórdão do TRL, P. 99/21.6YHLSB-A.L1-PICRS, 10.03.2022, <https://www.dgsi.pt/>

vertente de conhecimento mais técnica, informações patenteáveis ou não[7]. Deste modo, segredo comercial *lato sensu* comporta todas as informações que por serem valiosas são tomadas medidas para manter o seu secretismo.

Como ponto de clarificação desta análise, o conceito atual de segredo comercial tem o mesmo que segredo de negócio[8]. E deste modo, o termo segredo de negócio deve ser entendido como um termo *latu sensu.* Compreendendo duas espécies, o segredo comercial e o segredo industrial.

1.3 Da Qualificação Jurídica - A Conflitualidade de Institutos

A temática da qualificação jurídica dos segredos comerciais não segue um rumo linear, tanto quanto, há todo um caminho a percorrer até chegar ao instituto *sui generis*[9] que os segredos comerciais revelam ser.

A tutela do segredo de negócio é multidisciplinar, são vários os sistemas e normas de diferente índole que visam proteger as suas várias valências: normas de direito do trabalho, direito dos contratos, direitos de autor, direito da propriedade industrial, direito penal, entre outros[10].

A par disso, a sua proximidade a outros ramos de Direito como é a concorrência desleal e a propriedade industrial levanta dúvidas de tutela e será relevante clarificar as suas diferenças.

Por outro lado, numa busca de enquadrar informações protegidas por segredo, é-nos impossível a associação a direitos de personalidade. Note-se que não está em causa um bem da personalidade do autor, quando muito, trata-se de um problema para o património dele. Tratando-se de segredos de objeto de negócio, serão objetos sujeitos a negócios jurídicos.

Caso não existissem regimes de proteção para informações comerciais, como o regime dos direitos exclusivos ou dos segredos de negócio, iria verificar-se uma estagnação no investimento científico, levando ao consequente bloqueio do desenvolvimento de indústrias e de diversas áreas de conhecimento, pela simples instabilidade e dificuldade de retorno económico e financeiro que novos conhecimentos iriam proporcionar ao titular e ao seu negócio.

Contudo, se formos falar de factos estatísticos do contexto social e comercial, o uso de segredo comercial destaca-se como meio privilegiado em relação os outros institutos jurídicos para cautelar

---

[7] SILVA, Nuno Sousa e, *Proposta de Diretiva em matéria de Segredos de Negócio – Estado e Perspetivas,* Revista de Direito Intelectual, N.º2, 2014, p. 265.

[8] Pelo que, ao longo da dissertação, nos referimos a segredo de negócio com igual sentido de segredo comercial, considerando como sinónimos.

[9] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 418.

[10] SILVA, Nuno Sousa e, *Quando o segredo é a "alma do negócio" – definição de um conceito*, Revista da Associação Brasileira da Propriedade Intelectual, n.º 126, set/out 2013, p. 12-14.

as suas informações secretas de vantagem industrial e comercial. Evoluindo no sentido da autonomização da proteção dos segredos comerciais, ainda que encontre relação a outros sistemas jurídicos.

1.3.1 Concorrência Desleal

Tal como veremos em diante na nossa abordagem à evolução histórica da proteção dos segredos de negócio, o primeiro instituto que surgiu foi a concorrência desleal, pelo que a sua densidade legislativa e doutrinal estendeu a alçada à proteção dos segredos de negócio, de forma a crer constante dependência dos segredos ao regime da concorrência desleal.

A concorrência desleal, ganhou tutela efetiva em 1883, na Convenção da União de Paris (doravante CUP), que surgiu em prol da harmonização internacional de normas de propriedade industrial. Como tal, surgem o reconhecimento de bens jurídicos de natureza imaterial.

No ordenamento português, houve uma inerência obrigatória entre os dois institutos até a entrada em vigor do CPI de 2003. Desde então e até o momento, houve a separação do regime da propriedade industrial do regime da concorrência desleal, que comportava os segredos de negócio, e separação do regime da concorrência desleal do instituto da proteção do segredo comercial, admitindo a sua autonomia mas também a sua consideração como tipo de concorrência desleal.

MOURA VICENTE defende que a absorção da tutela do segredo comercial por parte do regime da concorrência desleal leva a uma limitação subjetiva do seu âmbito de aplicação[11]. O instituto jurídico da concorrência desleal tem por base a relação subjetiva de concorrência entre empresas do mesmo setor de atividade.[12] Este pressuposto, por sua vez, limita o âmbito de aplicação da tutela de segredos comerciais, visto que esta relação pode coexistir no âmbito dos segredos comerciais, mas pode também não existir, deste modo, não será um pressuposto essencial desta tutela, libertando-a deste entendimento.

Pelo artigo 311.º do atual CPI (2018) entende-se que estamos perante concorrência desleal por qualquer ato de concorrência contrário às normas e usos honestos no contexto da prática económica. A concorrência desleal pressupõe a prática de condutas enganosas que gere prejuízo aos concorrentes. Que por sua vez, estes atos podem abranger a violação de segredos de negócio, mas não se considerando a correspondência absoluta.

---

[11] VICENTE, Dário Moura, *Código da Propriedade Industrial Anotado,* Almedina, 2021, Anotação do artigo 313.º p. 1186.

[12] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 420.

Em ambos os casos, está associada a ponderação de interesses opostos, pelo que, atualmente, o CPI comporta ambos os institutos, artigo 311.º e artigo 313.º, respetivamente. Verificando-se que o instituto da concorrência desleal opera de forma autónoma em relação ao instituto da proteção do segredo comercial. Contudo a qualificação da proteção conferida em razão de concorrência desleal reporta ao juízo valorativo dos comportamentos contrários às normas e usos honestos, enquanto a proteção conferida ao segredo comercial advém da sua violação pela apropriação, utilização e divulgação do segredo, pelo que não está prevista a sua tutela absoluta, abrindo lugar à possível licitude de aquisição, nos termos do artigo 315.º. Nesta senda, é apresentada a ideia de promoção de concorrência saudável de mercado, deixando em aberto a possibilidade de descoberta de segredos de negócio tutelados independente de qualquer violação, por mero acaso ou situação de engenharia inversa *(reverse engineering)* de um produto legalmente adquirido. Pelo facto de não estar em causa um direito exclusivo, (como vamos compreender de seguida), o desenvolvimento das mesmas informações por parte de outra pessoa é válida e esta poderá usá-las livremente.

Para maior clarificação deste ponto, e exemplo da complementaridade dos institutos, há que fazer a advertência que a aquisição por ato lícito pode ser classificada como ato de aproveitamento parasitário, no sentido de lesar os titulares pela cópia ou imitação que explora gratuitamente a reputação da empresa e inerentes investimentos para a inovação, pelo que deste modo, cabe aplicação do instituto da concorrência desleal, por aplicação da alínea c), número 1.º, do artigo 311.º do CPI e considerando 17 da Diretiva Europeia 2016/943. De ressalvar também que a aquisição lícita, nem sempre dita a divulgação ou utilização lícita. Pode ocorrer que estes atos sejam realizados por práticas comerciais desonestas, e.g. em razão de fusão de empresas e celebração de contratos de franquia, que na sua maioria se considera lícito, mas pode representar uma motivação económica que lese o titular do segredo comercial e que encontra sentido na cláusula geral da concorrência desleal[13].

Deste modo, a concorrência desleal passa a operar como um expediente legal passível de aplicação na proteção do segredo de negócio, sem que entre eles haja uma relação de dependência, mas quando possível, um complemento e reforço da sua proteção.

1.3.2 Direito Exclusivo de Propriedade Industrial – O Caso da Patente

À semelhança de outros bens incorpóreos, natureza da informação secreta caracteriza-se por não ter figura física, pelo que a sua existência permanece de forma abstrata na mente da pessoa[14]. De tal

[13] ASCENSÃO, José Oliveira de, *Concorrência Desleal*, Coimbra, Almedina, 2002, p. 476.

[14] Por abordagem da sua classificação jurídica ou natureza jurídica, pois efetivamente, o segredo pode ser comportado num documento físico.

modo, por correspondência ao artigo 1302.º do Código Civil (doravante CC), também não pode ser considerado um direito de propriedade que prevê aplicação a bens materiais.

De outro ponto de vista, as informações secretas nunca poderiam seguir o regime jurídico do direito de propriedade pela sua insuscetibilidade de posse. No caso do segredo comercial, pode haver um titular da informação ou múltiplos, podendo ser divulgada ao mesmo tempo, em lugares diferentes e por várias pessoas, sem que isso diminua a sua disponibilidade ou utilidade[15].

A análise de OHLY a vários modelos de proteção dos segredos comerciais levou-o a constatar e definir que os segredos comerciais são considerados a "*Cinderela*" ou o "*Órfão*" do direito da propriedade intelectual[16] quando em comparação com os seus ramos. Segundo o autor, a matéria não fomentou interesse científico e jurídico por parte da Europa, que para além do artigo 39.º do *TRIPS* não se preocupou em procurar harmonizar o conceito/instituto no contexto jurídico europeu[17].

Já com o avançar do tempo, em 2016, passou a constar do número 16 do preâmbulo da Diretiva Europeia 2016/943[18], que os segredos comerciais não são equiparáveis a direitos exclusivos. Os direitos exclusivos pressupõem um prazo de proteção e facilidade de transação, sem que o seu valor seja posto em causa, conferindo aos seus titulares um forte proteção contra quem tentar explorar a informação exclusiva.

Neste sentido a patente confere o direito exclusivo de excluir terceiros do fabrico, utilização, venda ou importação de um determinado produto em troca da divulgação pública total da invenção[19].

Ambos os institutos colocam o titular em vantagem no mercado que operam. Contudo, apresentam muitas diferenças que ditam um regime jurídico muito distante.

Primeiramente, o âmbito da concessão da patente circunscreve apenas a invenções. Enquanto que o regime dos segredos comerciais aumenta muito mais o âmbito do objeto, pela proteção de qualquer informação comercial que seja mantida secreta e que represente uma vantagem competitiva.

---

[15] VICENTE, Dário Moura, *A informação como objeto de direitos*, Sociedade da Informação, Revista de Direito Intelectual, n.º1, 2014, p. 119.

[16] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 422.

[17] *Idem,* p. 423.

[18] Tratado internacional relevante para o nosso estudo e com destaque mais adiante. Diretiva da União Europeia 2016/943, do Parlamento e Conselho Europeu, de 8 de junho de 2016, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0943>

[19] Aequitas Victoria Foudation, *Patent vs Trade Secret: Detailed study on Coca-cola brand*, <https://www.aequivic.in/post/patent-vs-trade-secret-detailed-study-on-coca-cola-brand>

A patente representa uma concessão exclusiva dada ao autor por meio de descrição específica, enquanto o segredo de negócio, por vezes, não tem descrição concreta, nem é exigível que tenha para que seja considerado segredo.

Outro ponto de relevante diferença, é que os direitos de propriedade industrial são difundidos aos interessados, pelo que a divulgação resulta do requisito da descrição. Logo, a concessão do direito exclusivo exige a divulgação do segredo na própria descrição da patente, dando o acesso ao domínio público. Pelo contrário, para operar o instituto do segredo comercial não é necessária qualquer divulgação, exigindo-se o requisito da confidencialidade da informação.

A proteção obtida pelos direitos de propriedade industrial é norteada por uma limitação temporal, estabelecendo um prazo máximo de 20 anos a contar desde o seu registo. Findo o prazo estabelecido na concessão de proteção legal, cessa a exclusividade da exploração económica. Pelo contrário, a tutela do segredo comercial não tem limitações temporais, funcionando *ad eternum* enquanto for da intenção do titular, manter a informação secreta.

Geograficamente, também é de realçar que a patente é somente válida no país em que tenha feito pedido e concedida a patente, pelo que, para esta valer fora do território nacional, deve ser feito pedido de concessão internacional, pedido europeu, ou pedido no país específico que releve interesse ao criador. Comportando logicamente mais custos e burocracia. Por sua vez, o segredo comercial não encontra limite nas fronteiras, pelo que a sua proteção, em princípio, vale de forma absoluta na maioria dos países.

A patente também pode representar um limite no que concerne à adaptação da invenção. Caso seja feita alguma alteração à invenção patenteada, o mais provável, é que seja exigido novo registo, a menos que seja uma alteração mínima que não comprometa a descrição anexa ao pedido inicial. Por sua vez, o segredo comercial pode ser alterado sem que seja necessário confirmar ou voltar a legalizar a sua proteção.

Para mais, a natureza sigilosa dos segredos de negócio é conflituante com a hipótese de transação da mesma. O direito de patente pode ser objeto de contratos de cessão que ditam a transferência do direito exclusivo sobre aquela informação patenteada a outrem - pessoa singular ou coletiva. Ao fim, trata-se da venda da vantagem competitiva patenteada. No que concerne à natureza dos segredos de negócio, tal transferência não seria tão simples, questionando se era preservada a sua natureza secreta.

Para o segredo comercial ter proteção jurídica não necessita de nenhum processo ou procedimento legal, pelo que deste modo, entram em vigor imediatamente. Por sua vez, é exigido aos interessados pela aquisição da patente, o cumprimento de trâmites legais e burocráticos tendencialmente demorados, com custos monetários de obtenção e manutenção associados. No entanto, concedida, o seu titular pode defender a criação de qualquer violação ou exploração.

Resta-nos a comparação do risco de perda. No caso da patente, o prazo dita o momento em que a informação pode ser livremente utilizada, ditando a cessação da sua proteção. Já o segredo comercial só perde a proteção quando este é apropriado, utilizado ou divulgado fora do círculo normal do seu conhecimento.

De todo o modo, observa-se que o instituto de segredo comercial é alternativo ao regime dos direitos exclusivos, dadas as suas desvantagens: âmbito do objeto, necessidade de dispor da informação, limitação temporal e geográfica, constrangimento na flexibilidade de adaptação, custos de obtenção e manutenção e morosidade da concessão, pelo que as empresas acabam por ponderar e escolher manter a proteção jurídica conferida pelos segredos de negócio. No entanto, se a informação for de fácil apreensão e compreensão, o registo de patente é o regime que proporciona a melhor tutela.

Segundo AZEVEDO DE AMORIM, "*o regime jurídico dos segredos comerciais pode constituir uma alternativa ou um complemento dos direitos de propriedade industrial (…) quando se encontrem preenchidos os respetivos pressupostos*"[20]. Ou seja, nada proíbe os regimes de coexistir, pensemos no período anterior ao pedido de reconhecimento de direito exclusivo ou mesmo entre o pedido e a sua aprovação, durante este tempo já existe informação secreta que pode ser passível de tutela de segredo comercial, caso contrário, poderia estar em causa o seu valor e razão de ser da elegibilidade de reconhecimento de direito exclusivo. Podem ambos ser usados para salvaguardar a mesma informação secreta em diferentes etapas.

Também por não ser exigível que o segredo comercial seja absoluto, pode ocorrer o caso de ambos os institutos operarem de forma combinada. Imagine-se um pedido de patente para uma tecnologia inovadora, mas com reserva confidencial no que toca ao *know-how* prático[21]. Portanto, considera-se que o segredo de negócio pode servir de meio de proteção complementar de direito exclusivo – é feita a descrição e divulgação da invenção, mas o modo de utilização é mantido em segredo.

1.3.2.1 Caso da Receita Coca-Cola

Exemplo histórico será o da Coca-Cola. Há poucas empresas do ramo alimentar com o impacto e sucesso desta empresa e marca, em que o próprio nome do produto tornou-se sinónimo da marca que o criou, sendo provavelmente o refrigerante mais conhecido no mundo. O segredo da sua

[20] AMORIM, Ana Clara Azevedo de, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* Revista Eletrónica de Direito, Faculdade de Direito da Universidade do Porto, n.º2, vol. 19, junho de 2019, *Op. cit* p. 22.

[21] SILVA, Nuno Sousa e, *Um retrato do regime português dos segredos de negócio*, Seminário – A Proteção Legal de Segredos de Negócio, Universidade Católica Portuguesa, Porto, 2014, p. 249.

receita é submetido à forma escrita, fechado a "sete chaves" num cofre e de conhecimento de apenas duas pessoas (rezando a lenda que ambas não se podem locomover no mesmo transporte, de modo a evitar riscos de perda derivados de possíveis acidentes), a complementar também a estrita proibição da sua inserção no mundo digital[22].

O caso da empresa Coca-Cola costuma ser relevante para abordar as diferenças entre segredo comercial e patente, no sentido de se justificar pelo meio de tutela dos segredos de negócio e não pela concessão de patente.

A empresa tomou em consideração as várias características que norteiam ambos os regimes de modo a fazer um juízo de adequação com as suas necessidades e interesses empresariais.

Pelo que, patentear a sua receita não se enquadrava com a estratégia e trajetória do negócio. De destacar para o caso, em primeiro lugar, a limitação temporal que determina um prazo de utilidade, pelo que, findo o prazo, a vantagem competitiva que a empresa mantém sobre a concorrência deixa de existir. Por outro lado, a concessão de patente depende de uma descrição específica, neste caso seria necessária a transcrição pormenorizada da receita, e mais relevante ainda, a possibilidade de conhecimento público da receita, que pode, ou não, ser de fácil recriação, e que vai no sentido contrário do sucesso a longo prazo que a Coca-Cola procura obter.

Por sua vez, a proteção por via do segredo comercial é norteada pela manutenção do segredo, ou seja, manter a confidencialidade da receita de modo que não se verifique a sua divulgação ao público. Além disso, pode-se mencionar que o secretismo em torno da receita da Coca-Cola a tornou atrativa para os consumidores que procuram esta bebida pela sua singularidade, dando origem a uma forma de *marketing* que sustenta o estatuto que a empresa detém no mercado mundial.

1.3.3 *Know-how*

O *know-how* consiste no conjunto *"de conocimientos técnicos que no son de dominio público y que son necesarios para la fabricación o comercialización de un producto, para la prestación de un servicio o para la organización de una unidad o dependencia empresarial, por lo que procuran a quien los domina una ventaja sobre los competidores que se esfuerza en conservar evitando su divulgación"*[23].

Por serem figuras com conceitos muito aproximados gere alguma confusão. Característica obrigatória do segredo comercial é o sigilo e o seu valor do seu secretismo, já o *know-how* não tem

[22] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 419.

[23] Resolução BOE 21.01.20, de 4 de dezembro de 2019, Espanha, *Op. cit,* <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-873>

necessariamente que ser secreto para existir. A divulgação do *know-how* pode não impactar o seu valor subjetivo, este pode ser secreto ou não, pelo que não se exige a obrigatoriedade do sigilo.

Como também podemos ter um *know-how* que também é segredo de negócio, mas quando temos um segredo de negócio não temos necessariamente um *know-how*. Pense-se na situação em que o *know-how* é o conhecimento que alguém detém de manusear uma máquina muito específica e crucial para o funcionamento de uma empresa, neste sentido, essa pessoa demonstra ser fundamental para o negócio, mas o seu conhecimento não é confidencial, simplesmente mais ninguém ou pouca gente tem conhecimento para o cumprimento da função, sendo possível reverter essa situação por meio de aprendizagem. Já um *know-how* que constitui igualmente um segredo comercial, é quando uma pessoa ou um grupo restrito produz um produto em que alguma componente do processo representa um segredo comercial, seja o ingrediente de uma receita ou uma etapa elaboração do produto, o conhecimento de o fazer é limitado e protegido para se manter restrito e preservar o sigilo comercial.

1.4 A Origem

Não se sabe precisar o momento em que o segredo se tornou um fator psicológico e sociológico do ser humano, contudo não podemos negar a sua naturalidade e inerência quase inata ao indivíduo. De certa forma, não será igualmente surpreendente pensar que os segredos de negócio encontram origem em muitos séculos passados.

O desenvolvimento de mercados e de negócios triviais, como a comercialização de bens, levaram à necessidade de omitir a mais variada condição ou fator que colocava um negociante em posição superior à do outro. Por seu turno, os comerciantes desenvolviam os seus métodos primitivos de preservação de segredos comerciais, nomeadamente a não transcrição dos mesmos para a forma escrita, remetendo-se à transmissão, quando assim o entendiam, por via oral[24]. Assim a tutela do segredo de negócio surgiu como forma de controlo à possível apropriação de valores intangíveis, nas primeiras sociedades[25].

Um dos primeiros indícios concretos da proteção dos segredos comerciais remota ao antigo Egipto, no ano 2000 a.C., quando o monarca faraó Mentuhotep inscreve numa tábua a restrição ao

[24] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 414.

[25] SILVA, Nuno Sousa e, *Um retrato do regime português dos segredos de negócio*, Seminário – A Proteção Legal de Segredos de Negócio", Universidade Católica Portuguesa, Porto, 2014, p. 224.

acesso a segredos comerciais e industriais dos quais era titular, excecionando o acesso ao seu filho primogénito[26].

Também na Antiga Roma parece surgir um instituto de proteção a segredo comercial: a *actio servi corrupti*[27]*,* determinando que quem tivesse dado abrigo a escravo de outrem, com a intenção de comprometer o escravo de forma a desvalorizá-lo, seria condenado ao pagamento em dobro da consequente perda de valor. Contudo, surgem algumas discussões sobre a legitimidade do instituto como meio de proteção ao segredo comercial. Schiller assume uma interpretação *lato sensu* que leva à contemplação da tutela realçando situações mais semelhantes com concorrência desleal como seria caso da utilização de marcas, firmas ou utilizar escravos de outrem para a obtenção de segredos, observando deste modo a clara violação de segredos comerciais. De posição contrária e de certo modo negacionista, Watson considera que o instituto tinha por base o valor do escravo e não uma violação de segredos comerciais, a compensação era devida pela desvalorização por efeito de má conduta do impulsionador da ação[28].

Por mais interessantes que sejam estes dois exemplos, o verdadeiro desenvolvimento e impacto deveu-se ao rápido desenvolvimento da atividade industrial e comercial das Revoluções Industriais, que levou ao destaque da importância do segredo comercial para a indústria e, por conseguinte, à necessidade de proteção das mais-valias. Foi após a Revolução Francesa, que se estabeleceu o conceito de segredos de fábrica, pela redação do artigo 418.º do Código Penal francês de 1810[29], punindo gerentes e empregados que comunicassem segredos de fábrica a franceses ou a estrangeiros, prevendo-se sanção por multa e pena de prisão.

De forma semelhante a França, Portugal movimenta-se no mesmo sentido, ao prever a criminalização da revelação de segredos de fábrica por parte do corpo constituinte da fábrica como um crime contra a propriedade (artigo 462.º do Código Penal de 1852[30] e no Código Penal de 1886)[31].

1.5 A Evolução Histórica da Tutela dos Segredos de Negócio

Em 1883, a Convenção da União de Paris para a Proteção da Propriedade Industrial (CUP) procurou assegurar a primeira tutela internacional efetiva de propriedade intelectual. Estabelecendo um

[26] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 414 e 415.

[27] *Idem,* p. 415.

[28] *Idem*, p. 416.

[29] Código Penal Francês de 1810, <http://cdigital.dgb.uanl.mx/la/1190000683/1190000683_MA.PDF>

[30] Decreto de 10 de Dezembro de 1852 - Código Penal Português, <https://www.fd.unl.pt/anexos/investigacao/1829.pdf>

[31] Decreto de 16 de Setembro de 1886 - Código Penal Português, <https://www.fd.unl.pt/anexos/investigacao/1274.pdf>

regime jurídico para as patentes, como também a obrigação de criação de uma proteção contra a concorrência desleal em cada país participante. Ditando, no documento internacional, os termos gerais que definiam uma proteção mínima a ser observada pelos regimes de proteção nacional. Passando por mencionar "*matéria industrial ou comercial*"[32] como parte do âmbito da concorrência desleal.

1.5.1 TRIPS - Trade Related Aspects of Intellectual Property Right

No mesmo seguimento surgiu em 1994 o acordo internacional *Trade Related Aspects of Intellectual Property Right* - TRIPS[33]. Um importante tratado internacional de conjugação de leis de propriedade intelectual.

Tem como grande finalidade a liberalização do comércio para que a inexistência de tutela de segredos comerciais não fosse fator de bloqueio do fluxo dos produtos comercializados. O TRIPS passou a constituir parâmetro mínimo de proteção exigível fora dos países nos quais o negócio tinha origem, proporcionando confiança na circulação de bens e estabelecendo o dever de atuação de concorrência leal entre os signatários. Beneficiando da mesma proteção no mercado interno, como no mercado externo.

Vem exigir que os países membros protejam os segredos comerciais enquanto propriedade industrial conforme o artigo 39.º, que passamos a citar:

"1 – Ao assegurar uma proteção 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 conformidade 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 sua 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

[32] Decreto n.º 22/75, de 14 de Julho de 1967 - Acto de Estocolmo da Convenção de Paris para a Protecção da Propriedade Industrial, Artigo 10.º *bis.*, <https://dcjri.ministeriopublico.pt//sites/default/files/documentos/instrumentos/dec22-1975.pdf>

[33] Em português, Acordo sobre os Direitos de Propriedade Intelectual relacionados com o Comércio – ADPIC, de 15 de abril de 1994, <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>

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 secretas."*

Compreende uma tutela jurídica à violação de "*informações não divulgadas"* através da aquisição, utilização e divulgação de informações. Estabelecendo os elementos obrigatórios e cumulativos para que a informação seja passível de proteção. Logo à partida, delimita que pela remissão ao 10.º *bis* da CUP, estas informações têm de revestir matéria industrial ou comercial, determinando que este será o bem jurídico em causa.

Por atuar no âmbito da Organização Mundial de Comércio (OMC)[34], o TRIPS é revestido de um *enforcement* eficaz ao comportar sanções económicas verificada a violação das informações.

Tem a finalidade de proteger certo tipo de "*informações não divulgadas*" prevendo que a proteção era devida se: *(i)* as informações forem secretas, *(ii)* possuírem valor comercial dado o facto de serem secretas, e *(iii)* serem objeto de diligências consideráveis por parte do titular das informações para as informações permaneçam secretas.

De acordo com o número 2 do artigo 39.º ficam regulados 3 tipos de atos que presumem a violação do segredo comercial: *(i)* a aquisição[35], *(ii) a* utilização e a *(iii)* divulgação do segredo, de forma desleal. Pelo que segundo SOUSA E SILVA é necessária uma ação contrária às práticas comerciais honestas para que se verifique uma concorrência desleal[36].

Abrindo caminho para vários tipos de conduta: *(1)* a aquisição lícita com utilização e/ou divulgação ilícita; *(2)* a apropriação[37] com utilização – definido como ato de aproveitamento, e *(3)* apropriação seguida de divulgação – admitida como ato de agressão[38].

Em suma, a tutela legal é válida à partida (ou seja, pelo preenchimento dos elementos das alíneas do número 2 do artigo) se o segredo de negócio tenha sido utilizado e/ou divulgado de forma ilícita[39].

---

[34] Em inglês - *World Trade Organization* – WTC. Organização criada em 1995, com o objetivo de supervisionar e liberalizar o comércio internacional.

[35] Entende-se igualmente por apropriação quando exclusivamente obtida de modo ilícito.

[36] SILVA, Nuno Sousa e, *Quando o segredo é a "alma do negócio" – definição de um conceito*, Revista da Associação Brasileira da Propriedade Intelectual, n.º 126, set/out 2013, p. 8.

[37] Sendo que nos termos deste parágrafo, a aquisição comporta uma ideia de licitude e a apropriação comporta uma ideia de ilicitude.

[38] Ordem dos Advogados, *Concorrência desleal e direito do consumidor*, por Paúl, Jorge Patrício, <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados/ano-2005/ano-65-vol-i-jun-2005/doutrina/jorge-patricio-paul-concorrencia-desleal-e-direito-do-consumidor-star/>

[39] Podia-se sustentar a hipótese de aquisição lícita sem ser seguida de utilização ou divulgação, contudo, parece esvaziar o regime. Se alguém tiver acesso não intencional a uma informação secreta não está diretamente a violar o segredo comercial, mas, pode ser relevante a discussão sobre as diligências necessárias do titular para manter a informação secreta, que por esta hipótese, sem análise de caso específico, leva a crer que estaria fora do âmbito do instituto deixando de ser passível à tutela do segredo comercial.

1.5.2 Diretiva Europeia 2016/943, de 8 de Junho de 2016

A crescente consciencialização e necessidade de afirmação de uma integração política e económica da Europa para harmonizar a proteção dos segredos comerciais resultou na aprovação da Diretiva da União Europeia 2016/943 de 8 de junho de 2016[40] (doravante Diretiva/Diretiva Europeia), mais especificamente para a proteção de *know-how* e de informações comerciais confidenciais contra a sua aquisição, utilização e divulgação ilegais, deixando de se reconduzir exclusivamente ao instituto da concorrência desleal.

A Diretiva surge num momento em que as práticas desonestas em contexto comercial são recorrentes. O fator novidade surge com a inserção de novas formas de atuação ilícita e apropriação indevida de segredos comerciais. A urgência da harmonização deve grande destaque ao processo de globalização e desenvolvimento tecnológico e digital que aumenta o risco destas práticas. A União Europeia decidiu tomar um passo em frente e criar meios jurídicos eficazes, uniformizando a proteção de segredos comerciais no contexto europeu. Conferindo um *standard* mínimo de proteção comum a todos os Estados-Membros, podendo estes transpor para os seus ordenamentos jurídicos com maior proteção jurídica.

Destacando que *"(…) os segredos comerciais permitem aos criadores e inovadores retirar lucros das suas criações ou inovações, pelo que são especialmente importantes para a competitividade das empresas, para a investigação e o desenvolvimento e para o desempenho relacionado com a inovação"*[41].

Deste modo, as informações nutridas de segredo comercial passaram a ser aquelas que atendiam os seguintes requisitos cumulativos: *(i)* serem secretas, *(ii)* terem valor comercial pelo facto de serem secretas, e *(iii)* terem sido objetivo de diligências razoáveis, tendo em conta as circunstâncias, para permanecerem secretas pela pessoa que exerce legalmente o seu controlo[42]. Notando-se que estes elementos já constavam do artigo 39.º do TRIPS.

1.5.3 Do Direito Comparado – A Evolução do Regime Jurídico Norte-americano

Nesta análise, que não podia deixar de ser comparativa, é necessária a análise da evolução do sistema legal norte-americano, sistema este bastante relevante pela constatação de que é pano de

[40] Diretiva Europeia 2016/943 do Parlamento Europeu e Conselho, de 8 de junho de 2016 – Relativa à proteção de *know-how* e de informações comerciais confidenciais contra a sua aquisição, utilização e divulgação ilegais, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0943>

[41] *Idem*, Considerando 2, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0943>

[42] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 425.

inspiração para a Diretiva Europeia de 2016, mais precisamente no artigo 2.º da mesma, e para o CPI de 2018, no seu artigo 313.º[43].

A evolução da proteção dos segredos comerciais no território norte-americano partiu de base em princípios jurídicos, faseado em diferentes momentos e mudança de preceitos.

Num primeiro momento, por volta de 1920, os segredos comerciais eram interpretados como uma espécie de propriedade - *The Dominance of the Property Theory*[44]. De seguida, e até 1940, começou-se a afastar a teoria da propriedade no sentido de uma aproximação jurisprudencial da proteção dos segredos comerciais como ato de concorrência desleal -*Rise of Unfair Competition Theory*[45].

Já durante o ano 1979 é aprovado o *Uniform Trade Secrets Act* (doravante UTSA)[46], após a perceção de necessidade de autonomização da proteção dos segredos comerciais. Sendo um país organizado por estados, não é rara a situação de inconsistência entre os diferentes regimes jurídicos estaduais, pelo que à semelhança da situação de instabilidade que veio mais tarde configurar na União Europeia, foi necessário estabelecer uma uniformização na tutela de segredos comerciais. O UTSA, pela sua natureza não vinculativa, tinha a intenção de contribuir como modelo de exemplo normativo para cada estado adotar e desenvolver no seu perímetro jurídico.

Importante contributo do UTSA, é a discussão conceptual do segredo de negócio, por passar a definir *trade secret* como a "*informação, fórmula, padrões, compilações, programas, aparelhos/instrumentos, métodos, técnicas e processos"* de que resulta algum valor comercial, atual ou potencial, por não ser de conhecimento geral e por não ser de fácil acesso a pessoas que possam obter ganhos económicos com a sua utilização ou divulgação. Por herança da *Theory Property* de 1920, a ideia de posse leva ao entendimento de uma necessidade de proteção por parte do seu "proprietário", transpondo para os segredos comerciais a necessidade manter as informações secretas por meio de reforços razoáveis[47].

Contudo, o conceito de segredo comercial não se fixou com este Ato, surgindo em 2016 o *Defend Trade Secrets Act* (doravante DTSA)[48]. A atualização do conceito de segredo comercial

---

[43] Decreto-Lei n.º 110/2018, de 10 de dezembro de 2018 - Código de Propriedade Industrial, <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2018-117279941>

[44] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 427.

[45] *Idem,* p. 428.

[46] *The Uniform Trade Secrets Act* - UTSA, publicado por *Uniform Law Commission* (ULC), 1979, <https://www.wilmerhale.com/-/media/files/wilmerhale_shared_content/files/pdfs/trade_secrets.pdf>

[47] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 429.

[48] Em português, Lei de Defesa dos Segredos Comerciais, de 11 de maio de 2016, *Public Law* N.º 114-153, *United States of America*, <*https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf*>

resultou no entendimento que este abrangia todas as formas de informação financeira, comercial, científica, técnica e económica ficando incluindo "*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*"[49]. Já os elementos normativos que revestiam a proteção dos segredos comerciais no UTSA, foram adotados para a redação do artigo 39.º do TRIPS, e por sua vez, foram herdados e consagrados assim pelo DTSA, mas este já a nível federal. Concluindo-se pela autonomização da proteção do segredo comercial da ideia de propriedade e concorrência desleal.

1.5.4 No Ordenamento Jurídico Português

A par de outras ordenações, historicamente, a tutela de segredos comerciais surge intrinsecamente ligada ao regime da concorrência desleal. A par da tutela penal conferida pelo Código Penal de 1896, a Carta de Lei de 12 de maio desse mesmo ano, qualificava como ato de concorrência desleal as situações "*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*"[50]. Retirando deste preceito que a proteção do segredo fica delimitada pela componente subjetiva – ser agente industrial e pela componente objetiva – tratar-se de segredos de fábrica. Demonstrado ser insuficiente por uma clara limitação à panóplia possível de violação de segredos de negócio que se observa hoje em dia.

Em 1940, o número 9 do artigo 212.º do CPI manteve esta relação do segredo comercial como ato de concorrência desleal, considerando como ilícita a "*apropriação, utilização ou divulgação dos segredos da indústria de outrem se ao agente não couber maior responsabilidade pela aplicação do artigo 462.º do Código Penal*"[51].

Em 1995 não houve alteração no entendimento como violação associada à concorrência desleal. Este CPI passou a prever na alínea i) do artigo 260.º 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*

---

[49] Traduzido de inglês para português. DTSA 18 U.S. Code § 1839 <https://www.law.cornell.edu/uscode/text/18/1839#3>

[50] Artigo 201.º da Carta de Lei de 21 de maio de 1896, por meio de GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 431.

[51] Decreto-Lei n.º 30679, de 24 de agosto de 1940 - Código da Propriedade Industrial, <https://files.diariodarepublica.pt/1s/1940/08/19700/09060932.pdf>

(…) a ilícita apropriação, utilização ou divulgação dos segredos da indústria ou comércio de outrem"[52], prevendo pena de prisão de até 3 anos e pena de multa até 360 dias.

Já em 2003, concretizou-se o TRIPS no ordenamento jurídico português[53]. Foi usado como modelo de exemplo para a nova redação do CPI[54] que formalizou a autonomia da proteção do segredo comercial e a sua consideração como "informações não divulgadas" (pelo prefácio do artigo 318.º) como tipo de proibição normativa, ainda que em prol do regime jurídico da concorrência desleal pela remissão normativa dos artigos 317.º e 318.º, do CPI de 2003. O artigo 318.º é uma transposição do número 1 e 2 do artigo 39.º do acordo TRIPS, sendo que manteve a relação subjetiva concorrencial no sentido de que quem age é tido como um "*concorrente*".

MENEZES LEITÃO defende esta interligação entre segredo comercial e concorrência desleal como uma dependência natural, no sentido que a violação do segredo de negócio consistia na apropriação de vantagem alheia, de forma a prejudicar o seu concorrente[55]. Parece-nos mais sensata a posição de REMÉDIO MARQUES, que para se verificar a violação de um segredo comercial é dispensável a conexão com a ideia de ato de concorrência. A pessoa que se apropria da informação de segredo comercial não precisa necessariamente de ser concorrente do titular do segredo. A exemplo, um trabalhador pode partilhar informações protegidas no meio digital por mero ato de vingança ou ter objetivo de prejudicar a entidade empregadora, não deixando de ser merecedor de tutela jurídica, não com o fundamento na concorrência desonesta, mas sim na vantagem que o segredo representava para a empresa[56].

Parece-nos importante a referência à terminologia "*segredos de negócio*" no número 1 do artigo 318.º do CPI de 2003, passando a comportar de forma abrangente qualquer tipo de informação confidencial de natureza empresarial, passível de compreender os restantes requisitos, para se revestir de proteção legal. Esta alteração também foi ponto de retorno no sentido que, até então, o Código Penal comportava as consequências para a violação de segredos comerciais. Em 2003 observa-se um desagravamento das medidas punitivas, deixando de comportar ilícito penal, bastando-se por mero ilícito de ordenação social. Neste momento Portugal enquadra-se numa

---

[52] Decreto-Lei n.º 16/95, de 24 de janeiro de 1995 – Código da Propriedade Industrial, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/16-139270>

[53] De notar que a adesão de Portugal ao Tratado TRIPS só se concretizou em 1996. Um ano após da entrada em vigor do CPI de 1995.

[54] Decreto-Lei n.º 36/2003, de 05 de março de 2003v- Código da Propriedade Industrial, <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?ficha=301&artigo_id=&nid=438&pagina=4&tabela=leis&nversao=&so_miolo=>

[55] LEITÃO, Luís Menezes, *Concorrência desleal e tutela do interesse público na liberdade de concorrência*, Estudos jurídicos e económicos em homenagem ao Professor Doutor António de Sousa Franco, Vol. 2, Coimbra Editora, 2006, p. 887.

[56] MARQUES, João Paulo Remédio, *Biotecnologia(s) e Propriedade Intelectual*, Vol. II, Almedina, Coimbra, 2007, p. 473.

relação de verdadeira semelhança com a proteção de segredos comerciais observada no panorama internacional.

Coube importância à Diretiva Europeia 2016/943, acordo de harmonização à proteção dos segredos comerciais no contexto europeu, a qual Portugal transpôs para o seu ordenamento jurídico através da publicação do Decreto-Lei n.º 110/2018, de 10 de Dezembro que introduz a entrada em vigor de um novo CPI. Por fim, com o CPI de 2018[57], observou-se a concreta autonomia da tutela dos segredos comerciais em relação à concorrência desleal, abandonando a ideia de necessária relação subjetiva de concorrência, estendendo-se o regime também a terceiros que não estejam em relação de concorrência. MOURA VICENTE comenta a importância desta alteração, dado que o CPI passa a permitir uma proteção transversal do segredo comercial[58], gerando uma ampliação do âmbito de aplicação altamente necessária para fazer face às novas formas de violação dos segredos comerciais originadas pela sociedade digital – "*sem serem objeto de direito de exclusivo, beneficiam de um regime muito próximo dos direitos de propriedade industrial*", batizado por MOURA VICENTE como "*o objeto de quase exclusivos*"[59].

Com o CPI de 2018, não são só abrangidas as situações que se verifica o elemento subjetivo concorrencial, como ainda se estende o regime a todos e quaisquer terceiros que se apropriem, utilizem ou divulgam segredos comerciais. Ditando a suficiência da ilicitude de um dos atos para ser legítima a proteção do segredo comercial.

Decompondo o número 1.º do artigo 313.º do CPI de 2018, que concerne ao objeto de proteção, podemos considerar 4 requisitos[60]:

"1 – 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, 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 objeto de diligências razoáveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas."

---

[57] Decreto-Lei 110/2018, de 10 de dezembro de 2018 – Código da Propriedade Intelectual, <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2018-117279941>

[58] VICENTE, Dário Moura, *Código da Propriedade Industrial Anotado,* Almedina, 2021, Anotação do artigo 313.º, p. 1186.

[59] *Idem, Op. cit.*

[60] Nuno Sousa e Silva segue o entendimento de que há quatro e não três requisitos, no mesmo sentido que a maioria da doutrina internacional, contudo há quem considere que o elemento "informação" não se tem por requisito, não seguimos esta posição por entendermos que o tipo de informação é relevante para obter o caráter de segredo de negócio.

1.5.4.1 Da Informação

MOURA VICENTE interpreta o conceito de modo a 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*"[61], acrescentando que não só cumpre informação confidencial de cariz empresarial como também o *know-how*, informações empresariais e informações tecnológicas. Tratando-se de informação protegida com relevância para o contexto empresarial e para o negócio em causa.

1.5.4.2 Da Natureza Secreta da Informação

Parte do prisma que essa mesma informação não poderá ser de conhecimento geral ou facilmente acessível (requisito objetivo), compreendendo o secretismo geral ou por compreensão casuística, para "*pessoas dos círculos que lidam normalmente com o tipo de informações em questão"*[62] (requisito subjetivo).

Cumpre destacar que não requer que seja de conhecimento de uma só pessoa, o seu titular na hipótese. O conhecimento pode ser partilhado com um grupo restrito de pessoas, não sendo relevante a sua quantidade, mas a sua qualidade, no sentido de perceber a relevância do segredo para aquelas pessoas, e não outras, de terem conhecimento ou acesso à informação. Mas daqui se deve exclusão, a pessoas que habitualmente lidam com o tipo de informação em questão.

Concluindo que a partilha, se feita, deve ser seletiva e de modo que o segredo não fique comprometido por esta transmissão. O que se espera do titular é um controlo estritamente necessário do conhecimento da informação secreta, excluindo uma ideia de exigência em segredo absoluto.

Contudo, por opção do titular do segredo, a tutela pode cessar no momento em que este entende apresentar a informação ao mercado.

Pela análise do requisito e tendo em consideração o contexto digital, SOUSA E SILVA faz a observação de que "*a partir do momento em que a informação seja publicada, o segredo perde-se*"[63] – uma visão absolutista, por certo, que não deixando de ser verdade, não parece de entendimento que de forma axiomática o segredo comercial deixe de o ser, sempre que exposto no universo digital.

---

[61] VICENTE, Dário Moura, *Código da Propriedade Industrial Anotado,* Almedina, 2021, *Op. cit*., Anotação do artigo 313.º, p. 1186.

[62] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, *Op. cit* p. 435.

[63] SILVA, Nuno Sousa e, *A nova disciplina dos segredos de negócio, análise e sugestões*, Homenagem ao Professor Doutor Germano Marques da Silva, Universidade Católica Editora, 2020, *Op. cit.,* p. 2182.

Juridicamente, cumpre perceber que a relevância desta exposição tem de pôr em causa o círculo legal subjetivo, nos termos do artigo 313.º. E como refere OLIVEIRA GERALDES, "*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*".[64] Deste modo, o risco de o segredo transpor o conhecimento limitado a este círculo de pessoas é altamente provável, mas não dita, com total certeza, a perda do valor secreto.

1.5.4.3 Do Valor Comercial da Informação Secreta

A informação para ser considerada secreta deve ser avaliada de forma pecuniária. Pois estas informações são legalmente consideradas como um bem jurídico autónomo que carece de proteção. A lei portuguesa não faz menção, contudo, sendo transposição da Diretiva Europeia de 2016, visa manter o seu espírito em tudo aquilo que não foi objeto de interpretação resultante da letra normativa nacional. Por sua vez, a Diretiva adotou a perspetiva ampla do conceito comercial atual e/ou potencial[65] original do UTSA e depois mantida na DTSA, não parecendo que possa ficar totalmente de lado no ato de interpretação desta premissa. A ideia de valor prende-se com a vantagem económica que o segredo, ao ser secreto, revela para o seu titular. Não existindo valor económico, não será compreensível a existência de segredo comercial digno de tutela.

Há quem defenda que se procura saber o custo associado ao seu desenvolvimento, o custo de manutenção preventiva do caráter secreto, ou que se quer depreender do requisito a perceção quantitativa da vantagem competitiva que o titular detém com aquele segredo de negócio. Parte-se de uma análise resultante do nexo de causalidade entre o valor e o facto de a informação ser mantida como secreta.

1.5.4.4 Diligências Razoáveis

O último requisito levanta algumas divergências doutrinárias. Por um lado, NUNO E SILVA considera como diligência razoável um cuidado mínimo com base na "*voluntariedade de proteção"*[66] e cuidado

---

[64] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, *Op. cit*, p. 436.

[65] Nuno Sousa e Silva exclui a hipótese da aferição do valor potencial, considerando apenas o valor real como relevante. Portanto, o valor no momento da violação do segredo de negócio, dado que a informação poderá ter sempre um valor potencial. Por sua vez, seguimos o entendimento que este valor potencial, mesmo que existente em todos os casos, não será o mesmo, sendo necessária a sua avaliação casuística.

[66] SILVA, Nuno Sousa e, *A nova disciplina dos segredos de negócio, análise e sugestões*, Homenagem ao Professor Doutor Germano Marques da Silva, Universidade Católica Editora, 2020, *Op. cit,* p. 2185.

adequado de forma a prever o princípio da proporcionalidade. Por sua vez, AZEVEDO DE AMORIM acredita que concretizar o critério da razoabilidade com base na ideia de proporcionalidade não pode encontrar fundamento na mera obrigação de mínimo[67]. Antes propõe uma análise jurídica relativa e dinâmica a ser observada caso a caso. Posição esta mais comum na doutrina e jurisprudência norte-americana.

Em primeira instância impõem-se ao titular que não seja negligente na defesa do seu segredo e no interesse de o manter assim. Comportando medidas de segurança e prevenção para manter o segredo longe do alcance de pessoas não autorizadas, que possam comprometer o seu caráter secreto.

Recai no titular do segredo de negócio o ónus de demonstrar que tomou as medidas adequadas para manter o sigilo das informações, a exemplo, a utilização de *passwords*, sistemas de vigilância, encriptação de plataformas ou cofres.

[67] AMORIM, Ana Clara Azevedo de, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* Revista Eletrónica de Direito, Faculdade de Direito da Universidade do Porto, n.º2, vol. 19, junho de 2019, p. 23.

CAPÍTULO 2

Do Espaço Digital

No livro "*1984*", de George Orwell, era imposta uma vigilância constante aos cidadãos. Hoje em dia damos conta que os cidadãos entregam voluntariamente um pouco de todo o tipo de informação *online*[68].

A expansão da *internet* e diversificação de aparelhos digitais modificou a forma de pensar e de agir da sociedade e dos seus cidadãos. De semelhante forma, face ao panorama da Economia Digital, as empresas vêm a aumentar o uso de tecnologia, vista como um fator determinante para a sua permanência no mercado.

Ao fim ao cabo, está em aberto um novo mercado de atuação para as pessoas enquanto indivíduos e, como enquanto pessoa com interesse comercial, ao se resumir num grande fluxo de informação a ser transmitida e partilhada. De modo a despoletar o crescimento de crimes associados ao ciberespaço: c*iber* espionagem, *hacking*, *ciber* roubo, e potencial roubo de segredos de negócio.

O direito, como área em constante mutação pelo regular desenvolvimento das relações sociais e evoluções científicas e tecnológicas, é confrontado agora com a tecnologia disruptiva da inteligência artificial, pelo que lhe será exigido correspondente adaptação de paradigma.

Especialmente no que toca ao fortalecimento da relação de confiança dos cidadãos, o direito tem o dever de providenciar estruturas jurídicas que disciplinem as ferramentas criadas para a maximização do bem-estar humano e diminuição, ou ideal, eliminação das fragilidades provocadas pelas alterações dos arquétipos sociais[69].

No âmbito da propriedade intelectual, industrial, concorrência desleal e segredos de negócio clama-se à adaptação face às tecnologias emergentes de inteligência artificial, uma vez que a sua criação não abrangia situações que hoje são uma realidade, partindo pela reforma de conceitos obsoletos e incorporação de novos institutos e regimes jurídicos[70]. Exigindo-se a reconfiguração no plano do Direito.

---

[68] Jornal Público, *Vivemos em plena distopia digital: Será que nos damos conta disso?,* <https://www.publico.pt/2022/07/12/p3/fotogaleria/vivemos-plena-distopia-digital-sera-damos-conta-disso-408412>

[69] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 34.

[70] *Idem*, p. 35.

2.1 Da Inteligência Artificial

Replicar a complexidade do cérebro humano parece roteiro de filme de ficção científica, no entanto, a era digital demonstrou que os cientistas e tecnológicos, não são só ambiciosos, como se sentem encorajados pela rápida evolução tecnológica que sustenta as suas crenças de superar invenção após invenção.

Tarefas triviais que o ser humano realiza diariamente de forma inata, implicam um processo de informação complexo que não é fácil reproduzir em sistema artificial.

Atualmente, encontramos um vasto conjunto de sistemas providos de Inteligência Artificial (doravante IA): *chatbots*, assistentes virtuais, *deepfakes*, sistemas de reconhecimento de som e imagem, carros autónomos, e muitos mais. Sem nos apercebermos, as aplicações de IA começaram a fazer parte do nosso quotidiano. Muitas das vezes nem se chega a ter perceção delas, e.g. a sugestão de produtos numa loja *online* ou sugestão de conteúdo numa plataforma de *streaming,* que encontra origem num sistema de IA que estuda os nossos comportamentos enquanto utilizadores e, principalmente, enquanto clientes. Seja pelas pesquisas, compras anteriores ou visualizações, o sistema elabora um histórico, que para a máquina dita a construção de um perfil com vista a personalização do uso das plataformas *online*.

O que estamos a presenciar é a transferência das tarefas rotineiras e consideradas mais fáceis para a inteligência artificial, surgindo condições mais favoráveis para o ser humano se dedicar a tarefas mais complexas. A IA comporta características às quais o humano não é capaz de atender. O nível de produtividade, o custo reduzido e a disponibilidade permanente estabelece fronteira com o ser humano, não descartando, contudo, a supervisão humana[71].

O grande desafio da inteligência artificial é constituir réplica da inteligência humana e a imitação de comportamentos humanos, nomeadamente, pelo facto que a mesma forma de apreensão não pode ser reproduzida pela falta de fatores inerentes à condição humana, como será a transmissão de conhecimentos ao longo de gerações.

Na obra "*Leviatã*" (1651), Thomas Hobbes menciona que o pensamento humano poderia operar por decomposição de símbolos, e que o processo de pensar seria a manipulação de tais símbolos. Que pela racionalidade métrica do pensamento humano, este poderia ser replicado por máquinas por um conjunto de operações mecânicas[72]. A partilha deste ponto de vista de Hobbes provocou o encorajamento de vários especialistas ao desenvolvimento do estudo da IA, como Blaise Pascal,

[71] LEITÃO, João Pedro, *O Impacto da Inteligência Artificial nos Direitos do Titular de Dados Pessoais: O Caso ChatGPT*, Almedina, 2024, p. 23.

[72] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 12.

Gottfried Leibniz ou Charles Babbage. Cada um deles, de diferentes formas e com diferentes níveis de complexidade, propuseram-se a construir máquinas de calcular operadas por processo mecânico.

Tal desenvolvimento modelou engenhos de invenções mais sofisticados no sentido de contribuir para o atual sistema de IA.

O século XX marca um ponto sem retorno. Alan Turing publica em 1936 um estudo do qual se retira a base de definição comportamental de um sistema IA simples. *" (…) demonstrou que qualquer computador com uma memória suficientemente grande, que manipule símbolos e que satisfaça algumas condições simples, consegue fazer os mesmos cálculos e obter os mesmos resultados que qualquer outro computador"*[73]. Não sendo possível de conhecer o facto na altura, este estudo revela que o engenho já existia abstratamente pela sua concretização teórica, restando a sua concretização prática.

Em 1950, Turing lançou o mote impulsionador: Poderiam as máquinas pensar?[74] Na ânsia de encontrar resposta, o matemático desenvolveu o *Teste de Turing* ou *Jogo da Imitação*, que consistia na interação de três intervenientes, uma pessoa a colocar questões a outros dois intervenientes, que sem a sua identidade comprometida, respondiam às questões. O sucesso do teste dependia de o questionador crer genuinamente que ambos os entrevistados eram seres humanos, quando na verdade, apenas um deles era uma pessoa, e o outro, era um sistema computacional. Apenas 70 anos depois o teste foi bem sucedido, não obstante, foi sem dúvida um dos marcos e pontos de viragem para a crescente pesquisa e evolução da IA.

Seis anos mais tarde, John McCarthy deu uso ao termo "inteligência artificial" pela primeira vez, durante uma conferência em Darmouth[75], que reuniu vários entendidos e pioneiros no estudo da computação.

2.1.1 Definição

Mais uma vez encontramos um conceito de difícil determinação. Não se pode dizer que exista posição consensual que define a inteligência artificial. Cabe efetuar uma aproximação da extensão de conceitos que a norteiam.

Pensemos de que forma se pode descrever a inteligência *per si*. Para obtermos uma visão completa poderemos considerar a seguinte formulação de inteligência: É *"uma capacidade geral de pensar ou resolver problemas em situações novas para o indivíduo, ou seja, não familiarizados com a*

[73] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, *Op. cit* p. 12.
[74] *Idem*, p. 13.
[75] O Berço da IA. LEITÃO, João Pedro, *O Impacto da Inteligência Artificial nos Direitos do Titular de Dados Pessoais: O Caso ChatGPT*, Almedina, 2024, p. 20.

experiência de aprendizagem, de modo que as rotinas de ação automatizadas não podem ser usadas para resolver esses problemas[76]*".*

Complementando este pensamento, a perceção de artificial - por algo produzido pelo homem, geralmente uma cópia de algo natural que não envolveu a mão do ser humano.

A interligação dos dois conceitos conduz ao termo inteligência artificial. Segundo a Organização Mundial da Propriedade Intelectual (OMPI) pode ser resumida nos seguintes termos: *"A IA é geralmente considerada uma disciplina da ciência da computação que tem por objetivo o desenvolvimento de máquinas e sistemas capazes de realizar tarefas em que se considera exigida a inteligência humana"* [77].

De forma mais simples, RUSSEL e NORVIG procuraram definir o conceito como: *"A inteligência artificial é o estudo da inteligência humana e das ações para replicá-la artificialmente, de modo que o resultado do seu projeto envolva um grau razoável de racionalidade"* [78].

Podemos concluir que a inteligência, tanto na vertente humana, como na sua vertente artificial, encontram conexão em se tratar de habilidades intelectuais para executar tarefas.

2.1.2 Evolução

Falando-se de avanços científicos e tecnológicos, remetemos sempre às Revoluções Industriais (compreendendo o século XVIII até meados do século XX). Contudo, o início da era digital, nomeadamente pela evolução da indústria robótica e da internet provocou a Quarta Revolução Industrial, conhecida por Revolução Digital.

A evolução não foi linear, os cientistas foram confrontados com uma realidade limitativa, era impossível replicar capacidades humanas intelectuais que advêm da perceção e interação humana no mundo real, que envolvem, não só o lado racional, como também o lado emocional. Esta conclusão resultou num período de abrandamento da inovação. O incentivo tinha sido comprometido, mas nunca ia deixar de existir.

Em 1942, Alan Turing desenvolve uma máquina (batizada de *Bombe*) capaz de decifrar mensagens criptografadas da máquina *Enigma*, utilizada pelos alemães à época da Segunda Guerra Mundial. Contribuindo para a leitura da localização dos exércitos adversários e a ser possível para o

[76] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 13.

[77] Traduzido de inglês para português. WIPO, *Artificial Intelligence and IP.*, maio 2021, <https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html>

[78] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, *Op. cit* p. 15.

ser humano o planeamento de estratégias militares com maior precisão e previsão de novos acontecimentos, revelando-se uma grande vantagem sobre os inimigos.

Em 1956, Allen Newell e Herbert Simon inventaram o *Logic Theorist,* um programa que expunha teoremas matemáticos através da manipulação de símbolos e busca de soluções.

Em 1958, McCarthy desenvolveu um programa de linguagem batizado de *LISP*, algo bastante presente em sistemas providos de IA.

Dois anos depois, Arthur Samuel desenvolveu um programa focado em aprender e jogar damas. O sistema era alimentado por dados, de modo que o seu software conseguisse desempenhar a tarefa e vencer o seu criador. Seria esta a primeira invenção de *machine learning*.

Por 1960, surge um *software* focado na reprodução de linguagem natural, denominado de *ELIZA*, capaz de comunicar através da absorção de expressões simples e naturais do ser humano. Apesar de não conseguir seguir o rumo da compreensão da conversa, o seu criador, Joseph Weizebaum conquistou a confiança dos utilizadores, que acreditavam estar a interagir com outro ser humano.

Entre 1970 e 1980 observou-se o abrandamento da investigação, período conhecido por *Inverno da IA*, com base no problema incontornável da impossibilidade de nutrir consciência às máquinas. Contudo, a partir desse período a perspetiva dos cientistas mudou, após o desapontamento com a conclusão acima descrita, veio a coragem de assumir os desafios. Iniciando a agora a programação de sistemas de IA que produziam o objetivo para que foram criados, mas sem serem totalmente dependentes do seu criador. Após a introdução de uma vasta quantidade de dados relevante para o objetivo do sistema, o programador via o resultado sem que fosse necessária a sua interferência no processo. Este avanço estava dependente do desenvolvimento da ciência da computação. Era necessário aumentar o número de transmissíveis e velocidade dos processadores, deste modo, a transmissão de dados em massa seria uma realidade. Neste sentido, a evolução de um acompanhou, e fez avançar a outra. O aumento de dados disponíveis *online* permitiu um treino intenso da IA, com base na capacidade de processamento, agora, também melhorada.

Passou-se à fase do investimento por parte dos capitalistas, que viam na transição para metodologias de IA, proveitos para a prosperidade das suas empresas e negócios[79].

Em 1994 surge a primeira invenção gerada por IA, à qual foi reconhecida a concessão de patente. A *Máquina da Criatividade* de Stephen Thaler era capaz de gerar ideias através da sua rede neural artificial, uma verdadeira espécie de cérebro artificial que consiste essencialmente num conjunto de interruptores que se interligam entre si[80].

---

[79] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 19.

[80] Apenas o criador foi mencionado como tal no pedido de patente, em momento algum se referiu à máquina como inventor da ideia inovadora – *Idem*.

Em 1997, o computador *Deep Blue* derrota o campeão mundial de xadrez decorrente da desistência deste a meio do jogo. A invenção da IBM (*International Business Machines Corporation*) tinha na sua base de dados uma grande "biblioteca" de jogos de xadrez, conseguindo escolher a melhor jogada face à situação em que se encontrava. Analisando as jogadas do adversário, adaptava a sua estratégia. Estava provado que a IA podia chegar à capacidade humana e até superá-la.

Em 2014 continuou o desenvolvimento da máquina para a linguagem natural, o protótipo do *robot Pepper* estava programado para acompanhar seniores. Conseguia dialogar com o humano, no entanto, revelava as fragilidades de não ter perceção do mundo real, baseando a sua ação nos dados que haviam sido pré-transmitidos.

Em 2017, surge o *Libratus*, um programa de IA desenhado para jogar póquer. Apenas com uma extensa base de dados relativa às regras do jogo, a máquina pôde identificar uma estratégia e analisar o comportamento dos adversários, nomeadamente, a prática de *bluff* e identificar as suas fraquezas, terminando o jogo com a vitória da IA sob os outros 4 jogadores.

Nas palavras de DUARTE NUNES, "*os cientistas provaram que, em ambientes controlados, com ajuda de bases de dados que fornecem informação aos programas equipados com sistemas de deep learning, a IA consegue competir e mesmo superar a inteligência humana, na área específica para que foi construída*"[81].

No entanto, eram esperados avanços da IA além da área dos jogos, o mesmo sucesso era ansiado para a vertente da utilidade social e pública.

Esse desejo encontrou concretização em sistemas complementares para o setor médico e farmacêutico, de uma forma mais eficaz que qualquer ser humano, foram desenvolvidos sistemas de IA que diagnosticam e ajudam no tratamento de patologias em tempo e precisão recorde, caso do *Watson*, *BabyX* ou *MultiSense*. Imagine-se o cenário observado em séries como o *Dr.House,* em que é comum a discussão entre médicos com vista ao apuramento de sintomas de um doente, para construir um diagnóstico pelo método da exclusão de hipóteses. Hoje em dia, já existem programas de IA, treinados com uma vasta rede de dados relevantes para o contexto médico, neste caso, uma base de dados com milhares de doenças e patologias e as suas correspondentes características, que pela inserção de sintomas podem obter uma correspondência em minutos. Revelando-se uma grande ajuda para os médicos, que apesar dos benefícios, não devem ver de forma absoluta e vinculativa os diagnósticos gerados pela IA, complementando sempre com os seus conhecimentos e sensibilidade humana da qual a máquina não atinge alcance.

[81] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, *Op. cit* p. 21.

De igual modo, este progresso foi transversal a outras áreas. Por exemplo, no Direito os equipamentos com IA passaram a ser verdadeiros assistentes dos advogados, como é exemplo o *Case Crunch*, capaz de prever 800 sinistros de venda indevida de seguros.

A primazia da IA é acentuada pela transformação do panorama da economia mundial, segundo SHOSHANA ZUBOFF: *"o capitalismo vigilante – surveillance capitalism, reivindica unilateralmente a experiência humana como matéria-prima para ser traduzida em dados comportamentais. Embora alguns destes dados sejam aplicados à melhoria de produtos e serviços, os restantes são declarados como excedentes comportamentais – behavioral surplus, alimentando processos avançados de manufatura conhecidos como machine intelligence, e transformados em produtos de previsão que antecipam o que se faz, agora, em breve ou mais tarde"* [82].

A IA demonstrou ser capaz de orientar a sociedade para o progresso ao culminar na prosperidade económica e qualidade de vida superior da população, no entanto, estas profundas transformações sociais geram, a par dos benefícios, alguns inconvenientes - *"A verdade é que cada um, individualmente, manipula a informação no seu interesse, sequela do egoísmo e capitalismo societários vividos atualmente"*[83].

2.2 *Chat Generative Pre-trained Transformer* – ChatGPT

O *Chat Generative Pre-trained Transformer*, criado pela empresa OpenAI, mais conhecido por ChatGPT é um sistema de IA de aprendizagem automática, isto quer dizer, que pela transmissão de um conjunto de dados, aprende de forma autónoma, para atingir o objetivo a qual foi programado.

Está em causa um tipo de *reactive machine*. Um modelo de funcionamento do algoritmo de IA que pressupõe a evolução do sistema informático através de *updates*, tendo por base as suas interações ao longo do tempo, que se traduzem em aprendizagens para futuras utilizações. Ou seja, estamos perante um algoritmo que tem capacidade autónoma para apreender e aprender com as tarefas que executa.

Dentro dos mecanismos de aprendizagem automática surge a capacidade de *deep learning* ou aprendizagem profunda[84], focada na análise de dados em massa. A aprendizagem profunda tem por base uma rede de neurónios artificiais, formados por uma imensidão de camadas e consequente infinitude de nós conectados. A perceção de profundidade resolve-se à volta da capacidade de uma camada ter unidades de neurónios que transformam dados de entrada em informações que podem

[82] XAVIER, Luís Barreto, *Notas sobre regulação da inteligência artificial: da ética ao direito*, Católica Talks – Direito e Tecnologia, Universidade Católica Editora, Lisboa, 2021, *Op. cit* p. 118.
[83] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 31.
[84] *Idem*, p. 27.

ser utilizados pela próxima camada. Deste modo, a máquina pode aprender por meio do próprio processamento de dados. Ao fim ao cabo, reproduz o que o sistema de neurónios humanos faz, mas artificialmente e com as limitações inerentes a essa característica *sui generis*.

Tem o objetivo de dar resposta a questões solicitadas pelos utilizadores, tendo por base as informações que possui na sua vasta rede de dados, incluindo a particularidade, que o seu sistema evolui à medida que as interações vão a acontecer. Quanto maior a pesquisa e conexão com as diversas informações, mais irá reter no seu histórico para que no futuro a interação seja mais clara, coerente e abrangente. Deste modo o utilizador obtém respostas cada vez mais específicas e desenvolvidas sobre o pedido em questão.

Os utilizadores destas ferramentas não têm perceção da informação que partilham e da hipótese de estas serem transmissíveis ou reutilizadas a partir do momento que ganham relevância no contexto do mundo digital. Pelo que, da utilização massiva de sistemas de IA e dados resulta a preocupação da falta de transparência e segurança dos dados dispostos pelos utilizadores no digital.

Surge também uma preocupação relacionada com o risco de inércia intelectual pela hipótese de perceção errada da IA em detrimento do raciocínio humano, que pode dar azo a um retrocesso da evolução e de desenvolvimento de competências humanas[85]. Deve-se procurar respeitar nuclearmente os direitos e princípios éticos sociais, e alocar a IA a uma posição de complemento humano e não de concorrente ou substituto[86].

Cabendo aos órgãos jurídicos e administrativos gerir um programa de políticas centradas no ser humano com vista ao aproveitamento máximo dos benefícios subjacentes à IA e diminuição dos riscos impostos pela existência e utilização desta.

No seguimento, a Comissão Europeia comunicou, em 2019, que: "*a tecnologia da IA deve ser desenvolvida de forma que coloque as pessoas no seu centro e seja, assim, digna da confiança do público. Tal implica que as aplicações de IA devem não só ser coerentes com a legislação, como também respeitar os princípios éticos e assegurar que a sua aplicação evita danos não intencionais*"[87].

---

[85] LEITÃO, João Pedro, *O Impacto da Inteligência Artificial nos Direitos do Titular de Dados Pessoais: O Caso ChatGPT*, Almedina, 2024, p. 24.

[86] NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023, p. 33.

[87] Comissão Europeia, *Aumentar a confiança numa inteligência artificial centrada no ser humano,* abril 2019, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52019DC0168>

2.2.1 Evolução

A par desta evolução surge um novo tipo de oferta no mercado. Hoje as empresas são o público-alvo de campanhas de promoção e inserção de sistemas de IA, nomeadamente o ChatGPT ou outros *chatbots* como o DALL.E, vocacionados especialmente para o uso de corporações empresariais[88]. São criadas verdadeiras campanhas de *marketing* para convencer os empresários da necessidade e vantagem produtiva que estas ferramentas podem trazer ao seu negócio inserido num *fast-paced market*[89].

O primeiro ChatGPT – o GPT-1, foi lançado em 2018, estabeleceu um marco na configuração de linguagem natural por parte de um mecanismo artificial.

No ano seguinte, é lançado o GPT-2, que veio com uma clara melhoria na capacidade de gerar texto coerente e pertinente. O sucesso da invenção fez com o que a OpenAI não lançasse o modelo completo, alegando que haveria um risco para o uso mal-intencionado da ferramenta.

No seguimento, em 2020, é lançado o GPT-3 com o significativo aumento de parâmetros de aprendizagem. Passa-se de uma rede com 1,5 bilião de parâmetros para 175 biliões, uma clara escala de aumento exorbitante.

Em 2023 surge o atual ChatGPT ou GPT-4, especializado em replicar diálogo humano ao fornecer respostas, e à semelhança dos seus antecedentes, possui um vasto corpo de dados que agora vão ser utilizados para fazer interligações entre eles e com cada interação que têm. Ou seja, estamos perante um mecanismo que se "autoalimenta" para se superar, ao proporcionar um serviço mais personalizado e preciso.

2.2.2 No Contexto Empresarial

No meio empresarial faz-se um rastreio de tarefas nas quais os humanos são facilmente substituíveis pela IA: para elaboração de códigos de programação; escrever e gerar conteúdo, atendimento e assistência ao cliente; elaboração de resumos e minutas de reunião; responder a pedidos padronizados[90], entre outras tarefas mais específicas à indústria da empresa que o utiliza.

Nos últimos 5, anos surgiu um aumento de empresas que recomendam e implementam o ChatGPT dentro das suas organizações. Deste modo, os trabalhadores podem se fazer auxiliar deste

---

[88] Uma versão paga disponível para negócios que contém uma rede de dados especialmente selecionada por ser relevante no setor empresarial e não apenas para atender necessidades sociais gerais.

[89] FastBots, *Chat GPT for Company Efficiency: Transforming Business Communication,* <https://fastbots.ai/blog/chat-gpt-for-company-efficiency-revolutionising-business-communication>

[90] LEITÃO, João Pedro, *O Impacto da Inteligência Artificial nos Direitos do Titular de Dados Pessoais: O Caso ChatGPT*, Almedina, 2024, p. 29.

meio de simplificação de tarefas e processos internos, acabando por deixar de perder tempo com tarefas mais triviais, concentrando-se nas mais complexas, das quais não se conseguem fazer substituir. Contribuindo assim para um aumento da produtividade, que é o grande interesse das empresas.

Atualmente, as empresas podem optar por um sistema de IA já existente no mercado ou criar uma ferramenta que respeita o algoritmo que assim entenderem. Proporcionando uma aplicação extremamente personalizada em razão do setor de atividade, objetivos do negócio, a cultura da empresa e as necessidades de conduta.

Será de estabelecer a máxima importância de que, apesar da autonomia do sistema, não se deve preterir o acompanhamento e monitorização da sua utilização com a finalidade de garantir que não é utilizado de forma abusiva ou ilegal, destacando quando pode estar em causa a partilha do utilizador, de informações sensíveis ou secretas da empresa.

2.2.3 Vantagens e Desvantagens

O ChatGPT tem resposta para uma infinitude de questões, a profundidade e detalhe de conhecimento é notável, contudo, tem de se fazer a advertência, que nem sempre esses dados correspondem aos mais atuais do ponto de vista temporal ou da precisão factual, revelando uma fragilidade neste ponto.

Para não falar da dependência de dados. Cada sistema de *chatbot* será relevante na medida e contexto dos dados com que foi treinado. Com destaque para a capacidade de distinção do bom e do mau, podendo recusar perguntas e pedidos inadequados ou ilícitos à luz dos dados que lhe foram transmitidos. Pelo contrário, os dados inseridos podem induzir respostas preconceituosas ou desigualdades de tratamento.

Após o treino do sistema, destaca-se a prescindibilidade da disponibilidade humana para a manutenção do sistema. Ao realizar a monitorização das interações estabelecidas e análise pormenorizada dos dados adquiridos, o sistema potencializa a sua *performance* e aumenta a sua rede de dados.

Outras vantagens que se observam são a sua gratuitidade (pelo menos nos sistemas mais simples e gerais que são precisamente os mencionados nesta análise) e a sua capacidade bilingue, em mais de 20 idiomas (dependendo da complexidade das questões e dificuldade do idioma). O facto de ser uma ferramenta que disponibiliza versões sem custo associado, releva para dois tipos de interpretação, por um lado, comporta uma vantagem clara e económica que agrada a qualquer utilizador comum, no entanto, não nos parece razoável deixar de questionar se faz sentido. Pois, por outro lado, o ser humano está habituado a que serviços que facilitem o dia a dia, especialmente os

que envolvem complexos mecanismos tecnológicos e científicos tenham um custo monetário. E neste sentido, que ANDREW LEWIS proferiu a seguinte frase que nos parece de interesse refletir: *"Se não estás a pagar por algo, então não és o cliente; és o produto que está a ser vendido"* [91].

Efetivamente, qual será o bem de troca na utilização destes sistemas do tipo ChatGPT? São programas com tecnologia bastante dispendiosa e sem qualquer obrigatoriedade de ser entregue ao mercado sem custo monetário associado, então, porque razão se faz exceção à regra e se dá livre passagem ao seu uso, sem restrições e limites de utilização? O que Andrew Lewis parece insinuar e que nos leva a presumir, é que os benefícios para os sistemas e para os fornecedores é obtido pelo uso que fazemos dos programas, pelos nossos *inputs,* não só enriquecemos a máquina como transmitimos, de forma, maior ou em menor escala, informações pessoais, sem que se dê conta que o fazemos. Pense-se no simples facto de se aceitar termos e condições ou criar *log in* num destes sistemas. E a outra escala, a troca de informações já no ato de interação com os programas. Persiste-nos a intriga do fundo desta questão.

No entanto, tem também demonstrado um impacto positivo no que toca a micro e pequenas empresas. No caso das *startups*, empresas de orçamento limitado, observa-se a diminuição de tarefas que precisam de ser executadas por seres humanos, deste modo, não se compromete o orçamento, precisamente pela menor necessidade de recursos humanos, como também nem se deixa aquém as necessidades da empresa e do processo comercial.

Cumpre destacar, a nosso ver, a maior desvantagem do uso de ChatGPT e sistemas semelhantes: a falta de transparência e segurança. Os utilizadores não sabem de que modo é utilizada a informação partilhada com as ferramentas. Assim que entra no domínio da inteligência artificial deixamos de ter controlo sobre a informação, o que levanta grandes preocupações sobre a proteção de dados, especialmente no que toca à partilha inadvertida de informações sensíveis.

No seguimento da insegurança no sistema, há ainda a desvantagem relacionada com o potencial risco e a atratividade que estes sistemas representam para os *hackers*. O facto de serem uma espécie de depósito das mais variadíssimas informações, em especial aquelas que são facultadas pelos utilizadores, é expectável que algumas dessas informações sejam confidenciais, das quais o utilizador não partilharia com outra pessoa, ou não prevê uma divulgação intencional, por respeitar apenas a si e aos seus interesses[92].

---

[91] Jornal Público, *Vivemos em plena distopia digital: Será que nos damos conta disso?,* <https://www.publico.pt/2022/07/12/p3/fotogaleria/vivemos-plena-distopia-digital-sera-damos-conta-disso-408412>

[92] Leia-se interesses próprios que podem ser, precisamente, os do sucesso de uma empresa.

2.2.4 Da Ética

A importância da privacidade e proteção de dados, dos quais, aqui introduzimos os segredos de negócio como um tipo de dados das empresas, nos sistemas de IA é multifacetada, no sentido que podemos relacionar com considerações éticas, jurídicas e de confiança por parte de quem as utiliza[93].

Em termos de valorização ética, os princípios éticos exigem que os dados confidenciais dos utilizadores sejam respeitados e protegidos. Os modelos de linguagem de IA processam uma abundante quantidade de dados, existindo a possibilidade de aprender e gerar informações sensíveis. O comprometimento destas informações pode gerar grandes prejuízos para os utilizadores. A garantia de privacidade e proteção de dados na IA é, pois, e primeiramente, um imperativo ético e de respeito aos Direitos Humanos.

[93] GLORIN, Sebastian, *Privacy and data protection in ChatGPT and other AI chatbots: Strategies for securing user information,* Georgia Institute of Technology, 2023, p. 3 e 4.

CAPÍTULO 3

Juízo Entre os Segredos de Negócio e o Mundo num Contexto Digital

O rápido desenvolvimento e utilização de ferramentas digitais e tecnológicas, das quais a inteligência artificial, onde o ChatGPT se insere, gerou o começo de litígios judiciais que originaram questões sem resolução objetiva.

As preocupações e receios relativos à utilização do ChatGPT relacionam-se principalmente com a potencial fuga de informação e violação da privacidade. Esta preocupação decorre da sua capacidade de processar e gerar grandes quantidades de dados, através do uso de sofisticados algoritmos de aprendizagem profunda. Deste modo, os algoritmos podem inadvertidamente conectar pontos e desvendar padrões nos dados que não se destinavam a ser divulgados, originando questões sobre a segurança e privacidade do sistema aquando da interação com o utilizador. Levando à necessidade de políticas e controlos de segurança desenvolvidos para mitigar estes riscos. Apesar das potenciais desvantagens, os criadores argumentam que os benefícios do ChatGPT superam os seus possíveis inconvenientes[94].

3.1 A Questão da Divulgação: A Divulgação de um Segredo Comercial *Online* faz Cessar a sua Proteção Jurídica?

Levanta-se a questão se a divulgação *online* de segredos de negócio gere e cessação da proteção jurídica como tal. Caso a resposta seja afirmativa, a sua tutela perde o fundamento, pelo que a sua inexistência vai comprometer a tutela processual cautelar e inibitória.

A complementar a análise da questão, o caso *United States of America v Genovese* (2005)[95] refere a situação em que dois códigos fonte da Microsoft Corporation foram divulgados na internet, em que posteriormente, Genovese faz o *download*, cópia do *download* e publicação de modo promocional para a venda do mesmo, sem a prévia autorização da empresa criadora. Genovese alegou que não tinha como saber que o código não era de conhecimento geral, visto que o encontrou por acaso *online* e que a Microsoft não tinha sido diligente, no que toca à manutenção do sigilo do segredo comercial, concluindo que o instituto de proteção de segredo comercial teria sido

[94] FALADE, Polra Victor, *investigating the security and privacy issues in chatGPT usage and their impact on organisational and individual security*, International Journal os Scientific Research in Multidisciplinary Studies, Vol. 10, Issue 3, 2024, p. 20.

[95] *United States of America v Genovese* – P. 409 F. Supp. 2d 253 (S.D.N.Y. 2005), <https://casetext.com/case/us-v-genovese-7> e GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 443.

esvaziado e que seria de impossível aplicação. Ora, o tribunal definiu que o segredo comercial só perde o seu estatuto se for geralmente conhecido, pelo que era preservada a sua natureza se for divulgado temporariamente, acidentalmente ou ilicitamente sem que se verifique o conhecimento geral do mesmo.

No mesmo entendimento, no caso Hurry Family Revocable Tr. v. Frankel[96], o tribunal decidiu a favor da não cessação da proteção de segredos comerciais, após publicação do segredo nos registos públicos e eletrónicos do tribunal, alegando que "*a publicação na internet não destrói necessariamente o segredo se a publicação for suficientemente obscura ou transitória ou limitada de outra forma de modo a que não se torne geralmente conhecida a pessoas relevantes, e.g. potenciais competidores ou outras pessoas às quais a informação pode ter algum valor económico*"[97]. Clarificando ainda, que assim que haja evidência clara que a informação, agora publicamente disponível, foi vista ou partilhada por terceiros, e que apesar de pública: *(1)* os alegados segredos não eram de fácil acesso ou localizados por concorrentes, *(2)* o público geral não conseguia aceder aos documentos nos registos eletrónicos sem saber o número do caso e a localização da ação, e *(3)* os segredos comerciais não eram rotulados e estavam localizados numa pasta que continha 28 ficheiros.

Estabeleceu-se a prerrogativa de que a divulgação *online* não extingue a proteção jurídica do segredo comercial, sendo necessário comprovar que a divulgação tornou o segredo geralmente conhecido ou facilmente acessível para que cesse a proteção do segredo comercial e se considere apenas uma informação sensível empresarial.

Constata-se que a publicação de informação secreta empresarial *online* é um fator decisivo para averiguar se há divulgação de segredo de negócio. Sendo necessária a análise holística e casuística para averiguar a exclusão, ou não, da proteção, pelo comprometimento do ato de divulgação.

3.1.1 Divulgação a Círculos Subjetivos Relevantes

A par de outras jurisdições, o sistema português prevê na alínea a), do número 1 do artigo 313.º do CPI, que a análise da divulgação como fator determinante para a existência de segredo comercial tem de ser juridicamente perspetivado, tenho em conta os círculos subjetivos legalmente exigidos.

---

[96] *Hurry Family Revocable Tr. v. Frankel* – P. 8:18-cv-2869-CEH-CPT (MD Fla. jan. 3, 2023), <https://casetext.com/case/hurry-family-revocable-tr-v-frankel-5>

[97] Traduzido de ingles para português Seyfarth, *Spilling Secrets to AI: Does Chatting with ChatGPT Unleash Trade Secret or Invention Disclosure Dilemmas?,* <https://www.tradesecretslaw.com/2023/04/articles/intellectual-property/spilling-secrets-to-ai-does-chatting-with-chatgpt-unleash-trade-secret-or-invention-disclosure-dilemmas/>

Importa agora perceber a qualidade das pessoas a quem foram divulgados os segredos de negócio e se estas se inserem na hipótese prevista do artigo 313.º do CPI.

Premissa que já resultava do artigo 39.º do TRIPS e do artigo 2.º da Diretiva Europeia é que a delimitação subjetiva resulta da qualidade da pessoa, como alguém que pertence a um grupo em relação de habitualidade e familiaridade com o tipo de informação exposta. Sendo relevante perceber se o segredo foi divulgado ou utilizado por uma pessoa que lida normalmente com este tipo de informação, de forma a conseguir depreender o seu sentido. Ora, imagine-se um segredo de negócio de uma empresa do setor farmacêutico sobre um protótipo base de um medicamento inovador, da qual um funcionário transmite a informação secreta por *e-mail,* enganando-se no destinatário, em vez de enviar a um colega de trabalho com igual condição de conhecimento do segredo, envia para uma pessoa externa à empresa. Por sua vez, esta pessoa poderia ser um eletricista, carteiro ou jovem estudante de ensino básico, nenhum deles, nos parece à primeira vista, compreender o sentido da informação e deste modo, desconhece também o seu valor enquanto segredo e enquanto informação potencialmente valiosa. O seu conhecimento é de âmbito superficial, o conhecimento efetivo e real não se concretiza.

A perspetiva norte-americana, parte da secção 1839 do DTSA de 2016, determinando que o limite para o círculo subjetivo legalmente previsto encontra resposta no benefício económico. Ou seja, a divulgação do segredo comercial não compromete o caráter sigiloso do mesmo, se a divulgação não comprometer o seu valor comercial. Desde que não seja geralmente conhecido ou facilmente acessível por pessoa que possa beneficiar economicamente da sua divulgação e consequente utilização, o segredo continua qualificado como tal[98].

De um ponto de vista de completude, parece-nos relevante atender os dois pontos de vista. A divulgação da informação só será relevante se os círculos subjetivos atenderem a: *(1)* qualquer pessoa que lide habitualmente com o tipo de informação em causa e *(2)* pessoas que possam beneficiar economicamente com a divulgação.

Podemos perspetivar a situação do seguinte modo, a aferição da cessação do estatuto de segredo comercial de uma informação secreta divulgada tem por base a definição do círculo subjetivo e se este se verificou. A cessação do estatuto não opera automaticamente, mas mesmo que não se verifique o conhecimento geral da informação, basta que seja do conhecimento do círculo subjetivo legalmente delimitado[99].

Como já exemplificado anteriormente, é necessária a delimitação do conceito de círculo subjetivo. Apesar da primazia da avaliação casuísta, os tribunais norte-americanos procuraram

[98] DTSA 18 U.S. Code § 1839 <https://www.law.cornell.edu/uscode/text/18/1839#3>

[99] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 447.

concretizar o conceito de círculos relevantes pela integração a "*membros de uma indústria*"[100]. Não satisfeitos com a fraca densidade explicativa, mais tarde os tribunais evoluíram no uso do critério da maioria, posto que, não cabe existência a segredo comercial quando a informação secreta é divulgada e de conhecimento geral da maioria dos membros da indústria relevante para o caso.

De relevante menção para a questão será a delimitação de "círculos subjetivos" elaborada por Kalbfus[101]. Para tal formulou a *Teoria do controlo* e a *Teoria do interesse comum*. Consoante a *Teoria do Controlo,* o segredo comercial estaria salvaguardado enquanto o titular tivesse o controlo efetivo sobre o círculo de pessoas relevantes, por meio de mecanismos como a utilização de acordos de confidencialidade. Do ponto de vista da *Teoria do Interesse Comum,* teria que existir um interesse comum para a manutenção da natureza sigilosa do segredo de negócio. Tanto o titular, como as pessoas que tivessem tido acesso à informação secreta, deviam zelar pela preservação do segredo e respetiva proteção como tal. No entanto, não é garantido que o valor que uma pessoa associa a algo será a mesma que outra pessoa associa. Mesmo tratando-se de segredos que constituem um benefício no mercado empresarial, não é garantido que todas as pessoas com conhecimento do segredo tenham o interesse de o manter assim ou de não tirar partido para si. Alguém com interesses mal-intencionados pode usar o segredo como meio de troca, chantagem ou como forma concorrencial futura, e claro, o erro humano continua sempre a ser uma possibilidade.

Pelo exposto, sustenta-se que a divulgação de um segredo de negócio *online*, não determina, necessariamente, a não observação dos pressupostos normativos de condição indispensável para a atribuição de tutela jurídica a certas informações. Decerto, a determinação delimitada do que respeita a círculos subjetivos é fator determinante para apurar se a divulgação respeita a um segredo comercial ou apenas a uma informação pela cessação da mesma como segredo de negócio.

3.1.2 Teoria da Preservação Sequencial

A teoria da preservação sequencial, promovida por ROWE,[102] determina que é necessário averiguar o tipo de divulgação *online* verificada. Confere uma espécie de testes, que ajudam a perceber o impacto da divulgação do segredo de negócio, e se esta divulgação impacta a aplicação do regime de proteção do mesmo enquanto segredo. No seu entendimento, nem todo o tipo de divulgação seria relevante do ponto de vista legal. Tal partia da análise faseada de três fatores, com o objetivo de cada um deles responda à pergunta – "a*s informações mantiveram o seu estatuto de segredo*

[100] *Idem*.

[101] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 449.

[102] *Idem*, p. 451.

comercial apesar de ter ocorrido a sua publicação na internet?"[103]: *(1)* o tempo de exposição do segredo e reação do titular, *(2)* extensão da divulgação, e *(3)* a relevância que teriam os destinatários no que toca ao conhecimento da natureza da informação.

O primeiro fator *(1)* refere-se ao intervalo de tempo da exposição do segredo de negócio e respetiva ação do titular, no sentido de suficiência na rapidez para salvaguardar o segredo, após tomar conhecimento da sua exposição. O fundo de ser resume-se a que existiria uma perspetiva de manutenção do segredo se o titular tomasse medidas no curto tempo em que a informação esteve exposta. Uma clara valorização de celeridade e urgência por parte do titular em preservar a situação anterior à exposição do segredo *online*. Na prática, e como todos os requisitos anteriormente analisados deste instituto, é necessário atender às especificidades de cada caso e notar que quando falamos de mecanismos digitais falamos de uma ferramenta alvo da expressão "tudo o que um dia entra na internet se perde". Deste modo, a reação suficientemente rápida para mitigar o risco de cessação do estatuto de segredo comercial poderá ser de difícil materialização, ou não ser bem sucedida, acabando por acontecer o conhecimento geral do segredo. De todo o modo, parece-nos que uma das medidas mais eficazes para concretizar o teste, seria o recurso a instâncias judiciais.

Mas a exemplo de relevância para a questão, o caso *Religious Technology Center v. Arnaldo Pagliarina Lerma/Washington Post (1995)*[104], refere a situação em que um antigo membro da igreja de cientologia, não só divulgou *online* informações obtidas através de um sistema digital de dados, como também enviou ao jornal Washington Post. Este, por sua vez, aproveitou o momento para publicar o artigo "*Churchin Cyberspace: It's sacred wrist in on the net. It's lawyers are on the case*". Dada a situação, a igreja alegou que os seus segredos comerciais haviam sido violados pelo jornal, contudo o tribunal distrital do estado de Virginia declarou o pedido improcedente, alegando que proteção legal que poderia ser conferida ao segredo comercial cessou com o momento de divulgação do mesmo por parte do antigo membro da entidade autora do pedido. Não satisfeita com esta conclusão, a igreja tentou obter tutela inibitória contra o ex-membro, à qual o tribunal alegou o fator temporal como determinante. Consideraram que decorridos dez dias desde o momento da publicação *online*, o segredo comercial já não se configurava como tal, pois já era de conhecimento geral: "*once a trade secret is posted on the internet, it is effectively part of the public domain, impossible to retrieve*"[105].

---

[103] *Idem*, *Op. cit* p. 455.

[104] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 440 e 441. E Religious Technology Center v. Arnaldo Pagliarina Lerma/Washington Post – P. 908 F. Supp. 1353 (E.D. Va. 29.11.1995), <https://law.justia.com/cases/federal/district-courts/FSupp/908/1353/1457462/>

[105] *Idem*, p. 441.

O segundo elemento *(2)* prende-se com se a exposição *online* do segredo comercial originou conhecimento do domínio público. Este fator foca a forma e o modo como a divulgação do segredo comercial é feita, comportando sempre, para o caso, o espaço digital. Mesmo quando se publica na *internet* podemos constatar que existem vários níveis de exposição. Exemplifique-se, a exposição será muito mais elevada numa rede social do que seria num blogue pessoal com poucos leitores. Pelo que o nível determina o conhecimento geral ou conhecimento pelos círculos subjetivos delimitados legalmente do segredo comercial. Pegando no exemplo anterior, imagine-se que as poucas dezenas de leitores do blogue onde foi divulgado o segredo comercial, pertencem ao círculo subjetivo delimitado legalmente. Isto só revela que é de máxima importância analisar o caso ao pormenor para tomar ponderações conceptuais. Não esquecendo a conjugação entre fatores, o nível de exposição vai conflituar com a necessidade maior ou menor suficiência de reação por parte do titular para salvaguardar o segredo comercial.

Ainda neste ponto, Rowe defende a importância da quantidade de informação que é revelada, compreendendo a possibilidade de divulgação parcial de segredo de negócio e correspondente proteção parcial[106]. No sentido que partes não divulgadas do segredo comercial merecem tutela através do instituto de proteção de segredo comercial, nos mesmos termos que esta funcionaria se tivesse em causa a totalidade do segredo. Dada a situação, pode sempre ocorrer que a divulgação parcial do segredo não seja insuficiente para apurar a função do segredo comercial, apenas sendo possível com a integralidade da informação conjunta, entre parte divulgada e parte não divulgada.

O terceiro fator *(3)* procura analisar a posição das pessoas que tomaram conhecimento do segredo comercial através da sua divulgação. A situação do destinatário da divulgação dedica-se em saber se este tinha conhecimento ou se não devia desconhecer a especial proteção legal que a informação continha. Pela conexão da apropriação indevida e a sua preservação, o titular do segredo comercial pode ter, mais uma vez, um papel determinante. O titular, ao entrar em contacto com os destinatários da divulgação, informa da ilicitude e dos termos da situação, estará a demonstrar o interesse de salvaguarda do segredo comercial.

Portanto, segundo o autor, e em acordo com ele, consideramos que se a informação divulgada sobreviver aos testes, mantém o seu estatuto de segredo de negócio e a sua tutela judicial poderá passar pela ordenação judicial de remoção da informação da *internet* e prever ainda uma ação inibitória de utilização da mesma.

[106] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 453.

3.2 A Transposição do Segredo Comercial para o ChatGPT

O uso de plataformas dotadas de inteligência artificial, como é o caso de *chatbots*, e proteção de segredos de negócio, não combina propriamente bem.

A Inteligência Artificial e o ChatGPT vieram colocar um dos maiores desafios sociais e jurídicos do século XXI, não apenas em termos de direitos de autor e de cibersegurança, mas também de proteção de segredos de negócio.

A maioria das pessoas já ouviu e ouve falar do ChatGPT, muitos já utilizaram, muitos usam com regularidade, mas poucos sabem verdadeiramente como funciona. Os *chatbots* entraram no mercado público à relativamente pouco tempo, e certamente que continuará a evoluir. Pelo que, a falta de informação e entendimento sobre o seu processo de operação aumenta o risco de, inadvertidamente, submeter informação de cariz privado[107].

O grande problema em análise parte da premissa que o risco surge do uso do ChatGPT e aplicações de IA por parte de trabalhadores de uma empresa.

No contexto empresarial, o uso do ChatGPT poderá se traduzir no comprometimento de segredos de negócio. Imagine-se, um trabalhador que se vê bastante atarefado e procura delegar tarefas mais simples para uma ferramenta de IA, no caso, o ChatGPT, para que assim se possa ocupar de tarefas mais complexas. Introduz os dados necessários, por exemplo, a gravação de uma reunião privada, com a intenção de obter uma minuta. Sem que neste processo pense que tal ação possa ter consequências sérias a nível judicial.

A urgência do assunto reflete-se pelo estudo que a Cyberhaven promoveu com conclusão de que 11% da informação colocada no ChatGPT representa informação sensível em contexto empresarial.

Poderíamos pensar na mais variadíssima forma de expor segredos comerciais na plataforma: descrever integralmente o segredo comercial com o objetivo de obter um resumo ou um título, introduzir uma receita e pedir que resume ou divide por passos o processo de criação, inserir um código de *sofware* com o objetivo de detetar erros, entre muitos outros.

Ao concordar com os termos e usos do ChatGPT cedemos tudo o que colocamos na plataforma, que não vem a prever uma cláusula de confidencialidade, nem algo que se pareça, sendo o mais comum, que a própria empresa também não o faça formalmente em relação aos seus trabalhadores[108].

---

[107] ComputerWeekly, *Could your employee's use of ChatGPT put you in breach of GPDR?*, <https://www.computerweekly.com/opinion/Could-your-employees-use-of-ChatGPT-put-you-in-breach-of-GDPR>

[108] KPMG Netherlands, *AI & the impact on trade secrets*, <https://kpmg.com/nl/en/home/insights/2023/06/the-copyright-aspects-of-free-ai-applications/ai-and-the-impact-on-trade-secrets.html>

Os utilizadores do ChatGPT devem tomar consciência de que os dados e informações que partilham com o *software* não serão tratados confidencialmente e poderão ser acedidos e trabalhados pelos programadores da plataforma para treinar e aperfeiçoar o seu sistema. Ao expandir o leque de conteúdo obtido pela ferramenta, este poderá ser utilizado numa nova utilização com outros utilizadores. Para não descartar a possibilidade de a ferramenta sofrer um ataque informático, dada a sua importância e sentido de oportunidade de obtenção de informação sensível, que nunca foi do interesse do utilizador, a sua revelação.

3.2.1 A Questão da Divulgação no ChatGPT

Nos primeiros estágios e findo em 2021, o ChatGPT era treinado com a informação obtida através da interação com os múltiplos utilizadores, o que implicava o armazenamento de todos os dados partilhados por tempo ilimitado. Após 2021, e atualmente, a OpenAI afirma que os dados fornecidos pelos utilizadores já não servem como aprendizagem, mas que, no entanto, estes eram armazenados por 30 dias para o controlo de abuso e utilizações indevidas[109].

Tal não invalida que direta ou indiretamente, a informação que é colocada no ChatGPT deixa de ser privada, levantando-se a questão se: quando partilhamos informação secreta no ChatGPT (e semelhantes plataformas), mas não há utilização dessa informação, estamos na mesma a divulgar um segredo comercial?

Apesar de não ser exigido o segredo absoluto, parece-nos contraproducente na manutenção do segredo, a sua partilha numa ferramenta de IA.

Para considerar que haja divulgação como fator determinante na cessação da proteção de segredos de negócio teremos de atender às circunstâncias de cada caso.

A questão poderá evocar o Paradoxo do Gato de Schrödinger: o segredo comercial quando submetido no ChatGPT está vivo, morto ou na fronteira entre os dois anteriores?[110]

Até que o sistema seja treinado, poderia se considerar que os segredos estão publicamente disponíveis, mas não podem ser visualizados ou divulgados por terceiros. Por conseguinte, poder-se-ia argumentar que os dados inseridos na ferramenta ainda são considerados segredos comerciais.

Mais uma vez, é importante relembrar que não existe nenhuma garantia implícita ou expressa de confidencialidade dos dados fornecidos ao ChatGPT. Pelo contrário, os "Termos de Usos" ditam explicitamente que os dados podem ser utilizados para futuras interações. Para mais, destacam uma cláusula de confidencialidade unilateral ao vincular somente o utilizador, pelo que a contraparte,

[109] Seyfarth, *Spilling Secrets to AI: Does Chatting with ChatGPT Unleash Trade Secret or Invention Disclosure Dilemmas?*, https://www.tradesecretslaw.com/2023/04/articles/intellectual-property/spilling-secrets-to-ai-does-chatting-with-chatgpt-unleash-trade-secret-or-invention-disclosure-dilemmas/.

[110] *Idem*.

ChatGPT, não tem que manter qualquer obrigação para com o utilizador e as informações fornecidas, das quais, conteúdo confidencial das empresas.

Poderia se discutir como seria possível o acesso a esses dados. Na prática, e dada a quantidade de dados no sistema, o terceiro teria de fazer uma questão muito específica ao ChatGPT para este desvendar os dados com uma completude que lhe conferia utilidade. Mas uma vez mais, o conteúdo e o tipo de segredo pode fazer com que o nível de acessibilidade varie, tornando, por exemplo, a receita de um refrigerante popular, facilmente acessível, em comparação a um código de *software*.

Fazendo agora uso da análise anterior da divulgação do segredo comercial *online* (subcapítulo 3.1) e sendo o ChatGPT uma ferramenta deste âmbito, cabe averiguar os termos da divulgação do segredo comercial pela sua transposição no c*hatbot*. Seguimos no sentido de considerar que, em princípio: *(1)* Não se verifica o conhecimento geral nem existe facilidade de acesso ao segredo, pelo que ele mantém o seu valor e é legítimo de proteção jurídica; *(2)* Tendo em conta o conhecimento por parte do círculo subjetivo relevante, este pode ocorrer ou não ocorrer, deixando em aberto para as especificações do caso; *(3)* Pelo teste da teoria da preservação sequencial, parece-nos que o terceiro fator é o que releva maiores questões, com possibilidade de comprometer a proteção do segredo por meio de aplicação desta perspetiva.

Desmitificando cada ponto de análise:

1) Quando há a transposição do segredo comercial de uma empresa para o ChatGPT, não nos parece que, por essa divulgação, haja extinção da proteção do segredo. No sentido que essa divulgação não origina o conhecimento geral público, como também não está em causa a acessibilidade facilitada da informação. Pode-se dizer que quando o segredo é colocado no sistema, a sua divulgação tem apenas valor potencial. Primeiramente, a divulgação que o trabalhador faz ao sistema, está em causa o conhecimento da máquina e no máximo, os gestores ou criadores dela. Num segundo plano, esse segredo pode ser subsequentemente partilhado com outro(s) utilizador(es), que contudo, não é razoável para preenchimento da condição de generalidade. Em terceira hipótese, pode ainda ser partilhada pelos utilizadores alheios ao segredo, mas que o receberam por meio do ChatGPT, e aí sim, a sua atuação pode-se revelar crucial para entender desta condição. Mas por enquanto, no que concerne ao ChatGPT não se pode considerar que haja divulgação geral, pelo que a informação preserva o seu valor como segredo comercial.

2) Pela perspetiva de que o segredo comercial é partilhado com o ChatGPT e este, por sua vez, por correspondência dos seus "Termos e Usos": "*Podemos usar o seu Conteúdo, em todo o mundo, para fornecer, manter, desenvolver e melhorar os nossos Serviços*[111]" armazena-o e usa para futura interação com os demais utilizadores, alheios à titularidade e legitimidade de acesso àquela

[111] OpenAI, Termos de Uso da União Europeia, <https://openai.com/pt-PT/policies/terms-of-use/>

informação. Mas cabe entender a qualidade destes sujeitos, será de maior probabilidade de ocorrência que o segredo seja partilhado se a pessoa fizer uma pergunta específica que recaia sobre o tema que compõe a informação secreta, pelo que há dificuldade em perceber se a pessoa está em condições de entender que se trata de informação confidencial. Em menor ocorrência, pode também se dar a situação em que o utilizador questione diretamente para obter o segredo de negócio de uma dada empresa, aumentando assim a probabilidade de este indivíduo estar ciente do seu secretismo. Ainda pela qualidade do recetor da informação, pode tanto ser um estudante que procurava saber mais para a realização de um trabalho, ou pessoa que detenha conhecimento para entender o conteúdo da informação, e será deste modo que a divulgação em ChatGPT possa ser relevante. Por ser partilhada em segundo momento, com a pessoa que lida habitualmente com aquele tipo de informação e que até possa beneficiar economicamente pela sua apreensão e compreensão.

3) Passando pelos testes da teoria da preservação sequencial desenvolvida por Rowe, começamos por averiguar a relevância do tempo de exposição da informação. Parece-nos, à partida, que assim que a informação é transposta para o ChatGPT, esta é armazenada na sua base de dados, sendo que a atuação por parte do titular deve passar pela ação judicial para que reverta esse facto. Em termos de razoabilidade da rapidez, parece-nos justificado que a ação não precisa de ser tão imediata como seria se estivesse em causa a divulgação numa rede social, no entanto, não confere mínima diligência conhecer do caso e escolher não tomar posição preventiva. Pelo nível de exposição, e como referimos, a comparação com outras plataformas *online* dita que o nível de risco de exposição não é elevado. Não deixando de considerar a existência desse risco, mas a sua exposição não é altamente provável, nem é dada acessibilidade direta ao segredo. De destacar também a relevância da quantidade de informação secreta revelada pelo ChatGPT a pessoas alheias, tema igualmente abordado anteriormente pela causa de divulgação *online* com a qual remetemos aplicação no mesmo sentido. Quanto à condição do destinatário que recebe a informação por via da sua interação com o sistema, será relevante os mesmos termos dos círculos subjetivos relevantes a acrescentar, a hipótese de conhecimento do caráter secreto da informação partilhada pelo ChatGPT, quando a pessoa procura, em especial, chegar à sua compreensão. Caso de um trabalhador concorrente que pretende obter do *chatbot* o segredo de certa empresa, segredo este, que muitas vezes é promovido, no sentido de ser de conhecimento geral, que o sucesso da empresa está dependente dessa informação confidencial, (caso da Coca-Cola, por exemplo), que pode ser o suficiente para elaborar questões específicas com a esperança de que essa informação faça parte do sistema de dados do ChatGPT ou que já tenha sido armazenada pela transposição de algum titular ou trabalhador dessa empresa.

Fica claro, que não existe um teste simples para determinar se algo entrou no domínio público. Como já vimos, o caráter secreto da informação pode ser moldada pelas circunstâncias da situação e

natureza da divulgação e não pelo prisma estanque de que uma informação é exposta *online*. Leva-nos a crer que, apesar da falta de garantia na confidencialidade entre utilizador e ChatGPT, as informações podem permanecer secretas se não forem de conhecimento geral do público[112].

Levando-nos a concluir que o ChatGPT e semelhantes aplicações são sistemas operados por pessoas alheias ao utilizador e às suas informações e dados. Utilizam algoritmos e processos tecnológicos próprios em que se destaca sobretudo o facto de serem desconhecidos ou de difícil compreensão. O que seria uma utilização inocente da mais recente ferramenta de produtividade pode constituir meio para dar origem a ações judiciais graves[113].

3.2.2 Caso da Samsung

A Samsung, seguindo as tendências das restantes empresas mais bem sucedidas mundialmente, estuda e planeia o mercado de forma a escolher melhores investimentos em pesquisa e desenvolvimento.

Não será de estranhar que um dos segredos do sucesso de uma empresa em posição de vantagem no mercado esteja relacionada com a importância de informações internas, como são os segredos de negócio.

Em 2023, a empresa multinacional sul-coreana especializada em telecomunicações e eletrónica, experienciou a perda de segredos comerciais devido a um descuido por parte de funcionários.

A par do observado no mercado empresarial tecnológico, a Samsung autorizou o uso do ChatGPT para a criação melhorada de códigos. Pela sua utilização, os trabalhadores introduziram um código-fonte interno com o objetivo de detetar os problemas que este detinha. Nos seus testes, colocaram código-fonte criado para um novo *software*, portanto, informação secreta da qual a sua divulgação não era interesse da empresa, como titular de um segredo de negócio.

O problema não reside no ato de divulgação da informação secreta no ChatGPT por si só. Torna-se uma divulgação de risco pela forma como o *chatbot* trata os dados que recebe, ou seja, ao armazená-los na sua rede de dados.

De notar também que apenas se verificou a introdução no sistema, não estando em causa para o caso qualquer outro efeito. Por acaso a empresa percebeu o ocorrido, e a maioria dos casos, até

---

[112] Seyfarth, *Spilling Secrets to AI: Does Chatting with ChatGPT Unleash Trade Secret or Invention Disclosure Dilemmas?,* <https://www.tradesecretslaw.com/2023/04/articles/intellectual-property/spilling-secrets-to-ai-does-chatting-with-chatgpt-unleash-trade-secret-or-invention-disclosure-dilemmas/>

[113] Sheppard Mullin, *Mind your audience: Disclosure of confidential information to AI programs can give rise to trade secret misappropriation claims,* <https://www.tradesecretslawblog.com/2024/03/mind-your-audience-disclosure-of-confidential-information-to-ai-programs-can-give-rise-to-trade-secret-misappropriation-claims/>

então, são de índole semelhante, destacando que o risco de divulgação por uso do ChatGPT é menor em comparação a outros meios, mas possível.

Apesar do sucedido, os trabalhadores que agiram não foram especificamente identificados, segundo se sabe estavam na empresa há longos anos, existia uma confiança e lealdade presumida na relação com a entidade empregadora. Pelo que se concluiu pela presunção de divulgação acidental, determinada pelo erro humano. Não dispensando um inquérito interno e medidas disciplinares proporcionais.

A par destas ações, a Samsung estabeleceu que os usos de sistemas generativos de IA seriam expressamente proibidos, estendendo a proibição a computadores, *tablets*, telefones de empresa, bem como em qualquer das suas redes internas[114]. Alertando também que a consequência da falta de comprimento das novas regras resultaria na demissão do trabalhador em incumprimento. Direcionando o seguinte apelo aos trabalhadores: *"Pedimos que vocês sigam diligentemente a nossa diretriz de segurança e a falha em fazê-lo pode resultar em violação ou comprometimento das informações da empresa, resultando em ação disciplinar e incluindo rescisão do contrato de trabalho"*[115].

No entanto, não querendo perder o avanço tecnológico e os benefícios que o ChatGPT traz para o ambiente laboral e empresarial, a empresa desenvolveu as próprias ferramentas internas de IA de objetivo semelhante ao *chatbot* da OpenAI. Com maior enfoque nas tarefas comuns, e de simplificação de processo e poupança de tempo, para a tradução, o resumo de documentos e desenvolvimento de *software*. Ao mesmo tempo, procura desenvolver um mecanismo de filtragem na inserção de informações e dados confidenciais em serviços externos à empresa.

Apesar de não terem sofrido repercussões graves, a empresa não ganhou para o susto. A sua divulgação podia resultar na exposição do conteúdo a pessoas, entidades rivais ou ser usado para a prática de atividades ilícitas. O risco de perder a vantagem competitiva, gerar má reputação e lidar com as consequências legais tornou-se prioridade evitar.

De notar que as circunstâncias ditaram o nível elevado de risco, pelo que falamos de um *chatbot* que era acessível ao público em geral e a um uso desprovido de qualquer regra ou controlo de segurança por parte da empresa.

---

[114] Exame, *Samsung proíbe uso de IA após vazamento de dados com ChatGPT*, <https://exame.com/tecnologia/samsung-proibe-uso-de-ia-apos-vazamento-de-dados-com-chatgpt/>

[115] *Idem*.

3.3. Do Risco

O instituto de proteção de segredos de negócio e os seus riscos ganham novos parâmetros pelo uso do ChatGPT. Os casos de desproteção do segredo comercial por uso do ChatGPT não se enquadram perfeitamente nos conceitos clássicos do direito comercial ou das empresas. O típico culpado num caso de violação de segredos de negócio é um concorrente que se apropriou indevidamente do segredo comercial do queixoso para obter lucros no seu interesse comercial. Um cenário de base, comporta que, nem a pessoa que divulga o segredo comercial, e.g. o trabalhador de uma empresa que partilha a informação objeto de proteção de segredo comercial no ChatGPT, nem o futuro utilizador, sabe que está a receber informação que comporta segredos comerciais[116].

Através do ChatGPT, os segredos comerciais podem se perder sem que seja essa a intenção e, por conseguinte, sem qualquer culpabilidade, deixando a empresa detentora do segredo, sem alguém para imputar responsabilidades. Deste modo, podemos compreender que a parte da intenção de conhecer que alguém está a lesar ou a comprometer o direito de outrem é determinante para averiguar o valor da culpa. Pelo que no cenário descrito e mais frequente não há intenção, nem mesmo conhecimento de que se está perante um segredo de negócio. O seu possível uso e exposição posterior seriam desprovidos de intenção maldosa ou de má-fé.

Observemos o caso *West Technology Group LLC v. Sundstrom*[117], apresentado no Tribunal Distrital de *Connecticut*, o qual realça a importância de tomar medidas preventivas e proativas para salvaguardar os segredos de negócio. A empresa tecnológica processou um antigo trabalhador por apropriação indevida de segredos de negócio e informações confidenciais pelo uso de um programa de IA, o Otter (com equivalente funcionamento ao ChatGPT), para transcrever reuniões privadas. Alegando que utilização deste sistema não era autorizado pela empresa lesada e também, que o registo das informações da reunião foi feito sem o consentimento dos seus participantes, para mais, sustenta que devido ao funcionamento personalizado e histórico de utilização, o ex-trabalhador mantém o acesso a essa informação, mesmo após ter cessado funções na empresa[118]. A empresa

---

[116] León Cosgrove, *ChatGPT: Business use may cause loss of trade secret protections, waiver of privilege, and other harms,* <https://leoncosgrove.com/news/chatgpt-business-use-may-cause-loss-of-trade-secret-protections-waiver-of-privilege-and-other-harms/>

[117] West Technology Group LLC v. Sundstrom – P. 3:24-cv-00178-KAD (02/08/2024), <https://pacer-documents.s3.amazonaws.com/32/157981/04118551595.pdf> E Intellectual Property Center, *Losing Valuable Trade Secret to AI: AI and Trade Secrets Misappropriation: West Technology Group v. Sundstrom Case,* <https://theipcenter.com/2024/03/ai-and-trade-secret-misappropriation/>

[118] Intellectual Property Center, *Losing Valuable Trade Secret to AI: AI and Trade Secrets Misappropriation: West Technology Group v. Sundstrom Case,* <https://theipcenter.com/2024/03/ai-and-trade-secret-misappropriation/>

apresentou queixa por apropriação indevida de segredos comerciais ao abrigo da DTSA e violação de contrato por violação pelo incumprimento de obrigações de confidencialidade.

Apesar da utilização ter sido utilizada para propósitos internos, a sua transposição para sistemas alheios pode dar azo a apropriação de segredos de negócio.

Não só pela situação deste caso há risco de divulgação do segredo comercial, sendo de destacar 5 formas, de tão importante relevo:

1. Partilha não intencional de segredos de negócio – Uma das formas mais comuns de comprometimento do segredo comercial é quando um utilizador partilha, inadvertidamente, informações confidenciais ao ChatGPT por acreditar que é de uso seguro. A empresa tecnológica anunciou que atualmente os modelos de ChatGPT não armazenem por tempo indefinido as informações partilhadas, estas permanecem durante 30 dias para efeitos de histórico e desempenho continuado, mas por contradição, vemos nos "Termos e Usos", que a OpenAI declara que a informação partilhada pode ser utilizada para melhorar a *performance*e, por sua vez, partilhada com outro utilizador. Prevendo possibilidade de ser partilhada autonomamente pelo sistema em novas interações e por ser uma ferramenta gerida por terceiros, que tal como qualquer humano, podem comprometer o caráter secreto da informação no momento posterior à sua transposição para IA.
2. Fuga de dados pelo funcionamento do sistema – Tal como descrito no último ponto, o ChatGPT pode gerar novas respostas em diferentes interações, com pessoas que não a que transpôs a informação para a ferramenta, podendo referir dados sensíveis e informações confidenciais. A este ponto, o modelo já está a inventar coisas pelo padrão do que aprendeu e pelas novas informações que adquiriu como resultado de interações.
3. Ataques de concorrência – deste ponto de vista, pessoas agem de forma maliciosa em favor dos interesses de uma empresa concorrente. Está em causa um uso abusado e manipulado da IA para que se comporte de determinada forma e que gere conteúdos confidenciais de outras empresas do setor. Um verdadeiro teste e erro, se a pessoa souber o que procura.
4. Extração de modelos – trata-se de uma ação de *hackeamento* em que um *hacker* acede a um modelo da ferramenta para criar uma cópia. Estando em risco de ser utilizado para fins prejudiciais, como venda a concorrentes, ou prejudicar o sistema em si, comprometendo ainda mais a sua segurança e a integridade do sistema original.
5. Envenenamento dos dados – no seguimento do anterior, o atacante pode introduzir novos dados no modelo de armazenamento que podem ser nocivos e com o objetivo de influenciar as suas respostas e comportamentos futuros, tais como partilha mais detalhada e repetitiva de segredos de negócio.

3.3.1 Caso da Itália

A 31 de março de 2023, após 10 meses de investigação, a Autoridade para a proteção de dados italiana (doravante GPDP pela sigla italiana) ordenou a imediata suspensão do ChatGPT no país, condicionando o seu retorno se fosse resolvido ou demonstrado como compatível com o Regulamento Geral sobre a Proteção de Dados (doravante RGPD), acusando a OpenAI de violação dos seus artigos 5.º, 6.º, 8.º, 13.º e 25.º.

Levantaram-se questões dada à grande quantidade de dados que eram automaticamente armazenados pelo sistema, tal como, a falta de base legal que justificasse a recolha massiva de dados e o facto de não existirem mecanismos de controlo da idade dos utilizadores, sendo a idade mínima considerada pela autoridade italiana, e que a OpenAI define nos seus "Termos e Usos", os 13 anos.

Uma grande preocupação parte da falta de transparência na informação do modo de funcionamento da ferramenta, ao que a autoridade italiana põe em causa a recolha excessiva dos dados sem que os utilizadores sejam devidamente informados desse processo "natural" de alimentação do sistema.

Este acordo estabelece a implementação de nove medidas por parte da OpenAI para que fossem mitigados os problemas levantados pela autoridade de proteção de dados italiana. Com o acordo fechado entre OpenAI e a autoridade italiana, o ChatGPT voltou a estar disponível ao público italiano sensivelmente um mês após a sua proibição[119].

Em resultado, o *chatbot* passou a comportar um sistema de verificação de idade e tornou possível a opção de impedir que a OpenAI use dados recolhidos das interações para o treino do seu algoritmo. Contudo, não obteve total satisfação por parte das autoridades italianas, pois esta opção de inverter o processo padrão do sistema se alimentar de dados introduzidos pelo utilizador está desligado por defeito, sendo necessária ação por parte do utilizador para reverter a situação, e primeiramente, conhecimento de causa e de modo para o fazer.

Em razão de circunstância, outros países europeus começaram a investigar potenciais violações legais e por sua vez o Conselho Europeu de Proteção de Dados criou uma unidade de trabalho dedicada à cooperação entre Estados-Membros da UE quanto ao uso de plataformas como o ChatGPT e outros sistemas de IA, que abordaremos no subsequente capítulo.

[119] Caiado Guerreiro, *ChatGPT and data protection,* <https://www.caiadoguerreiro.com/en/chatgpt-and-data-protection/>

3.3.2 Mitigar o Risco – Preservação do Valor do Segredo Comercial

Por estes motivos e máxime razão de falta de transparência e segurança verificam-se várias ações de índole governamental por parte de alguns países. Países como Cuba, China, Rússia, Coreia do Norte, Irão, Síria[120] optaram por proibir o ChatGPT. Por um lado, foram motivados pelos riscos de privacidade, por outro, por mero conflito tradicional político por constituir uma ferramenta criada e promovida pelos Estados Unidos da América. Os restantes países, destacando os países europeus, escolheram estudar a situação e seguir pela regulamentação geral da inteligência artificial.

A mitigação do risco associado a estas plataformas só é 100% atingível através da proibição delas, contudo, as empresas não deixam de admitir as vantagens que os sistemas de IA trazem para a sua produção e quotidiano empresarial. Neste sentido, parte da resolução passa por providenciar treino no sentido de educar os trabalhadores para os riscos da utilização de plataformas *online* de inteligência artificial.

Tomar um plano de medidas internas, orientadas para a proteção de informação sensível e prevenção para possíveis *cyber threats*[121], revela ser a melhor ação de manutenção do risco para as empresas que não querem comprometer o seu desenvolvimento tecnológico do ponto de vista competitivo.

À semelhança do acontecimento na empresa sul-coreana Samsung, várias empresas ao longo do globo sofrem ou vão sofrer do mesmo, tomando conhecimento ou não. O acontecimento deixou em alerta o setor tecnológico, tomando conta da importância de proteger segredos de negócio e as potenciais repercussões de não o fazer.

Posta a situação, da qual a Samsung não foi a única a passar por um "abre olhos", um pouco por todos os mercados principais se presenciou preocupações práticas quando à proteção dos segredos de negócio e informações sensíveis. Este incidente destaca a implicação clara para os direitos de propriedade intelectual e de proteção de segredos de negócio no setor empresarial.

Para tal é importante que as empresas adotem medidas eficazes para garantir que os trabalhadores se mantêm em conformidade com os limites empresariais consensuais perante o risco à exposição de segredos comerciais e especialmente às políticas e regras planeadas e operadas por cada entidade empregadora.

---

[120] Think Work, *ChatGPT pelo mundo: entenda banimentos e regulamentações*, <https://thinkworklab.com/transformacao-digital/regulamentacao-chatgpt/>

[121] Ameaça à cibersegurança com intenção de danificar ou roubar dados ou perturbar a vida digital de forma ilícita.

A mitigação dos riscos inerentes ao uso do ChatGPT e ferramentas semelhantes passa por reagir e tomar medidas[122] no sentido de:

1. Desenvolvimento de políticas internas para a proteção de segredos comerciais e informações confidenciais – as empresas devem implementar políticas que passam por um leque de medidas preventivas, tais como controlar acessos, proporcionar a formação contínua dos seus trabalhadores quanto à importância de salvaguardar dados confidenciais e estabelecer regras proibitivas de não transposição de informações secretas para sistemas de IA.

2. Monitorização e auditoria – as empresas podem monitorizar o acesso a segredos comerciais, primeiramente por diminuir o seu círculo de partilha pelo estritamente necessário e criar mecanismos de atuação em situações específicas, como aquando da cessação de funções ou demissão. A auditoria seria relevante para deteção de padrões suspeitos de acesso ou transferência de dados. A revisão regular aos acessos pode ajudar a identificar potenciais infrações.

3. Educar os trabalhadores para o contexto IA – informar e educar os trabalhadores quanto à inteligência artificial, e especialmente para programas potencialmente relevantes para o trabalho do setor em causa, e aqueles que são permitidos e promovidos dentro da empresa. Como também pode passar pela formação no sentido de capacitar os trabalhadores a identificar que informações são sensíveis e as que constituem segredo comercial.

4. Converter o problema em solução – há a possibilidade de as empresas aproveitarem a IA para melhorar os mecanismos de proteção de segredos comerciais. As suas ferramentas de monitorização e detenção de anomalias podem comportar *software* semelhante, mas não comportar tantos riscos[123] se forem de criação e desenvolvimento interno, ou seja, a empresa utilizadora for a empresa que gere o sistema. Deste modo, há a identificação facilitada de atividades irregulares de acesso ou transferência de dados que potencia a intervenção imediata.

5. Plano de ação de medidas corretivas e guia de procedimento judicial – espera-se que as empresas tenham plano de resposta para o incumprimento das medidas ou violação do segredo comercial. Ao se suspeitar de tal, é fundamental que as empresas ajam rápida e prontamente para intentar as ações judiciais, tais como ordens de restrição temporárias e medidas cautelares, ou as medidas internas proporcionais ao caso.

---

[122] Intellectual Property Center, *Losing Valuable Trade Secret to AI: AI and Trade Secrets Misappropriation: West Technology Group v. Sundstrom Case,* <https://theipcenter.com/2024/03/ai-and-trade-secret-misappropriation/>

[123] Há a diminuição de alguns riscos, mas não os elimina por completo. Os riscos externos, como o *hackeamento* dos sistemas, continuam a ser uma preocupação.

CAPÍTULO 4

Os Mecanismos de Proteção e Tutela do Segredo Comercial

Caberá agora fazer a abordagem de vários elementos, cada um de carácter diverso, e que constituem de alguma forma, a proteção e tutela do segredo comercial e da inteligência artificial, procurando, a fim, concretizá-la.

4.1 Das Medidas Razoáveis como Elemento do Instituto

Como já explicado, a proteção do segredo comercial comporta uma dimensão objetiva de existência efetiva de informação secreta, e uma dimensão subjetiva baseada num comportamento ativo, por parte do titular do segredo, em preservar a sua condição sigilosa.

A não observação do requisito de "*medidas razoáveis"* para evitar que o segredo comercial seja facilmente acedido e de conhecimento generalizado, culminará na impossibilidade jurídica de aplicação do instituto de proteção do segredo de negócio.

A sua importância particular surge da necessidade de densificar o conceito de diligências necessárias para a proteção do segredo comercial e que condutas o titular deve observar para proteger o segredo no contexto da Inteligência Artificial, em especial pelo uso do ChatGPT.

Está claro que não se poderá exigir ao titular do segredo comercial que adote todas as medidas de proteção no contexto informático, até porque tal seria impraticável e não será esse o sentido objetivo da lei - alínea c), número 1 do artigo 313.º do CPI. Tal exigência não seria razoável, a inovação tecnológica e informática leva a constatar que não se pode esperar que alguém preveja todos os riscos e todas as formas possíveis de desproteção do segredo comercial, pelo que uma ação de âmbito alargado e orientado para cada ameaça seria um tanto utópica. Deste modo, a exigência normativa não corresponde a uma conduta de cuidado máximo que pudesse prevenir todas e quaisquer situações de ameaça ao segredo de negócio no uso do ChatGPT.

O CPI, no seu artigo 313.º, número 1, alínea c), não traduz uma obrigação de resultado, bastando que o titular demonstre ter atuado de forma diligente para a manutenção da natureza secreta da informação, e que mesmo que não tenha sido bem-sucedido nessa tarefa, se comprove que tenha sido razoável e eficiente dada a exigência da situação concreta.

A necessidade de manter uma conduta vigilante renova o sentido quando se trata de ameaças do plano informático. Segundo CUNDIFF, *"o titular do segredo deve ser vigilante na identificação de*

novas ameaças e na identificação de novos meios digitais para as combater"[124]. Destacando que a falta de proatividade para adotar medidas e decisões empresariais informadas, sem ter em consideração as novas tecnologias, abre caminho para a desproteção jurídica por aplicação do regime dos segredos comerciais.

Para avaliar a diligência exigível é necessário relacionar e conjugar com diversos elementos de modo a observar a circunstância e o caso concreto. Tendo por base o critério da proporcionalidade.

4.1.1 O Acesso ao Segredo

O primeiro objetivo do titular tem por base o princípio da necessidade de acesso[125]. No contexto de proteção de segredos de negócio, traduzir-se-á em restringir o acesso aos segredos ao estritamente necessário, respeitando apenas a pessoas ou grupo de pessoas que, para manutenção da utilidade do segredo enquanto tal, ou que numa perspetiva de proteção, são necessárias tomar conhecimento do mesmo.

Na prática, estamos a referir-nos à adoção de medidas de restrição ao acesso a sistemas, bases de dados ou programas informáticos relevantes para o caso, deixando a conhecimento de pessoas que necessitam dele para a prática de funções torneadas pela informação secreta. A exemplo, quando uma lista de clientes configura um segredo de negócio, esta terá que ser conhecida para a prática laboral de um número específico de trabalhadores. Mesmo dentro deste círculo restrito é esperada a adoção de medidas preventivas, tais como, utilização de sistemas de reconhecimento de *passwords* de atualização periódica ou cartões de identificação, formação contínua e atual ou pela celebração de acordos de confidencialidade. Deste modo, é observado o parâmetro de razoabilidade da proteção. Dentro das fragilidades impostas pela necessidade de operação, criar formas de mitigar a expansão subjetiva do segredo comercial é uma exigência a concretizar.

Por seu turno, não deverá ser considerado razoável tomar medidas de caráter corretivo, como será o caso de celebração de acordos de confidencialidade, sem que sejam tidas em conta medidas preventivas, como a limitação de acesso nas redes informáticas internas da empresa titular de segredos comerciais. No prisma de que ambas as medidas devem operar em simultâneo, a razoabilidade não estará preenchida quando os segredos de negócio são facilmente acessíveis por qualquer pessoa da empresa. Manter o acesso geral, mesmo que interno, compromete a

[124] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 473.
[125] *Idem*, p. 474.

consideração da informação como segredo de negócio, por não se verificar o elemento dinâmico da proteção do segredo[126].

Para mais, e para verificação do critério de razoabilidade, observa-se uma tendência para os tribunais norte-americanos em exigirem algum tipo de *firewall* ou *software* análogo (que, no fundo crie uma barreira digital entre a rede interna da empresa e as redes externas, a exemplo das externas, o ChatGPT), justificando às empresas de maior dimensão exigência desse cuidado, destacando a ideia que as medidas de proteção têm de ser mais amplas e sofisticadas pelo risco mais elevado e frequente de ameaças informáticas, como também por se verificarem interesses concorrenciais mais elevados e vice-versa. Segundo os tribunais norte-americanos, no século XXI é a primordial considerar a proteção do segredo comercial no espaço digital para que o critério da razoabilidade seja considerado preenchido.

4.1.2. Da Divulgação do Segredo

Observando o princípio da necessidade no acesso à informação secreta, segue a necessidade de acautelar a não divulgação do segredo por parte das pessoas ou grupo restrito de pessoas que detêm acesso legítimo a ele.

Neste momento é preciso ter em conta que as medidas razoáveis não estarão a ser tomadas se adotarem-se apenas medidas de controlo de acessibilidade, pois tal pode não bastar para evitar a sua divulgação.

A proteção do segredo perante uma possível divulgação comporta medidas que observem os momentos "*ex ante*, *durante e ex post*"[127].

Primeiramente, antes de ser dado o acesso a qualquer tipo de informação, as empresas podem começar a pôr em prática as medidas de proteção aquando da assinatura do contrato de trabalho,[128] nomeadamente, com os trabalhadores que se inserem no grupo de relevância subjetiva ao acesso das informações confidenciais, densificando o dever de confidencialidade - alínea f) do artigo 128.º do Código do Trabalho (CT), precisamente pela inclusão de cláusulas de confidencialidade[129].

---

[126] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 475.

[127] *Idem*, p. 478.

[128] Tal como contratos de semelhante índole, como serão o caso de contratos de estágio ou contratos de prestação de serviços com entidades externas.

[129] GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 478.

Por sua vez, será igualmente prudente precaver pela proteção do segredo comercial no momento da cessação da relação laboral e adiante. Neste momento, é importante que as empresas procedam com algo conhecido como "entrevistas de *exit*"[130], onde se requer a devolução ou o apagamento de todos os dados e informações relacionadas com os segredos de negócio da empresa. A não observação de atos desta natureza, tem sido considerada pela jurisprudência norte-americana como indício de não adoção de medidas razoáveis.

Passando ao plano em que se verifica a divulgação não autorizada ou em que haja razões razoáveis para crer que tal ocorrência se verifica, é exigido ao titular do segredo, no caso a empresa, que haja imediatamente. Dada a anterior conclusão, que a divulgação nos meios informáticos não implica necessariamente a cessação da proteção do segredo, o titular deve manter a proatividade na manutenção do segredo e expandi-la pela verificação do acontecimento. Podendo considerar como medida mais adequada a solicitação de medidas judiciais cautelares, não só com o objetivo principal de proteger o conteúdo divulgado ou em risco de o ser, como garantir prova de que tomou as diligências que estavam ao seu alcance para preservar o segredo comercial.

Mais que nunca, neste momento da proteção do segredo, a inação, passividade ou demora na adoção de medidas por parte do titular, pode comprometer a aplicação do regime de proteção do segredo comercial. Tais fragilidades podem constituir uma falha na consideração de observação das medidas razoáveis para a proteção.

4.1.3 Planeamento Dinâmico de Segurança e Vigilância

Tomando por base as considerações do tribunal superior de Hamm (Alemanha), deve-se ter em consideração que *"o critério da razoabilidade não é absoluto e estático, mas sim relativo e dinâmico"*[131].

Do ponto de vista de um juízo relacional, estamos a analisar o sentido razoável pela comparação entre o valor económico associado ao segredo comercial e os custos inerentes às medidas adotadas para a sua proteção. De todo o modo, para efeitos de razoabilidade está em causa a proporcionalidade entre ambos, ditando a efetividade quando as medidas são na medida exata do valor do segredo ou superiores a esse valor. De outro modo, se os custos de proteção forem substancialmente insuficientes e inferiores ao valor do segredo, poderá estar em causa a diligência razoável e respetiva relevância jurídica da proteção do segredo comercial.

[130]GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital,* Revista da Faculdade de Direito da Universidade de Lisboa – *Lisbon Law Review*, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022*,* p. 479.

[131] *Idem*, *Op. cit* p. 482.

Do ponto de vista da dimensão dinâmica, o tribunal alemão pretende avultar a necessidade de adotar uma conduta vigilante, a par de uma atualização relacionada com o desenvolvimento tecnológico e os seus impactos.

Pretende-se enfatizar que a proteção do segredo comercial não é algo a ser ponderado num só momento, pois este não pode ser considerado como algo fixo, nem temporalmente, nem juridicamente.

Com isto não se quer só relevar a insuficiência da proteção circunscrito a um determinado período de tempo, mas também a avaliação e desenvolvimento das medidas pela evolução das necessidades. Tomar medidas de proteção apenas durante um tempo ou uma vez, não tem em conta a conduta vigilante e zelosa do titular, muito menos se pode considerar como diligência razoável. A proteção juridicamente exigida é permanente. É necessária a continuidade da proteção com vista o preenchimento do critério das medidas razoáveis. Da perspetiva da evolução das necessidades, é de entendimento simples que os riscos à proteção do segredo comercial podem evoluir. O que são os riscos atuais, não são os riscos de há 20 anos, e nem serão os mesmos riscos daqui a 30 anos. Por outro lado, a evolução em si da empresa titular de segredos de negócio também deve ditar a evolução proporcional das medidas razoáveis à sua proteção, uma empresa média que evolua para empresa de grande dimensão, deve atualizar o seu plano de proteção, e perante este cenário não nos parece diligente manter a atuação de outrora.

É neste mesmo prisma que segue a vigilância dinâmica. A plano de proteção do segredo comercial deve ser aprimorado e estar em constante evolução. Imagine-se que é detetado um novo risco – uma fragilidade potencial, um novo vírus para o qual os programas de segurança da empresa não são capazes de fazer ponto de bloqueio ou se, por outro lado, já sofreu violação de segurança informática por determinado mecanismo – uma fragilidade real, é exigível que o titular haja em conformidade com estes fatores e atualize o seu plano de ação para manter o sentido da atuação diligente e manutenção razoável dos segredos de negócio[132].

Expressão prática desta característica poderá passar por gerar uma cultura empresarial de proteção, através da programação de formações regulares e contínuas no tempo em contexto de segurança e proteção de informação sensíveis especialmente no âmbito tecnológico[133]. Tal será acentuado quando se refere às pessoas com acesso à informação sensível que denota importância subsequente de formar no sentido comportamental em ambientes externos aos da empresa, em cumprimento das funções laborais em viagem ou outras deslocações, como em cumprimento de obrigações laborais em ambientes sociais e que nada tenham a ver com a relação laboral.

[132] GERALDES, João de Oliveira, Sobre a proteção jurídica dos segredos comerciais no espaço digital, Revista da Faculdade de Direito da Universidade de Lisboa – Lisbon Law Review, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022, p. 483.

[133] *Idem*, p. 482.

4.2 A Aplicação do Direito Sem Previsão Legal de IA

O surgimento de avanços e novidades tecnológicas não ditam necessariamente o nascimento de novas questões jurídicas. Muitas se bastaram com a adaptação de regimes já existentes por adaptação da lei. No entanto, a IA não é um desses casos. Segundo BARRETO XAVIER[134] esta diferença deve-se à conjugação de vários fatores, tais como o impacto, risco, opacidade, poder de mercado, deslocalização, relevância geoestratégica, velocidade e evolução.

No que toca ao *(i)* impacto, refere-se à capacidade de afetar a sociedade e a transformar num novo paradigma; *(ii)* o risco, quanto à utilização de sistemas quase autónomos com impacto muito significativo que pode redundar na manifestação de danos na esfera jurídica das pessoas, e mesmo o seu possível uso abusivo para práticas maliciosas; *(iii)* a opacidade, como característica chave de ferramentas de *deep learning* como é o ChatGPT, referindo-se ao efeito *black box* nos sistemas, considerando o não funcionamento do sistema necessariamente da forma como o programador o previu, pelo que a suas decisões e *outputs* não configuram o fim pensado pelo criador, mas sim um resultado de processamento de avultados conteúdos de dados pelas redes de neurónios artificiais sendo difícil de descrever a transparência deste processo; *(iv)* o poder de mercado, no sentido que as empresas criadoras de IA e as que desenvolvem os seus próprios sistemas definem o seu próprio mercado, que por vezes se assemelha a situações de monopólio, que dificultam a aplicação de conceitos tradicionais do direito; *(v)* a deslocalização, dita que não se pode prever uma só jurisdição para regular as questões jurídicas levantadas pela IA, o seu uso global dita uma cooperação mundial no sentido de estabelecer novos mecanismos jurídicos, *(vi)* de relevância geoestratégica, pelos contornos da IA como investimento poderoso pelos países economicamente dominantes que passam a estender o seu uso a outros âmbitos, tais como no setor militar e ambiental e dependem do sucesso e desenvolvimento da IA, e *(vii)* a velocidade da evolução de IA, que é ímpar, e pelo que não se prevê o seu abrandamento, pelo contrário espera-se assistir à sua expansão e consequente melhoramento.

A inteligência artificial, é perspetivada como um reflexo da sociedade e fonte de desafios jurídicos, dado esse facto, está sujeita a constituir objeto de regulamentação legal, a par do que ocorre com grande parte das interações humanas. O direito visa estabelecer os limites da liberdade ao definir direitos e deveres, e ao contemplar a previsão de consequências para a sua violação. Assim, a pergunta central é se devemos estabelecer regras específicas para a inteligência artificial, visto que já há uma panóplia de regulamentações que, de maneira mais geral ou específica, visa a regulamentação das atividades humanas por trás da IA e que se interligam com ela. E saber se o

[134] XAVIER, Luís Barreto, *Notas sobre regulação da inteligência artificial: da ética ao direito*, Católica Talks – Direito e Tecnologia, Universidade Católica Editora, Lisboa, 2021, p. 118.

sistema jurídico atual possui ferramentas suficientes para oferecer um enquadramento legal adequado ao desenvolvimento e à aplicação da inteligência artificial, seja por meio de aplicação direta ou pela integração de lacunas, considerando todo o *corpus* hermenêutico disponível[135].

Segundo NICOLAS PETIT[136] a resposta à questão comporta duas dimensões: *(1)* A dimensão "*legalística*", que procura determinar se o direito atual se pode aplicar à IA ou se de alguma forma a IA se encaixa no direito vigente, a que a resposta será negativa. Os mecanismos jurídicos vigentes são insuficientes para fazer face às particularidades e dimensão da IA, não sendo sempre as normas mais adequadas a aplicar. *(2)* A dimensão tecnológica, que procura determinar as questões despoletadas pela IA que merecem tratamento e regulamentação específica.

De forma prática, imagine-se que estamos a analisar a situação de danos provocados por sistemas de IA, através da dimensão "*legalística*", neste sentido, iremos procurar correspondência legal com o direito vigente, responsabilidade civil ou enquadramento em responsabilidade pelo risco, da qual a dificuldade de compatibilização colocaria a ideia de insuficiência do quadro normativo corrente e necessidade de complemento de um regime especial para IA.

Do ponto de vista tecnológico, procurará analisar as especificidades e características únicas da IA e das questões legalmente relevantes, para tentar construir um regime jurídico que se adeqúe, a partir do entendimento da IA, e das suas várias componentes e responder de modo equilibrado à repartição de risco e ressarcimento de danos[137].

Nas palavras de BARRETO XAVIER "*a relevância e a novidade da IA na atualidade apontam no sentido da conveniência de pensar em regulação a partir da tecnologia existente e da sua aplicação real ou potencial*"[138].

Dada a entender a necessidade de regulamentação especial aplicável a IA, questionamo-nos agora qual o melhor modo de o fazer dado o seu elemento geográfico. Devido à sua proliferação, desenvolvimento e uso global, será viável a criação de legislação nacional por parte de cada país que entenda a sua relevância, ou à semelhança de questões que não respeitam fronteiras, como é o caso das alterações climáticas, é mais viável a celebração de tratados internacionais? Parece-nos que a segunda perspetiva será a mais adequada, contudo ainda não se verificou. No entanto, assiste-se agora ao avanço da União Europeia para a harmonização da regulamentação da IA. Esta proposta a ter aplicação no território dos Estados-Membros da EU, será um meio-termo entre a legislação nacional e mundial.

---

[135] XAVIER, Luís Barreto, *Notas sobre regulação da inteligência artificial: da ética ao direito*, Católica Talks – Direito e Tecnologia, Universidade Católica Editora, Lisboa, 2021, p. 122 e 123.
[136] *Idem*.
[137] *Idem*.
[138] *Idem*.

4.3 AI ACT – Regulamento (UE) 2024/1689 de 13 de Junho de 2024

Nos últimos anos a União Europeia procurou tomar lugar na regulamentação das novas tecnologias e desafios impostos pela inteligência artificial, colocando esta matéria no seu quadro de prioridades.

4.3.1 Enquadramento e Âmbito

Era abril de 2021, quando a Comissão Europeia veio propôs a primeiro quadro regulamentar para a Inteligência Artificial, e em junho de 2023 era publicado no jornal oficial da União Europeia o Regulamento de Inteligência Artificial – Regulamento (UE) 2024/1689, conhecido por AI Act.

Este regulamento é o primeiro instrumento de harmonização de IA no mundo, fornecendo medidas e obrigações sobre específicos usos da IA de modo a regular a autorização destes sistemas no mercado único da UE. Com o objetivo de por fim à fragmentação do mercado interno devido às diferentes leis nacionais, à insegurança jurídica em relação à inteligência artificial e garantir o desenvolvimento e utilização responsável dos sistemas de IA. Orientou-se no sentido da adoção de medidas centradas no ser humano que respeitem princípios de preservação da saúde, segurança, direitos fundamentais, ambiente ou democracia e estado de direito.

E apesar de a sua aplicação se circunscrever apenas aos Estados-Membros da UE, tal como aconteceu com o RGPD, é esperado que influencie o resto do mundo para criar um modelo de regulamentação da IA.

O ato legislativo analisou os desafios e destaca os riscos associados à IA, tais como os enviesamentos de dados, a discriminação e as lacunas legislativas em matéria de responsabilização.

A par da definição de um regime jurídico da IA, promove indiretamente a manutenção do mercado único digital, eliminando os obstáculos de falta de previsão legislativa e consequente aproximação dos utilizadores de sistemas munidos de inteligência artificial.

Como tal visou delimitar o conceito do seu objeto, definindo sistema de inteligência artificial como *"um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais"*[139]. Acrescentando a noção de modelo de base, modelo de treino por uma grande rede de dados, previstos para realização de inúmeros resultados e com possibilidade de

[139] Vieira de Almeida, *Regulamento da Inteligência Artificial – As base da regulamentação na EU*, 2024, *Op. cit* p.24,<https://www.vda.pt/xms/files/05_Publicacoes/2024/Insights/Regulamento_IA_Friendly_version_PT.pdf>

ser adaptado a diferentes tarefas. Culminando numa definição geral de IA, como o *"sistema de IA que pode ser utilizado e adaptado a uma vasta gama de aplicações para as quais não foi intencionalmente nem especificamente concebido"*[140].

O Regulamento comporta uma rede ampla de destinatários, os chamados "operadores de sistemas de IA"[141] que incluem: Fornecedores que coloquem sistemas de IA no mercado ou em serviço na UE[142]; utilizadores no território da UE; fornecedores ou utilizadores localizados fora da União, mas na qual o sistema tem efeito na UE; importadores e exportadores; fabricantes de produtos; representantes autorizados de fornecedores fora da UE e pessoas afetadas no espaço da UE[143].

Procura promover a utilização da IA na União Europeia, garantindo uma proteção que, ao mesmo tempo, fomenta a utilização de IA e estimula o desenvolvimento deste setor tecnológico de modo a que os benefícios superem as dúvidas e derivados prejuízos.

4.3.2 Suporte à Inovação

Um dos objetivos práticos do regulamento passa por atender às necessidades das pequenas e médias empresas (doravante PME), no sentido de diminuir o fardo económico e administrativo dos negócios, e dada a exigência normativa, prevê-se a criação de mecanismos acessíveis de avaliação e testagem em *sandbox* física, digital ou híbrida, ou em ambiente real (sob previsão de requisitos cumulativos), nomeadamente através uma autoridade nacional especializada para o efeito.

A *sandbox* consta na criação de um "ambiente teste" controlado e de tempo limitado, onde fornecedores, ou potenciais fornecedores, podem testar novos sistemas de IA em todas as suas fases, desde a criação, treino, validação, testagem e para treinos de um plano de objetivos de atividades. Este "faz de conta" pretende trazer muitos benefícios como o aumento da segurança, acesso seguro ao mercado, crescente cooperação e exercício de melhores práticas que combina os interesses das autoridades e das empresas.

---

[140] União Europeia, *Proposta de Regulamento da Inteligência Artificial pelo Parlamento europeu e Conselho. Alteração à proposta original* n.º 169, <https://eur-lex.europa.eu/eli/C/2024/506/oj>

[141] Morais Leitão, Galvão Teles, Soares da Silva & Associados. *Regulamento Inteligência Artificial – Pontos-chave*. p. 4, <https://www.mlgts.pt/xms/files/site_2018/guias/2024/Regulamento_Inteligencia_Artificial_-_Pontos-Chave.pdf>

[142] Independentemente da sua localização de origem ser dentro da UE ou fora.

[143] Artigo 2.º do Regulamento (UE) 2024/1689, de 13 de junho de 2024, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL_202401689>

As PME's beneficiam também no sentido de adquirirem prioridade na testagem dos seus sistemas de IA e redução de taxas imputadas após as avaliações de conformidade[144].

4.3.3 Qualificação e Classificação do Risco

A definição do risco através da abordagem da legislativa europeia, comportou uma das prioridades, desde logo, no desenho da Proposta de Regulamento: Para que *"o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deve seguir-se uma abordagem baseada no risco claramente definida. Essa abordagem deve adaptar o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos criados pelos sistemas de IA. Como tal, é necessário proibir determinadas práticas de inteligência artificial, estabelecer requisitos aplicáveis aos sistemas de IA de risco elevado e obrigações para os operadores pertinentes, bem como estabelecer obrigações de transparência para determinados sistemas de IA"*[145].

Claro está que podem sobrar as questões dos riscos práticos inerentes à utilização de IA, tal continua à mercê das discussões casuísticas e estabelecimento lógico e criativo dos jurisconsultos. Contudo, podemos desde já extrair que os riscos práticos serão os que resultam da forma de funcionamento dos sistemas. Qualquer sistema de IA é criado e gerido por seres humanos, deste modo, as suas funcionalidades estarão dependentes do que estas pessoas permitirem.

Deste modo, o espectro de utilização dos sistemas de IA depende de dois fatores: dos dados fornecidos para o alimentar e da sua atualização concreta.

A definição dos níveis de riscos resulta da ponderação da probabilidade de resultarem danos e a complexidade desse dano, do prisma que o risco será aquele que origine um resultado grave, intenso, com probabilidade de ocorrência e efeitos de duração prolongada e a afetação em relação ao lesado[146].

Constituindo-se o quadro regulatório de distinção de IA pelo risco do sistema através de 4 níveis, com correspondência a maior ou menor regulamentação: *(1)* risco inaceitável; *(2)* risco elevado; *(3)* risco limitado; *(4)* risco mínimo[147].

---

[144] Morais Leitão, Galvão Teles, Soares da Silva & Associados. *Regulamento Inteligência Artificial – Pontos-chave*. p. 19, <https://www.mlgts.pt/xms/files/site_2018/guias/2024/Regulamento_Inteligencia_Artificial_-_Pontos-Chave.pdf>

[145] Considerando 14 da Proposta de Regulamento de Inteligência Artificial – versão original, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206>

[146] BOURA, Marta, *Quadro jurídico e reflexões sobre a Proposta de Regulamento da Inteligência Artificial*, Revista Eletrónica de Direito, Lisboa, 2023,p. 118.

[147] Comissão Europeia, *Shaping Europe's digital future: AI Act,* <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

4.3.3.1 Risco Inaceitável e Proibitivo

Estatui a proibição de sistemas de IA que constituem uma ameaça para a sociedade e para as pessoas, pela utilização de métodos intencionalmente maliciosos ou pela exploração de "*vulnerabilidades individuais*"[148]. Como será o caso da identificação biométrica pela captação de imagens faciais da *Internet* ou de CCTV (sistemas de vigilância), tal como os sistemas que armazenem dados de reconhecimento fácil de forma não consentida pelo sujeito em questão ou que atuem através de manipulação cognitivo-comportamental dos utilizadores[149]. Com especial relevância para a ocorrência destes casos quando envolva grupos de pessoas vulneráveis, entenda-se por crianças ou pessoas em situações sociais, ou socioeconómicas frágeis.

O que está em causa é a proibição de sistemas que avaliem ou classifiquem os indivíduos por observação do seu comportamento e características pessoais, que conduzem ao uso dos dados apreendidos em situações diversas e que resultem em tratamentos diferentes, descontextualizados e até mesmo desfavoráveis. Denotando um mero ato desproporcional e injustificado[150].

O uso de mecanismos de identificação biométrica à distância e em tempo real só será permitida se observar-se o cumprimento de certos requisitos, tais como a utilização limitada no tempo e no espaço, a quem se aplica e a aprovação prévia de uma autorização judicial ou administrativa. Casos justificativos para estas exceções pendem de um *"juízo norteado pelo interesse público, um balanço entre potenciais prejuízos a evitar"*[151] podendo ser motivados para salvaguarda de iguais ou outros direitos fundamentais, como pode ser o caso da prevenção a ameaças específicas como a captura de um criminoso, prevenção de ataque terrorista ou busca por desaparecido.

4.3.3.2 Risco Elevado

Sistemas de IA que, devido ao seu alto risco, afetam ou constituem danos potenciais para a saúde, segurança, direitos fundamentais, ambiente ou a democracia e estado de direito.

Discriminando dois tipos de categorias de nível elevado: *(1)* sistemas de IA utilizados em produtos abrangidos pela legislação europeia em matéria de segurança dos produtos, caso de

---

[148] Pplware, *Histórica lei da IA entra hoje em vigor na UE: o que muda?*, <https://pplware.sapo.pt/inteligencia-artificial/historica-lei-da-ia-entra-hoje-em-vigor-na-ue-o-que-muda/amp/>

[149] Parlamento Europeu, *Lei da UE sobre IA: primeira regulamentação de inteligência artificial*, <https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>

[150] Morais Leitão, Galvão Teles, Soares da Silva & Associados. *Regulamento Inteligência Artificial – Pontos-chave*, p. 6, <https://www.mlgts.pt/xms/files/site_2018/guias/2024/Regulamento_Inteligencia_Artificial_-_Pontos-Chave.pdf>

[151] *Idem*, *Op. cit.*

brinquedos, automóveis, dispositivos médicos ou dispositivos aeronáuticos (presentes no Anexo II), e *(2)* sistemas de IA com especificidades que necessitam de registo junto da União Europeia para inclusão na sua base de dados e inclusão no mercado, por meio de uma avaliação de conformidade (Anexo III), estas relacionadas com educação, gestão e funcionamento de infraestruturas, contexto laboral, serviços públicos, contexto jurídico ou de gestão dos serviços de migração[152].

Está previsto um quadro legal complexo e obrigações rigorosas para a sua permanência ou entrada no mercado regulamentado da UE. A complexidade do quadro legislativo para os sistemas de IA de alto risco comporta obrigações para os múltiplos operadores. Dos fornecedores, exige-se a implementação de um sistema de gestão de qualidade, aos distribuidores, exige-se o cumprimento de medidas que permitam a disponibilização dos seus sistemas no mercado ou correção dos que já se encontram disponíveis, aos importadores e utilizadores, exige-se acima de tudo a conformidade das suas atuações e condutas para que se coadjuvam com o Regulamento. Na maior parte dos casos as medidas passam pela colaboração com as autoridades competentes de matéria, a concretização do dever de informação, a aplicação de medidas corretivas, conservação de registos automáticos e conservação de documentos.

No que toca a utilizadores, parece-nos relevante mencionar a qualidade e contexto de atuação de uma empresa a uso dos sistemas no contexto laboral e empresarial, devendo atender a obrigações universais aplicadas a todos os utilizadores: *(i)* a adoção de medidas e meios de supervisão humana conforme as recomendações de uso do fornecedor; *(ii)* o dever de monitorizar o sistema no sentido de acompanhar o seu funcionamento após a comercialização deste, tomando como referência as instruções de uso do fornecedor; *(iii)* dever de comunicação com fornecedor e às autoridades de fiscalização designadas; *(iv)* dever de suspensão de utilização pela identificação de riscos ou ocorrência de algum problema grave; *(v)* deveres gerais de cooperação e colaboração com as autoridades nacionais[153]; conjugando ainda deveres especiais dada a sua qualidade com o utilizador no contexto laboral - *(vi)* o dever de prestar informação aos trabalhadores que fiquem abrangidos por funções que façam uso dos sistemas de IA, antes de se iniciar essa fruição.

Claro que, a par da atuação por parte dos outros intervenientes, podemos mencionar vários níveis de proteção, a partir do momento que a segurança e verificação do cumprimento com a lei reverte em várias fases. De um fornecedor e de um utilizador, ou de um fornecedor para distribuidor para utilizador. No sentido que, qualquer um deles, em qualquer momento do processo pode e deve comunicar com as autoridades quando algo não esteja em conformidade com o plano jurídico

[152] Parlamento Europeu, *Lei da UE sobre IA: primeira regulamentação de inteligência artificial*, <https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>

[153] Artigo 29.º do Regulamento (UE) 2024/1689, de 13 de junho de 2024, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL_202401689>

regulamentar. Na falta de cumprimento ou descuido de um dos intervenientes, o próximo na linha do processo pode dar advertência da situação. Constituindo uma série de testes complexos para a preservação do sistema no mercado.

4.3.3.3 Risco Limitado ou de Finalidade Geral

Os sistemas de IA classificados com risco limitado estão associados a problemas de falta de transparência na sua utilização.

São considerados modelos de uso geral com potencial de colocar riscos inerentes à natureza de sistema que comportam. Então, o ato procura mitigar a questão pela imposição de obrigações orientadas para a informação. Deste modo, o sistema de IA deve informar o utilizador do seu modo de funcionamento e certificar que o conteúdo gerado é identificado como sendo gerado artificialmente. Cabendo, em última instância, ao utilizador, a decisão de avançar ou não com o seu uso. Deverão também se fazer cumprir de requisitos adicionais, como a prévia e contínua avaliação, de atenuar os riscos e comunicar incidentes com utilizadores e organismos de relevância.

4.3.3.4 Risco Mínimo

O risco mínimo comporta a maioria dos sistemas de IA, aqui estão incluídos os mecanismos de *spam* no e-mail e nos videojogos. A este nível o regulamento inibiu-se de associar qualquer medida, pelo que foi feita só a sua classificação, pelo que poderão ser usados normalmente como o são atualmente.

4.3.4 Governação e Quadro Sancionatório

O AI Act prevê não só um pacote de medidas para o desenvolvimento da IA de uma forma transparente e confiável para o utilizador, como veio introduzir o *AI Innovation Package* e *Coordinated Plan on AI*, os três instrumentos operam em conjunto para garantir o respeito pelos direitos fundamentais das pessoas e das empresas nas suas relações com IA.

A complementar, define a avaliação do risco e de *compliance* através de um Certificado Europeu de *Compliance*, e também a designação de uma autoridade reguladora nacional independente para cada um dos 27 Estados-Membros, com vista a supervisão do cumprimento da lei naquele território sob a alçada do Comité Europeu de Inteligência Artificial, como garantia de coerência entre o grupo.

Para tal, estas autoridades podem demandar auditorias, solicitar apresentação de documentação e aplicar medidas corretivas[154].

O Regulamento de IA entrou em vigor no dia 1 de agosto de 2024 e prevê a total aplicação no prazo de 2 anos. A par de outros grandes quadros legislativos, e especialmente, os precursores de novas condutas, comporta uma tolerância - o período de transição. No sentido de proporcionar tempo para aos destinatários da lei se ajustarem à complexidade do que é exigido e cumprirem com a legislação, determinando exceções que configuram um plano de aplicação gradual de certas matérias: - as normas proibitivas devem entrar em efetividade após 6 meses da entrada em vigor da regulamentação; - as regras de governação e as obrigações relativas aos sistemas de IA de uso geral que devem cumprir os requisitos de transparência tornam-se aplicáveis após 12 meses; - regras para sistemas de IA incorporados em produtos regulamentados serão aplicáveis após 36 meses.

O incumprimento resulta em graves sanções, por meio de coimas até 35 milhões de euros ou o valor correspondente a 7% do volume de negócios anual total da empresa geradora de IA, conforme o valor maior. As PME ou empresas em início de atividade (*start-ups*) estão sujeitas a coimas proporcionais[155].

O cumprimento das sanções passa pela criação de um Serviço Europeu para a Inteligência Artificial para desenvolver as valências da UE em relação à IA, passando pela aplicação do quadro normativo do regulamento, e o Comité Europeu para a Inteligência Artificial, integrado por representantes de cada Estado-Membro, peritos independentes especializados e um órgão consultivo com a função de assistir à Comissão Europeia e aos Estados-Membros no esclarecimento e aplicação plena e eficaz do AI Act.

Na vertente nacional, o Regulamento prevê a obrigação para cada Estado-Membro estipular uma autoridade de controlo e uma autoridade de fiscalização do mercado, que em conjunto, sustente a execução do Regulamento. Pode-se considerar que está prevista uma verdadeira *task-force* para a garantia da prática efetiva do AI Act.

4.3.5 E Quanto ao ChatGPT?

No caso do ChatGPT, tipo de inteligência artificial generativa, não será classificado com risco elevado, sendo considerado a nível de risco limitado. Pelo que, aborda a necessidade de cumprir os requisitos de transparência e a legislação europeia em matéria de direitos de autor, no sentido de: *(i)* informar

[154] Pplware, *Histórica lei da IA entra hoje em vigor na UE: o que muda?*, <https://pplware.sapo.pt/inteligencia-artificial/historica-lei-da-ia-entra-hoje-em-vigor-na-ue-o-que-muda/amp/>

[155] Conselho Europeu / Consilium, *Regulamento Inteligência Artificial,* <https://www.consilium.europa.eu/pt/policies/artificial-intelligence/#0>

os utilizadores, de forma clara e explícita, que interagem com um sistema de IA[156]e que o conteúdo foi gerado ou manipulado por IA, de modo a que o seu formato seja legível por outros sistemas e identificável como artificial; *(ii)* programar o sistema de modo a impedir o desenvolvimento de conteúdos ilegais e *(iii)* publicar resumos dos dados protegidos por direitos de autor utilizados para a aprendizagem do sistema[157].

O regulamento previu também a tutela da problemática com a proteção dos direitos de autor e *mining*[158] de textos e dados, determinando que o uso de conteúdo munido de proteção no âmbito da proteção de dados exige a autorização do titular do direito, para a realização do *mining* sobre esse conjunto de dados, em conformidade com o Mercado Único Digital.

Deste modo exige-se que os fornecedores de sistemas de IA: *(1)* preservem e atualizem uma documentação técnica relativa ao modelo de IA; *(2)* preservar, atualizar e disponibilizar a documentação a fornecedores de IA com o interesse de integrar o modelo GPAI no seu sistema; *(3)* elaborar e implementar uma política de acordo com a legislação europeia dos direitos de autor, e *(4)* garantir a transparência pela elaboração e disponibilização pública de uma síntese com detalhe suficiente sobre os dados utilizados para treino do modelo.

"A UE tentou incluir algum equilíbrio entre a proteção de dados e a promoção da inovação e adequar este quadro legislativo ao contexto atual, bastante marcado pela emergência de plataformas como o ChatGPT"[159].

Aguarda-se a plenitude da efetividade do regulamento da União Europeia – AI Act, além dos principais desafios práticos relacionados ao *compliance*. Portanto, é fundamental assegurar que os riscos sejam reconhecidos e que os criadores de IA compactuem e criem sistemas de inteligência artificial que estejam em conformidade com os atuais parâmetros europeus.

4.4 Hipótese Prática: A Violação de Segredo de Negócio Transposto para o ChatGPT

Coloquemos agora o cenário que consideramos ser, a hipótese prática com verificação real provável: Em contexto laboral, o trabalhador de uma grande multinacional com posição de acesso a segredos

---

[156] No mínimo, desde a primeira utilização.

[157] Parlamento Europeu, *EU AI Act: first regulation on artificial intelligence,* <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

[158] *"Mineração de dados é uma técnica assistida por computador usada em análises para processar e explorar grandes conjuntos de dados. Com ferramentas e métodos de mineração de dados, as organizações podem descobrir padrões e relacionamentos ocultos em seus dados*." AWS, *O que é mineração de dados?*, <https://aws.amazon.com/pt/what-is/data-mining/>

[159] O Jornal Económico, *LEI europeia da IA vai "alterar completamente" uso da tecnologia pelas empresas,* <https://jornaleconomico.sapo.pt/noticias/lei-europeia-da-ia-vai-alterar-completamente-uso-da-tecnologia-pelas-empresas/>

de negócio, recorre ao ChatGPT para que este tome por referência o conteúdo partilhado e gere um resumo. Conteúdo este, que comporta um segredo comercial, e que tem ditado o recente sucesso da empresa. Por sua vez, o ChatGPT, para além de executar a tarefa, armazena na sua base de dados esse segredo. Outro utilizador, recorre ao sistema de IA com o objetivo de receber uma informação específica que se adequa com o conteúdo anteriormente transposto, e que possa melhorar o seu próprio negócio sem que tenha alguma intenção ou conhecimento de que se trata de segredo comercial, ou no mínimo, informação confidencial de alguma empresa. Deste modo, o *chatbot* conecta o *input* do utilizador à sua rede de dados, levando o seu algoritmo a configurar uma resposta que contenha a informação adquirida na interação passada.

Cabe agora tentar enquadrar e procurar resposta na natureza jurídica do instituto, pela compreensão da letra da lei e necessária abordagem casuística. Para tal, partimos da aplicação dos 3 principais contributos jurídicos vigentes atualmente: A Diretiva Europeia 2016/943, o Código de Propriedade Industrial e o novo contributo regulamentar para a inteligência artificial, o AI Act.

Partimos da perceção de que o caso comporta três intervenientes*: (1)* o trabalhador do titular do segredo, *(2)* o utilizador alheio[160] e *(3)* o ChatGPT enquanto máquina de IA.

4.4.1 Preenchimento do Instituto de Proteção do Segredo Comercial

Primeiramente, devemos atender à configuração de segredo comercial do número 1.º do artigo 313.º do CPI (por transposição do artigo 2.º da Diretiva), para que a informação confidencial seja valorada como segredo comercial, deve atender os requisitos cumulativos da norma. No caso, podemos considerar que a informação transposta para o ChatGPT cumpre o critério da alínea a), na medida que é uma informação secreta, a qual não geralmente conhecida ou de fácil acesso. O trabalhador tem acesso especial a ela por inerência necessária ao cumprimento das suas funções laborais na empresa titular. Verifica-se também o elemento da alínea b), esta informação comporta um valor comercial e económico para a empresa, que graças a ela ganha uma vantagem competitiva no mercado do setor em que se insere, a que o seu conhecimento público, colocaria fim. No que concerne à alínea c), quanto às diligências razoáveis para salvaguardar a confidencialidade da informação, podemos considerar que a empresa detinha um plano de medidas destinadas a mitigar os riscos de desproteção da informação, e que por imposição geral, em tudo aquilo que não tinham previsto especificamente, os trabalhadores deviam cautela nas condutas que implicavam os dados secretos. Se considerarmos que tal configura medida razoável de proteção, tem se por verificado o facto e podemos assumir que estamos perante um segredo comercial. Se pelo contrário,

[160] Na perspetiva que não tem qualquer relação com o trabalhador, a empresa onde este trabalha, nem quanto ao segredo comercial em causa.

considerarmos ser devido um cuidado preventivo maior por parte da empresa, por exemplo, a proibição de ChatGPT ou manter vigilância do conteúdo partilhado com a ferramenta, temos que considerar que não está já em causa um segredo comercial, pela falta de diligência entendida como possível e necessária por parte do titular que tenha interesse em preservar o secretismo do segredo, pelo que se esvazia do seu valor e se trata apenas de informação com difícil proteção à luz do direito de propriedade industrial, restando apenas a aplicação de mecanismos de sanção ao trabalhador aplicáveis à luz do Código do Trabalho, nomeadamente pela violação do dever geral de lealdade, previsto na alínea f) do número 1.º do artigo 128.º, ou possível acordo de confidencialidade celebrado entre trabalhador e entidade patronal. Para efeitos de continuação desta análise, deixemos a discussão da suficiência de diligência em aberto e seguir pela consideração do segredo comercial para a análise da sua violação.

Focando agora na conduta do trabalhador ao transpor o segredo comercial para a plataforma ChatGPT, poderá se considerar obtenção por parte da máquina? Apesar de não depender diretamente desta, a realidade é que obteve "posse" do segredo. Por aplicação do artigo 314.º do CPI (transposto pelo artigo 4.º da Diretiva), parece-nos difícil encontrar no sentido da lei situação que configure o caso. No máximo, poderia estar em causa, a obtenção do segredo por acesso não autorizado, previsto na alínea a) do número 1.º, contudo, perguntamo-nos retoricamente em que medida se pode considerar que não foi autorizado quando foi o próprio trabalhador a partilhar com a máquina? Em último caso, poderia se discutir que o titular não autorizaria tal ato, derivado das medidas de proteção gerais que poderiam abranger situações destas.

Relativamente ao utilizador alheio podemos colocar novamente em perspetiva o artigo 314.º do CPI, para averiguar se está em causa uma obtenção ilícita do segredo comercial de outro titular. Decerto que o titular do segredo comercial não deu consentimento para a aquisição por parte desta pessoa. Pela alínea a) do número 1, podemos questionar a expressão "*estejam legalmente sob o controlo do titular*", se considerarmos que estamos perante um segredo comercial, pode-se considerar uma atitude juridicamente repreensível, dado que se verifica o acesso e consequente apropriação de materiais que comportam o segredo comercial. Podemos ainda ver se há correspondência mais clara com as hipóteses do número 2, pela alínea a), não nos parece haver correspondência, o utilizador fez uso de uma plataforma disponibilizada ao público geral, que por si só, não implica a prática de algum ilícito, e, por outro lado, o utilizador também não tinha intenção de obter qualquer informação protegida juridicamente a favor de outra pessoa, no caso a empresa enquanto titular. A alínea b) e c) não se aplicam, visto que não está em causa qualquer dever laboral ou acordo confidencial entre o utilizador alheio e a empresa. Ainda atendendo ao sentido do número 3.º do mesmo artigo, na hipótese, é deixada clara a condição de desconhecimento do utilizador em relação à informação que obteve por meio do ChatGPT, para mais, não nos parece razoável a

imposição de dever de conhecer que a informação derivada por interação com um sistema de inteligência artificial, que comporta uma infinitude de dados públicos, seja informação secreta e com valor comercial para uma empresa[161]. Apesar da dúvida em relação à alínea a) do número 1.º do artigo 314.º, é relevante observar a perspetiva de a aquisição e utilização para negócio próprio (sendo o mais provável também estar em causa divulgação) constituir um ato lícito. Neste sentido, o artigo 315.º, que representa transposição do artigo 3.º da Diretiva, configura exceções de proteção ao segredo comercial, por questão de relevância destaca-se a alínea a) e b), a primeira por levantar a questão de se é possível a consideração do que se afigura no caso é uma "*descoberta (…) independente*", se é "*objeto que tenha sido disponibilizado ao público*" ou ainda "*que esteja legalmente na posse do adquirente da informação*". Efetivamente, é dada a possibilidade de se considerar descoberta independente pelo mero acaso, ao que receber tal informação por meio de ChatGPT, sem que houvesse essa intenção, nos parece uma coincidência, já quanto a ser disponibilizado ao público não consideramos que o tenha sido, apesar de transposto para o sistema de IA e para este utilizador, e quem sabe mais utilizadores, ainda não é suficiente para considerar que é informação totalmente pública, para tal clamo à análise anterior sobre a divulgação do segredo comercial em contexto de uso de ChatGPT (ponto 3.2.1 da dissertação), por último, se considerarmos que de facto não houve preenchimento de algum elemento do artigo 314.º podemos considerar a sua confirmação por este elemento do artigo 315.º, determinando que se trata de aquisição, utilização e divulgação lícita.

Compreendemos ainda que deverá ser interessante para a questão, considerar a perspetiva do ChatGPT, enquanto sistema de IA, intermédio desta configuração. Não havendo previsão de tutela penal atribuída ao regime de proteção do segredo comercial, parece-nos que não entra nesta análise a razão de imputabilidade penal da máquina, o desafio jurídico que tem ocupado o legislador nos últimos anos. No entanto, cabe a ressalva de que a ferramenta só está a operar porque houve alguém que a construiu para o efeito, e para tal, os criadores, batizados de "*Fornecedores*" ou "*Prestadores*" pelo AI Act, devem observação de certos deveres que ditam o normal funcionamento do mercado interno europeu e um desenvolvimento de IA responsável. E é por este caminho que queremos apurar se o ChatGPT está em cumprimento com a mais recente regulamentação europeia relativa à inteligência artificial. Como já identificado anteriormente neste estudo, o ChatGPT é classificado com um nível de risco limitado ou de finalidade geral, que se traduz na necessidade de

[161] Caso seja considerada a verificação de aquisição, utilização ou divulgação ilícita está em causa um tipo de concorrência desleal por parte do utilizador do *ChatGPT* – por verificação do da alínea a), do número 1.º, do artigo 311.º do CPI, que por exemplo, tinha intenção de obter o segredo por esta via ou que, no mínimo, tinha conhecimento que lhe tinha sido fornecido um segredo comercial, e que agora escolhe usar para benefício de negócio próprio. Neste sentido, será necessária a conjugação do instituto de proteção do segredo comercial e o instituto de concorrência desleal, que apesar de autónomos, se complementam quando for necessidade do caso.

atender a certos deveres para cobrir os objetivos do regulamento, nomeadamente pelo preenchimento das condições do artigo 51.º do AI Act, e por atribuição de obrigações aos prestadores destes sistemas constantes do artigo 53.º, com destaque para a alínea b), do número 1.º que se traduz no objetivo de aumentar a transparência dos dados utilizados para treino do sistema, aqui incluídos os segredos de negócio, pela disponibilização pública de um resumo suficientemente pormenorizado dos dados utilizados para o treino do algoritmo, "*Embora tendo devidamente em conta a necessidade de proteger os segredos comerciais e as informações comerciais de caráter confidencial, esse resumo deverá, de um modo geral, ser abrangente no seu âmbito de aplicação*"[162], pela previsão da terminação de dados de treino, cria-se a dúvida se aqui se inclui os dados apreendidos após a transferência massiva de dados feita pelos seus criadores, não nos parece que esteja a referir os dados apreendidos durante a sua interação com e pelos utilizadores. Por sua vez, o que concerne a temática de segredos comerciais, o presente artigo faz remissão para o artigo 78.º, que vem estabelecer um dever de confidencialidade respeitante a "*informações e dados obtidos no exercício das suas funções e atividades de modo a proteger (…) os segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte*", contudo isto só respeita às autoridades competentes em razão de cumprimento e fiscalização do Regulamento. Pelo que nenhum dos deveres constantes do Regulamento parece tratar da questão dos segredos comerciais, mas faz-se a ressalva para o dever de cumprir a legislação em matéria de direitos de autor que é considerada nos "Termos e Usos" do ChatGPT, permanecendo a dificuldade de alocar responsabilidade quando envolva segredos de negócio, primeiramente porque, à partida, o ChatGPT não saberá reconhecer por ele próprio que os dados que lhe são fornecidos por utilizadores são segredos de valor comercial. Parece que neste âmbito, se passa a "bola" da responsabilidade para os utilizadores, que são informados e escolhem atuar conforme esses termos.

4.4.2 Medidas Preventivas e Quadro Sancionatório

Entendendo-se que em última instância se considera que se verifica a violação do segredo comercial e por aplicação de tudo o que esteja previsto na Diretiva, mas que não tenha transposição para a lei nacional, advém do artigo 6.º da Diretiva a previsão de que as medidas, procedimentos e vias de reparação devem às condições de "*a) ser justos e equitativos; b) não comportar meios desnecessariamente complexos ou dispendiosos, nem implicar prazos pouco razoáveis ou atrasos sem justificação; e c) serem eficazes e dissuasivos"*. O legislador nacional atendeu a estes elementos, de

[162] Vieira de Almeida, *Regulamento da Inteligência Artificial*, *Op. cit* p. 211, <https://www.vda.pt/xms/files/05_Publicacoes/2024/Insights/Regulamento_IA_Friendly_version_PT.pdf>

modo a constituir um quadro de tutela vasto, pela previsão de providências cautelares, ação de inibição ou ação de cessação, sanções acessórias e previsão de indemnização ao lesado. Em específico:

Providências cautelares – este mecanismo resulta do artigo 345.º do CPI e artigo 10-º da Diretiva europeia, que determina que a violação ou mero receio fundado de que possa existir lesão grave com difícil reparação do segredo comercial, pode ser pedida uma providência provisória com o objetivo de proibir a continuação da violação ou evitar a sua iminência. A sua previsão deve-se à natureza do objeto de violação que exige cautelar o efeito útil de uma ação judicial, que pela urgência e facilidade de lesão do direito, o processo normal constituiria uma demora prejudicial sem possível reparação. Exigindo-se do tribunal tomar consideração do exposto no artigo 354.º do CPI, nomeadamente, os elementos que norteiam segredo comercial em questão. Operada a medida cautelar, cabe ao requerente propor ação de inibição de natureza preventiva (artigo 356.º do CPI) ou a ação de cessação de natureza repressiva[163], que findo o prazo de 30 dias desde o trânsito em julgado da decisão de providência, dá-se a caducidade do ação cautelar, que gere o término do efeito das medidas tomadas – alínea a), número 1.º do artigo 373.º do Código de Processo Civil (CPC). Prevendo-se ainda para qualquer destas ações mencionadas, a possibilidade de aplicação de sanção pecuniária compulsória por via do artigo 829.º A do Código Civil (CC). Para o caso, esta medida será de máxima importância, dado que não há dependência da condição de intenção por parte do agente, podendo ser requerida sempre que haja violação do segredo comercial.

Tutela contraordenacional – segundo o artigo 331.º do CPI, verificando-se a aquisição, utilização ou divulgação ilegal do segredo comercial, pode operar uma tutela contraordenação económica muito grave.

Sanções acessórias – a par da tutela contraordenacional ou judicial, pode ainda operar a sanção acessória, que determina a privação do agente da infração beneficiar do delito e inibir a continuação da violação do segredo comercial. A previsão desta sanção verifica-se pelo artigo 317.º do CPI que descreve taxativamente as medidas possíveis e a forma de atuação no artigo 348.º. A acrescentar que a Diretiva adverte, no considerando 21, à necessidade de ponderação por parte dos tribunais nacionais na avaliação da gravidade e impacto da violação, devendo ter em conta um ponto de vista social, com vista a proteger os segredos de negócio sem que o seu excesso determine entrave ao normal funcionamento do mercado interno. O legislador nacional tentou prever este considerando no número 3.º do artigo 355.º do CPI, por conceder alternativa de pagamento de uma compensação pecuniária razoável e satisfatória ao lesado, pela configuração de que qualquer outra medida

[163] Pela aplicação de alguma destas ações opera uma ação declarativa de condenação, prevista na alínea b), do número 3.º, do artigo 10.º do CPC, pelo que não será meramente provisória como no caso da providência cautelar.

implicava um caráter desproporcional, pela condição de não conhecimento nem dever de conhecer da condição de violação de segredo comercial.

Indemnização – por último, pode ser cumulada com outras medidas, a constituição de uma indemnização, prevista no artigo 347.º do CPI (artigo 14.º da Diretiva). Para se dar a sua aplicação é necessário que o agente da violação aja com dolo, ou seja, tem que ter intenção, conhecimento ou era-lhe exigido que tivesse o conhecimento de que estava a violar o segredo comercial de outrem. De destacar ainda a previsão do número 4 do mesmo artigo, que determina a relevância de danos não patrimoniais causados pela violação do segredo comercial. A típica aplicação deste preceito, resulta do artigo 496.º do CC, mas neste caso estamos a analisar os danos de uma pessoa coletiva, pelo que os danos não poderão ser considerados de índole psicológica, mas pelos "*danos provocados no exercício de uma atividade mercantil configuram-se apenas como diminuição do volume de negócios decorrente do desvio de clientela*"[164] e quando em conjugação com a concorrência desleal, estes danos reportam ao resultado da lesão da reputação económica.

Por sua vez, o artigo 353.º do CPI determina a prescrição da violação do segredo comercial decorridos 5 anos, a contar do momento que o direito de tutela pode ser exercido pelo seu titular.

Ora, parece-nos que, para o caso que consideramos ser o que configura maior probabilidade de ocorrência, a empresa titular do segredo deve procurar agir assim que toma conhecimento da violação através de medidas preventivas, pela requisição de providência cautelar para por fim à violação, seguida de ação de inibição ou de cessação. Caso se considere que houve violação do segredo por parte do utilizador alheio, pode operar também sanção contraordenacional e sanção acessória, mas que sem dolo, não há aplicação de indemnização. No que toca à responsabilidade do trabalhador que, sem intenção, colocou ao segredo em risco, parece-nos mais adequado recorrer aos mecanismos de tutela previstos em Código do Trabalho, nomeadamente sanção disciplinar decorrente dos artigos 328.º e 334.º do CT e conjugação da responsabilidade civil decorrente do artigo 483.º do CC por obrigação de indemnização (artigo 562.º e seguintes do CC).

[164] AMORIM, Ana Clara Azevedo de, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial,* Revista Eletrónica de Direito, Faculdade de Direito da Universidade do Porto, n.º2, vol. 19, junho de 2019, p. 37.

CONCLUSÕES

1. Com a elaboração desta dissertação, explorámos a proteção do segredo comercial num mundo ditado pelo desenvolvimento emergente da inteligência artificial, em especial, quando este é comprometido pelo uso do ChatGPT.
2. O segredo comercial constitui fator determinante para as empresas conquistarem uma posição de vantagem competitiva e económica num mercado cada vez mais exigente e mutável.
3. A difícil tarefa de conceptualizar o segredo comercial ditou um longo caminho de instabilidade no enquadramento jurídico, a que por fim, se observou a concretização em instituto autónomo, fazendo jus às suas características, que apesar da proximidade a outros institutos, merece regulamentação específica.
4. O acordo internacional TRIPS, a Diretiva Europeia 2016/943 e o Código de Propriedade Industrial de 2018 configuram os principais contributos jurídicos para a construção de um quadro de proteção do segredo comercial.
5. A expansão e diversificação do mundo digital, pautada nos últimos anos pela forte afirmação da inteligência artificial no quotidiano da sociedade e no contexto laboral, colocou grandes desafios ao Direito, confrontado com a necessidade de adaptação para garantir a adequação de uma estrutura jurídica que não limite o funcionamento do mercado interno e que vise a maximização do bem-estar humano à luz do Estado de Direito.
6. Os significativos contributos dos sistemas de IA nas mais diversas áreas de atuação, gerou uma crescente aplicação no contexto empresarial e laboral, pelo que se tem assistido ao incentivo por parte das empresas para a transferência de tarefas rotineiras e consideradas mais fáceis para estas ferramentas, restando para o trabalhador as tarefas mais complexas, que carecem de fatores inerentes ao ser humano que a máquina não consegue replicar.
7. O ChatGPT constitui um dos principais sistemas de IA. Caracteriza-se pela sua capacidade de aprendizagem profunda e autónoma, na medida em que o melhoramento do sistema e correspondente algoritmo é feito por meio de interações com utilizadores, ao passo que o processamento de dados configura aprendizagem para a execução de tarefas futuras.
8. Da afirmação e utilização massiva de sistemas de IA, em especial, o ChatGPT, a par das suas variadas vantagens, faz-se ressalva da falta de transparência e segurança dos dados dispostos pelos utilizadores no digital, o que levanta grandes preocupações sobre a proteção de dados, e neles incluídos a partilha inadvertida de informações confidenciais com valor comercial para as empresas.

9. Entendemos que a publicação de informação secreta empresarial *online* é um fator decisivo para averiguar se há divulgação de segredo de negócio. Determinando a cessação da proteção quando a divulgação resulta no conhecimento geral ou é proporcionada a facilidade de acesso à informação secreta. Caso se confirme, a informação deixa de constituir um segredo juridicamente relevante e passa a integrar o domínio público como mera informação.
10. Quando partilhamos informação secreta no ChatGPT e esta não é utilizada, ficamos na dúvida se estamos, ou não, a divulgar um segredo comercial. Consideramos que essa partilha não implica necessariamente a divulgação ao público, nem é dado fácil acesso à informação confidencial. No entanto, embora o conhecimento do círculo subjetivo relevante, possa ou não ocorrer, não nos parece exigível que o titular tome medidas imediatas para reverter a situação, pelo que o nível de exposição associado a este meio é baixo. Por consideração da máquina como recetor do segredo, é difícil compreender a sua posição de conhecimento relativo à natureza secreta da informação. Assim, cremos que o segredo comercial inserido no ChatGPT mantém o valor enquanto informação comercial valiosa.
11. Casos verídicos, como o da Samsung, demonstram o interesse das empresas no aproveitamento dos sistemas de IA, mas também que essa relação de complementaridade cria um risco de desproteção do segredo comercial. Destacando a necessidade de implementar um plano de medidas internas com vista a mitigar o risco de violação dos segredos de negócio.
12. A aplicação prática de medidas internas na empresa atende à primeira medida preventiva contra a violação do segredo comercial, nomeadamente, das medidas razoáveis por parte do titular. Não é exigido o cuidado máximo, mas sim uma a tuação diligente norteada pelo princípio da necessidade e pelo critério relativo e dinâmico da razoabilidade.
13. A União Europeia ofereceu o primeiro instrumento de harmonização de IA no mundo. O AI Act fornece medidas e obrigações sobre os usos específicos da IA, de modo a regular o funcionamento destes sistemas no mercado único da UE, ao mesmo tempo que visa estabelecer suporte à inovação. Destacando o meio de classificação de risco dos vários sistemas de IA e correspondente atribuição de deveres aos seus operadores.
14. Nesta senda, o ChatGPT foi definido com nível de risco limitado ou de finalidade geral, destacando obrigações motivadas pela necessidade de cumprir requisitos de transparência e consideração da legislação europeia em matéria de direitos de autor.
15. Destaca-se a necessidade de interpretar a lei através de avaliação casuística, com vista o preenchimento de lacunas legais, de modo a averiguar a aplicação do instituto de proteção do segredo comercial, e o seu modo de operar, ao se verificar a partilha de segredos de

negócio para o sistema de ChatGPT, o armazenamento automático dos dados e posterior partilha com pessoa alheia.

16. De igual modo, as medidas preventivas e quadro sancionatório deve ser apurado caso a caso, revelando que encontrámos no Direito vigente, meios satisfatórios de tutela face ao trabalhador que transpõe o segredo para o ChatGPT, como para o utilizador alheio que adquire e utiliza o segredo para proveito próprio. Restando a dúvida quanto a possibilidade de tomar ação de remoção do segredo do sistema IA ou responsabilização dos seus fornecedores.
17. O AI Act não vem dar alento à dificuldade de alocar a responsabilidade do ChatGPT como interveniente deste processo. Apesar ser do nosso entendimento que o ChatGPT está em cumprimento com a mais recente regulamentação europeia, esta não prevê qualquer ação relativa a segredos de negócio transpostos para o sistema de IA.
18. Em suma, não podemos considerar que haja efetiva tutela do segredo comercial aquando da violação por meio do uso do ChatGPT. Apesar da tentativa de aplicação do regime jurídico atual, concluímos que mesmo a sua interpretação extensiva, comporta muitas fragilidades para avaliar adequadamente este caso, que se considera complexo pelas várias *nuances* que possa comportar.
19. No futuro, será necessário que o sistema jurídico nacional, europeu e, idealmente, o internacional se dote de ferramentas suficientes para oferecer um quadro legal adequado que abrange as situações de desproteção e possível consequente violação do segredo comercial por meio da utilização do ChatGPT.

REFERÊNCIAS BIBLIOGRÁFICAS

AMORIM, Ana Clara Azevedo de, *O regime jurídico dos segredos comerciais no novo Código da Propriedade Industrial*, Revista Eletrónica de Direito - RED, Faculdade de Direito da Universidade do Porto, n.º2, vol. 19, Junho 2019

ASCENSÃO, José Oliveira de, *Concorrência Desleal*, Almedina, Coimbra, 2002

BOURA, Marta, *Quadro jurídico e reflexões sobre a Proposta de Regulamento da Inteligência Artificial*, Revista Eletrónica de Direito, Lisboa, 2023

FALADE, Polra Victor, *Investigating the security and privacy issues in ChatGPT usage and their impact on organisational and individual security*, International Journal of Scientific Research in Multidisciplinary Studies, Vol. 10, Issue 3, 2024

GERALDES, João de Oliveira, *Sobre a proteção jurídica dos segredos comerciais no espaço digital*, Revista da Faculdade de Direito da Universidade de Lisboa – Lisbon Law Review, Número Temático: Tecnologia e Direito, n.º 1 e 2, 2022

GLORIN, Sebastian, *Privacy and data protection in ChatGPT and other AI chatbots: Strategies for securing user information*, Georgia Institute of Technology, 2023

GONÇALVES, Luís Couto, *Manual de Direito Industrial, Propriedade industrial e Concorrência Desleal*, 7ª Edição, Revista e Atualizada, Almedina, Coimbra, 2017

KIPRUTO, Rickcard Bett, The concept of trade secrets and its effect on economic growth, SSRN, Novembro 2022

LEITÃO, João Pedro, O *Impacto da Inteligência Artificial nos Direitos do Titular de Dados Pessoais: O Caso ChatGPT*, Almedina, 2024

LEITÃO, Luís Menezes, *Concorrência desleal e tutela do interesse público na liberdade de concorrência*, Estudos jurídicos e económicos em homenagem ao Professor Doutor António de Sousa Franco, Vol. 2, Coimbra Editora, 2006

MARQUES, João Paulo Remédio, *Biotecnologia(s) e Propriedade Intelectual*, Vol. II, Almedina, Coimbra, 2007

NUNES, Pedro Miguel Duarte, *A Inteligência Artificial e o direito da Propriedade Intelectual*, Almedina, 2023

SILVA, Nuno Sousa e, *A nova disciplina dos segredos de negócio - análise e sugestões*, Homenagem ao Professor Doutor Germano Marques da Silva, Universidade Católica Editora, 2020

SILVA, Nuno Sousa e, *Proposta de Diretiva em matéria de Segredos de Negócio – Estado e Perspetivas*, Revista de Direito Intelectual, N.º2, 2014

SILVA, Nuno Sousa e, *Quando o segredo é a "alma do negócio" – definição de um conceito*, Revista da Associação Brasileira da Propriedade Intelectual, n.º 126, SET/OUT 2013

SILVA, Nuno Sousa e, *Um retrato do regime português dos segredos de negócio, Seminário – A Proteção Legal de Segredos de Negócio*, Universidade Católica Portuguesa, Porto, 2014

VICENTE, Dário Moura, *A informação como objeto de direitos*, Sociedade da Informação, Revista de Direito Intelectual, n.º1, 2014

VICENTE, Dário Moura, *Código da Propriedade Industrial Anotado*, Almedina, 2021

XAVIER, Luís Barreto, *Notas sobre regulação da inteligência artificial: da ética ao direito*, Católica Talks – Direito e Tecnologia, Universidade Católica Editora, Lisboa, 2021

JURISPRUDÊNCIA

Portugal:

TRC 10.03.2022 - P. 99/21.6YHLSB-A.L1 - Acordão do Tribunal da Relação de Lisboa https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a0ef09be279c9c1b802588290049d96b?OpenDocument

Espanha:

BOE 04.12.2019 - 21.01.20 - https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-873

Estados Unidos da América:

United States of America v Genovese – P. 409 F. Supp. 2d 253 (S.D.N.Y. 2005) - https://casetext.com/case/us-v-genovese-7

Religious Technology Center v. Arnaldo Pagliarina Lerma/Washington Post – P. 908 F. Supp. 1353 (E.D.Va. 29.11.1995) - https://law.justia.com/cases/federal/district-courts/FSupp/908/1353/1457462/

Hurry Family Revocable Tr. v. Frankel – P. 8:18-cv-2869-CEH-CPT (MD Fla. Jan. 3, 2023) - https://casetext.com/case/hurry-family-revocable-tr-v-frankel-5

REFERÊNCIAS WEBGRÁFICAS

Aequitas Victoria Foudation, *Patent vs Trade Secret: Detailed study on Coca-cola brand*, <https://www.aequivic.in/post/patent-vs-trade-secret-detailed-study-on-coca-cola-brand>

AWS, *O que é mineração de dados?*, <https://aws.amazon.com/pt/what-is/data-mining/>

Caiado Guerreiro, *ChatGPT and data protection,* <https://www.caiadoguerreiro.com/en/chatgpt-and-data-protection/>

Comissão Europeia, *Aumentar a confiança numa inteligência artificial centrada no ser humano*, Abril 2019, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52019DC0168>

ComputerWeekly, *Could your employee's use of ChatGPT put you in breach of GPDR?,* <https://www.computerweekly.com/opinion/Could-your-employees-use-of-ChatGPT-put-you-in-breach-of-GDPR>

Conselho Europeu Website / Consilium, *Regulamento Inteligência Artificial*, <https://www.consilium.europa.eu/pt/policies/artificial-intelligence/#0>

CSO, *Coca-Cola trade secret theft underscores importance of insider threat early detection*, <https://www.csoonline.com/article/570561/coca-cola-trade-secret-theft-underscores-importance-of-insider-threat-early-detection.html>

DigEUCit, *Itália e ChatGPT: O Início do Braço de Ferro Entre Estados e Inteligência Artificial?*, <https://direito.up.pt/digeucit/2023/04/24/italia-e-chatgpt-o-inicio-do-braco-de-ferro-entre-estados-e-inteligencia-artificial/>

Equal Ocean, *ChatGPT May Leak Trade Secrets, U.S. FTC Claims to Focus on AI Violations*, <https://equalocean.com/news/2023042019648>

European Comission, *AI Act*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

European Comission, *Shaping Europe's digital future: AI Act*, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

European Parliament, *EU AI Act: first regulation on artificial intelligence*, <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

Exame, *Samsung proíbe uso de IA após vazamento de dados com ChatGPT*, <https://exame.com/tecnologia/samsung-proibe-uso-de-ia-apos-vazamento-de-dados-com-chatgpt/>

FastBots, *Chat GPT for Company Efficiency: Transforming Business Communication*, <https://fastbots.ai/blog/chat-gpt-for-company-efficiency-revolutionising-business-communication>

HÄRTING, *Samsung's ChatGPT Leak: AI Risks in the Workplace*, <https://haerting.de/en/insights/samsungs-chatgpt-leak-ai-risks-in-the-workplace/>

Human Firewall, *A Case Study on Samsung's ChatGPT Incident*, <https://humanfirewall.io/case-study-on-samsungs-chatgpt-incident/>

IBM, *What is the Artificial Intelligence Act of the European Union (EU AI Act)?*, <https://www.ibm.com/topics/eu-ai-act>

Intellectual Property Center, *Losing Valuable Trade Secret to AI: AI and Trade Secrets Misappropriation: West Technology Group v. Sundstrom Case,* <https://theipcenter.com/2024/03/ai-and-trade-secret-misappropriation/>

Jornal de Noticias, *Regras da IA são aplicáveis a partir de fevereiro. Empresas "vão ter de estar" preparadas*, <https://www.jn.pt/4622853185/regras-da-ia-sao-aplicaveis-a-partir-de-fevereiro-empresas-vao-ter-de-estar-preparadas/amp/>

Jornal Público, *Vivemos em plena distopia digital: Será que nos damos conta disso?,* <https://www.publico.pt/2022/07/12/p3/fotogaleria/vivemos-plena-distopia-digital-sera-damos-conta-disso-408412>

KPMG Netherlands, *AI & the impact on trade secrets*, <https://kpmg.com/nl/en/home/insights/2023/06/the-copyright-aspects-of-free-ai-applications/ai-and-the-impact-on-trade-secrets.html>

León Cosgrove, *ChatGPT: Business use may cause loss of trade secret protections, waiver of privilege, and other harms,* <https://leoncosgrove.com/news/chatgpt-business-use-may-cause-loss-of-trade-secret-protections-waiver-of-privilege-and-other-harms/>

Mashable, *Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT,* <https://mashable.com/article/samsung-chatgpt-leak-details?test_uuid=01iI2GpryXngy77uIpA3Y4B&test_variant=a>

Morais Leitão, Galvão Teles, Soares da Silva & Associados, *Regulamento Inteligência Artificial – Pontos-chave*, março 2024, <https://www.mlgts.pt/xms/files/site_2018/guias/2024/Regulamento_Inteligencia_Artificial_-_Pontos-Chave.pdf>

Nova Consumer Lab, *Outro artigo sobre o ChatGPT? O possível futuro dos modelos fundacionais no Regulamento sobre Inteligência Artificial*, <https://novaconsumerlab.novalaw.unl.pt/outro-artigo-sobre-o-chatgpt-o-possivel-futuro-dos-modelos-fundacionais-no-regulamento-sobre-inteligencia-artificial/>

O Jornal Económico, *LEI europeia da IA vai "alterar completamente" uso da tecnologia pelas empresas,* <https://jornaleconomico.sapo.pt/noticias/lei-europeia-da-ia-vai-alterar-completamente-uso-da-tecnologia-pelas-empresas/>

Ordem dos Advogados, Concorrência desleal e direito do consumidor, por PAÚL, Jorge Patrício, <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados/ano-2005/ano-65-vol-i-jun-2005/doutrina/jorge-patricio-paul-concorrencia-desleal-e-direito-do-consumidor-star/>

Parlamento Europeu. *Lei da UE sobre IA: primeira regulamentação de inteligência artificial*, <https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>

Pplware, *Histórica lei da IA entra hoje em vigor na UE: o que muda?*, <https://pplware.sapo.pt/inteligencia-artificial/historica-lei-da-ia-entra-hoje-em-vigor-na-ue-o-que-muda/amp/>

Público, *ChatGPT viola regras de privacidade europeias, conclui regulador Italiano*, <https://www.publico.pt/2024/01/29/tecnologia/noticia/chatgpt-viola-regras-privacidade-europeias-conclui-regulador-italiano-2078552>

Seyfarth, *Spilling Secrets to AI: Does Chatting with ChatGPT Unleash Trade Secret or Invention Disclosure Dilemmas?*, <https://www.tradesecretslaw.com/2023/04/articles/intellectual-property/spilling-secrets-to-ai-does-chatting-with-chatgpt-unleash-trade-secret-or-invention-disclosure-dilemmas/>

Sheppard Mullin, *Mind your audience: Disclosure of confidential information to AI programs can give rise to trade secret misappropriation claims,* <https://www.tradesecretslawblog.com/2024/03/mind-your-audience-disclosure-of-confidential-information-to-ai-programs-can-give-rise-to-trade-secret-misappropriation-claims/>

Sociedades Comerciais, *Entradas em Indústria*, por Mendes, Flávio Mouta, <https://www.sociedadescomerciais.pt/entradas-em-industria/>

Think Work, *ChatGPT pelo mundo: entenda banimentos e regulamentações,* <https://thinkworklab.com/transformacao-digital/regulamentacao-chatgpt/>

União Europeia, *Proposta de Regulamento da Inteligência Artificial pelo Parlamento europeu e Conselho. Alteração à proposta original n.º 169*, <https://eur-lex.europa.eu/eli/C/2024/506/oj>

Vieira de Almeida, *Regulamento da Inteligência Artificial*, <https://www.vda.pt/xms/files/05_Publicacoes/2024/Insights/Regulamento_IA_Friendly_version_PT.pdf>

WIPO, *Artificial Intelligence and IP*, maio 2021 <https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html>