UNIVERSIDADE D
COIMBRA

Miguel Vieira Contente Pratas Costa

A INTELIGÊNCIA ARTIFICIAL E A CRIMINALIDADE EMPRESARIAL

A INFLUÊNCIA DO *CRIMINAL COMPLIANCE* "INTELIGENTE" NA RESPONSABILIDADE PENAL DAS PESSOAS COLETIVAS

Dissertação no âmbito do Mestrado em Ciências Jurídico-Criminais orientada pela Professora Doutora Susana Maria Aires de Sousa e apresentada à Faculdade de Direito da Universidade de Coimbra

julho de 2022

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

A Inteligência Artificial e a Criminalidade Empresarial

A Influência do *Criminal Compliance* "Inteligente" na Responsabilidade Penal das Pessoas Coletivas

Artificial Intelligence and Corporate Crime

The Influence of "Intelligent" *Criminal Compliance* on Corporate Criminal Liability

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra, no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao Grau de Mestre), na Área de Especialização em Ciências Jurídico-Criminais, sob orientação da Professora Doutora Susana Maria Aires de Sousa.

Miguel Vieira Contente Pratas Costa

Coimbra, 2022

Agradecimentos

Em poucas palavras tecer agradecimentos a todos os que os merecem torna-se uma tarefa estranhamente semelhante à exigente responsabilidade que é a escrita de uma Dissertação. Facilmente este caminho se transforma numa solitária viagem que só acompanhada tem algum sentido.

À Exma. Senhora Professora Doutora Susana Aires de Sousa, pela orientação, auxílio, total disponibilidade, acompanhamento ao longo de todo o processo e, principalmente, pelas sugestões e reflexões que o concreto tema impõe.

Aos meus pais e Tomás, pelo chão, teto e paredes (metafóricas e não).

À Sofia, por tudo, todos os dias.

Aos meus avós, que, longe ou perto, são omnipresentes.

Ao "Leviatã", ao "Cardume" e aos restantes facilmente identificáveis amigos que são insubstituíveis e sempre dispostos a discutir e debater etimologia de palavras.

Aos Cóbóis, "velhos" e "novos", por serem Coimbra.

À ELSA Coimbra, pelas oportunidades.

À Faculdade de Direito da Universidade de Coimbra e a todos os seus docentes, por estimular e desenvolver intelectualmente a ânsia do conhecimento e do saber mais.

"(...)
Coimbra de tradições,
Cidade-mãe de doutores
E da velha Universidade;
Fazes vibrar corações
Por tantas recordações,
Numa palavra…és saudade!"

("Avô") Fernando Reis Costa

"Machine intelligence is the last invention
that humanity will ever need to make."
Nick Bostrom

Resumo

Representando a inteligência artificial uma ciência e um setor de inovação disruptivo, a sua utilização consuetudinária é uma questão de tempo. Com grande probabilidade, menos do que todos contamos. Isto porque, as suas capacidades extraordinárias, seguidoras de promessas quase "transhumanistas", consubstanciam já uma realidade presente (e não ficcional) em diversos setores da sociedade. O setor empresarial é, em diversos domínios, palco para este desenvolvimento.

Na presente investigação, apurar-se-á a interligação entre a inteligência artificial e o ambiente empresarial, em concreto, no domínio da prevenção da criminalidade através do *criminal compliance* da empresa (aquilo a que denominamos o *criminal compliance* "inteligente"). Esta interligação não está isenta de riscos, desde logo, pela falibilidade do sistema. A inteligência artificial não é infalível, pelo que esta característica, mas também outras (como a opacidade e inexplicabilidade), fundamentam as dificuldades que o Direito Penal poderá enfrentar caso permita uma introdução desregulada destes sistemas.

Em concreto, questões de responsabilidade penal empresarial emergem diretamente da falha de sistemas de inteligência artificial, tanto substantiva como adjetivamente. Por um lado, em sede de prevenção, questiona-se como é valorada a falha do *criminal compliance* "inteligente" (programado para a prevenção criminal) na responsabilidade penal da pessoa coletiva que comete o crime? Por outro, se o próprio sistema "inteligente" "cometer" um crime, quem responde? Já em sede processual, valerão os dados algorítmicos do *criminal compliance* "inteligente" como prova? Será legítimo atribuirmos uma "igualdade de armas" aos reguladores e titular de ação penal, com a utilização de sistemas de inteligência artificial por parte destes na prossecução das suas funções? Qual deve ser a resposta do legislador para estas questões?

Palavras-chave: Inteligência Artificial; *Compliance*; *Criminal Compliance* "inteligente"; *Machine Learning*; Responsabilidade Penal das Pessoas Coletivas; Direito Penal Económico.

Abstract

With artificial intelligence representing a science and a sector of disruptive innovation, its customary use is only a matter of time. With great probability, less than we all expect. This because its extraordinary capabilities, following almost "transhumanist" promises, are already a current (and non-fictional) reality in several sectors of society. The corporate sector is, in several areas, the stage for this development.

In the present research, the interconnection between artificial intelligence and the corporate environment will be analysed, specifically, in the field of corporate crime prevention through corporation's *criminal compliance* (what we call "intelligent" *criminal compliance*). This interconnection is not risk-free thanks to the fallibility of the system. Artificial intelligence is not infallible, so this characteristic, but also others (such as opacity and inexplicability), underpin the difficulties that Criminal Law may face if it allows an unregulated introduction of these systems.

Specifically, questions of corporate criminal liability emerge directly from the failure of artificial intelligence systems, both substantively and procedurally. On the one hand, in terms of prevention, the question is how is the failure of "intelligent" *criminal compliance* (programmed for criminal prevention) assessed in the criminal liability of the legal person committing the crime? On the other hand, if the "intelligent" system "commits" a crime, who is liable? In procedural terms, will the algorithmic data of the "intelligent" *criminal compliance* be valid as evidence? Is it legitimate to give an "equality of arms" to regulators and prosecutors, with the use of artificial intelligence systems by them in the pursuit of their functions? What should be the legislator's answer to these questions?

Keywords: Artificial Intelligence; *Compliance*; "Intelligent" *Criminal Compliance*; *Machine Learning*; Corporate Criminal Liability; Economic Criminal Law.

Abreviaturas, siglas, símbolos

§ - parágrafo

Ac. – acórdão

AML – Anti-Money Laundering

Apud – citado por

art. – artigo

B2B – business-to-business

Cap. – capítulo

CCO – Chief Compliance Officer

cfr. – confrontar com

colab. – colaboração de

COMPAS – *Correctional Offender Management Profiling for Alternative Sanctions*

coord. – coordenação por

CP – Código Penal

CPP – Código de Processo Penal

EBA – European Banking Authority

Ed. – edição

eds. – editores

e.g. – exempli gratia ("por exemplo")

ENAC – Estratégia Nacional Anticorrupção

et. al. – et alia ("e outros")

FCA – *Financial Conduct Authority*

FinTech – Financial Technology

HFT – High Frequency Trading

i.e. – *id est* ("isto é")

IA – Inteligência Artificial

Ibid. - *Ibidem* (na mesma obra)

Id. – Idem (do mesmo autor)

in – em

Infra - abaixo

IoT – Internet of Things

KYC – Know Your Costumer

KYD – Know Your Data

Loc. cit. – no lugar citado ("na mesma página")

MENAC – Mecanismo Nacional Anticorrupção

n. º - número

OCDE – Organização para a Cooperação e Desenvolvimento Económico

ONU – Organização das Nações Unidas

Op. cit. – obra citada

org. – organizado por

p. – página/páginas

passim – em vários sítios

PBCFT – Prevenção do Branqueamento de Capitais e Financiamento do Terrorismo

PPR – Plano de prevenção de riscos

RegTech – Regulatory Technology

RGPD – Regime Geral de Proteção de Dados

RSC – Responsabilidade Social Corporativa

séc. – século

ss. – seguintes

STJ – Supremo Tribunal de Justiça

STS – Sentencia Tribunal Supremo

Supra - acima

SupTech – Supervisory Technology

TC – Tribunal Constitucional

trad. – traduzido por

v. – versus

Vide – ver

Vol. – volume

XAI – *Explainable AI*

Índice

Introdução: prolegómenos de uma problemática futura

A transição digital é, nos dias que correm, palco de qualquer política estadual. Esta opção é fruto da cada vez mais premente consciência coletiva de que a tecnologia é uma ferramenta que potencia o desenvolvimento económico e social. Exemplo gritante da necessária e inevitável digitalização foi a pandemia da COVID-19 que veio pôr ao descoberto as situações daqueles que, sem acesso às tecnologias, necessitaram destas para trabalhar ou para aprender[1]. Já aqui se concebe a grande dependência da Humanidade nas novas tecnologias. Contudo, esta ideia de recurso a novos instrumentos que facilitem a realização de tarefas, seja na eficiência, no tempo ou nos custos, sempre foi algo presente na comunidade humana e é algo inerente à inovação. Desde logo, com as Revoluções Industriais, a Humanidade evoluiu das leis da termodinâmica para calcular os níveis eficientes de energia para o funcionamento de máquinas a vapor, para as leis do eletromagnetismo que permitiram a criação de produtos eletrónicos, e por conseguinte, para a alta tecnologia com os transístores e *lasers* que permitiram a criação de computadores, *smartphones* e a maioria dos instrumentos eletrónicos existentes atualmente. A última e atual época inovativa, consubstanciando para muitos a "Quarta Revolução Industrial", envolve o desenvolvimento de tecnologias a nível quântico e molecular (nanotecnologia, biotecnologia e inteligência artificial)[2]. Deste modo, factualmente, aqueles que negligenciarem as novas tecnologias correm um risco: o de ficar para trás.

Neste contexto, podemos assumir que a inteligência artificial é um dos pilares desta transição digital[3]. Porém, não é um conceito totalmente novo. A sua evolução tem passado por várias "estações" de forma cíclica, isto é, por fases de menor ou maior investigação e desenvolvimento (o chamado "inverno da IA" ou "*AI winter*" e "verão da IA" ou "*AI summer*", respetivamente). Atualmente, muitos consideram que desde o início do século

[1] Segundo o Mecanismo de Recuperação e Resiliência aprovado pelo Parlamento Europeu para fazer face às dificuldades económicas criadas pela pandemia da COVID-19, os Estados-membros terão de alocar, no mínimo, 20% das verbas que receberem na promoção da transição digital (Portugal irá alocar 3,67 mil milhões de euros nesta matéria).

[2] KAKU, Michio, «3 mind-blowing prediction about the future», *BigThink*, acessível em: https://bigthink.com/the-future/prediction-michio-kaku/

[3] Portugal, por exemplo, em linha com o Plano de Ação da União Europeia, adotou em 2019 a Estratégia Nacional de Inteligência Artificial que visa, até 2030, atingir um conjunto de objetivos para o ensino, investigação, inovação e desenvolvimento de novos produtos e serviços que utilizem inteligência artificial. Cfr. Estratégia Nacional de Inteligência Artificial (AI Portugal 2030), acessível em: https://www.incode2030.gov.pt/ai-portugal--2030

XXI entrámos numa fase de maior evolução da inteligência artificial com o surgimento e exponencial desenvolvimento de novas técnicas, amplitude de setores de aplicação e geral interesse governamental nestes sistemas em função das utilidades prementes. Um longo caminho foi percorrido até hoje: desde a criação de um *software* vencedor de um jogo de xadrez ao campeão mundial, de carros totalmente autónomos, de computadores capazes de vencer concursos televisivos, ou de vencer o ancestral jogo chinês de *Go*, que possui mais combinações que átomos no Universo. Só por aqui se percebe o natural entusiasmo neste setor nos últimos tempos, dada a confluência de tecnologias hoje ao dispor e as correspondentes utilidades no quotidiano da Humanidade.

O plano empresarial é aquele que mais tem sido associado a estas utilidades, pelo que se torna fácil perceber o interesse das pessoas coletivas em produzi-los e/ou utilizá-los. Isto porque «(a) inteligência artificial não ultrapassa a pessoa humana (apenas) no *como* – desde logo, na velocidade de desempenho –, mas no *o quê*, no resultado da atividade»[4]. Ora, o potencial de utilidade da inteligência artificial em contexto empresarial levou a sociedade a pensar na eventual utilização destes sistemas autónomos para a tomada de decisões. Mas será isto desejável? Queremos, nós humanos, atribuir o controlo a uma máquina ou, mais do que isso, perder o controlo?

Na parte que nos toca, importará analisar as situações em que a utilização destes sistemas se dá ao nível da prevenção da criminalidade dentro da empresa, onde o programa de *compliance* é carta de apresentação. É neste contexto que surge a presente investigação. Como se interligarão no futuro os setores da inteligência artificial e do *compliance*? Tecnicamente, se a eficiência e capacidade preditiva são caraterísticas da inteligência artificial, a promessa da sua conjugação com a prevenção criminal poderá tornar a consumação de criminalidade empresarial impossível. Porém, será mesmo assim?[5]

Num primeiro plano, interessará perceber qual a relevância jurídica da inteligência artificial e a sua importância numa perspetiva de vantagens/desvantagens da sua utilização

[4] MAIA, Pedro «*Compliance* Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Revista JULGAR*, n.º 45, Almedina, 2021, p. 187.

[5] SOUSA, Susana Aires de, «Introduction – AI in the economic sector: prevention and responsibility», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. xiv. («The paradox is clear: on one hand, the efficiency and predictive capacity of algorithms make them a tool for compliance and prevention of offences; on the other hand, this capacity of the machine, driven by big data, raises disturbing alarms linked to a progressive transformation of legal and social systems»).

no âmbito empresarial. Do mesmo modo, importará perspetivar o que já existe em sede de prevenção criminal empresarial por forma a aferir se este é um terreno fértil para a implantação destes sistemas. Como tal, releva concretizar conceitualmente ao que nos estamos a referir para que seja possível identificar com pormenor as utilidades práticas da interconexão dos setores, nomeadamente, identificar o que é o *criminal compliance* enquanto mecanismo de autocontrolo, quais as suas funções e efeitos, e também, perceber qual o seu estado no ordenamento jurídico português. Após a materialização das duas realidades, agora sim, é possível assimilar a existência concreta da inteligência artificial no domínio do *criminal compliance.* No entanto, esta relação não está isenta de riscos.

Como em qualquer inovação, a ponderação entre uma maior ou menor disrupção com o *status quo* baseia-se, entre outras, numa ponderação de risco/benefício. E o setor da inteligência artificial é especialmente propenso a riscos em função das próprias caraterísticas dos sistemas que podem conflituar com alguns aspetos da ordem jurídica. Isto é espelhado, aos dias de hoje, nos sistemas "inteligentes" que assumem uma capacidade semelhante à racionalidade humana, reproduzida através de processos matemáticos e deduções lógicas, mas também através de uma capacidade de aprendizagem com base na experiência, conseguindo deduzir e prever resultados (*machine learning*). É através destas capacidades inovadoras que os sistemas possuem um certo grau de "autonomia", o que, por si só, torna possível enxergar a suscetibilidade de lesões de bens jurídicos que decisões não controláveis pelo ser humano podem gerar. Um exemplo ilustrativo deste risco é a utilização de algoritmos de *high frequency trading* (*HFT*), que podem dar lugar a *flash crashes* dos mercados e manipular os preços para a obtenção de ganhos em função deste acontecimento[6]. Por outro lado, «em resultado de uma falha na tecnologia de reconhecimento de objetos, um

[6] Como ocorreu com o *flash crash* de 2010 com a Dow Jones a perder 9% nas suas cotações no espaço de 36 minutos, ou o *flash crash* de 2013 que gerou perdas de cerca de 1% da S&P 500 no espaço de segundos. O prejuízo daqui decorrente gera-se pelo facto de estes mecanismos de transação negocial algorítmica se sustentarem em informações ou notícias (não fazendo distinção entre a veracidade destas). Foi o que aconteceu no *flash crash* de 2013, onde a conta do Twitter da Associated Press foi alvo de um ataque informático, tendo sido publicado um *tweet* acerca de um suposto ataque à Casa Branca e ao Presidente Barack Obama, o que fez com que os mercados instantaneamente reagissem com base assimilação da informação obtida pelos sistemas de *HFT*, que realizaram diversas transações nesse curto espaço de tempo em função da previsão de descida dos mercados. Para mais desenvolvimentos sobre a relevância penal dos sistemas de negociação de alta frequência, RODRIGUES, Anabela Miranda, «Os crimes de abuso de mercado e a "Escada Impossível" de Escher (o Caso do Spoofing)», *Revista JULGAR*, n.º 45, Almedina, 2021, p. 65 – 86; e ainda, MARTINS, Alexandre Soveral, «Algo-trading», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, *passim*, e em concreto p. 52.

automóvel autónomo pode identificar erradamente um objeto na estrada e causar um acidente que causa lesões ou danos materiais»[7].

Ora, tendo em conta estas potenciais lesões, caberá ao Direito Penal tomar a sua voz e tutelar os bens jurídicos em perigo («*ubi lex ibi poena; ubi periculum ibi ius*»[8]). Este perigo advém, principalmente, da imprevisibilidade da tomada da decisão destes sistemas "inteligentes", o normalmente denominado *black box problem*. Uma tomada de decisão diferente da expectável por parte do sistema poderá lesar bens jurídico-penais, o que põe em cheque os atuais modelos de imputação da responsabilidade penal que foram construídos «sobre a atuação de uma pessoa, humana ou jurídica»[9].

É em função deste problema que as maiores interrogações sobre o presente estudo se dispõem. Se um sistema de inteligência artificial integrado no *criminal compliance* de uma empresa, programado para prevenir a criminalidade empresarial, falha, de que forma esta falha releva para a responsabilidade da pessoa coletiva que comete o crime? E se o próprio sistema praticar um crime, quem é responsável? Para além disto, numa vertente processual, poderão os dados gerados através do sistema na realização de diligências internas de *compliance* ser utilizados no processo penal como prova? E se, ao lado das empresas, entidades reguladoras e titular da ação penal começarem, elas próprias, a usar sistemas de inteligência artificial, de que forma poderá uma opção político-social como esta influenciar os direitos fundamentais dos cidadãos? Qual deve ser o papel do legislador em resposta a todas estas questões?

Numa última palavra, caberá mencionar que, ao longo de todo o discurso, reparar-se-á na constante utilização de aspas quando nos referimos à aplicação de termos antropocêntricos a sistemas de IA. Todavia, nem por isso se considera que estes são humanos ou podem subsumir categorias humanas. Termos como "inteligência", "vontade" e "atuação" por parte do algoritmo não se confundem com os mesmos termos levados a cabo por seres humanos. Como tal, parta-se para a discursividade com base numa premissa: sistemas de inteligência artificial são produtos e não "sujeitos". Iniciemos.

---

[7] Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança, Bruxelas, 19.2.2020, COM (2020) 65 final, 2020, p. 13.

[8] Brocardo romano «onde há lei, há pena; onde há perigo há lei». Cfr. MARQUES, Mário Reis, Introdução ao Direito, Vol. I, 2.ª Ed., Almedina, 2012, p. 11.

[9] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial: Vantagens e Desafios à Luz do Direito Penal», *Revista JULGAR*, n. º 45, Almedina, 2021, p. 195.

Capítulo I – A Inteligência Artificial e a Prevenção da Criminalidade Empresarial: uma primeira abordagem

1. A Inteligência Artificial no contexto (da criminalidade) empresarial

1.1. A Inteligência Artificial e a sua relevância jurídica

A juridicidade da inteligência artificial tem-se denotado ao longo dos últimos anos por argumentos percetíveis. Estes são essencialmente de duas índoles: um mais racional, outro mais empírico.

Quanto ao primeiro, releva-se que a *ratio* da inteligência artificial toca em diversos pontos da *ratio* do Direito. Concretamente, a inteligência artificial está inerentemente ligada a problemas metafísicos, à semelhança do Direito. Sendo o Homem um ser social, necessita de inteligência para a comunicação e para se regular em sociedade, cumprindo com a ordem jurídica. O problema metafísico aqui em causa está em saber "o que é a inteligência?" - questão que inquietou diversos pensadores em toda a história da Humanidade. Ora, a relevância desta questão deve-se ao facto de ser a partir dela que uma definição de inteligência artificial é possível.

Já na Antiguidade Clássica (meados do séc. IV a. C.), com Aristóteles, podemos identificar uma primeira idealização daquilo que conceptualmente está por trás da criação do algoritmo – a base dos sistemas de inteligência artificial[10]. Através da lógica aristotélica dos silogismos, baseando-nos em premissas, conseguimos racionalmente deduzir determinadas conclusões. Um sistema de inteligência artificial funciona a partir disto mesmo: através de determinadas premissas (traduzidas em algoritmos) visa-se a obtenção de certo resultado ou conclusão.

Só alguns séculos depois - na década de 50 do séc. XX, com JOHN McCARTHY (para muitos o "pai da inteligência artificial) – se encontra a primeira referência ao termo[11]. Este defendia que a inteligência artificial visa a compreensão da inteligência humana, utilizando para tal sistemas computacionais que atuem de forma análoga aos seres humanos[12]. Segue

[10] Sobre a evolução histórica da inteligência artificial RUSSELL, Stuart / NORVIG, Peter, *Artificial Intelligence: a modern approach*, Third Edition, Pearson, 2016. p. 16 – 28.

[11] Ainda que o primeiro trabalho reconhecido como sendo de inteligência artificial pertença a Warren McCulloch e Walter Pitts em 1943. Cfr. *Ibid.*, p. 16.

[12] McCARTHY, John, *What is AI? / Basic Questions*, University of Standford, 2007, p. 2-3: «is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the

também neste sentido, entre nós e nos atuais dias, ERNESTO COSTA e ANABELA SIMÕES que definem inteligência artificial como «uma disciplina que tem por objetivo o estudo e construção de entidades artificiais com capacidades cognitivas semelhantes às dos seres humanos»[13-14]. Neste prisma, podemos então identificar que a inteligência artificial tem por base a inteligência humana, isto é, visa replicar a inteligência humana em sistemas não humanos ou sintéticos. Não obstante, uma definição de inteligência artificial está longe de ser generalizadamente aceite[15], apesar da atualidade do teste idealizado por Alan Turing em 1950[16] para a aferição da inteligência da máquina. Numa palavra, na senda da JOHN McCARTHY[17], podemos afirmar que a inteligência artificial possui uma dupla função: (1) *compreender* a inteligência humana; (2) *criar* sistemas computorizados inteligentes.

Do que já se disse, muito resumidamente, poderá afirmar-se que um sistema informatizado é inteligente se conseguir interpretar dados, aprender através deles, utilizá-los

similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable».

[13] COSTA, Ernesto / SIMÕES, Anabela, *Inteligência Artificial: fundamentos e aplicações*, 3.ª Ed., FCA Editora, 2008, p. 3.

[14] Em termos de relevância na área, cabe ainda mencionar Stuart J. Russell e Peter Norvig, que conceitualizam uma definição de inteligência artificial espelhada em quatro categorias: duas orientadas no ser humano (*human oriented approach*) e duas centradas na racionalidade (*rationalist approach*), distinguindo-as no âmbito da capacidade para atuar e para pensar/racionalizar. Segundo estes Autores, a contraposição entre "Homem" e "Razão" não pressupõe que o Homem seja irracional, mas antes que o ser humano está sujeito a pressões exógenas, emoções, erros involuntários e à moral, enquanto a Razão corresponde à capacidade abstrata de um pensamento dedutivo. Cfr. RUSSELL, Stuart / NORVIG, Peter, *Op. cit.*, p. 2 – 5. Para uma definição de inteligência artificial ambivalente em termos das suas funcionalidades e da disciplina científica, ver também *The European Commission's High Level Expert Group on Artificial Intelligence*, «A definition of AI: Main capabilities and scientific disciplines», dez. 2018, p. 9.

[15] Como mostra STONE, Peter *et. al.*, *Artificial Intelligence and Life in 2030 - One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford, Stanford University Press, 2016, p. 12, a evolução da ciência da inteligência artificial fez com que constantemente se descortine o chamado "AI Effect", ou seja, a descoberta de uma nova tecnologia faz com que as pessoas se acostumem a ela, deixando de ser considerada inovadora, levando à descoberta de uma nova. Assim, percebe-se a dificuldade de definição de inteligência artificial pela mutabilidade e suscetibilidade para a inovação desta ciência.

[16] TURING, Alan M., «Computing Machinery and Intelligence», *Mind*, Vol. LIX, n. º 236, 1950, p. 433-450, considerava que se o ser humano tendo por base informação que obtém, racionalmente, atua em função dela tendo em vista a solução de um problema, porque não poderiam sistemas computacionais proceder da mesma forma? Para tal, teorizou o denominado *Turing Test* para a aferição da inteligência da máquina, através do que chamou o "jogo da imitação" (*The Imitation Game*), numa tentativa da máquina aprender a imitar o comportamento humano. O *Turing Test*, apesar das críticas de outros autores, consubstancia atualmente um critério para aferir a inteligência da máquina, tendo por base questões que um painel de júris faz a um ser humano e a um sistema computorizado. O objetivo da máquina é enganar os júris através das suas respostas, fazendo-se passar pelo ser humano, por forma a que estes não saibam distinguir o autor da resposta. Prova da eleição deste critério é o Loebner Prize, um prémio anual que condecora os sistemas computorizados que melhor desempenham o *Turing Test*, procurando passá-lo. Nos dias hoje, ainda nenhuma máquina conseguiu passar o teste.

[17] MCCARTHY, John, *Op. cit.*, p. 2

para um determinado fim e criar novos dados com base na prévia aprendizagem[18]. É neste ponto que se parte para o segundo argumento da juridicidade da inteligência artificial, este, de caráter mais empírico.

É no plano da aprendizagem do sistema que, através da experiência, se espoleta a base para toda a problemática jurídica em volta da inteligência artificial. Isto porque é a aprendizagem do sistema que lhe permitirá ter um maior ou menor grau de autonomia e, a partir desta, poderá resultar, no âmbito do fim para o qual o sistema foi programado, um dano, analogamente ao ser humano dotado de inteligência e livre-arbítrio para agir e de o causar.

Em abstrato, a aprendizagem resulta na assimilação de informações e dados para a tomada de uma decisão. E este processo é transversal aos seres humanos, animais ou sistemas computorizados, bastando, numa primeira fase, uma "capacidade cognitiva" para a dedução de uma conclusão através de premissas. Em termos práticos e exemplificativos, ninguém ensina um bebé a andar, estes aprendem porque, através da prática e da queda, passam a conseguir equilibrar-se. Especificamente no âmbito dos sistemas de inteligência artificial, esta aprendizagem denomina-se *machine learning*, que, aliada à *big data*[19] e à *cloud computing*[20], permite uma aprendizagem com maior amplitude e eficácia de resultado.

Nesta perspetiva, existem, pelo menos, três tipos de recursos na promoção e desenvolvimento da inteligência artificial: *knowledge representation* (representação de conhecimento) – diz respeito à tradução para linguagem algorítmica da racionalidade humana, isto é, da forma como os seres humanos pensam questões ontológicas -, *natural*

---

[18] Neste sentido, HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, 1st Ed., Springer, 2015, p. 9, apresenta 5 requisitos que considera expectável um sistema inteligente possuir: (1) comunicação; (2) autoconhecimento ou conhecimento interno; (3) heteroconhecimento ou conhecimento externo; (4) comportamento orientado para um determinado fim; (5) criatividade.

[19] *Big Data* pode ser definido como o ambiente de dados volumoso que permite aos algoritmos a análise e o processamento desses dados no âmbito da sua aprendizagem de forma mais ampla e rápida cfr. EMMANUEL, Isitor / STANIER, Clare, «Defining Big Data» *in Proceedings of the International Conference on Big Dta and Advance Wireless Technologies (BDAW)*, Association for Computing Machinery, New York, Article 5, 2016, p. 1 – 6; noutra perspetiva, RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização» *in A Inteligência Artificial no Direito Penal*, coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 23, carateriza *big data* como sendo o «novo petróleo» para a inteligência artificial no âmbito do que afirma ser a «sociedade algorítmica».

[20] *Cloud Computing* corresponde ao conjunto de serviços e recursos ligados em rede (normalmente *internet*, podendo também ser *intranet*) que permite o armazenamento de dados acessíveis através dessa rede. Neste caso, a *cloud computing* é bastante utilizada na inteligência artificial, pois facilita a aprendizagem (*machine learning*), aumentando o leque de dados acessíveis ao sistema ao ponto de não se limitar ao seu algoritmo, mas aos dados existentes na *cloud*. Em geral, sobre a relação entre *cloud computing* e robótica, DU, Zhihui *et al.*, «Robot cloud: bridging the power of robotics and cloud computing», *Future Generation Computer Systems*, n.º 74, 2017, p. 337 – 348.

language processing (processamento de linguagem natural) – corresponde à capacidade de compreensão de texto e língua (e.g. utilizado em tradutores virtuais, texto preditivo, filtros de *e-mail*) – e, a referida, *machine learning* (aprendizagem automática) – consubstancia a atribuição de capacidade de aprendizagem semelhante à dos seres humanos.

Cada uma destas categorias possui funcionalidades e caraterísticas distintas, sendo muitas vezes combinadas nos sistemas computorizados consoante o fim a que se destinam: a utilização de algoritmos com capacidade interpretativa, de aprendizagem e de correspondência entre padrões que se assemelham à capacidade cognitiva humana (*cognitive computing*) utiliza técnicas de *machine learning* e de *knowledge representation*; a apreensão e leitura de conceitos e a relação entre si integra técnicas de *knowledge representation* e *natural language processing* (*semantic computing*); o reconhecimento, categorização e caraterização de padrões humanos recorre a *machine learning* e *natural language processing* (*perceptual computing*)[21-22]. Em termos esquemáticos, podemos então definir a inteligência artificial como o conjunto de soluções que podem ser obtidas com o recurso a técnicas de *cognitive computing*, *semantic computing* e *perceptual computing*.

Para o propósito que nos serve, tendo por base os perigos que poderão daí advir, a utilização de *machine learning* é o recurso que nos prende mais a atenção. Como tal, existem quatro tipos de aprendizagem automática nos sistemas de inteligência artificial: *reinforcement learning* (aprendizagem de reforço) que consiste no processo de aprendizagem através da tentativa e erro, sem haver um próprio controlo de etiquetas (exemplificando, é o equivalente ao treinamento de um cão, onde este, após a ordem do dono para se sentar, cumpre-a, recebendo um "prémio" – este, no nosso caso, é o *input* positivo ou negativo dado pelo treinador do sistema com base na sua resposta -, para que das próximas vezes em que a ordem for feita, esta seja já automática sem a necessidade do correspondente "prémio"; um outro exemplo de escola é o caso do rato que é posto num labirinto e, chegando ao fim, tem um pedaço de queijo como "prémio" para que, com a experiência e número de

[21] DAVENPORT, Thomas H. / RONANKI, Ranjeev, «Inteligência artificial para o mundo real», *Harvard Business Review*, *in* DAVENPORT, Thomas H. *et al.*, *Inteligência Artificial Análise de Dados e a Nova Era das Máquinas*, Actual Editora, 2021, p. 16 («As aplicações de perceção cognitiva são normalmente usadas para melhorar o desempenho em tarefas que apenas as máquinas podem fazer – como a compra de publicidade programática, que implica o processamento e a automação de dados em alta velocidade -, portanto, não são, em geral, uma ameaça para os empregos humanos»).

[22] Com esta equematização mais desenvolvida, BUTLER, Tom / O'BRIAN, Leona, «Artificial Intelligence for regulatory compliance: Are we there yet?», *Journal of Financial Compliance*, Vol. 3, N.º 1, Henry Stewart Publications, 2019, p. 46 e ss.

vezes que faça o percurso, já o faça de uma forma plenamente eficaz ao ponto de saber que caminho terá que tomar para chegar ao objetivo); *supervised learning* (aprendizagem supervisionada), que consiste no processo de aprendizagem com um controlo de etiquetas, isto é, o supervisor corrige os erros da aprendizagem (por exemplo, o caso dos professores, que transmitem os seus conhecimentos aos seus alunos, corrigindo-os quando erram); *unsupervised learning* (aprendizagem não supervisionada), que consiste no processo de aprendizagem sem haver um controlo de etiquetas (um exemplo prático da utilização desta técnica surge na deteção e prevenção de fraude onde, segundo um conjunto de transações acima de *y*, o sistema emite um aviso ("*red flag"*) para a potencial atividade fraudulenta, servindo essa informação para, mais tarde em futuras transações, assimilar o risco de fraude nas transações correspondentes a valores acima desse *y*); *semi-supervised learning* (semi-aprendizagem supervionada), que diz respeito à combinação de dados pré-definidos e aleatórios para a sua classificação.

No fundo, qualquer técnica de aprendizagem exige a supervisão humana. Ou seja, a principal distinção entre as técnicas apresentadas não é a ausência completa de intervenção humana, mas o grau de intervenção humano, onde a mínima intervenção humana se dá em técnicas de *unsupervised learning* e a máxima intervenção em técnicas de *supervised learning*[23]. De igual modo, a distinção tipológica entre todas técnicas não implica que sejam autonomizadas de um ponto de vista prático, sendo muitas vezes combinadas entre si por forma a desenvolver um sistema de inteligência artificial aprimorado em determinada caraterística. Assim, se existe sempre a intervenção humana, por mais eficazes que estes sistemas sejam, estes estarão sempre sujeitos a erros.

É graças a este facto que se admite que o sistema possa ter uma capacidade preditiva "autónoma" suficiente para produzir determinados resultados não previsíveis nem programados. Ora, é com esta falta de previsibilidade que as preocupações do Direito (e do Direito Penal) começam a surgir. Concretamente, porque os juízos de previsibilidade, especialmente no âmbito da responsabilidade penal, são um elemento essencial para poder fazer responder algum agente pela conduta desvaliosa que praticou. Como afirma ANABELA MIRANDA RODRIGUES, «(u)m processo de tomada de decisão algorítmico é – ou deve ser – o oposto de arbitrariedade, assegurando-lhe – de um ponto de vista teórico

[23] FRIDMAN, Lex, «MIT 6.S091: Introduction to Deep Reinforcement Learning (Deep RL)», 2019, YouTube – Lex Fridman.

– objetividade, acessibilidade e, em último termo, *fairness*». Esta «acessibilidade implica transparência o que não é uma qualidade inerente aos algoritmos»[24].

Outra preocupação do Direito advém opacidade e falta de transparência da decisão (o chamado *black box problem*[25]), onde a introdução dos dados inicial (*input*) pode gerar um *output* diferente do previsto, não sendo possível explicar a razão ou processo de decisão algorítmica (nem pelos seus programadores). Uma razão técnica por detrás deste acontecimento poderá justificar-se na programação inescrutável do sistema através de técnicas de *machine learning*. Por exemplo, através de *deep learning*, que utiliza complexas redes neurais artificiais (*artificial neural networks*[26]) para aprimorar os *outputs* com a conjugação de milhões de camadas de dados[27], ou através de *support vector machine*[28], que apesar da sua pouca complexidade - por apenas categorizar variáveis segundo caraterísticas comuns - implica um acervo vasto de dados inalcançáveis ao cérebro humano[29]. Em concreto, esta inescrutabilidade ocorre porque o sistema adquire dados tendo por base não a solução específica que deve seguir para o problema, mas antes, de forma genérica, como deve atuar quando se depare com um ambiente daquele género, fazendo ele próprio a seleção

[24] RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 25. Também a Comissão Europeia demonstrou as suas preocupações relativamente a este problema no Livro Branco sobre a inteligência artificial, *Op. cit.* p. 13 («(...) as características específicas de muitas tecnologias de IA, incluindo a opacidade («efeito de caixa negra»), a complexidade, a imprevisibilidade e o comportamento parcialmente autónomo, podem dificultar a verificação do cumprimento e prejudicar a aplicação efetiva das regras do direito da UE em vigor destinadas a proteger os direitos fundamentais»).

[25] Esta problema pode ser definido como a incapacidade de compreender o processo de decisão algorítmica e a incapacidade de prever o *output* de um sistema de inteligência artificial. Definição proposta por BATHAEE, Yavar, «The artificial intelligence black box and failure of intent and causation», *Harvard Journal of Law & Technology*, Vol. 31, 2018, p. 905.

[26] SOUSA, Susana Aires de, «Um Direito Penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial» *Revista da Defensoria Pública da União,* n.º 14, 2020, p. 29; e também, ZEDNIK, Carlos, «Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence», *Phiolosophy & Technology*, Vol. 34, 2021, p. 266.

[27] Por todos, DIAMANTIS, Mihailis E., «Vicarious Liability for AI», *in* JOHNSON, Kristin Johnson / REYES, Carla (eds.), *Cambride Handbook of AI and Law*, 2022, University of Iowa Legal Studies Research Paper No. 2021-27, p. 10 e 11; RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 50; SOUSA, Susana Aires de, «"Não fui eu, foi a máquina": teoria do crime responsabilidade e inteligência artificial», *in A Inteligência Artificial no Direito Penal*, coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 68.

[28] Amplamente sobre estas duas técnicas poderem gerar o *black box problem* pela sua complexidade e dimensionalidade, BATHAEE, Yavar, *Op. cit.*, p. 901 e ss.

[29] A doutrina distingue, em geral, três fontes de opacidade: uma opacidade corporativa, onde as empresas deliberadamente optam por não divulgar o processo de formação do algoritmo como segredo de negócio; uma opacidade cognitiva, gerada a partir da iliteracia e inacessibilidade da população em geral em entender o funcionamento e o processo de decisão algorítmica; e uma opacidade técnica, resultante da própria formação algorítmica que impede os próprios programadores de explicar o processo decisório. Aqui, com adicionais fontes bibliográficas, BARBOSA, Mafalda Miranda, «Dos Expert Systems aos Data Systems AI: impacto ao nível da proteção de dados», *Revista JULGAR*, n.º 45, Almedina, 2021, p. 22 e 23.

da melhor resposta para o problema em causa, baseando-se em premissas derivadas da sua experiência[30].

Uma analogia compreensiva possível para este problema da "caixa negra" estabelece-se entre as estruturas cerebrais humanas, que são compostas por redes complexas de neurónios, e os sistemas de inteligência artificial que possuem, também eles, redes neurais eletrónicas – as referidas *artificial neural networks*. Aqui, assim como o processo de decisão humana é (para já) inexplicável, do mesmo modo as redes neurais artificiais procedem a apresentação de um resultado tendo em conta operações de combinação de variáveis imprevisíveis. Deste modo, enquanto biólogos estudam a origem dos erros na replicação do ADN e neurocientistas o processo de decisão humana, os cientistas de dados procuram encontrar uma resposta para a origem e processo das decisões algorítmicas. Como tal, têm tentado criar soluções de explicabilidade da inteligência artificial (*Explainable AI – XAI*[31]), que visam tornar transparente a renderização de decisões de algoritmos, especificamente, respondendo a questões de "o quê", "porquê", "como" e "onde" destas decisões.

Não sendo o propósito entrar em muitas mais tecnicidades, cumpre referir apenas que o comportamento do algoritmo quanto ao "porquê" da decisão diz respeito à ligação que este tem com o ambiente onde se insere[32]. A relevância da autonomização desta questão para o nosso caso centra-se no âmbito da aferição de responsabilidade. Isto porque, perante algoritmos programados através de técnicas de *machine learning* – ou seja, aprendendo tendo por base a experiência - que "atuem" ilicitamente, torna-se necessário explicar em juízo qual a causa para o resultado concreto, para que posteriormente se possa imputar a responsabilidade a um agente. Com efeito, com estas ferramentas de explicabilidade abre-se a porta à resolução do problema da "caixa negra", facilitando o apuramento de responsabilidades. Ainda assim, uma solução como esta não é simples, implicando uma análise casuística do algoritmo em causa, pois a grande maioria das vezes os algoritmos deste género são *strong black boxes*[33].

---

[30] ZEDNIK, Carlos, *Op. cit.*, p. 266.

[31] *Ibid.*, p. 272. Estes processos de explicabilidade vão de encontro às provisões do Regulamento Geral de Proteção de Dados que tutelam o direito à explicação sobre a decisão automatizada. Cfr. BARBOSA, Mafalda Miranda, «Dos Expert Systems aos Data Systems AI: impacto ao nível da proteção de dados», *Op. cit.*, p. 21 e ss.

[32] ZEDNIK, Carlos, *Op. cit.*, p. 273.

[33] A concretização do conceito é possível encontrar em BATHAEE, Yavar, *Op. cit.*, p. 906, que distingue *strong black boxes*, enquanto sistemas onde o processo de decisão é totalmente opaco para o ser humano, de *weak black boxes*, enquanto sistemas opacos, mas possíveis de aplicar determinadas ferramentas de engenharia

De todo o modo, tendo em conta o que se disse até esta parte, a problemática aqui em causa não é totalmente nova. Apesar de estarmos perante produtos ou instrumentos novos, a *ratio* mantém-se. Isto é, a problemática da potencialidade lesiva da inteligência artificial situa-se dentro do fenómeno premente da expansão do Direito Penal e de novas formas de cometimento de crimes[34]. Por isto, dada a envolvência que a inovação potencia, com ela traz também riscos e potenciais lesões de bens jurídicos aos quais tem o Direito Penal a função de tutelar. Para tanto, conclui-se que o argumento empírico da importância da juridicidade da inteligência artificial dispõe-se graças a um claro dualismo que esta assume na esfera penal. Por um lado, num âmbito perverso, para a prática de crimes, por outro, num âmbito preventivo, para o *law enforcement* (isto é, para a regulação das condutas dentro do risco permitido)[35]. Especialmente no ambiente empresarial, as pessoas coletivas, apesar de poderem beneficiar economicamente com a utilização da inteligência artificial no seu quotidiano, não se desvinculam de um conjunto de riscos que não só se mantêm como podem até incrementar com a introdução desta ferramenta[36]. Com efeito, podemos afirmar que a inteligência artificial se relaciona com o Direito Penal numa perspetiva de direta proporcionalidade: a evolução da inteligência artificial é (e deve ser) acompanhada da intervenção do Direito Penal, fazendo, ainda assim, cumprir os princípios que o balizam.

Em síntese, a relevância da juridicidade da inteligência artificial a que nos referimos diz respeito aos potenciais obstáculos que uma realidade artificial poderá trazer para uma dogmática primordialmente antropocêntrica. Contudo, com isto não se considera a

---

reversa (a denominada *backpropagation*) para se perceber a origem e o processo de decisão, prevendo decisões futuras semelhantes.

[34] LIN, Tom C.W., «Compliance, Technology, and Modern Finance», *Brooklyn Journal of Corporate Financial & Commercial Law*, Vol. 11, Issue 1, Art. 6, 2016, p. 172 («Many significant crimes and aggressions against financial firms now involve computer as the weapons of choice and cyberspace as the preferred crime scene. The robber with a gun has been replaced by the hacker with a laptop»); SIMMLER, Monika / MARKWALDER, Nora Mark, «Guilty Robots? – rethinking the nature of culpability and legal personhood in an age of artificial intelligence», *Criminal Law Forum*, n. º 30, 2019, p. 3 e ss.

[35] PAGALLO, Ugo / QUATTROCOLO, Serena, «The impact of AI on criminal law, and its twofold procedures» *in Research Handbook on the Law of Artificial Intelligence*, Cheltenham, UK: Edward Elgar Publishing, Chapter 14, 2018, p. 386.

[36] DIAMANTIS, Mihailis E., «The Extended Corporate Mind: When Corporations use AI to Break the Law», *North Carolina Law Review*, Vol. 98, N. º 4/6, 2020, p. 896 («Algorithms promise to make corporations more efficient and (perhaps) more objective, but they do not remove (or even always reduce) the possibility that things will sometimes go awry»). Também, RODRIGUES, Anabela Miranda, «The Last Cocktail – Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence» *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dez. de 2021, p. 127 («The introduction of AI into business activity introduces new difficulties to the difficulties already known from the models of imputation to legal persons, through both individual and collective individuals»).

dispensabilidade da inteligência artificial. Situamo-nos, por outro lado, no lado otimista e agregador do problema. Desde logo pois a evolução parte da rutura com o *status quo*, passando sempre por um período de transição ao qual, no nosso caso específico, deve o Direito Penal acompanhar e moldar-se envolta desta nova realidade.

1.2. O algoritmo empresarial: riscos e benefícios do uso da Inteligência Artificial no âmbito empresarial

Para além da factual e necessária regulação da inteligência artificial, há concretos aspetos que fazem com que esta seja a tecnologia e realidade do futuro.

A (aparente) invisibilidade algorítmica poderia iludir-nos na sua inexistência. Facto é que a inteligência artificial está presente na vida humana e permite uma nova variedade de funções que podem auxiliar a sociedade nas mais diversas áreas: na geolocalização (sistemas de GPS), no reconhecimento facial e de voz, na conceção de créditos bancários, na área da saúde com a utilização de robôs auxiliadores em contexto cirúrgico, no recrutamento de emprego e avaliação laboral, na condução de veículos, na publicidade digital direcionada, na avaliação e gestão de risco empresarial (*risk assessment*) mas também, tão ou mais importante para nós, no cumprimento normativo (*compliance*)[37]. Numa palavra, importa enaltecer que as utilizações destes algoritmos não consubstanciam uma total substituição do Homem (para receio de muitos), mas antes um complemento à vida em sociedade por forma a facilitar o quotidiano. Até porque a elevada capacidade de eficácia, eficiência, rapidez de previsão e medição do risco dos sistemas "inteligentes" ultrapassa já a capacidade humana (apesar de ainda haver certamente espaço para maiores desenvolvimentos)[38]. Contudo, isto

[37] Sobre as funcionalidades e utilização da inteligência artificial em diversas áreas (transporte, robôs de serviço, saúde, educação, solidariedade social, segurança, emprego e local de trabalho, entretenimento), STONE, Peter *et. al.*, *Op. cit.*, p. 18 – 40. Ou, especificamente na interligação entre o Direito Penal e a inteligência artificial, ver SOUSA, Susana Aires de, «Um Direito Penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial», *Op. cit.*, p. 21 – 37; e também, PAGALLO, Ugo / QUATTROCOLO, Serena, *Op. cit.*, p. 385 – 409.

[38] Todavia, podemos afirmar que vivemos atualmente numa época de inteligência artificial fraca (*weak AI* ou *narrow AI*), no sentido em as funcionalidades disponíveis pelos atuais sistemas de inteligência artificial possuem uma capacidade limitada de tarefas (e.g. reconhecimento facial e de voz, assistentes virtuais, motores de busca, carros autónomos etc.). Esta distingue-se da inteligência artificial forte (*strong AI* ou *artificial general intelligence*), que se carateriza pela replicação daquilo que a inteligência humana é capaz. Cfr. COSTA, Ernesto / SIMÕES, Anabela, *Op. cit.* p. 4. Alguns autores falam ainda da superinteligência, que se carateriza por ultrapassar a capacidade humana, cfr. BOSTROM, Nick, «What happens when our computers get smarter that we are?», TED Talks, 27. abr. 2015; também, BUTLER, Tom / O'BRIAN, Leona, «Artificial Intelligence for regulatory compliance: Are we there yet?», *Op. cit.*, p. 46, onde se mostra que o que chamamos hoje "inteligência artificial" não consubstancia estritamente uma "inteligência" já que vivemos numa realidade de inteligência artificial fraca que será difícil de ultrapassar a curto-médio prazo.

não significa que a capacidade humana seja dispensável. Por outro lado, é certamente benéfica a conjugação entre as diversas capacidades humanas com as potencialidades dos sistemas "inteligentes" (falando-se hoje de uma inteligência aumentada)[39].

Esta ideia não é propriamente nova. Historicamente, o Homem sempre procurou a encontrar formas de eficiência aliada à eficácia nos seus objetivos, para que com uma diminuição ou manutenção do seu trabalho pudesse ter os mesmos ou mais benefícios ou lucros. É com base nesta premissa que as grandes invenções surgem. O esplendor máximo desta inovação e evolução decorre das Revoluções Industriais, que vieram agora desaguar na inteligência artificial e naquela que já muitos chamam a "Quarta Revolução Industrial", onde, para além dos próprios sistemas terem uma capacidade praticamente autónoma e sem necessidade de intervenção humana, comunicam entre si em rede (*Internet of Things – IoT*)[40].

Já na Primeira Revolução Industrial podemos identificar nas grandes fábricas as primeiras máquinas automatizadas que, apesar de não possuírem qualquer tipo de algoritmo como fonte para a sua automação, eram, de facto, autónomas. Foi apenas com o desenvolver de novas tecnologias e com a transição mecânico-digital que se permitiu a inclusão num autómato, que antes tinha por fonte um agente natural (vento, energia, força gravitacional ou outras forças motrizes), um "agente sintético" (o algoritmo – figurado através de *softwares* ou, mecanicamente, através de robôs). É como uma espécie de "código genético" destas máquinas que os algoritmos, enquanto conjunto de dados que tipificam as ações a realizar pelo sistema, se incluem neste âmbito[41]. Aqui, podemos ter sistemas mais ou menos desenvolvidos, com maior ou menor capacidade de aprendizagem e, consequentemente,

---

[39] Falando no conceito de inteligência aumentada como instrumento de cooperação entre a inteligência artificial e a inteligência humana, ZHENG, Nan-ning, *et al.*, «Hybrid-augmented intelligence: collaboration and cognition», *Frontiers Information Technology & Electronic Engineering*, n.º 18**,** 2017, p. 154 («Intelligent machines have become the intimate companions of humans, where the interaction and cooperation between a human and an intelligent machine will become integral in the formation of our future society»). Também neste sentido da futura cooperação, STONE, Peter *et. al.*, *Op. cit.*, p. 9: «(…) the field of AI is shifting toward building intelligent systems that can collaborate effectively with people, including creative ways to develop interactive and scalable ways for people to teach robots». Também, WILSON, H. James / DAUGHERTY, Paul R., «Inteligência colaborativa: seres humanos e IA estão a unir forças», *Harvard Business Review*, *in* DAVENPORT, Thomas H. *et al.*, *Inteligência Artificial Análise de Dados e a Nova Era das Máquinas*, Actual Editora, 2021, p. 161.

[40] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 194.

[41] Cfr. RAUB, McKenzie, «Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices», *Arkansas Law Review*, Vol. 71, n. º 2, art. 7, dec. 2018, p. 532 – 533 («(a)lgorithms give computers guidance on how to solve problems. There is no artificial intelligence without algorithms»).

mais autónomos: os sistemas algorítmicos mais elementares caraterizam-se através da regra *If This, Than That* (*code-driven regulation*[42]), contrariamente aos algoritmos mais desenvolvidos com capacidade de aprendizagem e uma certa autonomia de decisão (os chamados *cognitive robots*[43]).

Como aponta SUSANA AIRES DE SOUSA, os sistemas de inteligência artificial possuem cinco funções primordiais com espelho total no âmbito empresarial: «uma função descritiva e de aconselhamento sobre o que fazer; uma função de diagnóstico que identifica um determinado acontecimento; uma função de previsão capaz de antecipar o que é incerto; uma função decisória capaz de tomar opções e de as implementar; e ainda uma função criativa capaz de apresentar soluções inovadoras e inesperadas»[44]. Neste prisma, a cada função acima descrita será possível atribuir-lhe uma utilidade prática na vida da empresa.

Em primeiro lugar, numa perspetiva de gestão empresarial, em sede de recursos humanos, a introdução de sistemas de inteligência artificial permite a contratação de trabalhadores para determinado posto de trabalho específico, tendo em conta os requisitos e as competências do candidato, fazendo o sistema a correspondência entre as caraterísticas necessárias ao desempenho da função e as caraterísticas do candidato por forma a facilitar a escolha do recrutador. Para além disto, permite também uma monitorização de produtividade, efetuar avaliações, calcular remunerações e promoções dos trabalhadores[45].

Em segunda instância, ainda no âmbito da gestão empresarial, mas agora numa perspetiva económica, em sede de produtividade e de valorização económica, a utilização destes sistemas representa um aumento exponencial de eficiência e eficácia na realização do

---

[42] A expressão é atribuída a HILDEBRANDT, Mireille, «Algorithmic regulation and the rule of law». *Philosophical Transactions of the Royal Society A*, Vol. 376, Issue 2128, p. 2 - 3, que distingue a *code-driven regulation* da *data-driven regulation* tendo em conta a sua capacidade de aprendizagem. Enquanto a *code-driven regulation* rege-se pela premissa *if this, than that*, ou seja, perante um determinado *input* o sistema responde com o *output* pretendido, segundo um algoritmo determinístico e previsível, a *data-driven regulation* diz respeito à aprendizagem algorítmica (através de técnicas de *machine learning*) onde o *output* dado pelo sistema é preditivo e não determinístico, modelando-se em função das circunstâncias e do ambiente que o rodeia; ver também, RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 13.

[43] Que se distinguem dos *deterministic robots* programados segundo uma *code-driven regulation* analisada na nota anterior. Cfr *Report of World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) on Robotics Ethics, SHS/YES/COMEST -10/17/2 REV*, 2017, p. 4; e também, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 62.

[44] *Ibid.*, p. 60.

[45] Utilizando o exemplo da "Mya" e "ARYA" enquanto sistemas "inteligentes" de recrutamento, RAUB, McKenzie, *Op. cit.*, p. 537 e 538. Contudo, há variados riscos quanto a este ponto que se analisarão *infra*, no entanto, *vide* BALES, Richard A. / STONE, Katherine V. W., «The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance, Under the Labour Laws», *Berkeley Journal of Employment and Labour Law*, Vol. 41, n. º 1, UCLA School of Law, Public Law Research Paper, n. º 19 -18, 2020, p. 9 – 21.

objeto social[46]. Isto deve-se ao diminuto índice de erro do sistema - contrariamente ao erro humano[47] -, à diminuição de custos laborais, à «criação de valor através de produtos financeiros inovadores, de que constituem exemplo a moeda e os ativos digitais» e também «meios de transação de elevada segurança como é o caso da *blockchain* (cadeia de blocos)»[48], à providência de serviços inovadores e mais acessíveis como é o caso dos bancos digitais, e, principalmente, pela análise e avaliação de risco de atos empresariais[49].

Em terceiro lugar, no setor financeiro, poderá auxiliar na conceção de empréstimos (através da medição do risco de incumprimento contratual)[50] ou, no âmbito da prevenção do branqueamento de capitais e financiamento do terrorismo, na identificação de «padrões de suspeição no comportamento de um cliente, conferir informações prestadas pelo cliente – desde logo, no *on boarding* -, confrontar informações sobre beneficiários efetivos, identificar relações entre pessoas ou entre entidades, confrontar destinatários com listas de PEP (pessoas politicamente expostas)»[51]. Poder-se-ia afirmar que, de facto, as pessoas físicas também conseguem desempenhar estas funções (como já fazem). Só que «a inteligência artificial oferece a possibilidade de analisar, filtrar, etc., o *universo total das operações* – independentemente do seu montante, do lugar em que sejam ordenadas, da jurisdição a que pertençam os beneficiários, da hora e do dia de semana em que ocorram, etc.-, *em tempo real* – determinando, por exemplo, o bloqueio de uma operação de pagamento com um cartão de crédito -, considerando um acervo de informação (*big data*) inacessível ao conhecimento humano»[52].

Também no âmbito dos mercados de valores mobiliários, a utilização destes sistemas está já presente no aconselhamento e na gestão do risco ao investimento (com a utilização

[46] DAVENPORT, Thomas H. / RONANKI, Ranjeev, *Op. cit.*, p. 16. Os Autores revelam que setor de auditoria da Deloitte tem usado técnicas de *perceptual computing* (ver *supra*) «para extrair termos de contratos, o que permite a uma auditoria tratar uma proporção muito maior de documentos, muitas vezes 100%, sem que os auditores humanos tenham de os ler com todo o cuidado».
[47] LIN, Tom C.W., *Op. cit.*, p. 174 («IBM recently estimated that 95% of all data breaches involve human error»).
[48] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 199.
[49] Cfr. AZIZ, Saqib / DOWLING, Michael, «Machine Learning and AI for Risk Management», *in LYNN, T. et al. (eds.), Disrupting Finance: FinTech and Strategy in the 21st Century*, Palgrave Studies, p. 43
[50] *Ibid*., p. 40.
[51] MAIA, Pedro «*Compliance* Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Op. cit.*, p. 188.
[52] *Ibid., Loc. cit.*

de *robo-advisors*[53]) e ainda nos instrumentos de negociação algorítmica de alta frequência (*high frequency trading*), caraterizado pela velocidade de processamento e vastidão de dados que é capaz de assimilar[54].

Numa palavra, todos estes exemplos de utilidade da inteligência artificial no ambiente empresarial mostram a sua potencialidade não só do dia-a-dia das tarefas da empresa, mas principalmente, em termos amplos, no cumprimento legal. Em concreto, releva-se aqui a importância e a utilidade destes sistemas no que diz respeito ao *compliance* empresarial[55] (tanto na vertente da prevenção da criminalidade empresarial como dos próprios gastos a que o cumprimento normativo obriga[56]). Por esta razão, surgiram diversos conceitos emanados do setor financeiro, visto que foi principalmente aqui que a vertente do *compliance* e da digitalização se manifestaram em primeiro e em maior dimensão[57], fruto dos escândalos financeiros dos primórdios do séc. XX, da crise de 2008 e do «"tsunami legislativo" ou "dilúvio regulatório"»[58] daqui decorrente. Fala-se dos conceitos de *FinTech* (*Financial Technology*)[59], *RegTech* (*Regulatory Technology*) e *SupTech* (*Supervisory Technology*)[60]. Todos eles possuem um denominador comum: a utilização da tecnologia, e.g. inteligência artificial, ora como ferramenta na providência de serviços financeiros (*FinTech*),

---

[53] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 200.

[54] Cfr. MARTINS, Alexandre Soveral, *Op. cit.*, p. 54 e ss. E também, AZIZ, Saqib / DOWLING, Michael, *Op. cit.*, p. 41 e 42.

[55] PACKIN, Nizan Geslevich, «RegTech, Compliance and Technology Judgment Rule», *Chicago-Kent Law Review*, Vol. 93, Issue 1: *FinTech's Promises and Perils*, Art. 7 2018, p. 206 – 210.

[56] AZIZ, Saqib / DOWLING, Michael, *Op. cit.*, p. 45 - 47, afirmam que as maiores instituições financeiras gastam cerca de $70 mil milhões de dólares em *compliance*.

[57] Como mostra MAIA, Pedro, «Intelligent Compliance» *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dez. 2021, p. 17 («financial activity has always promoted and surrounded itself with the most developed tools and instruments that technology has to offer at each point in time»); e, *ibid. Loc. cit.*, nota 48 (« (…) *Goldman Sachs* employs 33 thousand engineers, more than those employed by *Twitter, Facebook* or *LinkedIn* (…), or that *JP Morgan Chase* is estimated to have more software developers than *Google* or *Microsoft*»). Ainda, *Id.*, «*Compliance* Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Op. cit.*, p. 187.

[58] As hipérboles pertencem a MAIA, Pedro, «*Compliance* Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Op. cit.*, p. 170 (cfr. nota 41 da obra).

[59] Sobre a evolução deste conceito até ao momento presente da *FinTech 3.0*, ARNER, Douglas / BARBERIS, Jànos / BUCKLEY, Ross, «The Evolution of FinTech: a New Post-Crises Paradigm?», *University of Hong Kong Faculty of Law*, Research paper n.º 2015/047, UNSW Law Research paper n.º 2016-62.

[60] Sobre a distinção material dos três conceitos, JUNG, John Ho Hee, «RegTech and SupTech: the future of compliance», *in* MADIR, Jelena (ed.), *FinTech*: Law and Regulation, 2nd ed., UK: Edward Elgar Publishing, Chapter 12, p. 255 e ss. *FinTech* consubstancia a utilização da tecnologia nos serviços financeiros, enquanto *RegTech* procura melhoramentos no âmbito da análise de risco empresarial (*risk management*) e *compliance* (não exclusivamente no âmbito financeiro) e a *SupTech* permite dar uma igualdade de armas aos reguladores e entidades supervisoras por forma a permitir-lhes, com ferramentas semelhantes, eficaz e eficientemente supervisionar a atuação dos agentes económicos.

na autorregulação, prevenção e *compliance* (*RegTech*) e na supervisão dos agentes económicos (*SupTech*). Para já, a *RegTech* é o conceito que mais importará pela função de monitorização da atuação da empresa e de delimitação e análise dos riscos, «evitando que o regulado (a empresa) tenha que responder perante o regulador e outras autoridades judiciárias»[61]. Concretamente, a introdução deste mecanismo permite à empresa através da prospeção de dados (*data mining*) e da análise de dados (*data analysis*)[62], averiguar, em tempo real e de forma eficaz e precisa, o tipo de riscos que correrá em agir de determinada forma. Ao mesmo tempo, para uma tomada de decisão eficaz do sistema (*output*) será necessário um amplo *input* (onde os *big data* e a *cloud computing* têm um papel preponderante), isto é, é necessário a introdução de dados suficientes e corretos para que o sistema consiga emitir um resultado cada vez mais preciso e concreto[63]. Daí que, neste âmbito, hoje já se fale em políticas de "*know your data"* (*KYD*) ao lado de políticas de "*know your client*" (*KYC*).

Do outro lado da barricada, afiguram-se também certos riscos e dificuldades com a introdução da inteligência artificial no ambiente empresarial.

Em primeiro plano, numa vertente mais técnica e nuclear para a inteligência artificial, existem riscos inerentemente ligados aos próprios algoritmos. Estes sistemas de alta tecnologia são extremamente complexos, mas nem por isso deixam de estar expostos a erros[64]. Os algoritmos não são, de todo, infalíveis, ainda para mais aqueles que forem programados através de técnicas de *machine learning* que impliquem a intervenção humana. Isto porque, com a intervenção humana abre-se a inevitabilidade do erro humano. A maior dificuldade neste prisma é o facto de, contrariamente ao erro humano que se limita à atuação do errante, ou seja, é individual e parcial, o erro algorítmico tende a ser universal e integral,

[61] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 201.
[62] *Data mining* é um processo de padronização de dados que recorre a técnicas de *machine learning* para, em função desses padrões, prever resultados futuros. Já *data analysis* procede à avaliação de cada dado inserido e, em função da finalidade pretendida, retira uma conclusão (seja para explorar novas variáveis e padrões, seja para confirmar certa hipótese ou para dirimir uma conclusão de dados não quantitativos). Cfr. RAMOS, José Ricardo Marcondes, «The use of Big Data and Artificial Intelligence to prevent and detect fraud», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 94 - 100.
[63] Mostrando o crescimento exponencial do mercado dos *big data*, *idem*, p. 94.
[64] Como afirma, RAUB, McKenzie, *Op. cit.*, p. 535 («(u)nfortunately, the use of algorithms created with good intentions can lead to inadvertent, negative consequences»).

espelhando uma realidade *"murphyana"*[65], uma vez que o seu efeito se dispõe em todo o sistema, ou seja, não se limita à atuação deste, e, portanto, tem consequências mais gravosas em quantidade e/ou em qualidade. Como fator catalisador deste erro estará necessariamente uma malformação no algoritmo graças aos dados inseridos: ou estes estão incompletos, são falsos, estão desatualizados, ou possuem, eles próprios, um viés introduzido pelo programador[66].

Recuperando as vantagens acima mencionadas quanto à utilidade dos sistemas de inteligência artificial em sede de recursos humanos ou no sistema financeiro, estas não são gratuitas. Existem riscos que têm que ser tidos em conta. Concretamente, o viés a que se aludiu é (ou pode ser) particularmente expressivo no âmbito da contratação, avaliação, remunerações, promoções dos trabalhadores, na conceção de créditos ou numa operação de compra ou venda de ativos financeiros. Como mostram RICHARD BALES e KATHERINE STONE, neste âmbito é possível que os sistemas sigam a premissa de "*bias in, bias out*", isto é, se os programadores do algoritmo estão eles próprios enviesados, facilmente o algoritmo fica "contaminado" por esse viés[67]. Um caso emblemático que espelha o efeito discriminatório que o algoritmo pode causar em sede laboral foi a estratégia de recrutamento utilizada pela Amazon que, em 2015, utilizou o seu sistema inteligente AMZN.O para filtrar e escolher os currículos mais indicados às posições que tinha disponíveis. O algoritmo foi concebido tendo por base os dados dos anteriores 10 anos de contratação da empresa, que era maioritariamente composta por homens. Tendo por base estes dados, o sistema considerou que todos os currículos pertencentes a mulheres fossem excluídos ou preteridos relativamente aos dos homens[68]. Para procurar uma proposta de resolução deste problema do recrutamento enviesado, McKENZIE RAUB apresenta o exemplo de sucesso da empresa *Pymetrics* que utiliza a inteligência artificial para a hierarquização dos candidatos a

[65] A *"Lei de Murphy"* consubstancia uma visão pessimista dos acontecimentos que prevê que algo que possa correr mal, vai correr no pior momento possível. Remetendo para a situação aqui em causa, em caso de erro algorítmico as consequências deste serão amplamente danosas.
[66] MAIA, Pedro, «Intelligent Compliance», *Op. cit.*, p. 34 e ss. Também, LUCA, Michael / KLEINBERG, Jon / MULLAINATHAN, Sendhil, «Os algoritmos também precisam de gestores» *Harvard Business Review*, *in* DAVENPORT, Thomas H. *et al.*, *Inteligência Artificial Análise de Dados e a Nova Era das Máquinas*, trad. Alexandra Cardoso, Actual Editora, 2021, p. 44 os Autores mostram que os algoritmos, no atual estado da arte, são literais, comportando-se segundo o seu objetivo final, ignorando outras considerações.
[67] BALES, Richard A. / STONE, Katherine V. W., *Op. cit.*, p. 22.
[68] DASTIN, Jeffrey, «Amazon scraps secret AI recruiting tool that showed bias against women», *Reuters*, 11 Out. 2018.

determinada posição consoante a sua prestação em jogos mentais de lógica que os categoriza em função das tarefas a desempenhar[69].

Ainda no âmbito laboral, a introdução destes sistemas poderá pôr em causa a privacidade dos trabalhadores no exercício das suas funções. Na monitorização dos trabalhadores para fins avaliativos existem atualmente sistemas de inteligência artificial tanto sob a forma de *software*, como também sob a forma de *hardware* (e.g aparelhos mecânicos como pulseiras, geolocalizadores, exoesqueletos), que monitorizam a localização, os movimentos, a frequência cardíaca, os intervalos em horário de trabalho ou até a atividade cerebral e os níveis de fatiga[70]. Certamente sistemas como estes violam a privacidade, a identidade pessoal, o direito à autodeterminação informacional dos trabalhadores, exercendo um estado de contante vigilância (assemelhando-se à ideia orwelliana "*Big Brother is watching you…"*).

Num outro prisma, outro risco ou dificuldade que se poderá apontar à utilização destes sistemas é uma caraterística estrutural dos algoritmos e transversal à sua utilização, ou seja, não limitada ao uso empresarial. Trata-se da opacidade da decisão por parte do sistema (o aludido *supra black box problem*)[71]. Aqui, «(a) opacidade será tanto maior quanto mais complexos (e precisos) sejam os modelos de *machine learning* utilizados, sendo que, em alguns casos, o estado atual de desenvolvimento tecnológico não permite determinar, atendendo ao grau de complexidade do sistema, como se chegou àquele resultado, seja ele um juízo de previsibilidade, um aconselhamento, ou uma decisão»[72].

No que diz respeito à utilização de *RegTech* pela empresa, esta não é a solução milagrosa que irá resolver todo e qualquer problema de ilicitude nesse âmbito (apesar de prometer isso num futuro próximo[73]). De facto, como afirmámos, a utilização destes sistemas pode ser bastante benéfica de um ponto de vista da eficácia, rapidez e precisão na deteção da ilicitude empresarial, todavia, de uma perspetiva de introdução de uma cultura corporativa

---

[69] RAUB, McKenzie, *Op. cit.*, p. 539.
[70] Relativamente a estes aparelhos eletrónicos, BALES, Richard A. / STONE, Katherine V. W., *Op. cit.*, p. 15 e ss.
[71] Sobre o problema da "caixa preta" no âmbito da análise de risco, AZIZ, Saqib / DOWLING, Michael, *Op. cit.*, p. 40 («This has obvious implication for use in risk management, where the very presence of a black box at the centre of decision-making can be its own source of risk in a firm»); e também, ZEDNIK, Carlos, *Op. cit.*, p. 267.
[72] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 67.
[73] BURCHARD, Cristoph, «Artificial Intelligence as the End of Criminal Law? On the Algorithmic Transformation of Society», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 176.

cumpridora com a lei dificilmente se introduz qualquer novidade. Isto é, na prevenção da criminalidade empresarial – como se analisará no ponto seguinte - para além do cumprimento normativo é necessário introduzir um cunho ético-social às condutas e à sua prevenção. O que os sistemas de inteligência artificial neste âmbito fazem é, através de processos puramente racionais, analíticos e matemáticos, identificar e reportar as ilicitudes cometidas na, pela ou através da empresa de forma preventiva, impedindo, se possível, a sua total consumação. Ora, a mera deteção e prevenção individual de cada conduta não garante que estas não reincidam. Esta reincidência mitiga-se com a introdução de uma ordem moral ou ética na cultura empresarial, algo que os sistemas inteligentes não possuem (por enquanto). Por esta razão, a utilização destes sistemas poderia inclusive fomentar ou facilitar uma *tick-box culture* no âmbito empresarial, ou seja, reverter a própria *ratio* da *RegTech* em algo puramente instrumental, tendo em vista a mera subtração de responsabilidades[74]. Tendo isto em conta, apenas com um complemento humano seria possível atingir um ponto ótimo de eficácia.

Uma última dificuldade que se enaltece no âmbito da *RegTech* diz respeito à multiplicidade de terminologias e conceitos técnico-jurídicos que não são unânimes. Esta desregulação conceitual transposta para o ambiente digital faz emergir o problema da «"Torre de Babel" digital»[75], podendo dar lugar a soluções diferenciadas para os mesmos problemas.

Numa palavra e numa perspetiva estritamente empresarial (descorando para já os problemas jurídico-penais que o legislador terá que ter em conta com a introdução exponencial da inteligência artificial nas estruturas empresariais), afigura-se que, de facto, estes sistemas são uma mais-valia, onde a *ratio* vantagens/desvantagens é positiva. Esta ponderação é sustentada e corroborada pelo estudo de 2021 da consultora McKinsey & Company sobre o estado da inteligência artificial[76]. Neste estudo estatístico, que inquiriu perto de 1900 participantes de diversas regiões, indústrias e funções, apurou-se que 56% dos inquiridos responderam que a sua organização já recorreu a soluções de inteligência artificial

[74] Sobre as dificuldades da *RegTech vide* PACKIN, Nizan Geslevich, *Op. cit.*, p. 210 – 218. A Autora denomina inclusivamente esta instrumentalidade da *RegTech* como «*anti-RegTech*», o que mostra o próprio caráter contrastante com a *ratio* da *RegTech.*

[75] BUTLER, Tom / O'BRIAN, Leona, «Understanding RegTech for Digital Regulatory Compliance», *in* LYNN, T., et. al (eds.), *Disruptive Finance*, Palgrave Studies in Digital Business & Enabling Technologies, Palgrave Pivot, Cham, Chapter 6, 2018, p. 87.

[76] Cfr. McKinsey & Company, *Global Survey: The state of AI in 2021*, mai. - jun. 2021

em pelo menos um setor funcional da organização. Para além disto, numa vertente de custos/benefícios, 27% dos inquiridos afirmam que, pelo menos, 5% dos lucros que obtiveram foi graças à utilização da inteligência artificial (seja numa vertente de diminuição de custos, mas também no aumento da receita através das soluções que esta ferramenta pode trazer). No âmbito da prevenção e mitigação dos riscos, cerca de 50% dos inquiridos possuem soluções de inteligência artificial para mitigar os riscos derivados da cibersegurança e 39% assumem que estão a trabalhar para encontrar soluções deste tipo para evitar falhas dos programas de *compliance*.

Em suma, empiricamente, aqui se percebe que as empresas vão cada vez mais procurar soluções digitais, pela sua utilidade na realização do seu trabalho, na mitigação dos riscos, diminuição dos custos, redução do erro, sempre com os olhos postos no seu objetivo: o lucro. Contudo, esta obtenção de lucro não pode ser feita alheada dos perigos envolventes, devendo, para tal, haver sempre uma política de análise dos riscos (*risk based approach*) que permita delimitar as suas condutas e definir as balizas de atuação espelhadas segundo os termos das políticas de cumprimento normativo internamente seguidas (que se analisará de seguida)[77].

2. Do *Compliance* em especial

2.1. *Compliance* como instrumento de prevenção da criminalidade empresarial

2.1.1. Integração conceitual do *Compliance* no caos terminológico

A ordem jurídica, enquanto «conjunto, estruturado em sistema, de todos os elementos que entram na constituição de um direito que rege a existência e o funcionamento de uma comunidade humana»[78], é composta não só por uma ordem normativa, mas também por uma ordem moral ou ética. Como consequência e de uma forma transversal a todos os organismos da sociedade, a ordem jurídica espera não só um cumprimento legal, mas também um cumprimento ético. É aqui que a problemática do *compliance* reside e é relevante.

[77] MAIA, Pedro, «Intelligent Compliance», *Op. cit.*, p. 7. Também, ESAYAS, Samson / MAHLER, Tobias, «Modeling compliance risk: a structured approach», *Artificial Intelligence and Law*, n. º 23, 2015, p. 278 («From a risk management perspective, failure to ensure adherence to obligations and prohibitions constitutes a source of risk that needs to be managed»).
[78] MARQUES, Mário Reis, *Op. cit.*, p. 431.

Derivando do neologismo "*to comply"*, *compliance* diz respeito ao cumprimento normativo de fundamento ético. Não é comumente aceite uma utilização unívoca para esta mesma realidade, existindo uma diversidade de terminologias propostas tanto pela doutrina como pelo próprio legislador[79]. Por nós, adota-se o termo anglo-saxónico de *compliance* pela sua amplitude de conceito e de conteúdo prático[80]. Justifica-se esta escolha.

C*ompliance* distingue-se de cumprimento, conformidade, de programas de *compliance*, programas de cumprimento normativo, sistemas ou mecanismos de ética e *compliance*. No que diz respeito aos primeiros dois termos, a distinção é meramente sinonímica, enquanto a dos restantes é propriamente conceitual (sendo entre estes, eles próprios, sinónimos entre si). Por isto se diz que o «*compliance* constitui uma realidade "camaleónica"»[81].

Enquanto o *compliance* diz respeito à abordagem de cumprimento ético-legal da organização (analisada de uma perspetiva ampla), um programa de *compliance* corresponde às medidas concretas que as empresas utilizam e implementam na sua estrutura para que possam nela introduzir uma cultura ética e de cumprimento normativo. Todavia, os programas de *compliance* não se cingem apenas à prevenção do incumprimento normativo *per se* pelos membros integrantes da estrutura empresarial e pela própria empresa. Estes deverão ter como escopo, por um lado, numa perspetiva negativa, a implementação de medidas para prevenir, detetar e reprimir práticas infracionais nos diversos ramos da sua atuação e, por outro, numa perspetiva positiva, a inclusão de uma cultura ética e de integridade empresarial (através de princípios, valores e normas organizatórias) por forma a deixar de tolerar internamente comportamentos *contra legem* e antiéticos, conduzindo a atuação individual e empresarial dentro da esfera de ação da organização[82]. Numa palavra, os programas de *compliance* visam a prevenção do incumprimento, através da promoção de um cumprimento ético-legal.

---

[79] Nestes termos, MAIA, Pedro, «Compliance Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Op. cit.*, p. 161.
[80] *Ibid.*, p. 162 e 163.
[81] A expressão pertence a *Ibid.*, p. 160 e ss. Sobre a discussão à volta das variadas terminologias utilizadas doutrinal e legislativamente, *ibid.*, p. 161 – 164.
[82] Sobre esta distinção, *Ibid.*, p. 165, o Autor faz uma distinção binária do *compliance*: uma dimensão positiva «de cariz prático e de gestão, ditada pela conveniência de instituir uma função específica de controlo interno, autonomizada dos departamentos jurídicos», sendo «um instrumento ou fator de robustecimento da atividade empresarial e do seu êxito», e uma dimensão negativa, «determinada pela necessidade de introduzir nas organizações um corpo destinado a zelar pela observância do edifico normativo aplicável ou prevenir a transgressão nas sociedades», que «serve para evitar ou impedir que a organização infrinja o seu contexto normativo». E também, RODRIGUES, André Alfar, *Manual Teórico-Prático de Compliance*, Coimbra: Almedina, 2022, p. 33.

No ponto em que nos encontramos, postula-se uma distinção conceitual adicional e necessária para futura compreensão: o *compliance* regulatório (*regulatory compliance*) e o *compliance* de PBCFT (compliance de prevenção do branqueamento de capitais e financiamento do terrorismo ou *AML Compliance*)[83]. Esta destrinça provém do sistema bancário, onde é imperativo fazer uma separação entre a visão interna e externa da regulação. Isto é, «(a)pesar de inscritos num mesmo conceito, o *compliance* regulatório é, num certo sentido, *essencialmente diferente* do *compliance* de PBCFT, porque aquele versa sobre a própria instituição de crédito – visa assegurar que ela cumpre (e identificar se corre o risco de não cumprir ou mesmo se não cumpre), nos seus normativos internos, nos seus sistemas, nos seus procedimentos, na sua prática, na sua cultura o regime legal (em sentido amplo) – ao passo que o *compliance* de PBCFT versa (também essencialmente) sobre *terceiros* – visa assegurar que a instituição de crédito cumpre os seus deveres de exame, de abstenção, de recusa, de comunicação de operações suspeitas de branqueamento de capitais dos seus clientes». Assim, «o *compliance* regulatório está virado para dentro, ao passo que o *compliance* de PBCFT está virado para fora»[84]. No nosso caso, iremos ver que o *criminal compliance*, por definição, corresponde a uma figura que se relaciona de forma diferente com o *compliance* regulatório e com o *compliance* de PBCFT, sendo necessário estabelecer as linhas limítrofes entre estes. Lá chegaremos.

Como é percetível, existe aqui uma sinalagmaticidade entre a ética corporativa e *compliance*. Desde logo porque, sendo o ambiente empresarial um espaço complexo e ambíguo, há uma inevitabilidade da existência de riscos gerados, por exemplo, pelo conflito de interesses ou deveres que certas decisões podem causar. Caberá ao programa de *compliance* minorar estes riscos por forma a efetivar o cumprimento ético-legal e a prevenção da criminalidade empresarial, balizando a atuação da pessoa coletiva dentro da ética e do risco permitido[85]. Este risco permitido é o que delimita a atuação empresarial, que tem por base duas variáveis: por um lado, a maximização do lucro, que tem que ser

[83] Para esta distinção conceitual, novamente, MAIA, Pedro, «Compliance Bancário na Era da Inteligência Artificial – Uma Breve Introdução», p. 179 e ss.
[84] *Ibid.*, p. 179 e 180.
[85] Como mostra LASCURAÍN, Juan Antonio, «Los programas de cumplimiento como programas de prudencia penal», *Revista Portuguesa de Ciência Criminal*, ano 25, n.º 1 a 4, IDPEE, Coimbra, jan.-dez., 2015, p. 96 e 97 («(…) podemos decir que una empresa es prudente cuándo actúa dentro de la frontera del riesgo permitido. Esa *prudencia* es la que procuran los programas de cumplimiento penal en las empresas (…) (u)na segunda característica de las empresas como colectivo en materia de cumplimiento penal es precisamente su tendencia al incumplimiento. Su tendencia congénita de hacer daño – ciertos daños – a los demás»).

balanceada em função da ordem normativa, por outro. Isto é, a finalidade da empresa de obtenção e maximização dos lucros não poderá ser feita a todo e qualquer custo, sendo neste ponto o Estado o titular preponderante e responsável pela tutela e defesa de bens jurídicos. Desde início, foi com base nesta ideia da intervenção estadual que a problemática do *compliance* surgiu.

2.1.2. O fundamento do *Compliance* e as suas origens histórico-dogmáticas

Originalmente, imputa-se ao ordenamento jurídico norte-americano o pioneirismo das políticas que fomentaram o desenvolvimento do *compliance,* que veio mais tarde influenciar os restantes ordenamentos jurídicos a seguirem o mesmo caminho.

As primeiras movimentações destas políticas surgiram pela posição estadual de intervenção na economia, que foi evoluindo em resposta aos escândalos financeiros ocorridos durante o séc. XX e inícios do XXI[86]. Este ambiente volátil e de dificuldade (ou mesmo incapacidade) do Estado em controlar todas as esferas de responsabilidade no âmbito das complexas estruturas empresariais contribuiu para o surgimento do conceito de autorregulação regulada. Este consubstanciava «um novo modelo de intervencionismo público (…) baseado na cooperação entre poderes públicos, sujeitos regulados e outros agentes sociais»[87]. Aqui, o Estado não se abstinha totalmente do seu papel de regulador, mas antes procurava regular de forma mais direta os regulados, passando-lhes o "ónus" de se autorregularem sob pena de faltarem ao cumprimento legal. Contudo, não se pretendia aqui que os regulados se tornassem no regulador, mas antes que, individualmente, se fizessem cumprir com a ordem jurídica. Em específico, JOHN BRAITHWAITE – um dos impulsionadores desta visão nos EUA – caraterizou esta opção político-social como uma *enforced self-regulation*[88]. O Autor afirma que a escolha pela cooperação privada com a Administração facilita a vertente investigatória pela proximidade e conhecimento de causa

[86] A bibliografia relativamente à evolução histórica do *compliance* é vastíssima, portanto, *vide,* por exemplo, MAIA, Pedro, «Compliance Bancário na Era da Inteligência Artificial – Uma Breve Introdução», p. 165 – 173; RODRIGUES, André Alfar, *Op. cit.*, p. 19 – 22; ou, com incidência maioritariamente no ordenamento jurídico norte-americano, HAUGH, Todd, «The Criminalization of Compliance», *Notre Dame Law Review*, Vol. 92, issue 3/5, 2018, p. 1219 – 1233.

[87] RODRIGUES, Anabela Miranda, *Direito Penal Económico*: *Uma Política Criminal na Era Compliance,* 2.ª Ed., Coimbra: Almedina, 2020, p. 84.

[88] BRAITHWAITE, John, «Enforced Self-Regulation: A New Strategy for Corporate Crime Control», *Michigan Law Review*, Michigan: Vol. 80, issue 7, 1982, p. 1470 e ss.

do ambiente onde se insere[89]. No entanto, a relutância numa solução como esta é percetível tendo em conta o potencial choque com as garantias fundamentais dos investigados[90]. Para além disto, o Autor admite uma fraqueza deste sistema, referindo-se ao excessivo voluntarismo das empresas que poderia levar a uma falta de investigação *ab initio*[91]. Contudo, contra-argumenta que, segundo um modelo de *enforced self-regulation*, o departamento de *compliance* das empresas seria legalmente obrigado a reportar ao Estado as ilegalidades sob pena de incorrer em responsabilidade criminal, tanto o responsável pelo departamento como a própria empresa[92].

Nesta autorregulação empresarial não estamos perante uma autorregulação pura, mas antes uma autorregulação regulada, uma vez que cabe ao Estado exercer o seu *ius imperii*, utilizando os instrumentos reguladores à sua disposição. Não quer isto dizer que o Estado utilize apenas as suas ferramentas administrativas, exercendo meramente um controlo tutelar. Este não esquece (nem deve esquecer) o Direito Penal, que mantém a sua essência de *ultima ratio* e de «último convidado», mas que nem por isso se deixa de "sentar à mesa" e fazer-se ouvir em caso de lesão de bens juridicamente relevantes[93]. Por esta razão, fala-se hoje, neste âmbito, no conceito de *criminal compliance*.

Neste sentido, os programas de *compliance* mostram-se relevantes pelo seu objetivo de «promoção de uma cultura empresarial ética e de cumprimento legal, sendo que o seu objetivo final é evitar a lesão de bens jurídicos e a violação de direitos humanos e a correspondente responsabilidade administrativa, civil e, em última linha, mas sobretudo, penal»[94]. Em específico, os programas de *compliance* abarcam diversas dimensões do cumprimento normativo: a prevenção, a deteção e a repressão. É através destes três critérios que a efetividade do programa de *compliance* é aferida. Aqui, deve relevar-se que efetividade

---

[89] *Ibid.*, p. 1468 e ss. («Corporate compliance personnel are more likely than government inspectors to know where "the bodies were buried" and to be able to detect cover-ups»).

[90] Sobre as potenciais lesões dos direitos processuais dos investigados, PAIS, Ana, «Os programas de *compliance* e o risco da privatização do processo penal, em especial, a problemática da "prova emprestada" e o princípio *nemo tenetur se ipsum accusare*», *Estudos em Homenagem ao Prof. Doutor Manuel da Costa Andrade* (org. José de Faria Costa *et al.*), Stvdia ivridica Vol. II, Coimbra: Universidade de Coimbra, 2017, p. 663 – 686.

[91] Como afirma BRAITHWAITE, John, *Op. cit.* p. 1469 («(w)e have seen that corporations may be more capable than the government of regulating their business activities. But if they are more capable, they are not necessarily more willing to regulate effectively»).

[92] *Ibid.*, p. 1470 e ss.

[93] Cfr. RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 85; e *Id.*, «The Last Cocktail…», *Op. cit.*, p. 121.

[94] *Id.*, *Direito Penal Económico*…, *Op. cit.*, p. 100.

não se confunde com infalibilidade, ou seja, os programas de *compliance* apesar de visarem a prevenção da ilicitude na, para, ou através da empresa, não podem ser caraterizados como um "super-*compliance*" que vai erradicar o crime, mas antes como um elemento complementar e auxiliador na prevenção da criminalidade empresarial. Para tal, não basta implementar uma política de *compliance* de feição *tick-box*, isto é, meramente formal, não incutindo qualquer caráter ético nessas políticas, preenchendo simplesmente os elementos mínimos exigidos de um programa de *compliance*[95]. Concretamente, estes devem possuir o apoio da alta administração, por forma a promover uma política de *tone at the top* (isto é, para que a direção da pessoa coletiva "dê o exemplo" e faça com que os seus subordinados não pratiquem atos ilícitos que possam vinculá-la criminalmente), mas também de *mood in the middle* (onde as «pessoas que estão no meio da hierarquia (…) têm contacto direto com, tanto os órgãos de administração, como os demais funcionários e colaboradores» e portanto podem servir de elo de ligação entre as duas estruturas)[96], ferramentas de análise de riscos (*risk assessment tools*), códigos de conduta e ética, realizar controlos internos e auditorias, assegurar canais de denúncia anónimos e eficazes, proceder a investigações internas, formações e comunicações e integrar um órgão específico de coordenação e manutenção de todas estas medidas (o departamento de *compliance*, liderado por um *Chief Compliance Officer*, enquanto principal garante e responsável do bom e eficaz funcionamento do programa). Só deste modo, com a integração de todos estes elementos, que promovam uma cultura corporativa, se poderá falar num programa de *compliance* efetivo[97]. Ainda assim, novamente, um programa de *compliance* efetivo não se confunde com um programa de *compliance* impenetrável, de onde daí "escapem" infrações.

O que importa ressalvar é que o programa de *compliance* corresponde à maneira de ser e estar da pessoa coletiva na ordem jurídica, pelo que este serve para fundamentar o seu "bom comportamento corporativo" (*good corporate behavior*) e, caso o programa de

---

[95] Nas palavras de MAIA, Pedro, «Compliance Bancário na Era da Inteligência Artificial – Uma Breve Introdução», p. 167, nota 26, «((…) "programas de papel" (programas propositadamente ineficientes) ou seguir "compliance de cosmética" (…))».

[96] RODRIGUES, André Alfar, *Op. cit.*, p. 35 – 38; também, SCHEMMEL, Alexander / DIETZEN, Alexandra, «"Effective Corporate Governance" by Legal Tech & Digital Compliance», *in* BREIDENBACH, Stephan / GLATZ, Florian, *Rechtshandbuch Legal Tech*, C.H. Beck, München, 2017, p. 141.

[97] Apresentando falhas de um *compliance* não eficaz, MENDES, Paulo de Sousa, «*Law Enforcement & Compliance*», *in Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. PALMA, Maria Fernanda *et al.*, 2.ª Ed., Almedina, 2020, p. 15 («conflitos de interesses consentidos; deveres de segregação de funções desrespeitados; auditorias ou investigações internas por realizar; falta de independência dos auditores; desrespeito pelas recomendações relativas ao governo das sociedades (*corporate governance*); inexistência de responsáveis de boas práticas e controlo interno (*compliance officers*)».

compliance deixe "escapar" infrações, este é o álibi da pessoa coletiva, podendo servir como fator a ter em consideração em sede de apuramento de responsabilidade criminal (na sanção ou como método de diversão processual). Aqui se entende a concreta ligação do *compliance* com o Direito Penal, que dá o mote para aquilo que designamos por *criminal compliance*.

2.2. *Criminal compliance* como categoria autónoma do *Compliance*

2.2.1. O que é o *Criminal Compliance*?

De facto, nos últimos tempos, os programas de *compliance* têm ganho relevância e espaço no plano criminal. A começar pela própria linguagem punitiva característica da ciência criminal[98], mas também nos efeitos preponderantes que poderá trazer para a responsabilidade penal da pessoa coletiva: seja na delimitação do risco proibido, como causa de exclusão de responsabilidade criminal, na pena aplicável ou ainda como condição de negociação processual[99]. Todavia, caberá em primeiro lugar estabelecer as traves mestras que fazem distinguir o *compliance*, dos programas de *compliance*, do *criminal compliance*, definindo este último tendo por base o que se disse *supra* relativamente aos restantes dois conceitos.

Grande parte da doutrina não define autonomamente o *criminal compliance*, aglomerando no termo *compliance* toda e qualquer promoção ética do cumprimento e prevenção do incumprimento normativo (incluindo o incumprimento penal) no contexto da empresa. Outros fazem o inverso e englobam tudo o que corresponde ao termo *compliance* no termo *criminal compliance*. Todavia, entre nós, não usamos indistintamente estes conceitos, pois se considera que o *criminal compliance* é uma tipologia do termo mais amplo que é o *compliance* e, consecutivamente, os programas de *compliance*.

Em termos simples e amplos, pela própria etimologia do conceito, o *criminal compliance* visa a prevenção da criminalidade empresarial. Como vimos na evolução do *compliance*, a sua origem funcional dizia respeito não à prevenção de ilícitos criminais, mas a um cumprimento das regulações a que as empresas em concreto estavam sujeitas, aliadas a uma cultura ética desse cumprimento (historicamente primeiro, no setor financeiro). Só mais tarde se percebeu que a utilidade deste estímulo ao cumprimento poderia ser estendida e

[98] HAUGH, Todd, *Op. cit.*, p. 1215.
[99] SOUSA, Susana Aires de, «As diferentes faces dos programas de compliance», *in Legitimidade e efetividade dos programas de compliance* (org. Adan Nieto Martin / Eduardo Saad Diniz), Tirant lo blanch, 2021, p. 30.

aproveitada, de forma indireta, pelos órgãos titulares da ação penal. É este o motivo que explica a existência de um *compliance* cada vez mais "agressivo"[100].

Criminal compliance é definido por FRANK SALIGER como a epítome das normas substantivas e adjetivas através das quais as pessoas coletivas procuram assegurar o cumprimento ético-normativo pelos seus membros integrantes, bem como a deteção e, se possível, sanção das infrações a bens penalmente relevantes no contexto empresarial, através de uma prospeção dos riscos de responsabilidade penal no período antecedente à intervenção do Direito Penal[101]. Noutras palavras, podemos afirmar que o *criminal compliance* é a "antecâmara"[102] do Direito Penal, já que tem como objetivo a prevenção criminal ("impedindo" o facto de se consumar e de chegar ao sistema judicial), a deteção e a sua sanção (de forma interna), por forma a evitar a reincidência. Assim, como afirma o Autor, o *criminal compliance* reporta-se a uma realidade prospetiva e futura por forma a evitar a responsabilidade criminal, contrariamente ao Direito Penal que se ocupa de atuar em função de factos típicos, ilícitos, culposo e puníveis passados[103].

Por nós, *criminal compliance* consubstancia uma realidade que tem como *ratio* o próprio Direito Penal, em concreto, o seu caráter de *ultima ratio*. Bem assim, «*ultima ratio* não é *nula ratio*»[104].

Em concreto, as pessoas coletivas possuem programas de *compliance* onde incluem normas preventivas especiais condicentes à sua esfera de atuação e objeto social (*antitrust compliance, tax compliance, labour compliance, securities compliance, banking compliance, energy compliance, privacy compliance, cyber compliance*, etc.). Ora, no fim da linha – à semelhança do Direito Penal -, encontra-se o *criminal compliance* enquanto

---

[100] Expressão de *Ibid.*, p. 37.

[101] SALIGER, Frank, «Grundfragen von Criminal Compliance», *Rechtswissenschaft, Zeitschrift für rechtswissenschaftliche Forschung*, Heft n. º 3, 2013, p. 273 e ss.

[102] Expressão pertence a ANTUNES, Maria João, «Privatização das investigações e *compliance* criminal», *Revista Portuguesa de Ciência Criminal*, ano 28, 2018, p. 127, neste caso, reportando-se à vertente exclusivamente processual das investigações internas.

[103] SALIGER, Frank, *Op. cit.*, p. 274. Também, ROTSCH, Thomas, «Criminal Compliance», InDret, 1/2012, p. 9, para quem o *criminal compliance* corresponde a um desenvolvimento que vai para além do Direito Penal tradicional como instrumento de reação, no sentido de um mecanismo de controlo para a prevenção da responsabilidade penal.

[104] A expressão pertence a BASOCO, Juan Terradillos, «Derecho penal económico: lineamentos de política penal», *Revista del Instituto de Ciências Jurídicas de Puebla*, México, ano IX, n. º 35, IUS, 2015 p. 18 *apud* RODRIGUES, Anabela Miranda, *Direito Penal Económico*…, *Op. cit.*, p. 55, nota 89.

instrumento de prevenção da criminalidade em cada um dos setores. Posto isto, verdadeiramente, o *compliance* possui «diferentes faces»[105].

O principal argumento que distingue o *criminal compliance* das restantes vertentes do *compliance,* incluindo aqui o *compliance* regulatório e o *compliance* de PBCFT, é a sua amplitude de conceito. Enquanto o *compliance* regulatório, como *supra* referenciado, é «virado para dentro»[106], logrando o cumprimento das regulações a que a organização está vinculada – normalmente integrando normas do chamado Direito Penal secundário - (por exemplo, o *antitrust compliance* corresponde às medidas preventivas que a empresa implementa na sua estrutura com o intuito de estar em conformidade com a Lei n.º 19/2012, de 08 de maio que dispõe o Novo Regime Jurídico da Concorrência, mas também todas as outras disposições normativas relevantes neste setor, ou o *privacy compliance* visa a implementação de medidas tendo em visa o cumprimento da Lei n.º 58/2019, de 8 agosto que assegura a execução do Regulamento Geral da Proteção de Dados). Já o *compliance* de PBCFT é um instrumento que visa a concreta prevenção do crime de branqueamento de capitais e financiamento do terrorismo, impondo às entidades tipificadas no art. 3.º e 4.º da Lei n.º 83/2017, de 18 de agosto um conjunto de deveres nesse sentido, ou seja, nesta vertente do *compliance* apenas as entidades sujeitas à dita lei estão vinculadas a estas medidas de controlo.

Ora, do lado do *criminal compliance*, este expõe-se como uma figura ampla e aglutinadora entre as duas visões acima descritas em dois âmbitos: num âmbito objetivo, uma vez que visa o cumprimento das regulações a que as pessoas jurídicas em causa estão vinculadas, prevenindo, detetando e reprimindo as condutas típicas, ilícitas, culposas e puníveis potencialmente daí resultantes (portanto, condutas com maior densidade axiológica e que, caso não fosse a efetividade do *criminal compliance* o facto consumar-se-ia em crime); e num âmbito subjetivo, as pessoas coletivas e entidades equiparadas vinculadas ao *criminal compliance* são todas aquelas contempladas nos termos do art. 11.º do Código Penal e não apenas entidades circunscritas a determinada lei específica. Daí que o *criminal compliance* seja uma figura mais ampla e agregadora de ambos os conceitos, já que visa detetar, prevenir e reprimir todas condutas que possam vir a tipificar ilícitos que integrem tanto o Direito Penal primário, como o Direito Penal secundário. Podemos ainda afirmar que

[105] SOUSA, Susana Aires de, «As diferentes faces dos programas de compliance», *Op. cit.* p. 29 e ss.
[106] *Vide* nota 83.

da mesma forma que o "Estado Regulador" se relaciona axiologicamente com o Direito Penal (numa lógica qualitativa), também o *compliance* regulatório se relaciona com o *criminal compliance* na mesma medida.

Neste sentido, uma autonomização do *criminal compliance* face às outras vertentes do *compliance* tem uma vantagem clara de delimitação do risco permitido e, mais especificamente, de prevenção da lesão de bens jurídico-penais. No entanto, por outro lado, existe um potencial perigo: «o risco é o de termos um direito penal da pessoa coletiva que se transfere para um direito de *compliance* de natureza privada, menos societário e mais punitivo»[107].

Por fim, o ponto essencial que se enaltece aqui é que o *criminal compliance* constitui uma realidade tipológica e autónoma do *compliance*. Contudo, é uma autonomia meramente conceitual, uma vez que o *criminal compliance* integra ainda o conceito mais amplo que é o *compliance*. Por sua vez, o *criminal compliance* é uma modalidade supletiva relativamente ao *compliance* regulatório justificada na densidade axiológica de condutas que visa prevenir; e é uma modalidade integrativa do *compliance* de PBCFT, pois este corresponde à especificidade das medidas preventivas do crime de branqueamento de capitais e financiamento do terrorismo.

Posto isto, a autonomização deste conceito pode ainda mais densificada com a concretização das funções e dos consequentes efeitos que o *criminal compliance* poderá trazer para a empresa.

2.2.2. Funções do *Criminal Compliance*

O funcionalismo respeitante aos programas de *compliance* têm uma base comum em qualquer dos setores ou áreas de atuação a que o *compliance* diz respeito. Assim, embora o *criminal compliance* seja uma vertente dogmática autónoma não significa que produza efeitos totalmente distintos das restantes realidades de *compliance*. Isto porque todas as abordagens de *compliance* no quadro empresarial têm por base o mesmo intuito: a prevenção da ilicitude empresarial (seja na vertente regulatória ou criminal) através da criação

[107] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 211 e 212.

normativa interna, tendo em vista a dissuasão do incumprimento e a promoção do cumprimento ético[108]. No entanto, foquemo-nos apenas nas funções do *criminal compliance*.

Na senda de FRANK SALIGER, poderá categorizar-se as funções do *criminal compliance* relativamente à sua primordialidade[109]. Como tal, a função primordial do *criminal compliance* é, mais do que a prevenção do incumprimento normativo, a promoção de um cumprimento ético-legal por forma a evitar responsabilidade penal. Esta função principal é concretizada através das complementares subfunções de prevenção, deteção e repressão. Cabe relembrar que estas subfunções estão ainda perspetivadas dentro da prevenção do incumprimento, isto é, a prevenção, deteção e repressão decorrentes do *criminal compliance* correspondem a uma atuação prévia relativamente à intervenção estadual ou judicial[110]. Daí que se fale neste âmbito em dois tipos de *compliance*[111]: um *compliance ex ante*, que corresponde à verdadeira essência do *compliance* e razão de ser da sua existência *ab initio*, dizendo respeito à implementação de medidas preventivas antes da comissão da infração; e um *compliance ex post*, ou seja, concebido após o cometimento da infração, que corresponde a uma, agora sim, «verificação do cumprimento»[112] através da aferição da eficácia do *criminal compliance*, mediante a aplicação de medidas indicadas ao melhoramento deste. Por exemplo, espelhando esse caráter *ex post* do *compliance*, em França, já se atribui aos programas de *mise en conformité* a qualidade de pena, prevendo-se a sua aplicação quando esteja em causa um crime de corrupção ou tráfico de influência, sendo essa empresa vigiada pela *Agence de prévention de la corruption*[113].

No que diz respeito à subfunção de prevenção, sendo esta a subfunção de maior alcance no *criminal compliance* uma vez que se destina a antecipar a responsabilidade penal[114], esta permite à empresa delimitar o risco de atuação dentro daquele que é o risco permitido. Não obstante, caso as infrações destas normas internas não sejam detetadas e sancionadas

---

[108] Neste sentido, HAUGH, Todd, *Op. cit.*, p. 1220 – 1221.
[109] SALIGER, Frank, *Op. cit.*, p. 266 e ss.
[110] Sobre este caráter "pré-judicial" do *criminal compliance*, *Ibid.*, p. 267.
[111] Quanto ao caráter *ex ante* ou *ex post* dos programas de *compliance*, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, Coimbra: Almedina, 2019, p. 127.
[112] MAIA, Pedro, «Compliance Bancário na Era da Inteligência Artificial – Uma Breve Introdução», *Op. cit*., p. 163.
[113] Esta medida foi aditada pela Lei Sapin II (a Lei n.º 2016-1691, de 9 de dezembro de 2016, referente à transparência, combate à corrupção e modernização da vida económica). Sobre a influência desta lei e dos programas de *compliance* na negociação processual, SOUSA, Susana Aires de, «A colaboração processual dos entes coletivos: legalidade de oportunidade ou "troca de favores?», *Revista do Ministério Público*, n.º 158, abr. – jun. 2019, p. 27.
[114] SALIGER, Frank, *Op. cit.*, p. 267.

internamente, a implementação de normas preventivas, por si só, não garante um *criminal compliance* efetivo e eficaz. Por esta razão, aditam-se as subfunções de deteção e repressão, que visam evitar um "*compliance* de máscara", não se limitando a empresa a um puro cumprimento normativo. A subfunção de deteção utiliza, através das denúncias recebidas nos respetivos canais internos e anónimos, investigações internas para apurar responsabilidades daí emergentes, enquanto a subfunção de repressão recorre a sanções laborais ou disciplinares para concretizar a função primordial. Em boa verdade, estes programas de *compliance* pretendem dar uma resposta socializadora «às empresas, nas empresas e através das empresas»[115], no sentido em que visa sensibilizá-las a cumprir com a ordem jurídica e a cumpri-la de uma forma ética[116]. Até porque no cumprimento do *criminal compliance* há uma confluência de interesses dos vários agentes empresariais (*stakeholders*), mas também do Estado e dos trabalhadores[117].

Assim, amplamente, poder-se-á sumular as funções do *criminal compliance* em três pontos: (1) a criação de normas legais reguladoras da atividade empresarial, tendo por base a análise dos riscos existentes na esfera de atuação da empresa; (2) a criação de uma cultura corporativa de cumprimento com a lei; (3) gestão dos interesses estaduais, dos interessados empresariais (*stakeholders*) e dos trabalhadores na prossecução do cumprimento legal[118].

2.2.3. Efeitos do *Criminal Compliance*

É com base nas próprias subfunções do *criminal compliance* que se consegue extrair os seus efeitos práticos, nomeadamente, através da avaliação da sua eficácia[119]. Isto porque, é através da eficácia dos programas de *compliance* que a pessoa jurídica poderá atenuar ou

---

[115] ANTUNES, Maria João, «Privatização das investigações e *compliance* criminal», *Op. cit.*, p. 119; RODRIGUES, Anabela Miranda, «The Last Cocktail…», *Op. cit.*, p. 122 («This compliance strategy uses a new type of law enforcement (…) making them able to avoid similar behaviours in the future (…) In the context of business activity, this means that state intervention through compliance fulfils a socializing function»).

[116] RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 100.

[117] SALIGER, Frank, *Op. cit.*, p. 275 e ss. No âmbito dos interesses dos *stakeholders*, o *criminal compliance* visa evitar a responsabilização penal da pessoa coletiva, com isso evitando mais gastos (o Autor fala na maximização dos lucros analisada numa perspetiva negativa, já que há uma prevenção dos custos avultados a que o *compliance* obriga). No caso do Estado, o interesse óbvio é o do cumprimento legal, a manutenção da paz social, mas também dos custos do acionamento da ação penal. Por fim, os trabalhadores incluem-se também nesta convergência de interesses, uma vez que um *compliance* efetivo protege-os de eventuais violações dos seus direitos.

[118] Neste sentido, RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 100 e 101, nota 202.

[119] Sobre a aferição da eficácia do programa de *compliance*, relembrado as *U.S. Federal Sentencing Guidelines* enquanto primeira fonte de estabelecimento de critérios para a avaliação da eficácia dos programas de *compliance*, SCHEMMEL, Alexander / DIETZEN, Alexandra, *Op. cit.*, p. 139.

demonstrar a sua irresponsabilidade. Nomeadamente, podemos distinguir os efeitos processuais e os efeitos económicos.

No âmbito dos efeitos processuais, dispõem-se em três prismas: no prisma do facto criminal, no plano da sanção e na perspetiva da negociação processual[120].

No que concerne à relação entre o *criminal compliance* e a factualidade típica, o efeito direto daqui resultante é a possibilidade de exclusão ou atenuação da responsabilidade criminal da pessoa coletiva quando se mostre que o programa de *compliance* vigente foi eficaz. Esta discussão leva-nos para o debate aceso relativo aos modelos da responsabilidade penal das pessoas coletivas. Distingamos sucintamente estes modelos.

Enquanto criação do Direito, especialmente em sede de imputação do facto criminal, as pessoas coletivas são uma realidade jurídica elástica. Os atuais modelos de imputação são espelho disso mesmo. Para que as pessoas coletivas respondam criminalmente, por um lado, segundo um modelo de heterorresponsabilidade ou responsabilidade derivada ou vicarial, é necessário identificar as pessoas físicas pertencentes à sua estrutura capazes de a vincular criminalmente (que atuam em nome e no interesse da pessoa coletiva e exerçam uma posição de liderança) e a consequente aferição da culpa da pessoa ou pessoas físicas que atuaram no âmbito dos seus poderes funcionais, legitimadas para fazer corresponder a sua vontade à da pessoa coletiva. Neste caso, o facto típico é imputado à pessoa coletiva pelo vínculo empresarial existente entre o autor material e a empresa, ou seja, há aqui uma ideia de extensão do elemento mental da culpa da pessoa coletiva à da pessoa física que o factualmente praticou. Por outro lado, muito pelas dificuldades apresentadas pelo modelo de heterorresponsabilidade, a doutrina procurou apresentar alternativas a este modelo[121]. O modelo de autorresponsabilidade ou responsabilidade direta é o principal exemplo desta via. Neste modelo, a imputação é feita diretamente à pessoa coletiva pelos factos que esta, enquanto entidade autónoma com poderes funcionais e capacidade de ação (ainda que indissociável do facto de ter que ser praticado através de pessoas físicas), praticou. Aqui, a pessoa coletiva responderia por, dentro da sua estrutura organizativa, incluindo-se aqui todos os órgãos dentro da sua "esfera de influência", não se ter organizado internamente por forma

[120] Fazendo esta distinção tipológica, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 127.

[121] Apresentando as dificuldades do modelo de heterorresponsabilidade, SILVA, Germano Marques da, *Responsabilidade Penal das Sociedades e dos Seus Administradores e Representantes*, Lisboa: Editorial Verbo, 2009, p. 180 e ss.

a evitar a comissão do crime. A culpa neste caso traduz-se num juízo de atuação negativa, punindo-se pela falta de eficácia ou omissão de atuação na fiscalização, isto é, pune-se pelo "défice de organização"[122]. Como mostra GERMANO MARQUES DA SILVA, os modelos de autorresponsabilização e heterorresponsabilização tocam-se pelo facto de em ambos se pôr «a questão de quais as pessoas físicas que podem comprometer a sociedade (…) porque é sempre necessária a prática de um facto típico». O que distingue um modelo de outro é que «no modelo de imputação direta se busca a culpa diretamente na sociedade e a eventual responsabilidade dos agentes físicos é autónoma da responsabilidade da sociedade»[123]. Neste caso concreto, podemos identificar que a pessoa jurídica assume uma «posição de garante, cuja omissão, ou não observância, faz emergir responsabilidade penal»[124], sendo que esta responsabilização emana da sua falta de organização empresarial.

Feitas as distinções quanto aos concretos modelos de imputação, a eficácia do *criminal compliance* depende do modelo que se adotar. Nas situações em que o modelo de responsabilidade penal da pessoa coletiva adotado é o modelo de heterorresponsabilidade (como acontece no ordenamento jurídico português), a existência do *criminal compliance* é meramente o instrumento gerador de deveres objetivos para as pessoas físicas que estão organicamente ligadas à pessoa coletiva e que a podem vincular criminalmente. Assim, neste tipo de modelo não será possível isentar a pessoa coletiva de responsabilidade, pois a prova do *criminal compliance* eficaz não é possível, já que a pessoa física (*vis-à-vis* a pessoa coletiva que representa), fê-lo contrariamente ao próprio programa. A única possibilidade será a atenuação da responsabilidade se a pessoa coletiva provar que a atuação da respetiva pessoa singular correspondeu a um incumprimento adverso[125]. Por outro lado, quando em causa esteja o modelo de autorresponsabilidade, ainda assim, não basta à pessoa coletiva meramente demonstrar que possui um programa de *compliance* e que, por isso, deve ser automaticamente isentada de responsabilidade. Tem antes que demonstrar a sua eficácia e

---

[122] Expressão de TIEDEMANN, Klaus, *Wirtschafstrafrecht*, 5, Auflage, Freiburg: Verlag Franz Vahlen, 2017, p. 181, §499.; também, SILVA, Germano Marques da, *Op. cit.*, p. 184 e ss.; e, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 91 e ss.

[123] SILVA, Germano Marques da, *Op. cit.*, p. 184. Também neste sentido, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa, Op. cit.*, p. 107.

[124] BRAVO, Jorge dos Reis, *Direito Penal de Entes Coletivos. Ensaio sobre a Punibilidade de Pessoas Coletivas e Entidades Equiparadas,* Coimbra: Coimbra Editora, 2008, p. 199.

[125] Neste sentido, BRITO, Teresa Quintela de, «*Compliance, cultura corporativa e culpa penal da pessoa jurídica», in Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. PALMA, Maria Fernanda *et al.*, 2.ª Ed., Almedina, 2018, p. 72 («por o delito da pessoa singular então surgir indiciariamente como "acidente ou desgraça" para a pessoa jurídica»).

que possui uma cultura ética empresarial de cumprimento, tendo o facto ilícito sido praticado apesar da existência do programa de *compliance* e da cultura corporativa existente na pessoa jurídica[126]. Fazendo-se esta prova, casuisticamente, seria de admitir a sua isenção ou atenuação da responsabilidade[127].

Em termos exemplificativos, o art. 31 bis do Código Penal espanhol exclui a responsabilidade penal da pessoa coletiva, mediante o preenchimento de certos requisitos cumulativos (tanto requisitos objetivos, das condutas típicas, como requisitos do conteúdo do próprio programa de *compliance*). Também o ordenamento jurídico italiano prevê uma cláusula semelhante no Decreto Legislativo 231/2001, onde a pessoa coletiva apenas não responde (administrativamente) pelo crime desde que prove que adotou um modelo de organização e gestão idóneo a impedir um crime daquela natureza e que os seus dirigentes tenham iludido de forma fraudulenta este modelo. Entre nós, há Autores que propugnam que um efetivo programa de *compliance* poderá ser relevante nos termos do art. 11.º/6 do Código Penal, considerando que «a existência de mecanismos efetivos de *compliance* pode servir para demonstrar que o ilícito foi cometido contra ordens ou instruções expressas de quem de direito, o que determina o efeito desresponsabilizante para a pessoa coletiva (…), mas só se houver clareza, eficiência e eficácia dessas ordens ou instruções à luz da cultura corporativa e do modo de organização, funcionamento e atuação ética e jurídico-económica da empresa»[128]. Ainda assim, veremos de seguida, no nosso ordenamento jurídico qual a relevância destes mecanismos. Por outro lado, surge também na doutrina quem considere

[126] RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 114 («A prova da prática do crime deve, assim, basear-se num teste de adequação abstrato-concreto do programa de *compliance*, traduzida numa apreciação da adequação do programa, quer quanto aos seus aspetos gerais quer quanto à eficácia no caso específico. (…) Esta primeira parte do teste tem a ver com a cultura de legalidade instalada na empresa e com os controlos estabelecidos e pretende detetar falhar na efetividade do programa (…). Na segunda parte do teste, deve demonstrar-se que a empresa, de maneira continuada, não tomou as medidas especificas para prevenir os factos delinquentes da espécie daqueles que foram cometidos e para prevenir os factos que foram cometidos. Trata-se, agora, de averiguar da existência de medidas preventivas para factos semelhantes aos que ocorreram e, caso elas existam, a razão por que não foram eficazes naquele caso concreto»).

[127] BRITO, Teresa Quintela de, «*Compliance, cultura corporativa e culpa penal da pessoa jurídica*», *Op. cit.*, p. 72; e também, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 129.

[128] MENDES, Paulo de Sousa, «*Law Enforcement & Compliance*», *Op. cit.*, p. 17. O Autor faz ainda referência aos efeitos úteis para a responsabilidade contraordenacional da pessoa coletiva no âmbito do Regime Jurídico da Concorrência. Mas também, BRITO, Teresa Quintela de, «Relevância dos mecanismos de compliance na responsabilização penal», *Anatomia do Crime – Revista de Ciências Jurídico-Criminais*, N.º 0, jul. - dez. 2014, p. 83.

que a exclusão da responsabilidade penal da pessoa coletiva é irrazoável, com base no princípio da igualdade de tratamento entre pessoas físicas e pessoas jurídicas[129].

No plano da sanção, uma aferição positiva da eficácia do programa de *compliance* da pessoa coletiva visada poderá servir de atenuação para a determinação da medida concreta da sanção. E fala-se aqui em sanção, e não necessariamente apenas em pena, uma vez que em termos regulatórios ou contraordenacionais também aqui se atribui relevância a um programa de *compliance* eficaz. Tal exemplo poderá ser retirado do sistema brasileiro, da Lei 12.846, de 13 de agosto de 2013, que tem em consideração na determinação da sanção «a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica».

Por fim, no plano da negociação processual, a relevância de um programa de *compliance* eficaz advém essencialmente (mas não só) dos sistemas processuais onde vigora o princípio da oportunidade. Isto porque a visão oportunística do processo permite ao titular da ação penal "aliciar" as pessoas jurídicas com formas de diversão processual que, ao promover a colaboração destas com a justiça, faz atingir o seu objetivo de descoberta da verdade material a troco de vantagens[130]. Num sistema como este pergunta-se se não estaremos a "converter o lobo em pele de cordeiro"[131], passando as empresas a ser um braço do Ministério Público na prossecução do seu objeto social e do interesse público, a fim de beneficiar de vantagens ou de deixar de ser prejudicadas, nomeadamente, através de métodos de negociação e diversão processual (*deferred prossecution agreements* ou *non-prossecution agreements*)[132].

---

[129] BUSATO, Paulo César, «O que não se diz sobre o *criminal compliance*», *in Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. PALMA, Maria Fernanda *et al.*, 2.ª Ed., Almedina, 2018, p. 45 e ss. O Autor considera que, indiscutivelmente, «as pessoas jurídicas deveriam submeter o seu comportamento às regras – inclusive as penais – nas mesmas condições das pessoas físicas». Isto porque, ainda que admita que as diferenças entre pessoas físicas e jurídicas exijam tratamentos distintos, «é preciso sempre ter em conta que ao menos as pessoas jurídicas de maior dimensão gozam potencialmente de mais autossuficiência – económica, estrutural e social – frente ao Estado, do que o individuo. Portanto não seria justificável que uma eventual desigualdade de tratamento entre pessoas físicas e jurídicas pudesse levar a um privilégio para as últimas»: neste caso, a exclusão da responsabilidade penal «(…) não é razoável propor, justamente a favor de quem se encontra em melhores condições de se defender das intervenções estatais, uma eximente que não se possa aplicar a quem se encontra em posição mais débil», referindo-se aqui ao facto de os programas de *compliance* servirem de instrumento de utilidade jurídico-penal às pessoas coletivas.

[130] Sobre esta troca de vantagens, mas também sobre a contraposição entre legalidade e oportunidade, SOUSA, Susana Aires de, «A colaboração processual dos entes coletivos…», *Op. cit.*, p. 9 – 36.

[131] RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 85.

[132] Estes métodos de diversão processual advieram do chamado *Brooklyn Plan*, onde o *Department of Justice* dos EUA, a troco de cooperação com a investigação, pagamento de multa e/ou outras injunções, procedia a um acordo de não acusação. Cfr. HAUGH, Todd, *Op. cit.*, p. 1238 e ss.

Neste sentido, o Estado olha para as empresas segundo uma visão puramente utilitarista, incentivando o cumprimento com determinadas "cenouras" pelo seu bom comportamento e cumprimento (*carrot and stick approach*)[133].

Do lado das empresas, para além da própria vantagem de não ver contra si um processo penal e eventual responsabilidade penal, um dos argumentos favoráveis da utilização destes métodos de diversão processual «é a ideia de que a mera acusação formal pode resultar numa condenação à morte da empresa com consequências nefastas para aqueles que dela dependem ou que com ela se relacionam economicamente»[134]. Estes efeitos negativos consubstanciam danos reputacionais, tendo ficado conhecidos como o "efeito Andersen"[135], em virtude da falência da consultora Arthur Andersen ao ter sido condenada no seguimento do caso *Enron* - empresa para a qual fazia auditoria.

O que é facto é que «a responsabilidade da pessoa jurídica passou assim a ser negociável (…)», onde «(…) entre as condições dessa negociação, estava, de novo, a existência prévia de um programa de *compliance*, tido como efetivo, ou a obrigação de o implementar (…)»[136].

Quanto aos efeitos económicos decorrentes de um programa de *compliance* eficaz, estes dispõem-se de forma cíclica e causal. Em concreto, poderá aqui enaltecer-se o conhecimento e informação da empresa acerca dos riscos que corre tanto na relação empresa-cliente como em relações B2B (*business-to-business*). Isto porque, quanto melhor delimitada esteja a esfera de atuação da empresa no cerne do risco permitido, mais ambientada e adaptada esta se encontra para responder aos seus problemas internos. Isto gera confiança tanto nas relações empresariais externas como nas relações laborais, criando por sua vez um ambiente mais harmonioso no plano interno, que, com efeito, poderá resultar numa maior eficiência produtiva[137]. Para além disto, a própria reputação junto do mercado aumenta numa empresa que seja cumpridora e que não possua um "registo criminal", trazendo assim vantagens

---

[133] Esta visão surgiu nos anos 90 com a publicação das *U.S Sentencing Guidelines for Organizations* com este incentivo à cooperação judicial. Sobre o que caraterizou como a terceira era do *compliance*, onde inclui esta abordagem, *vide* HAUGH, Todd, *Op. cit.*, p. 1218. Mas também, em geral, RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 88 e ss.

[134] SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 132.

[135] *Id.*, «A colaboração processual dos entes coletivos…», *Op. cit.*, p. 14.

[136] *Id.*, «As diferentes faces dos programas de compliance», *Op. cit.*, p. 35.

[137] Neste sentido, LAMBSDORFF, Johann Graf, «Preventing corruption by promoting trust: insights from behavioral science», *Passauer Diskussionspapiere-Volkswirtschaftliche Reihe*, Vol. 69, n.º 15, 2015, p. 3 – 5, mostra que o princípio da confiança é o que determina uma boa relação empresarial (seja interna ou externa) - («(c)ompanies have faith that their employees will contribute to the corporate goals») -, mas também a "motivação intrínseca" (expressão do autor) de cada trabalhador consubstancia o desempenho e produtividade empresarial.

concorrenciais. Por fim, a súmula de todos estes efeitos vai condizer com o próprio fundamento da empresa: a maximização do lucro. Neste caso, analisado numa perspetiva negativa, pela diminuição dos gastos com as sanções decorrentes do incumprimento e/ou com o aprimoramento dos programas de *compliance* incompletos, espelhando uma imagem de que o "crime não compensa" pela ponderação custos do *compliance*/custos do não *compliance* (sejam custos diretos ou indiretos)[138].

2.3. *Criminal Compliance* no ordenamento jurídico português

Como já ficou exposto da evolução do *compliance*, os maiores desenvolvimentos advieram como resposta aos escândalos e fraudes financeiras que marcaram os últimos anos do anterior século e os primeiros do século atual. Nestes termos, foram sendo adotadas diversas disposições normativas, especialmente na União Europeia, a alertar para a importância desta regulação. O principal setor onde confluiu este destaque foi o setor financeiro, onde surgiram diversas imposições normativas às instituições financeiras em sede de promoção ao cumprimento. Foi como consequência desta evolução e crescente relevância e utilidade destes mecanismos de autocontrolo que o Estado reconheceu a sua importância não só na promoção do cumprimento, mas também na prevenção da criminalidade. Foi neste contexto que o *criminal compliance* surgiu, enquanto uma realidade póstuma e mais recente.

Poderíamos fazer uma menção taxativa da diversa legislação que foi sendo produzida com conexão à problemática do *compliance* (muita derivada das obrigações de transposição de diretivas da União Europeia), principalmente no setor financeiro, no entanto, apenas se irá relevar aquela que, entre nós, aborda diretamente a relevância do *criminal compliance.*

Até ao momento, era residual a disposição de esforços que legislador português impunha para esta matéria. Poderá tentar "desculpar-se" a falta de impulso legislativo, em função da composição do tecido empresarial português (composto maioritariamente por pequenas e médias empresas), ou com os custos da implementação destas políticas, ou ainda com uma

[138] HAUGH, Todd, *Op. cit.*, p. 1241 e 1242, revela que um estudo de 2011 demonstrou que empresas multinacionais gastam, em média, $3.5 milhões de dólares em *compliance*, onde 20% é exclusivamente alocado para litígios judiciais daí decorrentes. Estes são custos diretos, não se incluindo aqui as sanções potencialmente aplicáveis. Isto porque, do lado dos custos indiretos, estão todos os prejuízos decorrentes dos danos reputacionais. O Autor revela que o preço das ações da Volkswagen tivera diminuído quase 30% após a constatação pela EPA (Agência de Proteção Ambiental dos Estados Unidos) do escândalo das emissões poluentes.

imperativa reflexão profunda no sistema jurídico-penal. De todo o modo, mais uma vez, o Direito Penal não pode "navegar à bolina", devendo, por outro lado, ser um instrumento preventivo (especialmente numa matéria como *criminal compliance* caraterizado precisamente por essa particularidade). Ainda assim, até aos dias de hoje, sabendo que a perfeição do sistema é utópica, foram, entretanto, introduzidos no nosso ordenamento jurídico pilares sólidos para progresso a respeito do *criminal compliance*, enquanto instrumento preventivo da criminalidade empresarial.

2.3.1. Lei n.º 83/2017, de 18 de agosto

Um exemplo paradigmático de positiva consideração do legislador nesta matéria (ainda que parcialmente compelido por disposições legislativas comunitárias) é a Lei n.º 83/2017, de 18 de agosto. Esta lei transpôs para o ordenamento jurídico português as Diretivas 2015/849/UE, do Parlamento Europeu e do Conselho, de 20 de maio de 2015 e 2016/2258/UE, do Conselho, de 6 de dezembro de 2016, estabelecendo as medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo. Esta lei não é, de facto, a primeira neste contexto, mas optámos por iniciar o percurso do *criminal compliance* no ordenamento jurídico português por aqui, pois esta é a disposição normativa de maior alcance e importância para a nossa problemática.

Em concreto, a presente lei alterou o Código Penal (aditando o art. 368.º-A), trazendo para o domínio do Direito Penal primário o crime de branqueamento de capitais, mas, mais do que isto, implementou um conjunto de medidas preventivas, vinculativas às entidades objeto dessa lei (enumeradas nos artigos n.º 3, 4 e 5), intentadas para evitar não a responsabilidade do agente, mas antes a comissão do crime *ab initio*[139]. Neste sentido, como vimos, o escopo desta lei diz respeito ao *compliance* de PBCFT que se inclui tipologicamente, na nossa perspetiva, dentro da categoria *criminal compliance*.

Com efeito, o art. 12.º da Lei n.º 83/2017 dispõe o conteúdo obrigatório do «sistema de controlo interno», que mais não é do que um programa de *compliance*, dispondo nos artigos 14.º e seguintes as medidas concretas desse sistema, fixando ainda o dever da sua implementação e de promoção de uma cultura de cumprimento ao órgão de administração

[139] DURO, Pedro, «O Compliance nas áreas aparentemente não reguladas – a propósito do art. 11.º do Código Penal», YouTube - Conselho Regional de Lisboa OA, 3 de julho de 2020.

das entidades obrigadas (art. 13.º). Outra disposição relevante diz respeito à designação de um responsável pelo cumprimento (um *Chief Compliance Officer*), nos termos do art. 16.º, para garantir a implementação e a fiscalização das medidas concretas[140].

Esta lei, no seguimento dos impulsos político-criminais da União Europeia, abriu a "caixa de Pandora" relativamente à importância do seguimento de políticas de autorregulação regulada, que impõe às entidades obrigadas a urgência deste controlo como forma de prevenção da criminalidade em contexto organizacional.

2.3.2. Lei n.º 94/2021, de 21 de dezembro e Decreto-Lei n.º 109-E/2021, de 9 de dezembro

Em face do combate ao fenómeno corrosivo da democracia que é a corrupção, o XXII Governo Constitucional incluiu como um dos seus objetivos principais a criação de uma estratégia que abarcasse a prevenção, deteção e repressão destas práticas[141]. Para tal, integrou um grupo de trabalho de especialistas heterogéneo para delimitação destas medidas. Daqui, surgiu a Estratégia Nacional Anticorrupção (ENAC), aprovada pela Resolução do Conselho de Ministros n.º 37/2021, de 6 abril, que deu lugar a dois diplomas que vieram implementar, com força de lei, as medidas aprovadas: a Lei n.º 94/2021, de 21 de dezembro, que vem aprovar as alterações ao Código Penal, Código de Processo Penal, Código das Sociedades Comerciais e leis conexas, e o Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que cria o Mecanismo Nacional Anticorrupção e estabelece o Regime Geral de Prevenção da Corrupção.

No que diz respeito à Lei n.º 94/2021, de 21 de dezembro, esta veio alterar diversos diplomas na senda dos objetivos da ENAC, colmatando algumas lacunas tanto em matéria de combate à corrupção e criminalidade conexa, como da sistemática jurídico-penal, em concreto, das alterações à lei processual penal.

---

[140] Para uma análise desenvolvida das medidas concretas da prevenção do branqueamento de capitais e financiamento do terrorismo relevantes no âmbito do *criminal compliance*, cfr. RODRIGUES, André Alfar, *Op. cit.*, p. 139 e ss.

[141] Segundo os dados do Fundo Monetário Internacional, o custo anual da corrupção no mundo corresponde a 2% do PIB mundial (cerca de 2 triliões de dólares). Cfr. IMF Staff Discussion Note, «Corruption: Costs and Mitigating Strategies», mai. 2016, p. 5; já segundo o relatório emitido pelo grupo parlamentar europeu "The Greens/EFA", Portugal perde anualmente cerca de 7.9% do PIB (cerca de 18 mil milhões de euros) para a corrupção. Cfr. The Greens/EFA, «The Costs of Corruption across the EU», dez. 2018, p. 48.

Não obstante a importância e relevância da globalidade das alterações, apenas discutiremos aquelas que, de todo o modo, se relacionam com a problemática ora em discussão.

Em concreto, uma primeira importante alteração ao Código Penal diz respeito ao art. 11.º/2 que, para além de alargar a possibilidade de responsabilidade penal das pessoas coletivas a 22 novos tipos, reformula as alíneas a) e b). Estas alterações são relevantes em sede de imputação do facto à pessoa coletiva. Como já analisado, o Direito Penal português optou por seguir o modelo de heterorresponsabilidade, imputando-se o facto criminal à pessoa coletiva tendo por base a conduta de pessoas físicas organicamente dependentes desta, que a representavam e agiram em seu nome e no seu interesse. Deste modo, quanto às alterações na alínea a), aditou-se a expressão «ou por sua conta e no seu interesse direto ou indireto», acrescentando-se agora como passíveis de vincular criminalmente as pessoas coletivas tanto aqueles que *de iure* exercem uma posição de liderança como os que *de facto* o fazem. Na alínea b) acrescentou-se a mesma expressão, incluindo agora todos aqueles que atuem sob poderes de autoridade dos que exercem posição de liderança. Feitas estas notas, importa, para o âmbito do *criminal compliance*, a leitura destes aditamentos em conjunto com a alteração ao art. 11.º/4, que define o que se entende por «posição de liderança». Aqui, para além dos órgãos e representantes de pessoa jurídica com poderes de autoridade e controlo, acrescentaram-se os «membros não executivos do órgão de administração e os membros do órgão de fiscalização». Quer isto dizer que, nos termos das alíneas a) e b), se passa a atribuir relevância ao *Chief Compliance Officer* (ou responsável pelo cumprimento normativo) quer este exerça funções executivas ou não, isto é, a atuação do CCO passa a vincular criminalmente a pessoa coletiva independentemente de ter funções executivas atribuídas pelo programa de *compliance*, uma vez que basta preencher o requisito da violação dos deveres de controlo ou fiscalização para ser possível imputar o facto criminal à pessoa coletiva.

Outra importante alteração diz respeito à introdução da relevância do *criminal compliance* quanto aos efeitos sobre a sanção. Esta relevância foi atribuída através do aditamento ao art. 90.º-A que possibilita agora a substituição da pena de multa por admoestação, caução de boa conduta ou vigilância judiciária (n.º 3) quando tal «realize de forma adequada e suficiente as finalidades da punição, considerando, nomeadamente, a adoção ou implementação por parte da pessoa coletiva ou entidade equiparada de programa

de cumprimento normativo adequado a prevenir a prática do crime ou de crimes da mesma espécie» (n.º 6). Pode ainda ser aplicada uma pena acessória sempre que tal se revele adequado e necessário para a realização da punição, com base no mesmo fundamento (n.º 5). Ainda no âmbito da sanção, nos termos do art. 90.º-A/4, pode haver lugar a atenuação especial da pena nos termos do art. 73.º, considerando-se como circunstância para essa atenuação a «de a pessoa coletiva ou entidade equiparada ter adotado e implementado, antes da prática do crime, programa de cumprimento normativo adequado a prevenir a prática do crime ou de crimes da mesma espécie». Até estas alterações, um programa de *compliance* eficaz apenas era relevante, numa perspetiva negociada, na determinação da medida da pena nos termos gerais do art. 71.º/2[142], relevando-se aqui o caráter *ex post* do *compliance*.

Na senda deste aditamento, também a lei processual foi alterada neste sentido. Atualmente, nos termos do art. 281.º/3 e 11 do Código de Processo Penal e do art. 9.º da Lei n.º 36/94, de 29 de setembro, pode haver lugar a suspensão provisória do processo por crime de recebimento indevido de vantagem, corrupção e/ou crimes conexos, tendo como injunção obrigatória a adoção, implementação ou alteração do programa de *compliance*, com vigilância judiciária nos termos do art. 90.º-G CP. Aqui, o tribunal pode revogar a pena de vigilância judiciária e aplicar uma pena de multa respetiva, pelo facto de a pessoa coletiva não ter adotado ou implementado um programa de cumprimento normativo (art. 90.º-E/5). O tribunal tem ainda a faculdade de, nos mesmos termos, ordenar a pessoa coletiva ou entidade equiparada a adotar ou implementar um programa de cumprimento normativo (art. 90.º-G/1/b)), podendo esta injunção ser cumulada com as penas acessórias de proibição de celebrar contratos e de privação do direito a subsídios, subvenções ou incentivos. Também em sede de medidas de coação a aplicar às pessoas coletivas, «a adoção e implementação de programa de cumprimento normativo deve ser tida em conta na avaliação do perigo de continuação da atividade criminosa, podendo determinar a suspensão da medida de coação» (art. 204.º/3 CPP).

Quanto ao Decreto-Lei n.º 109-E/2021, de 9 de dezembro, este estabelece Regime Geral da Prevenção da Corrupção, obrigando as pessoas coletivas públicas e privadas acima de 50 trabalhadores, a proceder à implementação de programas de *compliance*, havendo lugar a sanções pela não adoção ou adoção defeituosa destas medidas, nos termos do art. 20.º. Em termos de relevância para o regime, a criação do Mecanismo Anticorrupção (MENAC),

[142] SOUSA, Susana Aires de, «A colaboração processual dos entes coletivos…, *Op. cit.*, p. 18.

enquanto entidade administrativa reguladora da implementação e efetividade destes instrumentos, é uma mais-valia para o ordenamento jurídico português, pois o controlo especializado desta matéria permite, por definição, aumentar a eficácia das políticas de prevenção criminal neste âmbito. O que este diploma propõe é retirar o *compliance* do domínio do *soft law*[143], como se existisse uma "opção" para o cumprimento, ou seja, o que este decreto-lei espelha é uma mudança de paradigma no que diz respeito à regulação. Passa-se de uma autorregulação regulada, onde cada empresa tem um ónus jurídico de se regular - uma vez que «é um meio de se alcançar uma vantagem ou, pelo menos, de se evitar uma desvantagem»[144], neste caso, no plano penal, através de uma não acusação, suspensão da acusação, exclusão da responsabilidade ou atenuação da punição, ou, no plano económico, a maior credibilidade e fiabilidade, podendo gerar vantagens competitivas -, para uma heterorregulação mitigada, pois o Estado toma essa função de controlo, fazendo constituir para as pessoas jurídicas que empreguem mais de 50 trabalhadores um verdadeiro dever jurídico geral de implementação destas medidas.

Em termos práticos, este diploma vem concretizar aquilo que, até agora, estava no domínio do *soft law* no condicente às medidas concretas obrigatórias que cada programa de *compliance* deveria ter para aferir a sua eficácia. Até esta altura não existia uma forma universalmente aceite para aferir a eficácia dos programas de *compliance*, ainda que houvesse uma base comum quanto ao conteúdo concreto destes programas. Esta disposição vem agora, nos termos do art. 5.º, estatuir que os programas de *compliance* das entidades obrigadas incluem, entre outras medidas, um plano de prevenção de riscos de corrupção e infrações conexas (PPR), um código de conduta, um programa de formação e um canal de denúncias. Em síntese, esta concretização vem então pôr ao descoberto as medidas concretas que as pessoas coletivas devem tomar para provar a eficácia do seu programa de *compliance* e, com isso, procurarem atenuar ou mesmo excluir a sua responsabilidade.

---

[143] O domino do *compliance* existia em termos não vinculativos, mas recomendatórios promovido principalmente pela ONU, através do *Ruggie Report* de 2008 ou do *UN Global Compact* de 2000 - onde se promoveu a responsabilidade social das empresas segundo um conjunto de princípios em matéria de direitos humanos, direitos laborais, ambientais e anticorrupção-, mas também pelas Diretrizes da OCDE, recomendando às empresas a adoção de um cultura corporativa de boa governança e à implementação de um Código de Conduta Empresarial Responsável que balizasse a sua atuação.

[144] VARELA, João de Matos Antunes, *Das Obrigações em Geral*, Vol. I, 10.ª Ed., Coimbra: Almedina, p. 58.

2.4. Pontos finais e reticências

Em jeito conclusivo, parece ser percetível que, nos atuais dias, a adoção de programas de *compliance* é uma inevitabilidade. Em boa verdade, esta inevitabilidade depende da opção político-criminal de cada ordenamento jurídico em regular de mais perto, assegurando o Estado esta função de controlo, ou "delegando" nas próprias empresas este autocontrolo.

De todo o modo, a concreta eficácia da melhor opção político-criminal, mas também dos próprios programas de *compliance* apenas irá ser empiricamente aferida decorrido algum tempo, para se perceber se, de facto, o objetivo e função primordial do *criminal compliance* de prevenção da criminalidade empresarial foi concretizado. TODD HAUGH apresenta-se cético quanto à abordagem de um *criminal compliance*, pois considera que nem a "lente" do direito penal no âmbito dos programas de *compliance* assegura uma eficácia total na prevenção da criminalidade empresarial. Aliás, por outro lado, considera que o Direito Penal pode causar consequências adversas e inevitáveis aos membros das empresas, que espelharia uma ineficácia do programa. Concretamente, socorrendo-se de argumentos criminológicos, considera que uma abordagem mais "agressiva" de *compliance* põe os membros integrantes das empresas a procurar justificar os seus comportamentos ilícitos e antiéticos através de racionalizações[145]. Assim, o Autor afirma que o *criminal compliance*, ao procurar imitar o Direito Penal com o objetivo de dissuasão e prevenção da criminalidade, está, na verdade, a potencializar esses comportamentos[146].

---

[145] HAUGH, Todd, *Op. cit.*, p. 1252 e ss., descreve o processo através do qual estas racionalizações são possíveis: «(i)f rationalizations are drawn from an offender's environment, which includes from the criminal law itself, then criminalized compliance regimes that import the delegitimizing features of the criminal law into corporations play a significant role in fostering unethical and criminal behaviour within those corporations. Criminal law-driven compliance programs that employ command-and-control, deterrence-based strategies lack legitimacy in the view of many corporate employees. This perceived illegitimacy is critical because it provides space for employees to formulate the rationalizations necessary for their bad conduct. In this space, employees find "defences" to the internal corporate norms and external legal rules that are fundamental to the compliance function. Employees then internalize and incorporate these defences into their own thought processes. Once this occurs, there is little stopping an employee's future unethical or even criminal conduct from going forward, regardless of the compliance regime in place». Para mais, LAMBSDORFF, Johann Graf, *Op. cit.*, p. 4, afirma que, tendo por base a confiança e a "motivação intrínseca" – *vide* nota 137 – a prevenção através de medidas extensivas de controlo podem trazer um efeito perverso ao ambiente empresarial, causando uma desconfiança, incerteza e um espírito maniqueísta entre os pares. Daí que, por forma a tentar obviar a estes efeitos nefastos e a tentar equilibrar a confiança com a "motivação intrínseca" para atingir a produtividade marginal, os membros integrantes da organização procuram seguir a "vontade coletiva", ignorando a ética de certos comportamentos, havendo então lugar a racionalizações.

[146] HAUGH, Todd, *Op. cit.*, p. 1219. Neste sentido, seguido pelo próprio Autor anterior, ANAND, Vikas *et al.*, «Business as usual: the acceptance and perpetuation of corruption in organizations», *The Academy of Management Executive*, Vol. 19, n. º 4, 2005, p. 10 («(t)aken together, rationalizations and socialization practices allow perpetrators of unethical activities to believe that they are moral and ethical individuals, thereby allowing them to continue engaging in these practices without feeling pangs of conscience»).

Apesar disto, o núcleo ideológico por detrás do *criminal compliance* não pretende «criar um programa normativo que favoreça a sua *(da empresa)* atividade "no fio da navalha" e lhe permita fugir à responsabilidade penal, mas sim delimitar o perímetro dos comportamentos proibidos, de forma que possam se prevenidas e reprimidas práticas contrárias às normas de comportamento definidas»[147]. Ainda assim, este é um risco premente que se corre com a cada vez maior "criminalização" do *compliance*[148]. Daí ser legítimo questionar se a estratégia "ultra-defensiva" dos programas de *compliance* segue o verdadeiro propósito de prevenção da criminalidade através da implementação de uma cultura corporativa de cumprimento ético-legal, ou, se por outro lado, estes programas de *compliance* visam ser um escudo à punição e para que, segundo a máscara do *compliance*, as pessoas coletivas se possam subtrair à responsabilidade[149].

Esta subtração de responsabilidade é feita através do desvio da responsabilidade para outros agentes. Por esse motivo, WILLIAM LAUFER equipara a implementação de programas de *compliance* a contratos de seguro. Isto porque, este tipo de contratos e relações jurídicas baseiam-se no risco e na transferência da responsabilidade pelo risco do segurado para a seguradora. Ora, no caso do *criminal compliance*, este serviria como a seguradora da pessoa coletiva em sede de responsabilidade penal[150]. Com efeito, se assim é, a opção de *compliance* por parte das empresas passa a radicar apenas e só numa ponderação económica, o que, em termos de promoção de uma cultura corporativa de cumprimento ético-legal e de *good corporate citizenship* não augura nada de bom. Assim, as empresas optam por gastar o mínimo dispensável para que consigam, ao mesmo tempo, desviar a responsabilidade[151]. Como expectável, e daí a importância de políticas *tone at the top* no âmbito dos programas de *compliance*, o impulso para o desvio parte necessariamente das camadas superiores da

---

[147] RODRIGUES, Anabela Miranda, *Direito Penal Económico…*, *Op. cit.*, p. 85 (itálicos nossos).

[148] Justificando este aumento da "criminalização" do *compliance*, HAUGH, Todd, *Op cit.*, p. 1218 («(a)fter decades of scandal-driven legislation aimed at curbing corporate wrongdoing, companies have increasingly adopted criminal law-driven, deterrence-based compliance protocols to avoid criminal and quasi-criminal investigations and prosecutions»).

[149] Com fundamento para estas questões, cfr. SOUSA, Susana Aires de, «As diferentes faces dos programas de compliance», *Op. cit.*, p. 36 e ss.

[150] LAUFER, William S., «Corporate Liability, Risk Shifting and the Paradox of Compliance», *Vanderbilt Law Review*, Vol. 52, Issue 5, art. 9, 1999, p. 1402 e ss., («(…) firms purchase compliance to ensure against the inevitability of compliance failures.» (…) Compliance, like insurance, is a method of greatly reducing a known risk»).

[151] *Ibid.*, p. 1403 («The costs to the firm are highest where there is little-to-no compliance (costs rise due to significant employee deviance that is imputed to the firm), and overcompliance (employee deviance is not imputed to the entity, but costs rise due to compliance expenditures). Firms maintain a level of compliance within an operating range that minimizes costs while at the same time shifting liability»).

empresa, dos órgãos de gestão. Deste modo, se é o próprio órgão de gestão que começa por tolerar ou mesmo incentivar comportamentos ilícitos e antiéticos, a "moral interna" e a "vontade coletiva" da organização seguirá por esse caminho. Todavia, uma consequência direta daqui decorrente é que os principais prejudicados serão os próprios subordinados da empresa, havendo, na maioria das vezes, lugar a um fenómeno denominado de *reverse whistleblowing*[152]. Aqui, os responsáveis empresariais desviam a sua responsabilidade e transferem-na para alguém com maior fragilidade no âmbito laboral (por norma e em primeiro lugar, aqueles das camadas baixas e, seguidamente, intermédias) - já que estes se encontram numa posição hierárquica inferior e, pelo receio de repercussões laborais, assumem responsabilidades -, fornecendo elementos de prova (facilmente obtidos pela posição de liderança e controlo que ocupam) para se subtraírem às suas responsabilidades.

Não obstante, o *criminal compliance* é um instrumento da utilidade *ex ante*, pelo que, na eventualidade de falhas, caberá à própria empresa e ao responsável designado pelo bom funcionamento do programa – o *Chief Compliance Officer* – provar a sua eficácia. A mera existência de um responsável pelo cumprimento não legitima a transferência automática de responsabilidades ou desresponsabiliza a pessoa coletiva. Isto porque, da mesma forma que a existência de programas de *compliance ipso facto* não corresponde uma direta isenção de responsabilidade penal da pessoa coletiva, por outro lado, a existência de um *Chief Compliance Officer* não corresponde *ipso facto* à sua responsabilização, fruto da falta de cumprimento dos deveres de garante de *compliance*. Este, ainda que responsável pela função de supervisão do cumprimento, não poderá ser criminalmente responsável por toda e qualquer falha do programa de *compliance*, respondendo apenas, por omissão dolosa, «se a omissão do cumprimento do dever ou o seu cumprimento deficiente releve ao nível da realização típica ilícita – no sentido de que expressa o dolo do ilícito típico – do crime em causa por si ou por terceiro, revelando indiferença pelo bem jurídico protegido»[153]. Ou seja,

---

[152] A expressão pertence a LAUFER, William S., «Corporate prosecution, cooperation, and the trading of favors», *Iowa Law Review*, Vol. 87, 2001, p. 648 («Reverse whistleblowing (RWB) occurs when an organization, typically through the acts of senior management, identifies culpable employees and offers evidence against them in a trade with prosecutors for corporate leniency or possible amnesty»). Espelhando esta ideia noutra obra, *Id.*, «Corporate Liability, Risk Shifting and the Paradox of Compliance», *Op. cit.*, nota 267, p. 1406 («After paying that minimum expenditure toward compliance necessary to shift liability downward, firms have reduced incentives to ensure against deviance. Organizations at the lower operating range of compliance are, for obvious reasons, most at risk. Here the cost is minimal, a primary objective of compliance is achieved, and, with an often less than genuine commitment of top management, deviance or pressures leading to deviance may be encouraged with little to no risk to the firm»).

[153] SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 137 – 140, apresentando dois requisitos para o CCO ser criminalmente responsável: (1) o responsável pelo cumprimento

para o CCO responder criminalmente terá que ter preenchido os requisitos do dolo ou dolo eventual (tendo que mostrar indiferença para com a lesão do bem jurídico) e exercer uma posição de garante do cumprimento, posição essa que lhe poderá atribuir poderes executivos[154]. Pode, acrescido disto, ser sancionado pessoalmente num plano contraordenacional ou administrativo quando falte não com o dever de impedir a comissão do crime, mas com o dever de vigilância[155].

Questão diferente é o apuramento da responsabilidade criminal da pessoa coletiva, tendo por base a conduta omissiva do CCO. Com efeito, há uma autonomia expressa entre a responsabilidade da pessoa coletiva e do CCO, não se confundindo entre si. Ainda assim, muitas vezes o próprio CCO é utilizado como o «"bode expiatório" para absorção da responsabilidade que, em princípio, estaria atribuída entre a própria empresa e os seus diretores»[156]. Neste sentido, por forma a procurar minimizar o efeito da transferência de responsabilidades para camadas inferiores da empresa e fazer com que os que exercem posições de liderança nas pessoas jurídicas deixem de olhar para o *criminal compliance* como "moeda de troca", ou como um prémio como se de um contrato de seguro se tratasse, deve o legislador intervir neste ponto (como já fez no nosso ordenamento jurídico), reforçando o regime da responsabilidade penal das pessoas coletivas.

Estes são pontos que somados resultam em reticências. Como tal, não poderemos negar que, a par dos benefícios, ou mesmo das boas intencionalidades que o *criminal compliance* traz, a sua completa eficácia e prevenção eficaz da criminalidade empresarial é difícil de aferir. Desde logo, pela subjetividade que acarreta. Isto é, não basta implementar um programa de *compliance* com todos os requisitos para se afirmar que uma cultura ética de cumprimento foi introduzida na corporação e que o programa é efetivo. Contudo, é

---

tem que ter recebido a disposição da posição de garantia por aquele que lhe delegou essa posição (aquele que exerce uma posição de liderança na pessoa coletiva); (2) o «domínio potencial do risco (da fonte do perigo)» tem que estar delimitado para se aferir se o risco emergente da norma penal se inclui nesse ou não. Assim, a «(a)utoria por omissão, reitera-se, só poderá existir quando o dever violado se reporta a um risco protegido pela norma incriminatória, dever esse que integra a esfera de responsabilidade do *compliance officer*, tendo ele a possibilidade de o cumprir».

[154] Sobre a posição de garante, DIAS, Jorge de Figueiredo, *Direito Penal, Parte Geral*, Tomo I, colab. M. J. Antunes *et al.*, 3.ª Ed., Coimbra: GESTLEGAL, 2019, p. 1086 e ss.

[155] Tal está já previsto no art. 21.º e seguintes do Regime Geral da Prevenção da Corrupção, anexado ao Decreto-Lei n.º 109-E/2021, de 9 de dezembro.

[156] BUSATO, Paulo César, *Op. cit.*, p. 42. E também, MENDES, Paulo de Sousa, «A problemática da punição do autobranqueamento e as finalidades de prevenção e repressão do branqueamento de capitais no contexto da harmonização europeia», *Católica Law Review*, Vol. 1, n.º 3, 2017, p. 146.

necessário ir além da retórica do *compliance* efetivo e eficaz. Exige-se uma consistente aferição das avaliações organizacionais das pessoas jurídicas, procedendo-se a uma análise casuística, tendo em conta a *ratio* de cada programa de *compliance* no que ao seu conteúdo e pendor ético-legal diz respeito, no balanceamento do risco corrido/risco permitido e no custo/benefício[157].

Sintetizando, apesar de algumas reticências percetíveis, termina-se com uma expetativa otimista e positiva destes mecanismos. A intencionalidade por trás das medidas de prevenção criminal é louvável e são imprescindíveis. Isto porque, de facto, são as pessoas coletivas que exercem o poder de controlo direto sobre os seus subordinados e sobre a "mente criminosa coletiva", pelo que um auxílio à prevenção da lesão de bens jurídico-penais pela coletividade gera uma utilidade dual: na pessoa coletiva, para que não seja responsabilizada e seja prejudicada economicamente com isso (uma vez que a reputação é um elemento essencial para a vitalidade das pessoas coletivas), e no Estado que garante a paz jurídica.

[157] Ideia traduzia de LAUFER, William S., «Corporate Liability, Risk Shifting and the Paradox of Compliance», *Op. cit.* p. 1419.

Capítulo II – A Inteligência Artificial no *Criminal Compliance*

1. *Criminal Compliance* "inteligente": novos paradigmas

1.1. Um novo conceito?

É no presente momento que se lidará pela primeira vez com a interconexão entre as duas realidades abordadas até esta parte: a inteligência artificial e o *criminal compliance*.

À primeira vista parecem duas problemáticas distintas, porém, a realidade dos tempos carreada pela inovação, onde as novas tecnologias são a principal figura, assegurar-se-á de as cruzar. De certa forma, já se demonstrou a influência que as novas tecnologias têm tido no âmbito empresarial, em face das crises económicas vividas e da "bateria legislativa" daí emergente, por exemplo, no setor bancário e no setor do mercado de valores mobiliários, através da *RegTech*. Por esta razão, não se poderão negar os benefícios que os novos instrumentos tecnológicos trazem para esta problemática.

Em concreto, do que já se disse, é possível cruzar certos efeitos benéficos da utilização da inteligência artificial com o *criminal compliance*. É graças a este cruzamento que se poderá extrair o conceito de *criminal compliance* "inteligente"[158].

De facto, este é um conceito que consubstancia uma idealização futura e que junta duas realidades atuais com uma utilidade empresarial semelhante. A inteligência artificial traz para o plano empresarial uma capacidade distinta de tomada de decisão, com um baixo grau de falibilidade, que gera uma produtividade eficiente. Por outro lado, o *criminal compliance* visa prevenir o incumprimento penal por ou através da empresa. Assim, um sistema "inteligente" de previsão do incumprimento aumentaria a eficácia do programa de *compliance* idealmente até ao ponto de o ilícito nem sequer se chegar a consomar (pelo menos, é isto que promete), pelo que é notório o interesse que as pessoas jurídicas possuem em utilizar sistemas de controlo interno como estes[159].

Neste contexto, podemos definir o *criminal compliance* "inteligente" como o conjunto de medidas e normas internas integrantes de um programa de *compliance* que utiliza, por norma, um *software* de inteligência artificial para coordenar a atuação empresarial dentro do

[158] Daqui, não se pretende etiquetar o *criminal compliance* acima aludido como "não inteligente", até porque aos dias que correm – de *narrow AI* - nenhuma máquina é tão inteligente como o Homem. A menção expressa de "inteligente" diz respeito a uma necessidade de diferenciação entre uma inteligência artificial ou sintética e a inteligência humana.
[159] BURCHARD, Cristoph, *Op. cit.*, p. 178.

risco permitido, detetar infrações preventivamente, reprimindo-as no plano interno[160]. A principal diferença relativamente ao *criminal compliance* é, naturalmente, o auxílio prestado pelo sistema de inteligência artificial, isto é, a capacidade preditiva, com base numa prévia análise de risco, do cometimento de infrações empresariais. Ou seja, enquanto o *criminal compliance* consiste num conjunto de medidas preventivas e reativas, no *criminal compliance* "inteligente" releva-se o seu caráter descritivo, preditivo e prescritivo[161].

Numa primeira fase, não se pretende (nem é sequer aconselhável) que a inteligência artificial permita ao programa de *compliance* ser "autónomo" ao ponto de a função do responsável pelo cumprimento ser irrelevante. Procura-se antes utilizar a inteligência artificial para o benefício da empresa e do escopo do próprio *criminal compliance*, seja no auxílio na tomada de decisões ou na prevenção da ilicitude empresarial. Por um lado, a dispensa das funções de um CCO provaria uma falta de eficácia do próprio programa de *compliance* pelo não cumprimento com os elementos constituintes obrigatórios. Por outro, ao tempo que escrevemos, não existe (para muitos nem sequer é uma hipótese real ou, para outros, uma hipótese longínqua[162]) uma "inteligência artificial forte" (*strong AI* ou *artificial general intelligence*) ou uma "superinteligência" com uma capacidade cognitiva semelhante ou superior à humana ao ponto de revelar a inutilidade da função de CCO. A refutação destes argumentos poderá ser afirmada apenas e só a partir do momento em que a "inteligência" em causa seja suficientemente desenvolvida e certificada ao ponto de o ser humano ser substituível nestas funções. Algo que nos parece distante e, mais do que isso, indesejável.

Para além disto, sendo o ambiente empresarial ambíguo e complexo impõe-se a necessidade de acompanhamento constante das funções de prevenção, em função de problemas que, muitas vezes, podem fugir do escopo da programação dos algoritmos, dando

---

[160] Definindo antes estas ferramentas como *digital compliance* SCHEMMEL, Alexander / DIETZEN, Alexandra, *Op. cit.*, p. 143 e ss.

[161] *Ibid.*, p. 143, §40; e também, GIUFRIDDA, Iria, «Liability for AI Decision-Making: Some Legal and Ethical Considerations», *Fordham Law Review*, Vol. 88, 2019, p. 440.

[162] Um grupo de especialistas realizou um estudo para perceber o impacto da inteligência artificial e se e quando poderá esta ultrapassar a inteligência humana. Aqui os autores do estudo definem esta ultrapassagem («high-level machine intelligence (HLMI)») alcançada quando máquinas autonomamente consigam realizar as mesmas ou mais tarefas que o ser humano com maior eficiência e menor custo. A média das respostas aponta para a ultrapassagem da inteligência artificial relativamente à inteligência humana em áreas como a tradução de línguas (até 2024), condução e transporte autónomo (até 2026), trabalho no retalho (até 2031), escrever livros (até 2049), realizar cirurgias autonomamente (até 2053). Dos 352 inquiridos, a previsão é que haja 50% de probabilidade de haver esta ultrapassagem nos próximos 45 anos e 10% nos próximos 9. As previsões destes especialistas são que a automação de todas as funções laborais tem uma probabilidade de 50% de acontecer nos próximos 120 anos. Cfr. GRACE, Katja *et al.*, «When will AI exceed human performance? Evidence from AI experts», *Journal of Artificial Intelligence Research*, N. º 62, 2018, p. 729 e ss.

estes respostas imprevisíveis, porque são falíveis. Assim, como o sistema é falível, precisa ele próprio de monitorização. Daí que a função do *Chief Compliance Officer*, num futuro próximo, não será extinta, mas aprimorada no que diz respeito às suas competências técnicas e qualificações, concretamente, com o acréscimo de competências informáticas ou de ciência dos dados às competências jurídicas.

Neste prisma, importa referir que a utilização destes sistemas "inteligentes" no âmbito empresarial não corresponde a uma adulteração do substrato personalístico inerente à pessoa coletiva, ainda que hoje já se fale na utilização de sistemas de inteligência artificial na administração de sociedades comerciais[163]. De todo o modo, será a evolução desta área, mas principalmente, as opções legislativas, que vão demonstrar o caminho que a inteligência artificial vai seguir. Ou teremos um sistema auxiliador na tomada das decisões, pondo em perspetiva quais as consequências de determinado comportamento empresarial em função do risco de incumprimento, estando ainda o poder de decisão no agente físico, ou por outro lado teremos um sistema mais evoluído com poderes de decisão autónomos e autonomia suficiente para detetar, prevenir e reprimir ilícitos, impedindo que os riscos se constituam em factualidade sem passar por mãos humanas.

Qualquer que seja o caminho optado, apesar de não sermos isentos e críticos a uma opção de pura autonomia da máquina, para a questão que nos interessa, o problema acaba por ser o mesmo: o de saber, caso ocorra um crime, apesar da implementação de um *criminal compliance* "inteligente", se a empresa (programadora ou utilizadora), enquanto ente autónomo com personalidade jurídica suscetível de lhe ser imputada responsabilidade, ainda assim, assumirá a responsabilidade ou se, mais uma vez, procurará transferi-la para um "terceiro", nomeadamente, para o sistema autónomo que auxiliou a tomada da decisão e não conseguiu prever a ocorrência da factualidade típica. Trataremos desta problemática a seu tempo.

Cabe ainda nesta sede distinguir o *criminal compliance* "inteligente" do conceito de *RegTech*. Mantendo coerência de discurso no que diz respeito à relação do *compliance*

[163] Em 2014, a empresa de capital de risco *Deep Knowledge Ventures* integrou no seu órgão de administração um sistema de inteligência artificial – denominado "VITAL" (*Validating Investment Tool for Advancing Life Sciences*) que aconselhou os administradores a investir em determinadas empresas no campo das ciências da vida, tendo voto expresso nas deliberações sobre esses investimentos. Este voto por parte do sistema tinha por base uma análise de risco ao capital em questão, tendo em conta uma vasta gama de dados inseridos no sistema acerca de investimentos semelhantes em outras empresas da área, procurando fazer uma previsão da liquidez do investimento concreto. Cfr. WILLIE, Rob, «A Venture Capital Firm Just Named An Algorithm To Its Board Of Directors — Here's What It Actually Does», *Bussiness Insider*, 13 de mai. de 2014.

regulatório com o *criminal compliance*, o mesmo se dirá e a mesma relação se apresenta entre os instrumentos de *RegTech* e o *criminal compliance* "inteligente": a *RegTech* corresponde ao conjunto de medidas internas que utilizam inteligência artificial ou outras tecnologias (exprimidas através de *softwares*), procurando proceder à monitorização da atuação empresarial dentro do risco permitido decorrente das disposições normativas do sistema regulatório (axiologicamente menos denso do que o risco permitido no âmbito do sistema penal)[164]. Ou seja, a distinção entre estes dois conceitos, à semelhança da de *compliance* regulatório e de *criminal compliance*, faz-se tendo por base a densidade axiológica das condutas que pretende regular e prevenir, tendo para tal remédios distintos.

Feitas as necessárias distinção e integrações dogmáticas, importa concretizar a interligação entre estes algoritmos "inteligentes" e o *criminal compliance*, concretamente, na influência que estes poderão ter nos elementos integrantes do programa de *compliance*.

1.2. Elementos e efeitos do *criminal compliance* "inteligente"

A integração da inteligência artificial no *criminal compliance* espelha uma modernização relevante, útil e, provavelmente, inevitável. Este passou a ser visto, mais do que um custo da atividade empresarial[165], como um verdadeiro investimento e instrumento de valorização da empresa[166]. Para tal, nas clássicas funções de prevenção, deteção e repressão, a introdução da inteligência artificial neste âmbito permite melhoramentos distintos no incremento do valor económico, mas também numa maior eficiência dos processos. Desde logo, a elevada capacidade de resposta destes instrumentos permite «aumentar a segurança em contexto empresarial prevendo, prevenindo e detetando atos lesivos de interesses juridicamente

---

[164] Para distinguir a vertente de prevenção criminal com o escopo regulatório importa aproveitar a distinção tipológica de *RegTech* dada por ENRIQUES, Luca, «Financial supervisors and Regtech: Four roles and four challenges», *Revue Trimestrielle de Droit Financier* n. º 53, 2017, p. 3 e 4. O Autor distingue no conceito amplo de *RegTech* quatro outros conceitos quanto às suas finalidades: *Operations RegTech*, *ComplianceTech*, *OversightTech* e *PolicymakingTech*. Os dois primeiros estão interligados ao problema que ora nos ocupa, isto é, dizem respeito à análise de risco nas operações da empresa (de uma perspetiva económica) e à atuação dentro do risco permitido, dando cumprimento às disposições normativas. *OversightTech*, o Autor inclui neste conceito aquilo que nós designámos por *SupTech* (tal como a maioria da doutrina). Por fim, *PolicymakingTech* diz respeito à utilização de tecnologia por parte dos reguladores para fazer uma análise do próprio sistema regulatório e poder melhorar a eficácia normativa. Em síntese, percebe-se que a utilização do termo *RegTech* está intimamente associado ao setor regulatório.

[165] Expressão traduzida de Deloitte, «Compliance modernization is no longer optional: How evolved is your approach?», p. 3 («more than just a cost of doing business»).

[166] *Ibid.*, *loc. cit.*, como mostra o estudo estatístico feito, 61% dos mais de 550 inquiridos assumem que houve aumentos no investimento em *compliance* nas suas organizações entre 0 e 20% ou mais.

valiosos, vigiando e monitorizando o espaço e as pessoas que nele intervêm»[167]. No entanto, tudo dependerá do estado de maturidade e de desenvolvimento da "inteligência" do *criminal compliance*[168].

Num primeiro momento de desenvolvimento, temos aquilo que se designa por *robotic process automation* ou RPA (automação robótica de processos), que corresponde à utilização de um *software* composto por "trabalhadores virtuais" (*bots*) que realizam tarefas repetitivas por forma a agilizar processos com altos graus de eficácia e precisão, eliminando a variável dada pelo erro humano (tecnicamente, porque estes algoritmos terão sempre a intervenção humana). Estes sistemas apresentam-se no primeiro grau evolutivo pelo facto de terem apenas capacidade para executar as funções para as quais foram dados *inputs*, não tendo capacidade para aprender e melhorar em função do ambiente onde se inserem (são os chamados *deterministic robots* a que já nos referimos[169]). Como exemplos, existe RPA a nível mecânico, visível nas fábricas de automóveis na montagem de peças, ou a nível de *software*, como acontece na recolha e atualização de dados em *call centers* ou *help desks* e *chatbots* de *websites*, ou ainda certos *softwares* de *high frequency trading*. Os *bots* aqui em causa têm capacidade para recolher informação e compartimentá-la em função de uma certa padronização de comportamentos que lhes sejam cognoscíveis (através de transações, contactos suspeitos, utilização de palavras dissimuladas) ou caraterísticas específicas (montantes idênticos, datas de transações semelhantes), podendo auxiliar a função investigatória do *criminal compliance*, por exemplo, após o acionamento da "*red flag*" que considere uma transação suspeita. Sem estes sistemas, as funções aqui em causa seriam realizadas manualmente pelo departamento de *compliance* que, necessariamente, demorará mais a compartimentar e a averiguar a veracidade de toda a informação, pelo que um sistema como este facilita quantitativa e qualitativamente tarefas extremamente volumosas, eliminando ou mitigando das variáveis alguns fatores exógenos do ser humano como o erro ou o cansaço. Contudo, este não é um sistema totalmente perfeito já que estes algoritmos, porque não possuem uma capacidade de aprendizagem quando deparados com novas

[167] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 195.
[168] Distinguindo os conceitos e aplicações práticas dos sistemas inteligentes no âmbito do *compliance*, KPMG, «Intelligent automation in financial crimes: forging an innovative compliance strategy for the future», p. 4 - 6.
[169] Que se opõem aos *cognitive computers* ou *cognitive systems*, como vimos *vide supra* nota 42 e 43.

variáveis, podem dar azo a "falsos positivos", isto é, por exemplo, a sinalizar como potencial ilícito uma transação ou conduta lícita.

É com o desenvolvimento para o segundo estado de maturação que esta capacidade aumenta. Este segundo estado prende-se com a utilização de *softwares* mais desenvolvidos concebidos através de técnicas de *machine learning*, que conseguem prever resultados e aprender em função do ambiente onde se inserem. Estes sistemas procuram aumentar a eficiência dos processos já dados pela RPA, procurando eliminar ou mitigar os "falsos positivos", tendo em conta dados adquiridos anteriormente dentro e fora da instituição.

Por fim, o estado de maior desenvolvimento do *criminal compliance* "inteligente" utiliza já técnicas de *cognitive computing* e *semantic computing* (através de processos de *machine learning*, *knowledge representation* e *natural language process*) e representa a possibilidade de não só replicar o comportamento e racionalidade humana, nomeadamente a capacidade para analisar e interpretar grandes quantidades de dados, como para ultrapassá-la. Este tipo de sistemas não se baseia apenas em dados pré-concebidos, mas também em dados casuísticos da empresa, o que lhe permite com ainda mais exatidão atuar em função dos riscos, procedimentos e atuações anteriores.

Estes estados de maturação devem ser vistos como um *continuum*, servindo os dados adquiridos através de RPA (primeiro estado de maturação) úteis para a criação de algoritmos de *machine learning* (segundo estado de maturação) onde o *cognitive software* (terceiro estado de maturação) se vai basear para atingir o expoente máximo de eficácia e eficiência. No entanto, este tipo de sistema não se fica por aqui, isto é, não atua apenas em função de dados não estruturados ou estruturados previamente. Faz ainda previsões na identificação de padrões, fazendo o levantamento desse potencial risco antes sequer deste se consumar em algo factual (algo humanamente complexo e moroso). É por esta razão que se enaltece a importância destes sistemas para a problemática do *criminal compliance*, uma vez que poderão auxiliar a detetar novas formas de cometimento de crimes.

No que concerne ao próprio conteúdo do *criminal compliance*, é possível refletir sobre a utilização destes três tipos de sistemas em dois domínios[170]: na análise do risco e na eficácia do próprio programa.

[170] KPMG, «Intelligent automation in financial crimes: forging an innovative compliance strategy for the future», p. 10 – 13.

Quanto à análise do risco (incluindo-se aqui a monitorização de transações ou análise da contraparte (*know your costumer – KYC*)), a utilização deste tipo de sistemas é principalmente indicada uma vez que em causa estão, na maioria das vezes, juízos preditivos probabilísticos. Em concreto, a RPA poderá ser utilizada para verificação de dados relevantes e compilar toda a informação relevante num documento, facilitando, em tempo e trabalho, as diligências do departamento de *compliance* que o irá analisar e decidir em função disso[171]. Já os *softwares* que utilizam técnicas de *machine learning*, por se caraterizarem por estarem num estado de evolução seguinte, tudo o que a RPA consegue fazer, também o sistema com *machine learning* fará e, à partida, melhor e de forma mais rápida. Neste âmbito, procederá a uma análise dos dados destruturados e à sua revisão, emitindo o juízo probabilístico acerca da viabilidade da transação ou da decisão em causa, devendo, contudo, haver ainda uma tomada de opção consciente e racional do agente humano responsável, dado que há ainda a possibilidade de tipificação de "falsos positivos". Por fim, os chamados *cognitive systems* baseiam-se nos alertas emitidos anteriormente e, segundo os padrões da empresa, caso haja um desvio a essa norma, é emitido um alerta para a análise humana. É por esta razão que estes sistemas podem ser utilizados diretamente nas medidas de controlo interno, auditorias e análise de riscos (*risk assessment tools*) na deteção de crimes de branqueamento de capitais ou criminalidade empresarial conexa que possa implicar o cruzamento de dados. As finalidades destes tipos de sistemas acabam por se assemelhar ao intuito da *predictive policing*[172] (polícia preditiva), que procura identificar e impedir um crime antes de ele acontecer tendo em conta juízos analíticos e probabilísticos.

Mais a mais, estes sistemas podem utilizar técnicas de *semantic computing* para avaliar e verificar a veracidade dos dados presentes no sistema empresarial tendo por base *fact-checkers* (como é o caso da *Factiva* ou o *WorldCheck*[173]).

No que diz respeito à eficácia do *criminal compliance*, a utilização destes sistemas pode também ser benéfica no sentido em que os testes da eficácia das medidas internas são

[171] Neste sentido, *Ibid.*, p. 11: «Deploying the bot to complete these research and record-keeping tasks, saves the analyst valuable time».
[172] MEIJER, Albert / WESSELS, Martijn, «Predictive policing: review of benefits and drawbacks», *International Journal of Public Administration*, Vol. 42, Issue 12, 2019, p. 1032.
[173] KPMG, «Intelligent automation in financial crimes: forging an innovative compliance strategy for the future», p. 6 e 12.

processos repetitivos e morosos[174]. Em concreto, a RPA pode auxiliar na análise da consonância da conduta da empresa com os dados pré-concebidos nos códigos de conduta e ética. Os sistemas de *machine learning* podem auxiliar na eficácia do *criminal compliance* no âmbito dos canais de denúncias, podendo analisar as denúncias que possuem (ou não) fundamento para avançar para investigação interna, para que o departamento de *compliance* possa atuar em conformidade, evitando que seja o próprio departamento a realizar essas tarefas e a atrasar outros processos que possam, de facto, vir a constituir investigações. Por último, os *cognitive systems* têm a capacidade para, por exemplo, emitir juízos preditivos acerca do cometimento de crimes por determinado membro da empresa, no âmbito das investigações internas, determinar a mais adequada sanção interna a aplicar em caso de violação de alguma disposição interna, ou, mais ambiciosamente, antecipar a promoção processual e o seu desfecho quando seja esse o caso. Neste último ponto, poderão surgir algumas dúvidas relativamente à admissibilidade da utilização destes sistemas no desfecho das investigações internas, gerando-se as mesmas relutâncias originadas aquando da utilização de sistemas preditivos na justiça penal (o potencial viés e discriminação algorítmica e a falta de transparência na decisão)[175].

Ainda assim, qualquer uma destas soluções (mais ou menos desenvolvidas) ambiciona melhorar a eficácia do *criminal compliance*, tanto *ex ante* como *ex post*, pelo que se torna essencial a manutenção e o acompanhamento de soluções de inteligência artificial no âmbito da prevenção da criminalidade empresarial, sem nunca se prescindir do fator humano para a tomada da decisão final[176].

Mas, e no plano ético-legal? Como poderá o *criminal compliance* "inteligente" ser relevante?

---

[174] Refletindo sobre o caso concreto da utilização da inteligência artificial nas investigações internas, MUELLER, Tim / SISWICK, James, «How Can Artificial Intelligence Augment the Investigative Process?», *in Corporate Investigations* 2020, International Comparative Legal Guides, 4th ed., Cap. 3, 2020, p. 15 – 20.

[175] RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 20 e ss.

[176] Neste sentido, MUELLER, Tim / SISWICK, James, *Op. cit.*, p. 18 («AI cannot (at least not yet) take the place of human intuition – no matter how advanced the technology becomes»). Já quanto ao facto da modernização do *compliance* ser uma mais-valia, Deloitte, «Compliance modernization is no longer optional: How evolved is your approach?», p. 14 («A modernized Compliance function can be an organization's most finely tuned way to monitor what's happening inside its four walls and what's coming from outside them»).

2. A ética corporativa no âmbito do *criminal compliance* "inteligente"

Do que ficou dito, ficou assente que a utilização de um *criminal compliance* "inteligente" representa uma mais-valia para a função da prevenção da criminalidade empresarial em diversas vertentes. No entanto, estes algoritmos atuam em função da sua programação e, portanto, de dados analíticos baseados em proposições matemáticas, considerando o lícito e o ilícito de uma perspetiva estritamente programática. Para tanto, como já se disse, o cumprimento normativo não é (ou deve ser) apenas normativo num "cego" cumprimento da lei. Deve ser um cumprimento normativo de fundamento ético, baseado em princípios éticos. Será a decisão algorítmica uma decisão conciliável com princípios éticos?

Cabe, antes de tudo, esclarecer que, até por não ser o objeto do atual ponto de discussão, não se procederá a uma conceitualização e distinção desenvolvida entre ética e moral[177] e ética e direito[178]. Simplesmente considerar-se-á o termo ética, uma vez que é a opção doutrinal mais recorrente no âmbito empresarial, mas também pois falamos da atuação de uma coletividade na comunidade; coletividade essa composta por indivíduos cujos padrões de conduta, na globalidade, caraterizam a ética corporativa[179]. Por outro lado, a moral remete-nos para o prisma interno e pessoalista de cada agente individual. Tudo isto, porém, espelha uma realidade "transnormativa", pelo que não se pode olvidar «(…) que a moral se estende muito para além do direito (…)»[180-181].

Em concreto, a importância deste problema advém da relevância que a ética possui não só no âmbito do *compliance* como da inteligência artificial.

Em primeiro lugar, a integração da ética no meio coletivo (especificamente no âmbito empresarial) espelha-se na boa governança societária (*good corporate governance*) «não só

---

[177] Estes termos costumam inclusive ser utilizados como sinónimos. Etimologicamente a palavra ética, deriva do grego *ethos*, que foi traduzido para o latim *mores*, de onde deriva a palavra moral. Cfr. BARTNECK, Christoph *et al.*, *An Introduction to Ethics in Robotics and AI*, Springer Nature, 2021, p. 17. E também, fazendo a distinção filosófica entre estes dois termos, SOLOMON, Robert C., «Introduction to Ethics» *in* ZIMMERLI, Walter Ch. / RICHTER, Klaus / HOLZINGER, Markus (eds.), *Corporate Ethics and Corporate Governance*, Springer, Berlim, Heidelerg, 2007, p. 17 e ss.

[178] Para este propósito, MARQUES, Mário Reis, *Op. cit.*, p. 24 – 44; e, CUNHA, Paulo Ferreira da, *«Crimes & Penas: Filosofia Penal»,* Almedina, 2020, p. 101 – 116.

[179] RODRIGUES, André Alfar, *Op. cit.*, p. 32.

[180] DURKHEIM, Emile – La Science positive de la morale en Allemagne, (trad.) CASTANHEIRA, Paulo, *Ética e Sociologia da Moral*, 2.ª ed., São Paulo, Landy, 2006, p. 54 *apud* CUNHA, Paulo Ferreira da, *Op. cit.*, p. 113. Neste sentido também, BARTNECK, Christoph *et al.*, *Op. cit.*, p. 22 (« (…) ethics starts where the law ends»).

[181] CUNHA, Paulo Ferreira da, *Op. cit.*, p. 104. Desta forma, não nos podemos esquecer que «(n)em tudo o que é permitido é honesto, é moral ou eticamente positivo», mas principalmente que «o Direito não é a Moral, não se lhe subordina mecanicamente; mas, do mesmo modo, não pode ser intrinsecamente imoral».

com a necessidade de as empresas desenvolverem regras de comportamento técnicas, tendo em vista o cumprimento das normas legais (…), mas também com a exigência de que promovam valores éticos que orientem a sua atividade, imprimindo uma cultura ética empresarial, que, aliás, está na base do cumprimento normativo»[182]. Assim, por diversos fatores (poder de influência, poder económico, reputação e receio de os perder), a ética corresponde à trave mestra que norteia (ou deve nortear) a atuação da organização, valendo os princípios éticos de *soft law* quase como *hard law*[183]. Daqui se retira o conceito de responsabilidade social corporativa (RSC), enquanto rosto de uma visão empresarial de desenvolvimento sustentável daquilo que vai além da estrita obtenção de lucros[184]. É esta perspetiva que a visão ética dos programas de *compliance* visa trazer para o meio empresarial, isto é, a integração na empresa de princípios e valores com o objetivo de guiar o comportamento individual e do grupo nos negócios[185].

Por outro lado, a ética releva no âmbito da inteligência artificial em duas perspetivas consequenciais: a ética na programação da inteligência artificial e a ética da inteligência artificial. A primeira diz respeito à atuação humana dentro de padrões éticos na programação da inteligência artificial, enquanto a segunda diz respeito à atuação do próprio sistema dentro de padrões éticos[186].

---

[182] RODRIGUES, Anabela Miranda, *Direito Penal Económico*…, *Op. cit.,* p. 94. É neste contexto que se distinguem no âmbito do *compliance* dois modelos de abordagem: um modelo de promoção de cultura ética no cumprimento e um modelo de vigilância e controlo. Cfr. *Ibid*., p. 106.

[183] Sobre desta ideia, BARTNECK, Christoph *et. al.*, *Op. cit.*, p. 22.

[184] *Vide supra* nota 138. Podemos definir responsabilidade social corporativa como um conjunto de responsabilidades económicas, legais, éticas e filantrópicas vinculadas às empresas. Cfr. MATTEN, Dirk / MOON, Jeremy, «Pan-European Approach. A Conceptual Framework for Understanding CSR» *in* ZIMMERLI, Walter Ch. *et al.* (eds.), *Corporate Ethics and Corporate Governance*, *Op. cit.*, p. 181. Discordando de uma ideia de responsabilidade social das empresas, centrando-se, por outro lado, no individualismo corporativo, FRIEDMAN, Milton, «The social responsibility of business is to increase its profits» *in* ZIMMERLI, Walter Ch. / RICHTER, Klaus / HOLZINGER, Markus (eds.), *Corporate Ethics and Corporate Governance*, Springer, Berlim, Heidelerg, 2007, p. 173 («Presumably, the individuals who are to be responsible are businessmen, which means individual proprietors or corporate executives (…). In a free-enterprise, private-property system, a corporate executive is an employee of the owners of the business. He has direct responsibility to his employers. That responsibility is to conduct the business in accordance with their desires, which generally will be to make as much money as possible while conforming to the basic rules of the society, both those embodied in law and those embodied in ethical custom»).

[185] Um estudo empírico veio mostrar que a introdução desta visão de cultura ética no âmbito empresarial contribui para a eficácia dos programas de *compliance*, não os tornando meramente programas "de máscara". Cfr. WARREN, Danielle E. / GASPAR, Joseph P. / LAUFER, William S., «Is Formal Ethics Training Merely Cosmetic? A Study of Ethics Training and Ethical Organizational Culture», *Business Ethics Quarterly,* Vol. 24, n. º 1, 2014, p. 85 - 117.

[186] Fazendo esta distinção, SIAU, Keng / WANG, Weiyu, «Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI», *Journal of Database Management*, Vol. 31, issue 2, Missouri University of Science and Technology, 2020, p. 73.

No que concerne à programação, o necessário controlo ético surge da possibilidade de sistemas de inteligência artificial poderem lesar direitos humanos. Deste modo, o controlo terá que começar *ex ante*, na fase da criação do sistema, incutindo o programador as balizas éticas por forma a ser possível ter um sistema "(con)fiável" (*trustworthy AI*)[187].

Já a ética da inteligência artificial corresponde à consequência de uma programação eticamente balizada. É, todavia, neste ponto que surgem maiores obstáculos.

No nosso caso específico, um *criminal compliance* "inteligente" programado para prevenir a responsabilidade, em face de um risco que lhe é apresentado, terá, ao mesmo tempo, a capacidade de decidir pelo cumprimento e, mais do que isso, pelo cumprimento ético? Tal atuação irá ser definida, em primeiro lugar e obrigatoriamente, pelo seu algoritmo, mas também pelo seu grau de desenvolvimento e maturidade. Atuará o sistema seguindo o objetivo segundo o qual foi programado, isto é, o cumprimento, ignorando tudo o resto? E nas situações em que a opção pelo cumprimento (portanto, a de menor risco do incumprimento) corresponder a uma atuação antiética e/ou de maior risco de lesão de outros bens jurídicos penalmente relevantes (por exemplo, o programa de *compliance* "inteligente" de uma empresa detetou uma fraude interna e optou por não validar a deteção e proceder à investigação interna pelos riscos económicos ou reputacionais que tal poderia gerar; um *robo-advisor* induz o investidor em erro para que a empresa receba a comissão de utilização do serviço; um sistema "inteligente" de uma empresa cria inúmeras contas *bot* nas redes sociais para fins de *marketing*; uma empresa, através de um *software* "inteligente" para recrutamento, opta por excluir do processo todos os candidatos de uma determinada religião ou etnia).

A dificuldade aqui prende-se com a incapacidade de sistemas de inteligência artificial, programados através de processos lógicos e atuando através de inferências e deduções, possuírem uma "moral interna própria"[188]. Por esta razão, dificilmente sistemas como estes

[187] Em geral, são reconhecidos quatro princípios básicos na formulação destas balizas éticas: o princípio do respeito pela dignidade humana; o princípio da prevenção do dano; o princípio da justiça; o princípio da explicabilidade. Cfr. *The European Commission's High Level Expert Group on Artificial Intelligence*, «Ethics Guidelines for trustworthy AI», abr. 2019, p. 12 e ss. Para uma análise aprofundada dos vários critérios por diversos grupos de investigação, *vide* SIAU, Keng / WANG, Weiyu, *Op. cit.*, p. 77 e ss.; ou também, BARTNECK, Christoph *et. al., Op. cit.*, p. 28 e ss.

[188] BARTNECK, Christoph *et. al., Op. cit.*, p. 22 («The main difference between humans making moral decisions and machines making moral decisions is that machines do not have "phenomenology" or "feelings" in the same way humans do. They do not have "moral intuition" or "acculturation" either»).

têm a capacidade para se tornar no "cérebro ético" das pessoas jurídicas e decidir questões éticas para além daquele que é o seu fim programático[189].

Notoriamente é um problema de conflito de deveres. Contudo, é um conflito de deveres humanos. Só seres humanos têm a capacidade para distinguir binómios axiológicos (o bem do mal, o certo do errado, o lícito do ilícito). Caso se depusesse o mesmo conflito de deveres ao sistema de IA, este optaria friamente por aquele que consubstanciasse a solução mais conforme com o seu algoritmo, ignorando a ordem ético-moral que pudesse estar em causa, independentemente de a solução sacrificada ser de maior interesse ético-social em ser salvaguardada.

Daqui, poder-se-á concluir que quanto maior for a autonomia atribuída ao sistema, maior será a probabilidade da cultura ética sair prejudicada. Esta estatuição baseia-se no facto de o sistema apenas analisar o problema segundo um prisma programático e probabilístico do risco/benefício[190]. Com efeito, «(a) autonomia dos robots é uma autonomia tecnológica, fundada nas potencialidades da combinação algorítmica que é fornecida ao *software*. Está, portanto, longe do agir ético dos humanos, em que radica o ser pessoa»[191].

Neste sentido, apenas com a evolução exponencial da inteligência artificial será possível criar um sistema com capacidade moral autónoma (e será? e será viável ou desejável?)[192]. Desta forma, e remetendo para o *compliance* de cada empresa, apenas construindo o algoritmo empresarial com base em princípios éticos (nomeadamente aqueles presentes nos códigos de conduta e ética do programa de *compliance*) seria possível mitigar os conflitos éticos. No entanto, pelas caraterísticas que são inerentes ao algoritmo, certamente haverá situações imprevisíveis. Com efeito, conclui-se que da mesma forma que os programas de *compliance* «devem ser "feitos à medida" (*tailor made*)»[193], também os sistemas de inteligência artificial (principalmente aqueles que se inserem no âmbito do *criminal compliance*) o devem ser, nomeadamente, através da programação concreta dos valores

---

[189] Mostrando que a intencionalidade do sistema é a intencionalidade do seu programador, JOHNSON, Deborah G., «Computer systems: moral entities but not moral agents», *Ethics and Information Technology*, n.º 8, 2006, p. 201.

[190] VECCHIO, Fabrizio Bon / VIEIRA, Débora Manke, «Compliance Programs and Artificial Intelligence», *Studia Prawnicze: rozprawy i materiały*, Issue 1 (28), 2021, p. 61. Também, esclarecendo este quociente com exemplos concretos, BARTNECK, Christoph *et. al.*, *Op. cit.*, p. 23 e ss.

[191] BARBOSA, Mafalda Miranda, «Inteligência artificial, *e-persons* e direito: desafios e perspetivas», *Revista Jurídica Luso-Brasileira*, Ano n.º 3, n.º 6, 2017, p. 1482.

[192] RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 54 («Pode ser tecnicamente possível criar sistemas de IA que atendam aos requisitos contemporâneos de agência moral. Mas, mesmo que seja possível, nada disto faz com que seja necessário ou devamos fazê-lo»).

[193] *Id.*, *Direito Penal Económico…*, *Op. cit.*, p. 104.

éticos seguidos pela empresa, por forma a minimizar os efeitos desfavoráveis decorrentes de decisões antiéticas.

Até lá, numa perspetiva mais realista, novamente, antecipa-se uma preferência para as empresas "manterem o controlo" e utilizar sistemas de inteligência artificial para seu auxílio e não como sistemas autónomos de decisão final.

Capítulo III – O *Criminal Compliance* "inteligente" na Responsabilidade Penal das Pessoas Coletivas: da factualidade ao processo

1. O *Criminal Compliance* "inteligente" no par omissão-ação típica: prolegómenos de uma problemática futura

Chegámos, por fim, ao núcleo e propósito das ideias expostas até esta parte. As considerações feitas até aqui relevam para se compreender a importância prática que os problemas embrionários da inteligência artificial poderão gerar num futuro próximo na dogmática jurídico-penal que, como sabemos, foi construída tendo por "cortina de fundo" a pessoa física. Ainda assim, factualmente, são as pessoas coletivas que produzem, utilizam e mais beneficiam com a introdução dos algoritmos nas suas estruturas[194].

Ficou consolidado que a inteligência artificial é já uma realidade em diversos ramos e, em concreto no ambiente empresarial, soluções de prevenção criminal "inteligentes", pelas suas diversas utilidades económicas e processuais, serão cada vez mais desenvolvidas e adotadas pelos agentes económicos. Para além disto, não obstante as louváveis intenções da introdução destes sistemas no *compliance* empresarial, os riscos que daí poderão advir não são retirados da equação.

Recuando ao início da discursividade, o potencial cataclísmico associado à introdução da inteligência artificial enunciado por muitos advém, primordialmente, do receio da criação de um ente autónomo que se afaste da esfera de controlo do ser humano e que seja capaz de lhe causar danos e ao mundo que o rodeia. Já os próprios ficcionistas consideravam a existência de um "ente inteligente" que, apesar de toda a sua falta de humanidade (no sentido da palavra da presença de células orgânicas), fosse programado para respeitar o seu criador e, em geral, a espécie humana[195]. Já ficou também assente que é possível haver violações à

[194] DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 159 («(t)oday's most impactful algorithms are closely tied to the corporations who develop and use them for their own ends»).

[195] Um desses ficcionista, Isaac Asimov, criou aquelas que ficaram conhecidas como as Leis da Robótica: 1.ª Lei - um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum dano; 2.ª Lei - um robô deve obedecer às ordens que lhe sejam dadas por seres humanos, exceto nos casos em que entrem em conflito com a 1.ª Lei; 3.ª Lei - um robô devem proteger a sua própria existência, desde que tal proteção não entre em conflito com a 1.ª e 2.ª Leis. Normalmente designam-se apenas três leis da robótica, mas o Autor, mais tarde, acrescentou uma quarta lei (a Lei Zero - um robô não pode causar danos na humanidade, ou, por omissão, permitir a humanidade de sofrer danos). Cfr. RUSSELL, Stuart / NORVIG, Peter, *Op. cit.*, p. 1038 e 1039; e também, BARTNECK, Christoph et. al., *Op. cit.*, p. 32.

1.ª Lei de Asimov («um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum dano»)[196]. Neste sentido, «(o) dano associado à IA, fazendo-se presente, é ainda, num certo sentido, algo impercetível, seja pela sua novidade, seja por uma certa ausência na consciência coletiva»[197].

Este dano poderá ser potencializado e incrementado quando em causa estejam pessoas coletivas. Desde logo, porque ações concertadas levam, na grande maioria das vezes, a resultados muito mais danosos do que uma atuação individual[198]. Foi por esta e outras razões que o legislador procurou, através de expedientes normativos, estender a responsabilidade penal a coletivos de pessoas físicas. Assim, já longe do brocardo romano *societas delinquere non potest*, as pessoas coletivas enquanto «"obras de liberdade ou realizações do ser livre"»[199] passaram a ser pessoas jurídicas passiveis de lhes ser imputada responsabilidade penal[200].

Ora, com a utilidade que a inteligência artificial lhes pode trazer, as pessoas coletivas poderão passar a "desvincular-se" de certo tipo de decisões e deveres e, com isso, de responsabilidades inerentes que a «sociedade do risco»[201] lhes atribui, especialmente, no ambiente de risco a que o *criminal compliance* está sujeito. É neste contexto que se salienta a ideia de MIHAILIS DIAMANTIS de que o estado atual do Direito é alarmante pois estamos a caminhar para uma crescente imunidade empresarial, com a cada vez menor intervenção humana nas operações[202].

Hodiernamente, exemplos concretos destas possibilidades são reais. Relembra-se a morte de Wanda Holbrook em julho de 2015, onde, enquanto procedia ao seu quotidiano trabalho de inspeção de montagem de peças para automóvel, um dos braços de montagem

---

[196] DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 136 e ss. («The first law of robotics is already dead. Robots and the algorithms that run them injure people every day»).
[197] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 61.
[198] Neste sentido, apresentando mais duas ordens de razão pelas quais as pessoas coletivas devem ser responsabilizadas (no caso, por crimes internacionais), SLYE, Ronald C., «Corporations, Veils, and International Criminal Liability», *Brooklyn Journal of International Law*, Vol. 33, 2008, p. 960.
[199] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 347.
[200] Para uma análise extensiva desde os primórdios do direito romano até à atual doutrina portuguesa relativamente à admissibilidade dogmática da responsabilização das pessoas coletivas, cfr. BRAVO, Jorge dos Reis, *Op. cit.*, p. 33 – 48; de forma mais sintética e objetiva, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.* p. 77 – 84; ou para uma análise legislativa e jurisprudencial no ordenamento jurídico português, SILVA, Germano Marques da, *Op. cit.*, p. 24 – 48.
[201] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 154 e ss.
[202] DIAMANTIS, Mihailis E., «The Extended Corporate Mind: When Corporations use AI to Break the Law», *Op. cit.*, p. 899 («the current state of law is troubling because it all but guarantees that corporations will become increasingly immune to liability as their operations require less and less human intervention»).

"inteligente" excedeu a área de segurança delineada, entrando na secção onde esta se encontrava, infligindo-lhe uma pancada mortal na cabeça[203]. Também o caso de Elaine Herzberg que, em 2018, foi fatalmente atropelada por um carro autónomo da Uber que não a identificou, não tendo travado[204].

Estes e outros casos ocorrem, dado que a inteligência artificial, por mais desenvolvida que seja, é sempre falível. Desde logo porque é programada por seres humanos, que são, de forma inata, agentes que erram. Mesmo os algoritmos de *machine learning* que aprendem "por si", dependem sempre de uma primeira intervenção humana (existem é algoritmos que necessitam de maior ou menor intervenção no processo de aprendizagem). Por esta ordem de ideias, se o sistema falha inexplicavelmente, torna-se capaz de causar danos e de praticar factos (considerados por nós) ilícitos.

Deste modo, de uma forma genérica, dispõem-se quatro possíveis cenários de interligação da IA a factos ilícitos: (1) um robô[205] é deliberadamente programado para cometer o crime; (2) um robô comete um crime porque foi culposamente programado defeituosamente; (3) um robô comete um crime pois tomou uma decisão moralmente censurável pré-programada; (4) um robô comete um crime fruto de uma decisão gerada pelo seu próprio sistema "inteligente". Qualquer um dos cenários pode gerar problemas em sede de causalidade, mas também de culpabilidade[206]. Isto porque, havendo a lesão de um bem jurídico com a tipificação de uma conduta ilícita, a responsabilidade penal daqui decorrente pressupõe um juízo de imputação que estabeleça o nexo causal probabilístico entre o agente que praticou uma conduta desvaliosa e a lesão causada (imputação objetiva) e um juízo de imputação que censure ético-socialmente o agente pela conduta que praticou (imputação subjetiva). Ora, quando a inteligência artificial entra como variável, vários pressupostos ficam por subsumir em ambos os juízos.

No que diz respeito às primeiras três situações, não se trata de um problema absolutamente novo. Um crime consumado por ou através de um sistema de inteligência

---

[203] Caso *Holbrook v. Prodomax Automation Ltd. et al.*, 09-20-2021, 1:17-CV-2019, United States District Court, Western District of Michigan, Southern Division.

[204] O automóvel detetou o "obstáculo" 6 segundos antes do embate (a uma distância de 115m), mas apenas determinou ser necessário utilizar a travagem de emergência 1,3 segundos antes do embate. *A contrario*, isto significa que durante 4,7 segundos o sistema não considerou que fosse necessário a utilização da travagem de emergência. Cfr. National Transportation Security Board, Preliminary Report Highway HWY18MH010, 2018.

[205] Quando se utiliza a expressão «robô» neste contexto não se inclui apenas sistemas mecânicos, mas também informáticos.

[206] SIMMLER, Monika / MARKWALDER, Nora Mark, *Op. cit.*, p. 7 e 8.

artificial programado, ou programado defeituosamente para esse fim, não difere, em sede de imputação, de um crime cometido através da utilização de meios informáticos (os chamados crimes informáticos)[207]. Neste tipo de situações, o tipo objetivo e subjetivo é preenchido por uma pessoa singular ou coletiva, sendo o meio informático o instrumento ou o produto através do qual o crime foi cometido (é a "arma do crime"). Um exemplo deste tipo (mas com a utilização de um sistema de inteligência artificial) ocorreu no âmbito dos mercados financeiros com o caso *U. S. v. Coscia*[208], onde Michael Coscia, utilizando um algoritmo de *high frequency trading*, se tornou o primeiro condenado pelo crime de manipulação do mercado (por prática de *spoofing*)[209].

Neste prisma, a maioria das questões suscitadas nos três primeiros casos poderão incluir-se diretamente na atual dogmática jurídico-penal, através dos típicos modelos de imputação da responsabilidade das pessoas coletivas.

Por fim, a situação que apresenta maiores dificuldades em sede de imputação, e aquela que nos ocuparemos de tratar, é o caso dos chamados «*Hard AI Crimes*»[210]. Neste caso, o sistema «tem capacidade para, perante um *input* que lhe é dado, produzir, com autonomia, informação não previsível nem programada (…). Este *output* que resulta do algoritmo pode concretizar-se numa opção que causa danos a interesses jurídicos protegidos pelo direito penal»[211]. Numa palavra, falamos aqui das situações de *strong black box* acima explanadas. Recuperando, são as situações em que a decisão e o processo de decisão algorítmica é opaco, extrapolando as capacidades de compreensão e previsibilidade humanas. Estas situações ocorrem quando o sistema "inteligente" falha e produz autonomamente um resultado diferente do esperado, praticando um crime (delitos de ação) ou permitindo que este ocorra (delitos de omissão).

Neste contexto, e já que o *criminal compliance* "inteligente" se situa numa realidade *ex ante* da responsabilidade penal, um sistema deste tipo está programado para prever a

---

[207] Estabelecendo esta comparação, BATHAEE, Yavar, *Op. cit.*, p. 901 e ss. («For example, we may infer from a computer program designed to break into a computer system that its creator intended to use it for that purpose. In some cases, we can look at the computer program's instructions to determine what the designer of the program was trying to accomplish and what means could be used by the program to accomplish that goal»).

[208] Caso *United States. v. Coscia*, 08-07-2017, n. º 1:14-cr-00551-1, United States District Court for the Northern District of Illinois, Eastern Division.

[209] Sobre alguns contornos do caso e dos respetivos efeitos jurídico-penais, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 63 e ss.

[210] ABBOT, Ryan / SARCH, Alex, «Punishing Artificial Intelligence: Legal Fiction or Science Fiction», *University of California, Davis Law Review*, Vol. 53, 2019, p. 328.

[211] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 62.

ocorrência de ilícitos no seio empresarial e prevenir a responsabilidade penal da pessoa coletiva. Deste modo, torna-se uma ferramenta extremamente cobiçada no âmbito empresarial para estes fins. Ao mesmo tempo, cabe ao Direito Penal assegurar que a introdução da inteligência artificial nos programas de *compliance* não se torna num artificio ao dispor das pessoas coletivas para desviarem a sua responsabilidade, apresentando respostas para os vazios normativos e cumprindo a sua função de tutela subsidiária dos bens jurídico-penais.

Os obstáculos aqui surgem se o sistema falhar na prevenção e permitir a ocorrência de um crime. De que forma é valorada esta falha na responsabilidade? E caso seja o próprio sistema a praticar um crime, quem responsabilizar? Será o sistema de inteligência artificial um agente do crime, ou um instrumento a partir do qual ele foi cometido/permitido? São estas interrogações que catalisam o problema do vazio normativo em sede de responsabilidade penal quando o crime tenha sido cometido por um sistema "inteligente" através de uma decisão espontânea, imprevisível e autónoma (o chamado *AI accountability gap*).

Com a análise destas questões, interrogamo-nos se será este um problema totalmente novo ou se, por outro lado, não será a «responsabilidade das pessoas coletivas: mais uma vez?»[212]. Isto é, indaga-se se não será este um problema de falha do princípio da legalidade com o qual o legislador já se deparou.

Em suma, são as prévias proposições que abrem a discussão do contrabalanço das utilidades práticas e económicas destes sistemas "inteligentes" com o próprio *status quo* penal.

Notemos o seguinte caso hipotético que poderá (ou não) ocorrer num futuro próximo e que ilustrará as disposições seguintes[213].

1.1.Exposição exemplificativa do problema: o caso *NoLock*

A *TechCypher* é uma sociedade comercial de investimento e consultoria na área da tecnologia sediada em Portugal.

[212] Título retratado em RODRIGUES, Anabela Miranda, «The Last Cocktail…», *Op. cit.*, p. 125.
[213] Qualquer semelhança do caso com a realidade é pura coincidência. Ademais, grande parcela do caso em questão integra um *de jure condendo* a partir do qual se presumirão, por razões propositadas e académicas, determinadas situações.

A empresa, em virtude do Decreto-Lei n.º 109-E/2021, de 9 de dezembro, implementou um programa de *compliance* "inteligente" que adquiriu junto da *ComplyTeK*, empresa também sediada em Portugal.

O dito programa de *compliance* "inteligente", denominado *NoLock*, consistia num *software* programado e desenvolvido exclusivamente pela *ComplyTeK*, utilizando para tal técnicas de *machine learning*, *knowledge representation* e *natural language processing.* Mais concretamente, o *software* foi programado através de *deep reinforcement learning*, que utiliza as capacidades de *reinforcement learning* com a profundidade de dados que *deep learning* consegue providenciar através das redes neurais artificiais (*artificial neural networks*), permitindo ao sistema atuar segundo a sua experiência (da tentativa e erro) e tendo por base inúmeras camadas de dados não estruturados. Deste modo, a decisão, apesar de potencialmente opaca ou inexplicável, é extremamente precisa e eficaz.

O *criminal compliance* "inteligente" da *TechCypher* estava já num estado de maturação desenvolvido (há mais de 36 meses no ambiente empresarial em aprendizagem com as práticas de *criminal compliance* da empresa, exercendo funções de análise de risco operacional e prevenção criminal), podendo já ser considerado um *cognitive software.* Em função disto, a administração da *TechCypher* decidiu atribuir esta função exclusivamente ao sistema, mantendo-se o departamento de *compliance* como supervisor das funções inerentes, restruturando a equipa com juristas especialistas em informática e inteligência artificial.

No âmbito das suas competências, o *software* em causa produzia relatórios de risco operacional e criminal em cada ato empresarial (procedimentos de *KYC*), emitindo juízos preditivos sobre determinado acontecimento económico das sociedades a investir (baseando-se em *fact-checkers*), mas também, e principalmente, sobre a iminência de ocorrência de ilícitos interno e externos, com essas transações. Nomeadamente, em caso da deteção prévia de um crime, o sistema procedia ao levantamento de um alerta, podendo, mediante decisão do departamento de *compliance*, impedir ou anular transações económicas, dando conhecimento dessa intenção à sua instituição bancária através de um *e-mail* automático. Numa perspetiva *ex post*, mediante recebimento de denúncia interna, o sistema triava essa notícia com base na possibilidade de ocorrência de responsabilidade penal, mas também segundo os seus interesses económicos, sob pena denúncias infundadas prejudiciais à sua atividade. Não havendo fundamento para a denúncia (com base nos prévios relatórios de análise de risco), esta era armazenada e eliminada ao fim de 30 dias caso não houvesse novos

factos ou indícios idênticos. Por outro lado, procedendo a denúncia, o sistema realizava inquéritos padrão ao denunciante e potenciais testemunhas, agrupando as provas digitais e emitindo um relatório final acerca do caso e das medidas adequadas a tomar. Caberia, por fim, ao departamento de *compliance* a tomada de decisão final sobre o que fazer.

Em certo momento, prosseguindo políticas de globalização, a *TechCypher* passou a celebrar certos negócios jurídicos com empresas *off-shore*, confiando que o *criminal compliance* "inteligente" a avisaria se e quando estivesse em risco elevado de cometimento de ilícitos. Um desses negócios foi celebrado com a *HoldEra*, uma *holding* sediada no Panamá, que estava, naquele momento, a ser investigada pelas autoridades do Panamá por suspeitas de crimes de branqueamento de capitais.

Com efeito, a *TechCypher*, tendo conhecimento destas suspeições, recorreu, como normalmente, ao *criminal compliance* "inteligente" e este procedido às normais diligências de análise de risco operacional e prevenção criminal, não tendo o sistema reportado qualquer risco ou suspeita de crime. Com base no relatório produzido, a *TechCypher* confiou neste e, ainda assim, realizou o negócio, tendo recebido e aceitado uma proposta de 50.000€ por 100% das quotas de uma empresa sua.

Posteriormente, o *NoLock* recebeu uma denúncia interna por suspeitas de crime de branqueamento de capitais. Contudo, o sistema optou por não validar a denúncia, arquivando-a, pois valorou os riscos económicos e reputacionais que tal poderia gerar para a empresa se se tornasse público. Em função desta opção, autonomamente, ao fim dos 30 dias, eliminou a denúncia, mas também todos os registos do negócio com a *HoldEra* (o seu nome, a sua localização, os montantes em causa nos negócios). Para além disto, eliminou também todos os dados informáticos da memória *cache* da empresa onde constasse o nome e a transação do montante em causa (nomeadamente, no relatório de contas).

A *TechCypher* apercebeu-se da eliminação destes dados, tendo-se, ainda assim, conformado com a situação das coisas, pois acreditou que a denúncia que o sistema tivera recebido era danosa para o seu negócio e visava simplesmente o seu prejuízo.

Com o conhecimento desta factualidade, o Ministério Público deduziu acusação, nos termos do art. 368. º-A do Código Penal e do art. 104.º/d) da Lei n. º 15/2001, de 5 de junho, por crimes de branqueamento de capitais e de fraude fiscal qualificada contra a *TechCypher*.

Esta veio alegar que os crimes ocorreram independentemente da sua vontade, por uma falha do sistema, tendo confiado no *software* (que até àquela data tivera cumprido

eficazmente as suas funções) e este atuado autonomamente. Como tal, desresponsabilizou-se, imputando, por outro lado, a responsabilidade à *ComplyTeK* e ao *software NoLock*. Já a *ComplyTeK* veio estatuir a sua irresponsabilidade, afirmando que programou o *NoLock* dentro da licitude, sem qualquer intenção de cometimento de crimes, não conseguindo explicar qual o processo de tomada de decisão do algoritmo, pois este era já um *cognitive software* com capacidade para associar os dados pré-inseridos com os dados decorrentes da experiência e atuação empresarial. Para além disto, justificou o facto de ter programado o sistema segundo técnicas de *deep reinforcement learning* pela sua eficácia e porque o recurso às redes neurais artificias salvaguarda, pela sua opacidade, o algoritmo enquanto segredo de negócio.

Quid iuris?

1.2. A falha do *Criminal Compliance* "inteligente" e o dever de garante no cumprimento

A falha de qualquer programa de *compliance* espelha a sua falta de eficácia, sendo em função disto que uma eventual atenuação ou isenção de responsabilidade da pessoa coletiva pode ser apurada. Neste prisma, já tendo ficado explícitos os modelos de imputação do facto criminal da pessoa coletiva[214], cabe neste ponto apenas confrontar esses modelos e a consequente (falta de) eficácia do *criminal compliance* com os riscos que a introdução da inteligência artificial cria neste âmbito dogmático.

Em boa verdade, o problema a ser dirimido daqui espelha a vertente omissiva do chamado *accountability gap*. Concretamente, o que está aqui em causa é saber como e se podemos subsumir uma "conduta autónoma" de um *software* "inteligente" nos tipos omissivos impróprios. Estes dizem respeito a comportamentos juridicamente devidos (mas não normativamente previstos), tendo em vista a evitação da consumação do crime (art. 10.º CP)[215]. Questão diferente é saber quem é responsável quando o sistema atua, quando se devia ter abstido de atuar, praticando um crime. Aqui já falamos do teórico *accountability gap* que se gera com os resultados desvaliosos provocados por decisões "autónomas" de sistemas de IA[216]. Quanto a estes, abordaremos seguidamente.

---

[214] *Supra*, Cap. I, ponto 2.2.3.
[215] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 1064 e ss.
[216] *Infra* Cap. III, ponto 2.

Por agora, situemo-nos na compatibilização da falha do *criminal compliance* "inteligente" com eventuais deveres jurídicos que se gerem.

Como vimos, um modelo de heterorresponsabilidade (como é o caso do ordenamento jurídico português) baseia-se na imputação do facto à pessoa coletiva pela conduta que um terceiro teve (daí ser vicarial), especificamente, alguma pessoa física organicamente ligada a si (exercendo uma posição de liderança ou pela falha dos deveres decorrentes dessa função) que agiu em seu nome e no seu interesse. Sendo este modelo dogmaticamente antropocêntrico, impondo um elemento de conexão entre pessoas físicas e pessoa coletiva, importa saber como é que a inclusão da variável inteligência artificial no *criminal compliance* modifica a responsabilidade penal da pessoa coletiva. Em concreto, a questão que se impõe aqui é se, em função da sua atividade, é possível atribuir deveres objetivos de garante a um *software* "inteligente" para fundamentar a responsabilidade da pessoa coletiva que o utiliza.

Também com a adoção do modelo de autorresponsabilidade semelhante questão emerge. Este modelo baseia-se na cultura corporativa e no respeito pela organização interna da empresa, pelo que a existência de um *criminal compliance* eficaz por si só, apesar não isentar automaticamente a pessoa coletiva de responsabilidade, é estritamente valorado por demonstrar uma ordem normativa e ética de cumprimento empresarial. Mais a mais, quando se integra a inteligência artificial nesta vertente, maior valoração de cultura de cumprimento terá a empresa, uma vez que as capacidades tecnológicas destes sistemas asseguram, por definição, elevadas percentagens de eficácia. Com efeito, por um lado, estes *softwares* "inteligentes" poderão consubstanciar um útil instrumento de "escudo" às pessoas coletivas para provarem a sua organização e atenuarem ou isentarem a sua responsabilidade. Todavia, *a contrario*, a falha do sistema de *criminal compliance* "inteligente" mostrará o "défice de organização" da empresa. A nuance neste caso dispõe-se no motivo pelo qual o sistema falhou, ou seja, se a falha poderá ser imputada ao programador ou ao utilizador.

No apuramento da responsabilidade da pessoa coletiva, os dirigentes empresariais (e.g. todos aqueles que exerçam uma posição de liderança) são titulares de deveres de garante em função das competências concretas que possuem na estrutura empresarial, tendo a capacidade para dominar factualmente a causa do resultado[217]. Com a introdução de

[217] Definindo os limites jurídicos deste dever dos dirigentes empresariais, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa*, *Op. cit.*, p. 68 e ss. e p. 135 e ss.

departamentos de *compliance* passou a haver a delegação e transferência de certos deveres de garante para este estrato da organização. Assim, tal como dispôs em *obiter dictum* o conhecido acórdão da 5.ª secção penal do Supremo Tribunal Federal Alemão[218], os *compliance officers* estão vinculados a um dever de garante que os obriga a evitar a criminalidade empresarial[219]. No entanto, este dever de garante é um dever derivado, uma vez que o dever originário pertencerá sempre ao órgão de direção da pessoa coletiva[220]. Como tal, a transferência não faz extinguir nem elimina a posição primária de garante que os dirigentes empresariais (*vis-à-vis* aqueles que exercem posições de liderança) ainda possuem. No limite, poderá diminuir a exigibilidade do controlo, mas nunca o extinguindo[221].

Com efeito, a introdução da inteligência artificial nesta vertente, mais uma vez, não cria um problema novo. Este é um problema de legalidade com o qual o legislador já lidou e diariamente lida. Neste sentido, para suprir este espaço normativo, poderemos distinguir duas vias de resposta: a teoria disruptiva e a teoria clássica.

1.2.1. Teoria disruptiva: algoritmo titular do dever de garante?

A teoria disruptiva baseia-se na assunção de capacidade de sistemas de IA possuírem uma personalidade jurídica própria para que lhes possam ser atribuídos certos deveres jurídicos e, em função disso, poderem ser responsáveis[222]. O fundamento desta visão justifica-se nas capacidades *quasi*-humanas que certos sistemas de inteligência artificial

[218] BGH 5StR 394/08 de 17/07/2009.
[219] MENDES, Paulo de Sousa, «A problemática da punição do autobranqueamento …», *Op. cit.*, p. 145.
[220] *Ibid.*, p. 146 («(a) designação de um oficial de cumprimento através de uma suficiente *diligentia in delegando* não desonera, porém, o órgão de administração, pois o dever originário permanece no órgão de liderança e fiscalização da empresa»).
[221] Neste sentido, citando Lascuraín Sanchez, SOUSA, Susana Aires de, *Questões Fundamentais de Direito Penal da Empresa, Op. cit.*, p. 136 («a delegação não afasta o dever de garante originário, libertando-o de qualquer tipo de responsabilidade, mas antes modifica os seus contornos»); e também, citando Claus Roxin, DIAS, Jorge de Figueiredo, *Op. cit.*, p. 1105 («o pessoal dirigente deve cuidar de que a "fonte de perigos" "empresa" permaneça sob controlo de segurança, partam os perigos do potencial material ou pessoal da empresa»).
[222] Nesta ideia, entretanto deixada de parte, o próprio Parlamento Europeu, com a Resolução de 16 de fevereiro de 2017, com recomendações dirigidas à Comissão sobre disposições de direito civil sobre robótica, considerou ser importante «criar um estatuto jurídico específico para os robôs a longo prazo, de modo a que, pelo menos, os robôs autónomos mais sofisticados possam ser determinados como detentores do estatuto de pessoas eletrónicas responsáveis por sanar quaisquer danos que possam causar e, eventualmente, aplicar a personalidade eletrónica a casos em que os robôs tomam decisões autónomas ou em que interagem por qualquer outro modo com terceiros de forma independente».

apresentam. O Autor mais expressivo nesta matéria é GABRIEL HALLEVY[223] que admite que os sistemas de inteligência artificial são capazes de integrar, com culpa, ações penalmente relevantes. Deste modo, considera que da mesma forma que se responsabiliza hoje as pessoas coletivas (enquanto entidades fictícias e sem existência física), semelhante juízo deveria ser feito relativamente aos sistemas de inteligência artificial, bastando para tal que os pressupostos da responsabilidade penal estejam preenchidos para estes "agentes" (*actus reus* – elementos externos - e *mens reus* – elementos internos)[224].

Uma opção como estas, se pressupõe que um algoritmo tem a capacidade para ser responsabilizado, pressupõe também que este poderá ser titular do dever de garante de prevenção criminal, podendo, na mesma medida, responder pela falha com esse dever (como se de um *compliance officer* se tratasse). Para tanto, admissibilidade da transferência do dever de garante, acrescenta um "agente" à variável: o *software*. Assim, remetendo para o caso hipotético acima relatado, segundo esta teoria, o *software NoLock* seria responsabilizado nos mesmos termos que um *Chief Compliance Officer* seria, fundamentando-se esta na violação do dever de garante no cumprimento.

Contudo, esta opção não é, de todo, a mais favorável.

1.2.1.1.Crítica

A inovação inerente à tese disruptiva não a isenta de críticas. Por outro lado, até as exacerba.

Em primeiro lugar, a atribuição de responsabilidade penal, seja por ação ou omissão, pressupõe um «centro ético-social de imputação jurídico-penal»[225]. Como é também sabido, o facto punível corresponde a um conjunto de cinco elementos: uma ação, típica, ilícita,

---

[223] Esta visão foi originalmente criada a pensar para os "*Hard AI Crimes"*, ou seja, para as situações em que um algoritmo pratica um crime, algo que se discorrerá no ponto seguinte. Aqui, a adaptação é feita à realidade omissiva inerente à falha de deveres de garante.

[224] Assemelhando a personalidade jurídica atribuída às pessoas coletivas com a personalidade jurídica atribuída aos sistemas de IA, HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, *Op. cit.*, p. 24; e ainda, *idem*, «Virtual Criminal Responsibility», *Original Law Review,* Vol. 6, N. º 1, 2010, p. 9 e ss., p. 26 e 27 («Corporations participate fully in human life, and it was outrageous no to subject them to human laws, since offences are committed by corporations or through them. But corporations have neither body nor soul. Legal solutions were developed so that in relation to criminal responsibility, they would be deemed capable of fulfilling all requirements of criminal responsibility, including external elements and internal elements (…) Why should AI entities be different from corporations? AI entities are taking larger and larger parts in human activities, as do corporations. Offenses have already been committed by AI entities or through them»).

[225] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 346 e ss.

culposa e punível[226]. É no âmbito da ação e da culpa que podem surgir maiores obstáculos. Por sua vez, a ação pressupõe a existência de dois outros elementos: o agente e a conduta. Posteriormente, é neste agente, pela conduta seguida («uma atitude interna juridicamente desaprovada»), que será feita a censura «perante as exigências do dever-ser sócio-comunitário»[227]. Ora, os problemas daqui emergentes não decorrem da indagação acerca da suscetibilidade de sistemas "inteligentes" lesarem bens jurídicos (por ação ou omissão). Como já se disse, isso é um dado adquirido. A questão aqui é de que forma se poderá assacar a responsabilidade a algo que não evita um crime, mas não tem a capacidade para ser titular de deveres nem responder pela sua falha.

Desde logo, a inteligência artificial não integra a categoria de agente. Um agente pressupõe que tenha personalidade jurídica. E para lhe ser atribuída personalidade jurídica tem que ter a «aptidão para ser titular autónomo de relações jurídicas»[228] e a consciência e compreensão dos seus direitos e obrigações. É neste ponto que os adeptos da personalidade jurídica eletrónica suscitam o argumento de que pessoas coletivas também não têm essa compreensão. A questão é que, e independentemente das opções político-criminais em sede de imputação, as pessoas coletivas atuam sempre através de pessoas singulares[229]; e estes são agentes livres, conscientes com a compreensão ético-social do "dever-ser" em sociedade. Já os algoritmos, como já vimos e aconteceu no caso *NoLock*, poderão transcender a previsão da programação inicial, tomando uma opção espontânea e inesperada, pondo-se numa situação de ilicitude, mas não tendo consciência moral da lesão de bens jurídicos que ocorreu com essa atuação autónoma, ou falta dela[230]. Nestes termos, os algoritmos não têm capacidade para se autodeterminar seja moral ou ético-socialmente para que compreendam o sentido de ilicitude em que se introduziram[231]. Como tal, agora no âmbito da culpa, não

[226] *Ibid.*, p. 277.
[227] *Ibid.*, p. 318 e 319.
[228] PINTO, Carlos Alberto da Mota, *Teoria Geral do Direito Civil*, 4.ª Ed., Coimbra: Coimbra Editora, 2012, pág. 201.
[229] *Ibid., Loc. cit.*
[230] Sobre esta ideia da capacidade transalgorítmica, GLESS, Sabine / SILVERMAN, Emily / WEIGEND, Thomas, «If robots cause harm, who is to blame? Self-driving cars and criminal liability», *New Criminal Law Review*, Vol. 19, N.º 3, 2016, p. 414.
[231] No sentido da incapacidade de autoconsciência e determinação do lícito e ilícito, por todos, SOLUM, Lawrence B., «Legal Personhood for Artificial Intelligences», *Op. cit.*, p. 1264.; GLESS, Sabine / SILVERMAN, Emily / WEIGEND, Thomas, *Op. cit.*, p. 420; ABBOT, Ryan / SARCH, Alex, *Op. cit.* p. 349 CAPPELLINI, Alberto, «*Machina delinquere non potest*? Bervi appunti su inteligenza artificiale e responsabilità penale», Criminalia, 2018, p. 513.

tendo esta consciência, este é um "estado mental" que não é verdadeiramente um estado de culpabilidade: «é um dolo sem sangue, é uma aparência de dolo»[232].

Assim, não sendo possível integrar o conceito de agente e, em função disso, não sendo possível ser-lhes imputado um juízo de culpa, não poderão ser transferidos quaisquer deveres jurídicos aos sistemas de inteligência artificial.

Também relativamente à conduta, algumas alegações são inevitáveis. Está assente que a inteligência artificial pode espelhar certas capacidades cognitivas em sistemas computorizados que se assemelham às capacidades cognitivas humanas. Ora, um algoritmo "inteligente", seja mecanicamente corporizado através de um robô ou programado através de um *software*, tem a capacidade para tomar decisões e "agir" como humanos. Mas será esta "atuação" (ou, neste caso, "não atuação") uma ação penalmente relevante[233]? Isto é, sendo o Direito Penal uma ciência antropomorfizada, poderemos estabelecer como base de comunicação a mesma linguagem e os mesmos institutos dogmáticos para sistemas de inteligência artificial que estabelecemos para humanos, em concreto, o conceito de "ação", "dever" ou "vontade"? Não cremos que possamos "mecanizar" o conceito de ação e, muito menos, o de vontade[234].

Deste modo, estando aqui em causa a atribuição de deveres que fundamentam a responsabilidade, por estarmos perante algoritmos, esta atribuição torna-se impossível. É por esta razão que deverá o legislador penal encontrar formas para identificar a "atuação algorítmica" numa conduta penalmente relevante realizada por um agente penalmente cognoscível, nomeadamente, neste contexto, algum agente capaz de ser titular de deveres jurídicos.

1.2.2. Teoria clássica e os deveres de precaução

A teoria clássica, por sua vez, sustenta a base de toda argumentação na não admissibilidade de uma personalidade jurídica eletrónica e, portanto, na incapacidade de algoritmos "inteligentes" serem titulares de deveres de garante.

---

[232] Expressão traduzida de CAPPELLINI, Alberto, *Op. cit.*, p. 513 («è un dolo esangue, un'apparenza di dolo»).
[233] Sobre a debate do conceito da "atuação" do algoritmo e o conceito jurídico-penal de atuação, LIMA, Dafni, «Could AI agents be held criminally liable? Artificial intelligence and the challenges for criminal law», *South Carolina Law Review*, Vol. 69, 2018, p. 679 e ss.
[234] Distinguindo o conceito de ação no sentido legal e no sentido filosófico, DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *The George Washington Law Review*, Vol. 89, N. º 4, 2021, p. 809, nota 51.

Esta teoria considera que as soluções apresentadas no nosso ordenamento jurídico são suficientes para preencher este vazio de legalidade, estabelecendo como limite dogmático máximo, e excludente, o "salto de fé" da abordagem do problema segundo o prisma da assunção da responsabilidade penal direta do algoritmo. Por esta razão, não sendo possível os sistemas de IA serem titulares de posições de garante e responder por isso, resta-nos focar em quem integra esta posição, apesar da existência de um *software* "inteligente" cuja programação visava evitar a prática criminal.

Em concreto, basear-nos-emos na responsabilidade penal das pessoas coletivas. Por um lado, pois são os principais programadores, utilizadores ou beneficiários dos algoritmos; por outro, pois são titulares originários dos deveres de garante (através dos seus dirigentes, que a vinculam criminalmente) com a capacidade para dominar a causa do resultado. Esta ideia segue a rota de pensamento de MIHAILIS DIAMANTIS, que se subscreve neste âmbito, que faz corresponder a atuação algorítmica à atuação empresarial da mesma forma que a atuação dos trabalhadores integrantes de uma empresa corresponde a uma atuação da empresa[235]. Com efeito, esta identificação de atuação dos trabalhadores, que vincula a empresa, leva-a a controlar a atuação dos seus subordinados (através de programas de *compliance*) e a serem gerados deveres de controlo e autoridade sobre estes para evitar a sua responsabilização. Com a mesma lógica na atuação algorítmica, isso leva a que as empresas sejam encorajadas a exercer um controlo e monitorização dos seus algoritmos.

Neste ponto, parte-se da premissa que as funções de prevenção criminal não devem estar exclusivamente atribuídas a sistemas de IA pelos riscos e dificuldades de concretização de responsabilidade que daí adviriam. No entanto, um algoritmo com funções de prevenção criminal empresarial não é mais do que um produto a cargo do departamento de *compliance* no qual tem este o dever de fiscalizar, respondendo pelas suas falhas. Assim, no fundo, o que acontece com a introdução da inteligência artificial no *criminal compliance* é, ao lado dos benefícios da sua utilização, o aumento dos deveres de diligência para a estrutura empresarial.

Em concreto, há um acréscimo para o departamento de *compliance* dos deveres a seu cargo com a inclusão do dever de precaução[236]. Este apresenta maior complexidade para ser delimitado graças à capacidade de aprendizagem do sistema. Estes algoritmos de *machine*

[235] Sobre a doutrina original, aqui adaptada, *infra* nota 279 e 280.
[236] Esta ideia é originária e respaldada, nos delitos de ação, através da solução da responsabilidade pelo produto "inteligente" que se explanará *infra*.

learning refratam uma capacidade de aprendizagem que vai além daquilo que foi a primeira programação, valorando e associando os dados introduzidos através da experiência e do treino empírico.

Na prática, este dever diz respeito à própria programação do sistema, que poderá influenciar *in casu* a responsabilidade do utilizador pelo crime que cometeu, mas também poderá atribuir responsabilidade ao programador quando se prove que houve falha com o dever em causa. Com efeito, o dever de precaução subdivide-se no dever de precaução na programação, estando este vinculado ao programador (enquanto autor da primeira programação), e no dever de precaução na utilização, estando este vinculado ao utilizador do sistema (enquanto responsável pela aprendizagem empírica posterior). Em termos subjetivos, este dever estabelece-se para aquele que exerce o controlo efetivo do algoritmo, isto é, aquele ou aqueles que têm o poder para prevenir *de facto* a falha do sistema, seja o poder de treinar, monitorizar, eliminar o código algorítmico, o poder de o desligar, de o alterar ou anular decisões suas[237].

A prova com o cumprimento do dever de precaução na programação é relevante para o programador se isentar de responsabilidade, provando que o sistema falhou por razões externas à sua intervenção no processo produtivo. Por outro lado, do lado do utilizador, a prova do cumprimento do dever de precaução mostra que este teve uma utilização responsável do sistema, não introduzindo dados ilegítimos ou induzindo o sistema em erro ao ponto de este falhar. Assim, provando-se que o algoritmo falhou de forma inexplicável e pouco previsível e que a conduta da pessoa coletiva que praticou o crime se baseou na confiança da não falibilidade do sistema, poderá esta usufruir de uma atenuação da pena.

Numa palavra, com a falha do *criminal compliance* "inteligente" em prevenir o crime, porque este é um produto e tanto não tem capacidade de ter deveres como não pode ser responsabilizado pela sua falha, caberá delimitar os responsáveis que não cumpriram com os respetivos deveres. Com efeito, a pessoa coletiva que comete um crime não poderá alegar que apenas o cometeu porque o sistema falhou e tinha delegado neste as funções de prevenção. Deste modo, porque tem capacidade moral, tem capacidade para distinguir o

---

[237] DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 149.
Podemos neste ponto estabelecer o paralelismo com os termos utilizados quando, em vez de algoritmos, se referem a subordinados no âmbito empresarial. Isto é, nos termos do art. 11.º/4 do Código Penal considera-se que exerce poder quem tem «autoridade para exercer controlo da sua atividade». Estes poderes de autoridade incluem todos aqueles que permitem controlar a atividade do subordinado. Ora, considerem-se, com as necessárias adaptações, estes poderes de autoridade refratados no âmbito algorítmico.

lícito do ilícito e de se determinar na ordem jurídica, pelo que não se isenta deste cumprimento legal com a delegação de funções em produtos "inteligentes" que não são capazes de responder por essa falha. Estes deveres não chegam a sair da sua esfera jurídica, pelo que a pessoa coletiva é ainda responsável por eles.

Como tal, e remetendo para o caso hipotético apresentado, a alegação da *TechCypher* sustentada no princípio da confiança não a isenta do dever de garante na prevenção criminal, ou, muito menos, da responsabilidade pelo crime de branqueamento. Quanto a este, poderá sempre ser responsabilizada. A nuance aqui em causa diz respeito à falta de eficácia do sistema "inteligente", que poderá ser atribuída ou à *ComplyTeK* (programadora) ou à própria *TechCypher* (utilizadora), mediante a prova do cumprimento dos deveres de precaução a ambos vinculados.

Concretamente, a *TechCypher* responderia pelo crime de branqueamento a título de dolo eventual, pois, tendo conhecimento das suspeições envolventes relativas à potencialidade do crime em causa, ainda assim, confiou a sua atuação na infalibilidade do sistema, tendo-se conformado com as suas opções (até pelas prévias elevadas taxas de eficácia). A possibilidade de se aceitar como elemento mental para o crime de branqueamento de capitais a modalidade de dolo eventual gera alguma discussão. Porém, uma situação disruptiva como esta exige que se proceda a algumas alterações do *status quo* da sistemática jurídico-penal[238]. Deste modo, a verificação do dolo eventual sustenta-se na conformação por parte da *TechCypher* do efeito da falha do *criminal compliance* "inteligente", pelo que o elemento mental da culpa neste caso identifica-se com a figura anglo-saxónica da *willful blindness* (ou ignorância deliberada), como aquele que «deliberadamente "fecha os olhos" ou faz "vista grossa"»[239].

Esta atuação com base no princípio da confiança não isenta a *TechCypher* de responsabilidade, contudo, esta poderá beneficiar de uma atenuação da pena, desde que

[238] Antevendo esta necessidade futura, com uma correspondente indagação, DIAS, Jorge de Figueiredo, *Op. cit.*, p. 439 («Assim sendo, e tendo ademais em consideração o facto de na "sociedade do risco" aumentarem significativamente as necessidades político-criminais de tutela de uma imensidade de condutas que se situarão no âmbito do dolo eventual e da negligência consciente, parece justificado deixar aqui pelo menos (apenas isso…) a questão de saber se à bipartição tipo de ilícito doloso/ tipo de ilícito negligente, não deverá no futuro vir a substituir-se uma tripartição: dolo/negligência/temeridade»).

[239] Sobre a admissibilidade do dolo eventual no crime de branqueamento, MENDES, Paulo de Sousa, «A problemática da punição do autobranqueamento …», *Op. cit.*, p. 147. Também sustentando esta ideia, DIAS, Jorge de Figueiredo, *Op. cit.*, p. 429 e ss. e, concretamente, p. 438.

prove que cumpriu com o seu dever de precaução na utilização, não tendo contribuído para a falha do sistema, e que teria atuado diferentemente se este não tivesse falhado.

Já a *ComplyTeK*, caso falhasse com a prova do dever de precaução na programação, responderia autonomamente e nos mesmos termos de um *Chief Compliance Officer* pela falha do sistema.

Em suma, em função destes motivos, até porque como afirma FIGUEIREDO DIAS «a violação de deveres de ação não se apresenta, em regra, tão grave como a violação das proibições correspondentes»[240], a diminuição das exigências penais (condicionadas pelas provas de cumprimento dos deveres respetivos) nesta solução parece-nos espelhar um equilibrado expediente para as situações em que o *criminal compliance* "inteligente" falhe espontaneamente. De um lado, obsta à fuga de responsabilidade das pessoas coletivas, não permitindo que esta se isente de responsabilidade com a alegação de delegação de certas funções de prevenção a um sistema "inteligente" e, ao mesmo tempo, não limita o desenvolvimento tecnológico, promovendo a utilização destes sistemas no âmbito da prevenção criminal, pois atenua a responsabilidade da empresa utilizadora nas situações em que o sistema falha inexplicavelmente ou nas situações em que o programador falhou com seu o dever de precaução.

1.3.Conclusões preliminares

Em sede de primeiras conclusões, cabe esclarecer que sistemas de inteligência artificial não têm personalidade jurídica, nem capacidade jurídica e, portanto, não podem ser titulares de quaisquer deveres jurídicos. Desde logo pois estes produtos "inteligentes" são isto mesmo: produtos. Distinguem-se dos restantes produtos pelas caraterísticas distintivas que possuem, mas principalmente, pelos "novos riscos"[241] que geram.

Aliás, ainda quanto à transferência de deveres jurídicos para sistemas de inteligência artificial, graças aos riscos já aqui explorados inerentes às decisões algorítmicas e falibilidade destas, nem é desejável ou aconselhável que tal aconteça. Estes perigos só vêm

[240] Neste sentido, DIAS, Jorge de Figueiredo, *Op. cit.*, p. 1078.

[241] Distinguindo as três categorias de risco (riscos tradicionais, riscos do desenvolvimento industrial e os "novos riscos"), SOUSA, Susana Aires de, *A responsabilidade criminal pelo produto e topos causal em direito penal: contributo para uma proteção penal de interesses do consumidor*, 1.ª Ed., Coimbra: Coimbra Editora, 2014, p. 52 e ss., e referindo-se concretamente aos "novos riscos", no caso, longe destes sistemas "inteligentes", mas perfeitamente atualizado, *idem*, p. 58 («Os novos riscos são assim difíceis de controlar uma vez que padecem de um "deficit de previsão" fundamentado na incerteza das suas consequências e na dificuldade em determinar os seus limites»).

demonstrar que em setores de risco, nomeadamente o setor empresarial de prevenção criminal, que possam lesar ou influenciar a lesão de bens jurídico-penais, estes sistemas não podem ser totalmente autónomos, devendo ser monitorizados.

Novamente, impõe-se a ideia de que a inteligência artificial não deve ser utilizada como um instrumento para se fazer substituir ao ser humano, mas antes para auxiliar a sua atuação. Daí que sejamos bastante favoráveis a um conceito de inteligência aumentada em vez de uma inteligência artificial, ou seja, um instrumento que auxilie a inteligência humana e realize certas tarefas com maior celeridade e eficiência, mas não sendo decisão última ou permitindo gerar decisões autónomas inescrutáveis.

De todo o modo, independentemente do setor em causa, a regulação é a base para toda esta teorização. É neste sentido que a solução *de jure condendo* apresentada - relativamente à atenuação da pena no caso de cumprimento com os deveres de precaução pelo utilizador - é uma proposta que espelha o binómio de compatibilização e equilíbrio que o legislador deverá ter em conta: por um lado, a inovação, por outro, a responsabilidade.

O reverso do problema da falha da prevenção criminal e, em geral, a falibilidade do algoritmo faz emergir, pelas decisões inexplicáveis e imprevisíveis que poderão surgir, o problema conexo da potencial tipificação de crimes por parte do sistema. Concretamente em relação ao caso hipotético formulado, ficou por responder à questão de quem responsabilizar pelo crime de fraude fiscal. Vejamos então.

2. Problema conexo: Inteligência Artificial, o problema da imputação e o *accountability gap* nos delitos de ação

Do disposto no anterior ponto, ficámos a perceber que é possível que sistemas ditos "inteligentes" se mostram-se aptos, «em algumas situações, a modificar as instruções que lhe(s) foram dadas, levando a cabo atos que não estão de acordo com uma programação pré-definida, mas que são potenciados pela interação com o meio»[242]. Por outras palavras, de facto, a falibilidade, inexplicabilidade, opacidade e imprevisibilidade do sistema é real.

É por isso que o preenchimento do *accountability gap* (agora nos delitos de ação) passa por perceber quem é responsável quando um algoritmo toma uma opção "autonomamente", tipificando crimes.

[242] Cfr. BARBOSA, Mafalda Miranda, «Inteligência artificial, *e-persons* e direito…», *Op. cit.*, p. 1476 e 1477;

A importância do cobrimento desta lacuna baseia-se no facto de, com a introdução destes sistemas, se abrir um potencial "porto de refúgio" (*safe heaven*) para as pessoas coletivas, enquanto principais programadores e/ou utilizadores, escondendo-se por detrás do "véu algorítmico" e, muitas vezes, lucrando com isso[243]. Para além disto, os juízos de imputação saem dificultados pela multiplicidade e complexidade de relações que à teia empresarial se acrescenta, correndo-se o risco de esta responsabilidade se ir dissolvendo[244].

Em concreto, se toda doutrina do facto punível é desenhada por e para o Homem[245] e se um sistema de inteligência artificial é capaz de "agir autonomamente", tomando decisões que não foram pré-programadas ou previsíveis pelo programador ou utilizador humano, quem responde?

Esta questão encontra respaldo no caso concreto hipotético acima relatado. Na continuidade da concretização da resolução no ponto anterior, ficou por desvendar quem é responsável pelo crime de fraude fiscal que teve como fonte o *software NoLock*, quando este "autonomamente", no seguimento da eliminação da denúncia interna (que era verídica), desvalorizou-a tendo por base os danos reputacionais previsivelmente gerados com a publicidade desse crime, procurando "proteger" a empresa desse risco. Contudo, com esta atuação, o próprio sistema cometeu o crime fraude fiscal através da ocultação e falsificação de dados, nomeadamente, elementos probatórios relevantes exigidos pela lei tributária. Por sua vez, a *TechCypher* conformou-se com a decisão do sistema, tendo beneficiado com as vantagens patrimoniais decorrentes do negócio "dissimulado" e oculto pelo sistema.

Os problemas surgem a partir daqui.

Numa perspetiva de imputação objetiva, a questão que se impõe é saber como se estabelece a relação causal entre a conduta do sistema e o resultado gerado. Quem é o agente da conduta? Para além disto, em sede de imputação subjetiva, como e a quem imputar o juízo de culpa, visto que o sistema não foi programado para cometer qualquer crime ou representada tal possibilidade, e, ainda assim, num juízo de total autonomia e inexplicabilidade, foram lesados bens jurídico-penais? Isto porque, «as máquinas e os

---

[243] DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 139.

[244] Sobres as dificuldades que estes sistemas poderão trazer a dogmática penal, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 68 («Estas interrogações ganham densidade quando consideradas a partir de teorias normativo-causais assentes numa ideia de previsibilidade do resultado, em que a verificação da causalidade assenta na normalidade do acontecer e nas regras da experiência, de que é exemplo a teoria da causalidade adequada»).

[245] Neste sentido, OSMANI, Nora, «The Complexity of Criminal Liability of AI Systems», *Masaryk University Journal of Law and Technology*, Vol. 14, n. º 1, 2020, p. 60; e, CAPPELLINI, Alberto, *Op. cit.*, p. 500 e ss.

programas informáticos não têm intenção»[246], «somente as pessoas atuam com determinada intenção, propósito ou finalidade»[247].

Assim como quando foi abordada a falha de prevenção do sistema "inteligente" na prevenção criminal, semelhantes soluções surgem para responder a estas questões.

2.1. Propostas de solução: algoritmo responsável ou o novo (velho) problema de legalidade

As propostas de solução apresentadas pela doutrina ao *accountability gap* nos delitos de ação são já extensas. Ainda assim, podemos agrupar entre aqueles que consideram que devemos imputar responsabilidades diretamente aos algoritmos (chamamos-lhes, novamente, a teoria disruptiva) e aqueles que integram nesta problemática as atuais bases do sistema jurídico, sem irromper com grandes alterações estruturais (a teoria clássica).

Quanto à primeira visão, que já explanámos as suas bases *supra*, novamente, GABRIEL HALLEVY propõe que os algoritmos têm capacidade de atuação e de atuação com culpa desde que tipifiquem os pressupostos da responsabilidade penal. Para concretizar esta visão, o Autor chega inclusivamente a apresentar três propostas de solução para responsabilizar os algoritmos[248]. Um modelo de autoria mediata (*perpetration-by-another* e *command responsibility*), quando tenha havido a intenção por parte do programador ou utilizador para, deliberadamente, o sistema praticar um crime; um modelo de causalidade adequada (*natural-probable-consequence*), quando o programador ou utilizador não teve a intenção de praticar o crime através do sistema, mas era algo que lhe era exigível de prever; e um modelo de responsabilidade direta (*strict virtual responsibility*), que imputa diretamente a responsabilidade penal ao algoritmo.

Em linha com a visão crítica desta opção, surgem muitas dúvidas apresentadas pela doutrina quanto à possibilidade de adoção deste ponto de vista, nomeadamente, por três ordens de razão[249]: a diferença substancial entre as pessoas coletivas e os sistemas de IA; a (in)capacidade moral dos algoritmos[250]; e a impossibilidade e ineficácia de punição dos

---

[246] BATHAEE, Yavar, *Op. cit.*, p. 906.
[247] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 69.
[248] HALLEVY, Gabriel, «Virtual Criminal Responsibility», *Op.cit.*, p. 11 e ss.; e também, *idem*, *Liability for Crimes Involving Artificial Intelligence Systems*, *Op. cit.*, p. 67 e ss.
[249] Apresentando estas mesmas objeções, CAPPELLINI, Alberto, *Op. cit.*, p. 512 e ss.; e ainda, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 74 e ss.
[250] SOLUM, Lawrence B., *Op. cit.*, p. 1258 e ss., que apresenta um conjunto de objeções contra a atribuição desta personalidade eletrónica, identifica especialmente a objeção condicente à incapacidade moral (*the*

sistemas "inteligentes". Os primeiros dois argumentos foram já apresentados anteriormente quando se referiu a incapacidade jurídica dos sistemas serem titulares de deveres, pelo que neste ponto importa enaltecer a última objeção pois é aquela que melhor carateriza a refutação de uma responsabilização direta dos algoritmos nos delitos de ação.

Neste sentido, mais uma vez, só é possível responsabilizar o agente jurídico-penalmente cognoscível (i.e., que possua personalidade jurídica) e que preencha culposamente tipos incriminadores. Tendo já sido afirmado que sistemas de inteligência artificial são produtos e não agentes, esta última objeção diz respeito à impossibilidade e ineficácia de punição do algoritmo. Esta impossibilidade dá-se por duas razões: por uma razão abstrata e uma razão concreta.

Quanto ao primeiro motivo, de facto, o Direito Penal é caraterizado por uma natureza axiológica extremamente relevante. E é perante esta ordem axiológica que a sociedade se baseia para realizar o juízo de censura ético-social que determinada conduta do agente que lese um bem jurídico relevante impõe. Partindo desta premissa, a responsabilização de um sistema de inteligência artificial desvirtuaria esta mesma ordem axiológica presente na comunidade, podendo vulgarizar as finalidades do Direito Penal e da própria *ratio* da pena.

As finalidades preventivas intrinsecamente ligadas ao princípio da necessidade da pena espelham, numa perspetiva geral, a confiança que a comunidade deposita no Direito Penal enquanto instrumento reparador e restabelecedor «da paz jurídica comunitária abalada pelo crime»[251], procurando intimidar os restantes atores em não seguir o mesmo caminho da delinquência e, numa vertente especial, a ressocialização do agente que praticou o crime, evitando a sua reincidência[252]. Ora, a responsabilização do algoritmo esbate flagrantemente com estas finalidades, no sentido em que não é com a punição de um algoritmo que chegaremos, com intenções de intimidação, quer a outros algoritmos, quer a outros programadores ou utilizadores de algoritmos ou, em concreto, aos programadores ou

missing-something argument), onde afirma que os sistemas de IA não são autoconscientes, não possuem intenções humanas e não sofrem, no fundo, não são sencientes. Por outro lado, admitindo uma capacidade moral em certas condutas, ENDENMÜLLER, Horst, «*Robot's Legal Personality*», University of Oxford, 8 mar. 2017, afirma que os *smart robots* são capazes de ações propositadas, exibindo um caráter moral. Contudo, mostra que se se responsabilizar diretamente os algoritmos com base neste argumento isso implica que se possa admitir uma capacidade jurídica genérica destas entidades.

[251] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 91. Também neste sentido, seguindo a visão de Günhter Jakobs, SIMMLER, Monika / MARKWALDER, Nora Mark, *Op. cit.*, p. 22 e ss.

[252] DIAS, Jorge de Figueiredo, *Op. cit.*, p. 64 e 65. Mas também, SOLUM, Lawrence B., *Op. cit.*, p. 1247.

utilizadores daquele algoritmo que gerou o facto criminal[253]. Isto por dois motivos: em primeiro, a montante, não é possível estabelecer o nexo causal entre estes "agentes" e o facto criminal, porque não o são; e ainda, dado que o algoritmo não tem capacidade de compreensão da punição[254]. A interrogação que se manifesta é: como poderia um algoritmo compreender que a punição de um outro tem uma finalidade geral relativamente ao comportamento que aquele levou a cabo[255]? Certamente, não compreenderia…

A par disto, em especial, no que diz respeito às penas concretas, não há sequer forma de punir o algoritmo com as penas que existem atualmente no nosso ordenamento jurídico[256]. Isto porque o algoritmo não pode ser preso, pois não tem existência física (exceto se for um robô mecanizado), nem multado, pois não tem património[257]. GABRIEL HALLEVY contrapõe este argumento, afirmando que a punição a um sistema de IA deve seguir os mesmos moldes de punição de qualquer outra pessoa, havendo uma técnica de conversão entre as penas aplicadas aos seres humanos e a sistemas de IA[258]. O Autor assume como penas potenciais a aplicar aos sistemas de IA a pena capital (assemelhando-se à dissolução no caso das pessoas coletivas), a pena de prisão, a pena suspensa, serviço comunitário e pena de multa[259]. Não se discutirá em concreto a admissibilidade de cada uma das penas, já que

---

[253] Neste sentido, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 78 («não é por se "punir", proibir ou mesmo declarar a morte da máquina (a criatura) que se alcança o seu criador (…)»). Em sentido contrário, direcionando, numa segunda instância, uma punição conjunta, mas autónoma, do sistema de IA e dos intervenientes humanos, HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, *Op. cit.*, p. 210 (« (…) both retribution and deterrence may be relevant as punishment's purposes regarding the human participants in the commission of the offence (e.g users and programmers)», considerando para os algoritmos que decidiram autonomamente uma punição de reabilitação para que estes possam "aprimorar" as suas decisões («(t)he artificial intelligence system after being rehabilitated would be able to form better and more accurate decision after adding more limitation to its discretion and refining the process though machine learning. Thus, the punishment, if adjusted correctly to the particular artificial intelligence system would be part of the machine learning process»).

[254] Seguindo esta visão, ASARO, Peter. M. «A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics», *in* Robot Ethics: The Ethical and Social Implications of Robotics, 2012, p. 181.

[255] CAPPELLINI, Alberto, *Op. cit.*, p. 513.

[256] A este propósito, questionando a legitimidade desta punição, GLESS, Sabine / SILVERMAN, Emily / WEIGEND, Thomas, *Op. cit.*, p. 423 e 424.

[257] DIAMANTIS, Mihailis E., «The Extended Corporate Mind: When Corporations use AI to Break the Law», *Op. cit*, p. 906 («(w)e can jail or fine other "people", but algorithms lack bodies and pocketbooks»); ou, *idem*, «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 138 («(…) there is no way to sanction algorithms: they lack bodies to jail and pocketbooks to pay»). Ainda sobre a distinção entre as pessoas coletivas e os algoritmos, neste caso, quanto à punição, ASARO, Peter. M., *Op. cit.*, p. 182 («The most obvious difference from corporations is that robots do have bodies to kick, though is not clear that kicking them would achieve the traditional goals of punishment»).

[258] HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, *Op. cit.*, p. 212; e também, *idem*, «Virtual Criminal Responsibility», *Op. cit.*, p. 23.

[259] HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, *Op. cit.*, p. 217 e ss.; e também, *idem*, «Virtual Criminal Responsibility», *Op. cit.*, p. 24.

este é um problema ulterior relativamente a todos os outros, isto é, é um problema de escolha da pena e da sua medida, tendo já sido feito todo o processo causal de onde resultaria a responsabilidade do sistema de IA. Não sendo isso possível, os comentários tecidos anteriormente são válidos na exata medida.

Em síntese, a recusa por uma visão de responsabilidade direta dos algoritmos sustenta-se no seguinte: se «(s)ó pode existir responsabilidade onde exista um agente consciente, moral e com capacidade de entender o sentido da norma, enquanto destinatário dos comandos jurídicos nela inscritos» não se poderá responsabilizar um sistema "inteligente". «De outro modo, o ilícito penal desliga-se do seu fundamento ético, e a função de censurabilidade reconhecida à culpa é negada, tanto no plano da realização do facto, como no momento de determinação da pena»[260]. Por outras palavras, a incapacidade de imputação de responsabilidade penal ao próprio sistema tem por base o desvirtuamento de toda a essência do Direito Penal, enquanto instrumento ao serviço da comunidade de tutela subsidiária de bens jurídico-penais e que dá garantia de um ambiente onde, na sua dignidade, o ser humano se possa realizar sem perturbar a paz jurídica comum. Por fim, do lado da pena, esta fica sem relevância, tornando-se vulgar na sua existência por falta de substrato axiológico. Com base nisto, segue-se convictamente a ideia de que sistemas de inteligência artificial não podem ser responsabilizados (*machina delinquere non potest*[261]).

Quanto às outras propostas de solução, estas são menos disruptivas, exigindo, ainda assim, uma natural alteração às condições existentes.

Incorporando a inteligência artificial um espaço ambíguo, concretamente, entre a vítima e um qualquer arguido legalmente reconhecido[262], torna-se necessário cobrir o problema de legalidade deixado em aberto quando os verdadeiros *cognitive systems* - que não se limitam «a calcular a melhor opção de entre os milhares de dados que lhe foram introduzidos (…) (a)ntes, o algoritmo, alimentado com dados, ajusta-se continuamente, por forma a diminuir o erro e a criar a sua própria jogada»[263] - "atuam", gerando um "crime sem agente" e sem culpa. Há uma causa, que foi a decisão algorítmica, e uma lesão, mas não há um agente penalmente cognoscível que possa responder por este dano.

---

[260] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 77.
[261] CAPPELLINI, Alberto, *Op. cit.*, *passim*.
[262] A expressão pertence a DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 136 («between the victim and any legally cognizable defendant»).
[263] RODRIGUES, Anabela Miranda / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial…», *Op. cit.*, p. 208.

A questão que aqui se impõe diz respeito à «dúvida sobre se aquela ofensa pode ainda ter-se como uma conduta da pessoa coletiva ou a imputação é interrompida pela autonomia da máquina»[264]. Daí que a primeira abordagem de resposta a esta dúvida seja fazer uma análise à luz dos atuais modelos.

No entanto, os tradicionais modelos de imputação do facto tornam-se obsoletos com a introdução de sistemas de inteligência artificial. Concretamente, modalidades vicariais (*respondeat superior)* apenas cobrem o hiato legal das situações é possível estabelecer um nexo causal entre o resultado e a conduta da pessoa física, sendo visto o sistema de inteligência artificial como mero instrumento com o qual se gerou o crime[265]. Para as situações semelhantes ao caso *NoLock*, isto é, para os casos em que há uma decisão algorítmica que saia do espetro da sua programação previsível (e, portanto, fora do "estado mental culposo" dos programadores ou utilizadores), as clássicas abordagens são inoperantes. Como já vimos anteriormente, a base de todo modelo de responsabilidade vicarial faz depender o juízo de imputação a partir de um ato de ação ou omissão de uma pessoa física a ela organicamente ligada, pelo que esta não poderá ser a abordagem, uma vez que a autonomia da máquina não preencheria os requisitos da conexão[266]. A resposta alternativa seria a adoção de um modelo de responsabilidade direta sustentado na culpa por uma defeituosa organização. Ora, dificilmente podemos assumir que uma decisão algorítmica imprevisível consubstancia um defeito tanto do algoritmo como da própria organização da pessoa coletiva[267].

---

[264] *Ibid.*, *Loc. cit.*

[265] Reconhecendo as debilidades desta tese para os problemas em questão, DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *Op. cit.*, p. 819 («There is some work respondeat superior can do, and is doing, to address the algorithmic accountability gap. When employees purposely design algorithms to engage in misconduct, that misconduct is attributable to the individual employees, and from them, through respondeat superior, to corporate employers. (…) Although the use of respondeat superior just described is straightforward, it is not nearly enough to close the algorithmic accountability gap because there are, and increasingly will be, many algorithmic injuries that cannot qualify as employee actions»)

[266] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 73; e, DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 144 («Technologies widely recognize that smart algorithms can misbehave even if every human involved is innocent. Without human misconduct, respondeat superior's vision of corporate misconduct cannot apply»).

[267] *Ibid.*, p. 209 («A capacidade cognitiva da máquina torna-a imprevisível, capaz de reagir ao inesperado, retirando a sua decisão do domínio da previsibilidade do programador. (…) se a ofensa causada por uma aprendizagem do algoritmo leva a um resultado imprevisível, dificilmente se pode censurar a empresa por não evitar um risco que não podia conhecer»); e também, SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 82 («a complexidade aumenta quando o dano não se associa a qualquer defeito no produto, mas antes à imprevisibilidade e autonomia das suas decisões. Esta imprevisibilidade não tem origem num defeito de fabrico, mas é antes uma caraterística»).

Assim, resta-nos recorrer a soluções que não rompem bruscamente com os tradicionais modelos, mas que se adaptam a esta nova realidade. Neste sentido, podemos distinguir uma solução revisitada dos problemas já debatidos e uma solução mais inovadora.

A primeira solução, defendida por SUSANA AIRES DE SOUSA, procura adaptar as categorias penais à realidade da inteligência artificial, nomeadamente através da responsabilidade pelo produto ("inteligente")[268]. Este é, factualmente, um produto inovador e imprevisível e é por essa razão que a regulação terá que intervir. Do mesmo modo, apesar da imprevisibilidade do resultado, há um conjunto alargado de medidas que a pessoa coletiva pode tomar seja para prevenir ou para mitigar os efeitos de decisões algorítmicas. Esta visão parte de uma mudança de paradigma dentro do modelo clássico da responsabilidade pelo produto, isto é, «da *persona* para o *produto*»[269]. Aqui, relevam-se três ideias basilares para o estabelecimento desta responsabilidade: a responsabilidade pelo tipo de produção, o princípio da precaução e uma regulação dinâmica (*responsive regulation*). Em primeira instância, a inteligência artificial, pelas suas capacidades tecnológicas disruptivas que a tornam espontânea e imprevisível, poder-se-á inserir na categoria da produção de alto risco e perigosidade, falando-se neste caso de uma responsabilidade pela natureza ou pelo tipo de produto[270]. Com efeito, tal risco implica que haja maior diligência e acompanhamento no processo produtivo, concretamente, na programação do algoritmo. É a partir daqui que surge a relevância do princípio da precaução. Segundo este princípio, «perante atividades humanas que impliquem um dano cientificamente plausível, mas incerto, devem ser tomadas medidas que evitem ou diminuam esse dano»[271]. A replicação desta ideia no âmbito da inteligência artificial, especialmente, nos sistemas de inteligência artificial mais desenvolvidos (*cognitive systems*) «deve admitir-se logo no plano legal a incerteza sobre o seu funcionamento associada a uma quase "presunção genérica de perigosidade"»[272]. Isto porque, para além do próprio risco inerente à produção do algoritmo, acrescenta-se um risco

---

[268] De forma desenvolvida, com as necessárias adaptações, SOUSA, Susana Aires de, *A responsabilidade criminal pelo produto e topos causal em direito penal…, Op. cit*.; e, no âmbito específico da responsabilidade penal pelo produto "inteligente", SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 83 e ss. («há, quanto a nós, vantagens em explorar os problemas que foram sendo discutidos ao abrigo do tópico da responsabilidade do produto»).

[269] *Ibid.*, p. 83.

[270] Que se distingue da responsabilidade pelo modo ou método de produção explicada em detalhe em SOUSA, Susana Aires de, *A responsabilidade criminal pelo produto e topos causal em direito penal: contributo para uma proteção penal de interesses do consumidor*, *Op. cit.*, p. 106 e ss.

[271] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 85.

[272] *Ibid.*, Loc. cit.

adicional derivado de caraterísticas do algoritmo que, por aprendizagem futura, podem gerar resultados imprevisíveis e que causem lesões. Por fim, a regulação dinâmica (*responsive regulation*) diz respeito a medidas concretas que os produtores devem levar a cabo para dar efetividade ao princípio da precaução, nomeadamente, através de medidas de acompanhamento e monitorização em espaço seguro do produto "inteligente" (*sandbox approach* e *design tests*), diminuição das suas capacidades autónomas ou até da proibição de certos produtos ou tipos de produção. É com base nestas medidas que, mais facilmente, se delimitam os riscos inerentes ao sistema e, por conseguinte, se geram deveres objetivos de cuidado que podem levar à responsabilidade penal do produtor a título de negligência[273].

Por outro lado, a alternativa mais inovadora surge a partir da tese de MIHAILIS DIAMANTIS que, podemos dizer, pega no problema de duas formas: na vertente da culpa (com a *extended mind thesis*) e na vertente causal (com a *beneficial-control account*).

Antes de tudo, para o problema do resultado algorítmico imprevisível, o Autor distancia-se de uma abordagem clássica do modelo tradicional de responsabilidade vicarial, pois não é possível incluir nos moldes personalistas em que o modelo foi concebido as nuances que os sistemas de inteligência artificial trazem. Para além disto, distancia-se também da tese da responsabilidade direta do produtor, pois não considera *ab initio* os sistemas de inteligência artificial como sendo verdadeiros produtos definidos nos termos legais, mas também com base no facto de que uma aproximação a um modelo como este poderia atrasar ou mesmo obstar ao desenvolvimento tecnológico das empresas, pois seria demasiado oneroso para estas produzir estes sistemas[274].

Em contrapartida, o Autor propõe uma solução alternativa para o cobrimento do *accountability gap*, metaforizando um dualismo de opções. Ou o poderemos resolver com uma marreta ou com bisturi. Isto é, ou optamos por uma visão disruptiva e severa, demolindo o regime que existe, abrindo exceções aos princípios basilares do Direito Penal e criar novos

[273] *Ibid.*, p. 86 e ss,

[274] DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *Op. cit.*, p. 823 e ss. Considera que para serem produtos têm necessariamente que envolver uma distribuição ou troca desse bem, isto é, tem sempre que existir um produtor e um consumidor, enquanto individualidades distintas. Tal parece não acontecer nas situações que em que o algoritmo decide autónoma e espontaneamente num ambiente em que o produtor (o programador) é também o utilizador, não tendo havido qualquer distribuição do produto. Para além disto, considera que mesmo que se qualificasse o sistema "inteligente" como um produto, o dano causado por ele só é relevado se for causado a um utilizador ou consumidor ou à sua propriedade, coisa que, na maioria das vezes, não se verifica, pois o dano é causado a um terceiro.

regimes[275], ou, por outro lado, optamos por uma solução precisa e minuciosa sem alterar bruscamente o *status quo* da sistemática jurídico-penal. Em função disto, optou pela solução de bisturi, aplicando criativamente os modelos já existentes[276].

Deste modo, o Autor remete a solução do problema para uma visão análoga à que foi tida aquando da responsabilização penal das pessoas coletivas. Isto é, da mesma forma que o legislador encontrou expedientes legislativos para fazer responder entidades morais através do modelo de imputação da responsabilidade vicarial (isto é, a culpa da empresa é fundamentada a partir da culpa da pessoa física a si organicamente ligada atue em seu nome e no seu interesse), o mesmo deveria ser feito quanto à atuação algorítmica. Assim, no âmbito da imputação subjetiva, a sua solução passa por uma extensão do conceito de "estado mental da empresa" (*corporate mental state*[277]). Em concreto, propõe que os algoritmos empresariais sejam considerados parte integrante da empresa, fundamentando com as suas decisões as intenções da empresa, podendo vinculá-la criminalmente, tal como acontece com a atuação dos trabalhadores da empresa dentro de certas condições normativas. Uma solução como esta permite ao Direito Penal remeter a responsabilidade a um ente penalmente cognoscível (a pessoa coletiva), não sendo necessário recorrer à solução da atribuição da personalidade jurídica eletrónica e, ao mesmo tempo, incentiva as empresas a monitorizar, treinar e disciplinar os seus subordinados (trabalhadores e algoritmos)[278].

Não obstante, uma solução deste tipo analisada individualmente deixa por preencher a lacuna de responsabilidade no que ao nexo causal diz respeito, pois não concretiza que pessoa coletiva é criminalmente responsável, já que os algoritmos podem ter diversos intervenientes no seu processo de formação.

Quanto a este nexo causal, o Autor propõe uma resposta tendo por base os princípios da justiça (*fairness*) e da prevenção (*prevention*). Com efeito, defende a teoria do controlo-benefício (*the beneficial-control account*), que se sustenta na *ratio* do modelo de responsabilidade vicarial, onde, pelo vínculo orgânico e hierárquico, a pessoa coletiva exerce

---

[275] Sobre a criação de novas pessoas jurídicas enquanto instrumento útil ao Direito Penal e a necessária cautela, ABBOT, Ryan / SARCH, Alex, *Op. cit.* p. 384 («Legal fictions help turn the criminal law into a pragmatic tool for solving social problems. Nonetheless, legal fictions must be used with caution, as their overuse risks eroding public trust and weakening the rule of law»).

[276] DIAMANTIS, Mihailis E., «The Extended Corporate Mind: When Corporations use AI to Break the Law», *Op. cit*, p. 901 e ss.

[277] *Ibid.*, p. 912 e ss.

[278] DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *Op. cit.*, p. 827 - 829.

um controlo sobre os seus subordinados e beneficia com a suas condutas. Segundo esta ideia, a empresa é responsável sempre que um algoritmo sobre o qual tenha controlo (*control-based account*[279]) cause um dano benéfico para si (*benefits-based account*[280]). Numa palavra, podemos afirmar que esta teoria corresponde a uma aplicação criativa do modelo de responsabilidade vicarial, aplicando-a agora tendo em vista os algoritmos empresariais.

Numa obra mais recente, o Autor apresentou seis critérios que considera ser os moldes de solução válida para o *accountability gap*[281]: (1) a solução tem que identificar a plenitude de o/os agente/s a quem transferir a responsabilidade; (2) ser robusta o suficiente para evitar artifícios por parte dos responsáveis para fugir à responsabilidade; (3) ser coerciva e intimidatória para que os agentes não racionalizem a possibilidade de crime; (4) respeitar o princípio da justiça, apresentando soluções justas; (5) ser pouco onerosa para não limitar o desenvolvimento tecnológico; (6) promova valores éticos na programação, como a transparência algorítmica. Aqui, admitiu não ter encontrado uma solução que preenchesse todos os critérios, mas conclui que a solução mais equilibrada, cumprindo a maioria, seria a abordagem através de um modelo de negligência. Segundo esta visão, qualquer agente que tivesse contacto, no mínimo, negligente com o algoritmo seria responsável.

[279] Segundo esta tese baseada no princípio da prevenção, as empresas são os agentes em melhor posição para evitar e prevenir os factos ilícitos decorrentes da sua estrutura por exercerem autoridade e controlo sobre os seus subordinados. Assim, havendo a ameaça de responsabilidade da empresa, procura-se que a esta exerça os seus poderes de controlo para monitorizar a sua atuação interna. Deste modo, seriam atos empresariais quaisquer efeitos sobre os quais esta exerça um controlo substancial. Ora, com os algoritmos empresariais, a solução do Autor é semelhante. As atuações dos algoritmos correspondem a atuações empresariais sempre que causem lesões que a empresa tivesse o poder substancial de prevenir. Como estes não são infalíveis, há medidas que as empresas devem tomar como prova da sua diligência na prevenção da ocorrência dos crimes. Vista individualmente, esta tese não se demonstra viável pois deixa num plano demasiado abstrato uma imputação que tem que ser concreta, isto é, poderá levar a que uma empresa que exerça controlo sobre um algoritmo seja responsável por uma utilização irresponsável por parte de terceiros. Cfr. DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *Op. cit.*, p. 831 – 838.

[280] A *benefits-based account* é uma teoria que se baseia no princípio da justiça, estatuindo que da mesma forma que as pessoas coletivas beneficiam com a atuação dos seus subordinados, devem também participar nos encargos e responsabilidades. Da mesma forma se passa com os algoritmos empresariais. As empresas produzem e/ou utilizam algoritmos para seu próprio benefício pelo que, da mesma forma que têm vantagens com eles, deverão responder por estes quando haja repercussões da sua utilização. Novamente, esta tese analisada univocamente não se apresenta como uma solução prática, pois haverá casos em que os benefícios decorrentes de uma lesão criada através de um algoritmo poderão ter repercussões tais que a responsabilização desses "sub-beneficiários" deixa de fazer qualquer sentido axiológico, em especial e em nome do princípio da justiça. Cfr. DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *Op. cit.*, p. 838 – 843.

[281] DIAMANTIS, Mihailis E., «Vicarious Liability for AI», *Op. cit.*, p. 4 – 12.

2.2.Notas para uma solução *de jure condendo*

Apresentadas as ambivalências das teorias em debate, não se arriscará na proposição de uma solução definitiva ou, muito menos, incriticável, pelas dificuldades decorrentes de qualquer solução ao *accountability gap*. Do mesmo modo, não se pretende apresentar a resposta correta para o caso hipotético *NoLock*. Isto porque, não havendo uma solução definitiva para as teorias aqui em causa, naturalmente não haverá, na mesma medida, solução para o caso descrito. Serve e serviu este como exemplo para expor e abordar diversos problemas relativos aos riscos inerentes aos sistemas de IA quando introduzidos em ambientes complexos e de risco.

Antes de tudo, não poderemos começar qualquer proposição partindo de uma premissa errónea ou inverosímil. Já ficou demonstrado que as capacidades técnicas dos sistemas de inteligência artificial são exorbitantes. Contudo, nos atuais dias e apesar da evolução que a tecnologia na inteligência artificial tem tido, estes sistemas dificilmente consubstanciarão todos os requisitos para podermos assumir uma personalidade jurídica eletrónica. Neste sentido, os argumentos repelentes desta visão correspondem ao que acima se disse quanto a esta não admissibilidade. Por esta ordem ideias, a adoção da teoria disruptiva não é de admitir. Com efeito, por exclusão de partes parece-nos que é nas teorias clássicas que deve o legislador procurar encontrar uma potencial solução para a cobertura da lacuna da responsabilidade.

Tendo em conta os princípios basilares sustentados na doutrina penal, especialmente neste contexto, o princípio da legalidade e o princípio da culpa exigem que se procure uma solução espelhada no princípio da intervenção mínima, sem prescindir das traves mestras que sustentam todo o facto punível. Assim, numa primeira instância, a solução passa sempre por aquela que for menos lesiva para os princípios aqui em causa, procurando, ao mesmo tempo, não deixar situações de impunidade, nem limitar o desenvolvimento tecnológico.

A partir do momento em que a empresa utiliza um sistema de inteligência artificial sabe antecipadamente, porque a máquina é falível, do risco que lhe é inerente graças à sua (potencial) inexplicabilidade, espontaneidade e incontrolabilidade. Assim, dentro do julgamento empresarial e da tomada de decisão de recorrer a sistemas "inteligentes" deve pender também uma análise de riscos do sistema. Esta ponderação é ela própria uma precaução da empresa utilizadora para uma eventual responsabilidade. Estando presente e assumido este risco, a empresa recorre ao sistema de inteligência artificial como um

instrumento a partir do qual atua, faz previsões e se autorregula, pelo que uma decisão do sistema que seja imprevisível e autónoma, deverá entrar dentro da esfera de risco que lhe é inerente e ao qual a empresa se vinculou, aceitou e transferiu para si.

Tanto a tese do controlo-benefício como a solução da responsabilidade pelo produto "inteligente" espelham soluções equilibradas. A primeira está inerentemente associada ao modelo de heterorresponsabilidade, enquanto a segunda está ligada ao modelo de responsabilidade direta ou autorresponsabilidade.

O que está em causa quando falamos destes produtos é a sua capacidade imprevisível e lesiva, pelo que a solução mais indicada terá que ser aquela que imponha maiores constrições a quem domine os produtos, para evitar que estes lesionem bens jurídicos. Deste modo, não sendo possível responsabilizar os algoritmos, a única solução que responsabiliza concretamente os agentes que dominam o facto do resultado é a solução dada através pela responsabilidade pelo produto "inteligente". Aqui, até por estarmos perante um modelo de autorresponsabilização, que consubstancia, a nosso ver, o correto e único modelo de concreta responsabilização da pessoa coletiva, ou seja, não faz intervir terceiros no apuramento desta responsabilidade, esta solução demonstra um incisivo repto aos produtores no cumprimento com os respetivos deveres de precaução. Notoriamente, este é um modelo que pressupõe uma estrita ligação à regulação existente, já que é esta regulação que vai determinar e balizar as permissões setoriais e caraterísticas especificas dos sistemas.

No entanto, haverá situações em que o programador cumpriu com o seu dever de precaução e o sistema, ainda assim, cometeu um crime de forma imprevisível. Foi uma situação destas que ocorreu no caso *NoLock* com a prática do crime de fraude fiscal. Isto porque, estando em causa um algoritmo que era já um *cognitive software*, este aprendeu novos dados decorrentes da experiência, pelo que uma introdução defeituosa neste âmbito é o suficiente para o sistema falhar. Ora, seguindo estritamente a responsabilidade pelo produto "inteligente", o produtor seria diretamente responsável pela falha do algoritmo e, conseguindo fazer a prova que o resultado adveio de uma caraterística exógena à sua intervenção, ninguém seria responsabilizado. É por este motivo que o conceito de produtor nesta teoria teria que ser alargado por forma a abarcar também aqueles que têm a capacidade para influenciar *ex post* o algoritmo (utilizando os termos da teoria do controlo-benefício, aqueles que controlam o algoritmo).

Deste modo, uma potencial solução para o caso concreto seria responsabilizar diretamente pelo crime de fraude fiscal a título de negligência tanto a *ComplyTeK* como a *TechCypher*, devendo cada uma delas provar que cumpriu com o princípio da precaução na programação e na utilização, respetivamente[282].

Estando em causa um instrumento com um potencial risco de falibilidade e imprevisibilidade, estes agentes, porque tinham ou tiveram o controlo sobre o algoritmo, tendo este falhado, terão que demonstrar que internamente se organizaram através de medidas preventivas (procurando fazer monitorizações, testes e treinos do algoritmo através de uma *sandbox approach*[283], novos *inputs*, auditorias regulares, atualizações dos dados pré-existentes, executar diligências de explicabilidade das decisões algorítmicas, tornando estas decisões mais transparentes através de ferramentas de *XAI*, criação de um departamento de monitorização com um responsável por estas diligências[284]), mostrando que o crime ocorreu apesar de todas estas medidas. Só assim, se poderá pensar numa isenção de responsabilidade. Apesar de esta prova poder ser difícil pela opacidade dos algoritmos, começam hoje a existir de ferramentas de *Explainable AI (XAI)* para auxiliar a justificação do "porquê" da decisão algorítmica[285].

Em ambos os casos, como não houve a intenção da utilização do sistema *NoLock* para o cometimento de crimes não poderemos falar aqui em dolo, pelo que a violação destes deveres de precaução (na produção e na utilização) são geradores, no máximo, de responsabilidade penal por negligência, o que cria uma situação de podermos ter que abranger tipos negligentes para certos crimes que até agora apenas estavam previstos na sua vertente dolosa, ou mesmo dar lugar a novas incriminações (os já aludidos *«Hard AI Crimes»*[286]).

Não obstante, esta opção doutrinal, apesar de subir um degrau na atribuição de responsabilidade a um agente penalmente cognoscível não resolve por completo a lacuna. Deixa ainda em aberto as situações em que os produtores consigam fazer prova que cumpriram com os deveres de precaução, mostrando que fizeram de tudo para o evitar e ele

---

[282] Sobre a constituição destes deveres de cuidado e da imprevisibilidade do sistema, GLESS, Sabine / SILVERMAN, Emily / WEIGEND, Thomas, *Op. cit.*, p. 426 e ss.
[283] SOUSA, Susana Aires de, «"Não fui eu, foi a máquina" …», *Op. cit.*, p. 86.
[284] DIAMANTIS, Mihailis E., «Algorithmic Harm as Corporate Misconduct», *Op. cit.*, p. 148 e ss.; e ainda, sobre a ideia da criação de um responsável por estas diligências (assemelhando-se a um *Chief Compliance Officer*), mas segundo uma visão de transferência de responsabilidades para este responsável, ABBOT, Ryan / SARCH, Alex, *Op. cit.* p. 378 e ss.
[285] *Vide supra* nota 31.
[286] *Vide supra* nota 210.

ainda assim ocorreu. Isto é, é necessário ficar claro que ainda que a tese acima exposta proceda, é possível que os agentes em causa façam prova que foram diligentes e preventivos e o crime, ainda assim, ter ocorrido. Segundo esta ideia e seguindo o princípio da culpa (*nullum crimen sine culpa*) ninguém seria responsabilizado. *Quid iuris*?

Aqui, ou se admite uma responsabilidade direta do sistema (algo que se deixa categoricamente de parte). Ou simplesmente se reconhece que o *accountability gap* nesta fase deixa de ser uma lacuna para ser a realidade das coisas. Isto é, o Direito Penal não consegue regular todas as situações do quotidiano, prevenindo todas as esferas de risco existentes que possam levar à lesão de bens jurídico-penais. Para tal, a tutela subsidiária de bens jurídico-penais dita que, por vezes, poderá haver casos em que a lesão desses bens jurídicos resulta da "sociedade do risco" em que vivemos, não sendo possível identificar e responsabilizar qualquer agente[287]. A potencial dificuldade de uma solução como esta parte da própria essência do Homem em lidar penosamente com a falta de respostas. No entanto, nem tudo na Natureza tem resposta ou advém de uma causa penalmente cognoscível.

3. O *Criminal Compliance* "inteligente" e o processo penal

A concreta ligação entre a realidade preventiva que consubstancia o *criminal compliance* e a atribuição de responsabilidade penal dispõe-se no processo penal. Isto porque, como vimos anteriormente, este mecanismo de autocontrolo é valorado em juízo através da verificação e avaliação da sua eficácia. Ora, introduzindo-se a inteligência artificial neste meio, esta verificação poderá sofrer algumas alterações em função das próprias caraterísticas do sistema. Desde logo, pois certas tarefas que antes eram realizadas exclusivamente por seres humanos, com estes sistemas, passam a ser levadas a cabo por um *software* programado para o efeito.

Como tal, e como perspetivado, caberá analisar de que forma podem os dados produzidos, adquiridos ou compartimentados a partir de sistemas de inteligência artificial no âmbito do *criminal compliance* ser utilizados no processo penal. Aqui, juntam-se duas problemáticas: por um lado, a "transferência" e valoração de prova produzida fora do processo penal no processo penal e, por outro, o facto de se tratar de prova produzida por um *software*. Assim, às especiais atenções necessárias no âmbito do (já discutido na

[287] LIMA, Dafni, *Op. cit.*, p. 693 e 694.

doutrina) problema do "empréstimo" de prova terão que se acrescentar as preocupações resultantes da utilização de sistemas "inteligentes".

Para além disto, num segundo ponto, da mesma forma que atualmente as empresas adotam programas de *compliance* "inteligentes" para prevenir ilícitos de forma (teoricamente) mais eficaz, questiona-se se não poderá, ao mesmo tempo, o Ministério Público e órgãos de polícia criminal utilizar semelhantes meios, podendo inclusive facilitar a colaboração processual da empresa a troco de certas vantagens. Esta poderá ser uma ferramenta almejada por parte destes órgãos num futuro próximo para a prossecução dos seus objetivos, pelo que se teorizará que repercussões poderá ter uma opção político-criminal como esta nos direitos fundamentais dos investigados.

3.1.Investigações internas "inteligentes" como meio de obtenção de prova?

A inteligência artificial começa hoje a ganhar cada vez mais espaço nos tribunais. Em especial, o setor judicial tem sido particularmente curioso e disponível à inovação, tendo acompanhado a evolução tecnológica através de um aprimoramento dos serviços jurídicos com soluções informatizadas. Para além da utilização específica destes sistemas numa vertente interna em escritórios de advogados com soluções digitais de armazenamento de documentos ou de pesquisa jurídica[288], existem já instrumentos que recorrem à inteligência artificial na resolução de litígios, seja judicialmente, ou através de meios alternativos de mediação ou arbitragem (e.g. *online dispute resolution*)[289]. Neste contexto, como nos outros setores, a introdução de sistemas de inteligência artificial é necessariamente uma questão temporal.

A inclusão da inteligência artificial começa a surgir a nível processual em duas vertentes: a nível probatório, através da prova digital; e, no "banco do juiz", a nível decisório, auxiliando as decisões de prognose póstumas inerentes (aproveitando as capacidades preditivas dos sistemas de IA)[290]. Exemplo paradigmático neste contexto é o caso *Loomis*, em que o juiz, na determinação da sentença, recorreu à utilização de um sistema de inteligência artificial (COMPAS) para avaliar o risco de perigosidade e reincidência do

[288] SCHEMMEL, Alexander / DIETZEN, Alexandra, *Op. cit.*, p. 142.
[289] Como exemplo, a própria Comissão Europeia desenvolveu uma plataforma para resolução alternativa de litígios decorrentes de compras *online*; também empresas como a *eBay* ou a *PayPal* desenvolveram plataformas para a facilitação da resolução de litígios entre vendedores e compradores.
[290] RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *Op. cit.*, p. 11 e ss.

agente. Para tal, o *software* tinha como base de cálculo um questionário com 137 itens e o registo criminal do agente, indicando o índice de risco de reincidência deste. O algoritmo reputou Loomis com um elevado grau de perigosidade e reincidência, pelo que lhe foi aplicada uma pena de prisão efetiva de seis anos. A defesa do arguido recorreu tendo por base a violação dos seus direitos processuais, nomeadamente, pela violação do direito a um julgamento justo, do princípio do contraditório e do princípio da igualdade de armas. Isto porque, como já se disse, o algoritmo poderá ser opaco e enviesado. Contudo, o *Supreme Court* do Wisconsin «afastou a violação do *due process*, em função de considerar a mera possibilidade de o acusado comparar os dados individuais de entrada (*inputs*) e as valorações finais de risco (*outputs*) recorrendo ao manual de instruções do instrumento como capaz de assegurar o direito a contestar a validade dos resultados alcançados». Para além disto, afirmou também que o caso teria aquele desfecho mesmo que o sistema não tivesse sido utilizado[291].

Aqui, percebe-se que a introdução da inteligência artificial no âmbito processual seja mais um instrumento catalisador de reflexões sobre o confronto e concordância prática entre as finalidades do processo penal: da realização da justiça e descoberta da verdade material, proteção dos direitos fundamentais do arguido perante o Estado e o restabelecimento da paz jurídica posta em causa com a prática do crime[292].

Convocando o que antes se disse quanto aos efeitos processuais do *criminal compliance* com as valências da inteligência artificial neste âmbito, mais evidente se torna este embate finalístico. Por esta ordem de ideias, o *criminal compliance* "inteligente" pode ser um bom e útil instrumento em sede processual, pois o seu potencial de eficácia facilita a prova e, por conseguinte, a atenuação ou isenção de responsabilidade da pessoa coletiva. No entanto, o estigma do risco sempre inerente à inteligência artificial mantém-se. E aqui de forma ainda mais notória, pois o espetro de potenciais direitos fundamentais lesados, em detrimento da descoberta da verdade material e realização da justiça, aumenta[293].

Em concreto, no âmbito dos elementos do *criminal compliance*, um instrumento específico bastante útil na "fase pré-penal" são as investigações internas. Estas

[291] *Ibid.*, p. 28.
[292] ANTUNES, Maria João, *Direito Processual Penal*, 2.ª Ed., Coimbra: Almedina, 2019, p. 14 e ss.
[293] Neste sentido, FIDALGO, Sónia, «A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo», *in A Inteligência Artificial no Direito Penal*, coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 141.

correspondem ao expediente decorrente dos programas de *compliance* (apesar de poderem não estar necessariamente ligados a estes programas, uma vez que podem ser conduzidas por entidades externas à própria pessoa coletiva) que visam identificar e reprimir violações de normas internas da empresa ou regulatórias (não necessariamente factos criminosos)[294]. Estas investigações têm como fonte, principalmente, os canais de denúncias interno da empresa - elemento essencial do programa de *compliance* -, mas também pode ter outras fontes como denúncias externas, notícias, auditorias, notificações judiciais. Ou seja, as investigações internas são consequência da existência de uma denúncia, pelo que com estas procurar-se-á apurar as responsabilidades (seja disciplinar ou criminal).

De uma forma genérica, o sucesso e a eficácia de uma investigação interna depende da capacidade de recolher, processar e analisar dados[295]. Estes dados são compostos por todas as informações adquiridas ao longo do processo investigatório, que podem estar estruturados ou não, isto é, poderão estar categorizados segundo padrões comuns ou estar dispostos aleatoriamente, cabendo ao investigador fazer essa triagem e padronização para melhor interpretação. As dificuldades começam a aparecer aqui, já que estes dados são cada vez mais volumosos e advêm de fontes cada vez mais díspares (*emails*, redes sociais, documentos), aumentando a morosidade, complexidade e custos dos processos[296]. São estas razões que justificam, para que a qualidade do processo não saia comprometida, o recurso a soluções de inteligência artificial.

Com efeito, começa-se a aprofundar cada vez mais a área da computação forense (ou ciência forense digital), especialmente no âmbito empresarial[297]. Esta diz respeito à recolha, processamento e interpretação de dados digitais, tendo em vista a sua utilização como

---

[294] ENGELHART, Marc, *The Nature and Basic Problems of Compliance Regimes*, Max-Planck-Institut für ausländisches und internationales Strafrecht, Forschungsgruppe "Architektur des Sicherheitsrechts"(ArchiS), 2018, p. 3 e p. 19 - 21.

[295] MUELLER, Tim / SISWICK, James, *Op. cit.*, p. 16.

[296] *Ibid.*, *Loc. cit.* E, no mesmo sentido, ADAMS, Zachary / CHALK, Richard, «The Rise of AI in Corporate Investigations», Law360, New York, Set. 2017, p. 1 e 2. Referem os Autores do artigo que um relatório da IBM de 2016 afirmava que 90% dos dados de todo o mundo teriam sido gerados nos anteriores dois anos.

[297] Reconhecendo esta evolução a nível empresarial, MUELLER, Tim / SISWICK, James, *Op. cit.*, p. 16 («Enforcement agencies anticipate companies are doing their own internal monitoring, and AI is often the best way to do so. In April 2019, the U.S. Department of Justice (DOJ) released updated guidance to prosecutors working on compliance enforcement. The DOJ identified one hallmark of an effective compliance program as "its capacity to improve and evolve" and specifically pointed to improvements that ensure programs are "not stale". Another such hallmark the DOJ identified is "the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct". Capacity to improve? Not stale? Timely and thorough? Those all sound like adjectives that describe work well-placed in the AI fold»).

elemento de prova em tribunal, que recorre a técnicas de prospeção de dados (*data mining*), produzindo, categorizando e interpretando novos dados em função de caraterísticas e padrões comuns, mas também através da sua análise (*data analysis*)[298].

É neste seguimento que surge a questão epigrafada, tornando-se necessário desenvolver dois pontos consequenciais. Em primeiro lugar, é imprescindível analisar a validade probatória de informações adquiridas através de investigações internas no processo penal, isto é, analisar a admissibilidade do "transplante" de provas documentais adquiridas numa «antecâmara do processo penal»[299]. Posteriormente, cabe saber se os dados adquiridos, compartimentados e produzidos por sistemas "inteligentes" numa investigação interna são, desde logo, admissíveis e passíveis de ser utilizados como meio de prova num processo penal.

Quanto à questão do "empréstimo" da prova realizada fora do processo penal no âmbito das investigações internas, como já afirmado, esta é hoje uma questão já abordada, apesar de as preocupações daqui decorrentes não desaparecerem[300]. Estritamente de uma perspetiva de celeridade processual, redução dos custos e de descoberta da verdade material, de facto, a admissibilidade da prova produzida fora do processo penal seria favorável. No entanto, isso poderia acarretar um risco inalcançável para certos direitos fundamentais do arguido. Isto porque, as provas obtidas no âmbito das investigações internas baseiam-se em princípios distintos dos princípios de direito processual penal. Por exemplo, no direito laboral, o trabalhador investigado está sob o poder de direção do empregador e tem o dever de colaborar com este, sob pena de despedimento com justa causa. Contrariamente, no processo penal, o arguido não está obrigado a dizer a verdade e a contribuir para a sua incriminação (*nemo tenetur se ipsum accusare*)[301].

---

[298] *Supra*, nota 62.

[299] ANTUNES, Maria João, «Privatização das investigações e *compliance* criminal», *Op. cit.*, p. 127,

[300] Por todos, *Ibid.*, p. 119 – 127; MARTÍN, Adan Nieto, «Problemas fundamentales del cumplimiento normativo en el derecho penal», *in Temas de Derecho Penal Económico: Empresa y Compliance - Anuario de Derecho Penal 2013-2014*, p. 198 e ss.; MASCHMANN, Frank «Compliance y derechos del trabajador", *in* KUHLEN, Lothar et al., *Compliance y Teoria del Derecho Penal*, Marcial Pons, 2013, p. 155 - 159; PAIS, Ana, *Op. cit.*, p. 671 e ss.; COFFEE, JR., John C., *Corporate Crime And Punishment: The Crisis of Underenforcement*, Berret-Koelher Publishers, Inc., p. 44 - 49; ENGELHART, Marc, *Op. cit.*, p. 3 e p. 19 e 21.

[301] Ainda assim, no sentido da admissibilidade, o Ac. TC n. º 279/2022, de 26-04 veio concretizar o que o Ac. TC n. º 340/2013 já tinha vindo dizer, concretamente, de que não é inconstitucional a utilização e valoração de prova produzida fora do processo penal (no caso obtida através do cumprimento de um dever de cooperação numa inspeção tributária) previamente à fase de inquérito. Em sentido crítico desta opção, ANDRADE, Manuel da Costa, «*Nemo tenetur se ipsum accusare* e direito tributário. Ou a insustentável indolência de um acórdão (n.º 340/2013) de Tribunal Constitucional», *Boletim de Ciências Económicas*, LVII/I, 2014, p. 385 - 451.

No plano do direito a constituir, uma solução ideal (possivelmente de difícil compatibilização) seria a admissibilidade da utilização destas provas, desde que, na investigação, fossem garantidas as mesmas garantias básicas e irrenunciáveis do processo penal[302]. Para tal, uma indicação essencial neste âmbito diz respeito à finalidade da investigação. Concretamente, caso a investigação interna tivesse como escopo averiguar uma suspeita de crime a nível interno, tendo em vista a atenuação ou isenção de responsabilidade da pessoa coletiva, a utilização da prova poderia ser de admitir desde que o investigado fosse informado da possibilidade dessa utilização e fossem respeitadas as mesmas garantias processuais penais.

Neste caso, fala-se estritamente de provas documentais adquiridas com a contribuição do arguido e a partir das quais a investigação interna é relatada[303]. Quanto às provas testemunhais e periciais, devem estas respeitar o princípio da imediação e ser revalidadas no processo penal, devendo ser repetidas. Deste modo, numa perspetiva de colaboração processual da empresa na fase de inquérito, por forma a legitimar todo o processo, a admissibilidade destas provas estaria dependente de autorização judicial, estabelecendo-se aqui um paralelo com o regime das escutas telefónicas em que, para que estas sejam válidas enquanto meio de obtenção de prova, têm que ter autorização judicial prévia (art. 187.º CPP)[304].

Introduzindo-se a inteligência artificial neste contexto, poderemos perguntar se os dados decorrentes de investigações internas produzidos por sistemas de IA, por exemplo, no cumprimento dos deveres preventivos (dispostos na Lei n.º 83/2017, de 18 de agosto), concretamente, no dever de comunicação às autoridades judiciárias quando em causa esteja um crime de branqueamento de capitais, poderão ser utilizados no processo penal.

---

[302] Neste sentido, e relembrando a importância da criação de um Código das Investigações Internas nos programas de *compliance*, ANTUNES, Maria João, «Privatização das investigações e *compliance* criminal», *Op. cit.*, p. 126; e também, MARTÍN, Adán Nieto, *Op. cit.*., p. 199 («Si la investigación interna es la antesala del proceso penal, hay que ofrecer garantías similares»).

[303] Conforme PAIS, Ana, *Op. cit.*, p. 673 e ss., devem distinguir-se duas situações: a prova obtida contra a vontade do trabalhador e a prova obtida com a contribuição do trabalhador. Concretamente, no que diz respeito à prova testemunhal e da prova pericial, «os peritos e as testemunhas terão que ser novamente ouvidos no processo-crime (…)» e, portanto, aqui a prova será certificada por autoridade judiciária.

[304] Nestes termos, o Supremo Tribunal de Justiça Espanhol (STS 2844/2014) num acórdão de 16 de junho de 2014 afirmou que, ainda que a prova seja válida de um ponto de vista do direito laboral, não pode ser valorada em processo penal se tiver sido obtida em desacordo com as regras do processo penal, designadamente por via da autorização judicial. Assim, *a contrario*, a prova obtida de acordo com as regras do processo penal, designadamente por via da autorização judicial, seria de admitir. Também o Código de Processo Penal Alemão (*Strafprozeßordnung*), na secção §244 (2) e (3), admite a possibilidade de recurso a provas obtidas fora do processo penal desde que sejam relevantes para a decisão e cumpram determinados requisitos.

Em primeira vista, por estarmos no contexto de deveres jurídicos dir-se-á que sim. Contudo, as dificuldades não advêm daqui. Poderão, todavia, agravar-se graças ao facto de os dados relevantes como elementos de prova terem sido produzidos por sistemas de IA, que, por si só, geram problemas.

Em concreto, volta-se aqui às duas caraterísticas da inteligência artificial que sustentam as maiores reservas quanto à adoção destes sistemas neste âmbito. Falamos da complexidade e opacidade dos algoritmos. Em função disto, acompanhar-se-á SÓNIA FIDALGO na sistematização, em sentido amplo, dos direitos potencialmente lesados com este tipo de sistemas: o direito à privacidade e o direito de defesa[305].

Quanto ao primeiro, as preocupações surgem pelo facto de sistemas deste género acederem a uma grande quantidade de dados (através dos *big data* e *cloud computing*) e, no caso concreto das investigações internas, através destes, gerar um compêndio padronizado desses dados não estruturados (*data mining*). Ora, neste acesso poderão facilmente ocorrer violações dos direitos fundamentais seja das pessoas físicas integrantes da estrutura empresarial, nomeadamente através de intromissões na vida privada (digital), lesando a sua «expectativa razoável de privacidade»[306], como de terceiros que não têm qualquer ligação à investigação em causa[307]. Foi com base nestas considerações que o Regulamento Geral da Proteção de Dados veio já abordar o tratamento de dados gerados por sistemas de IA[308].

Quanto ao direito de defesa, objeções mais flagrantes se apresentam. Qualquer meio de prova validado no processo penal, nos termos do art. 127.º do Código do Processo Penal, está sujeito ao princípio da livre apreciação da prova, determinado por critérios de razoabilidade por parte do julgador que, na formação da sua convicção, exige uma

---

[305] FIDALGO, Sónia, *Op. cit.*, p. 137 e ss.

[306] Caso *Bărbulescu v. Romania* (processo n.º 61496/08) do Tribunal Europeu dos Direitos Humanos de 5 setembro de 2017, §56. Neste caso, um trabalhador foi despedido por usar o computador (propriedade da empresa) para fins diversos não-laborais, violando assim o código de conduta da empresa (que esta admitiu ter dado conhecimento da proibição de utilização para fins diversos dos profissionais). No âmbito do processo disciplinar que foi instaurado na sequência destes factos, o trabalhador negou as condutas. A empresa, em resposta, confrontou-o com mensagens privadas que foram trocadas pelo trabalhador através do computador da empresa durante o horário de trabalho. Tendo sido negada a impugnação do despedimento por fundamento na sua ilicitude em todas as instâncias internas, o Tribunal Europeu dos Direitos Humanos decidiu no sentido da ilicitude do despedimento por violação da Convenção Europeia dos Direitos Humanos no direito à reserva da intimidade da vida privada e o direito à inviolabilidade das comunicações (art. 8.º). Concretamente, considerou não bastar avisar o trabalhador que não podia utilizar os computadores para fins distintos dos profissionais, sendo necessário informar o trabalhador relativamente à possibilidade de controlo e monitorização do bom uso do computador.

[307] FIDALGO, Sónia, *Op. cit.*, p. 139.

[308] Sobre a proteção destes dados pessoais à luz do RGPD, BARBOSA, Mafalda Miranda, «Dos Expert Systems aos Data Systems AI: impacto ao nível da proteção de dados», *Op. cit.*, p. 17 e ss.

fidedignidade, certeza e explicabilidade das provas nas quais se baseou para a tomada da decisão[309]. Neste sentido, faz-se mister concretizar a sua origem e fundamento. Se a prova em questão foi obtida através de sistemas de inteligência artificial, a explicabilidade desta terá necessariamente que ser conduzida por um especialista pela complexidade e tecnicidade das questões aqui em causa (recorrendo-se à prova pericial)[310]. Não obstante, mais uma vez, uma das dificuldades aqui presente advém do problema da "caixa negra", onde pela vastidão, opacidade e inexplicabilidade dos algoritmos, os peritos poderão não conseguir auxiliar a tomada da decisão do juiz. Um outro ponto que poderá ser enunciado diz respeito à possibilidade de enviesamento dos dados a partir dos quais o algoritmo produziu a prova. Ora, com esta falta de transparência algorítmica, de uma perspetiva do direito de defesa do arguido, não tendo este acesso às informações técnicas do algoritmo, a prova produzida a partir de sistemas de IA não poderá ser contraditada "em igualdade de armas"[311].

Neste prisma, se for possível eliminar da equação o problema da complexidade e opacidade dos algoritmos, voltamos ao problema do "empréstimo" da prova, ou seja, os obstáculos que se põem aqui deixam de ter que ver com os próprios algoritmos, mas com a própria sistemática processual de contrabalanço das finalidades. Ora, uma aproximação à resolução do problema da complexidade e opacidade apenas é possível com o caminho da regulação.

Porta-estandarte desta ideia é a Proposta de Regulamento para a Inteligência Artificial da Comissão Europeia. Esta Proposta contém normas estritas para produtores e utilizadores de sistemas de IA, que divide os sistemas consoante o tipo de risco: risco inaceitável (práticas de inteligência artificial proibidas – art. 5.º), risco elevado (art. 6.º da Proposta e anexo III), devendo, como condição para colocação no mercado, cumprir um conjunto de requisitos e obrigações (art. 8.º a art. 15.º), riscos limitados, que devem cumprir obrigações de transparência (art. 52.º) e os riscos mínimos, que devem seguir códigos de conduta, mas não possuem obrigações concretas de cumprimento (art. 69.º). Com efeito, através de imposições

[309] Ac. do STJ de 12 de abril de 2000, proc. nº 141/2000-3ª; SASTJ, nº 40. 48 («Não dizendo a lei em que consiste o exame crítico das provas, esse exame tem de ser aferido com critérios de razoabilidade, sendo fundamental que permita avaliar cabalmente o porquê da decisão e o processo lógico-formal que serviu de suporte ao respetivo conteúdo»).

[310] GLESS, Sabine, «AI in the courtroom: a comparative analysis of machine evidence in criminal trials», *Georgetown Journal of International Law*, Vol. 51, n. º 2, 2020, p. 195 – 253.

[311] FIDALGO, Sónia, *Op. cit.*, p. 142 e ss. («Numa palavra, devem ser criadas ferramentas que permitam ao arguido contraditar a prova, designadamente, proporcionando-se acesso aberto ao código fonte, criando-se mecanismos de certificação dos sistemas e explicando-se o sistema em linguagem clara, indicando-se, por exemplo, as ferramentas utilizadas»).

normativas que garantam a adequação, certificação, rastreabilidade, transparência e garantia de supervisão humana dos algoritmos, conferindo uma situação de igualdade de acesso aos dados entre os intervenientes processuais, torna-se possível enxergar a sua utilização em processos judiciais como meios de prova.

Por outro lado, a utilização de dados gerados através deste tipo de sistemas pode ser uma realidade fraturante relativamente ao princípio da proibição da não autoincriminação, já que, se os dados forem adquiridos oficiosamente no compêndio de dados estruturados, facilmente poderá o Ministério Público ter acesso a informação incriminatória que de outra forma não teria. Assim, permitindo-se esta transferência de prova, as garantias processuais do arguido poderão ficar em xeque. Daí que seja da maior importância (e só desta forma é que seria de admitir esta utilização) que os dados sejam transparentes e explicáveis, mas principalmente, que sejam fornecidos com o consentimento e contribuição do arguido, devendo ser relevados aqueles que única e exclusivamente o possam vincular, ou seja, os dados existentes sobre terceiros devem ser desconsiderados. Para além disto, a admissibilidade deste tipo de prova não poderia nunca ser utilizada como único elemento a partir da qual o julgador pudesse sustentar a sua decisão.

Em suma, qualquer admissibilidade da utilização da prova produzida extrajudicialmente no processo penal é complexa. Segundo os moldes de legalidade onde está assente o nosso sistema processual penal, uma solução equilibrada implica sempre uma ponderação político-criminal sensata e de razoabilidade por forma a prosseguir a finalidade da descoberta da verdade material e realização da justiça, tendo sempre como plano de fundo as garantias processuais do arguido. Para o futuro, até por motivos políticos, sociais e económicos, deve o legislador largar certas intransigências e abrir a porta a novas soluções, mais céleres, menos dispendiosas e que dão, ao mesmo tempo, garantias bastantes aos arguidos num processo penal.

3.2.Uma nova forma de colaboração processual: *Criminal Compliance* "inteligente" e *SupTech*

Exemplo concreto de uma destas novas soluções e inovações é o caso da *SupTech*, enquanto instrumento ao cargo das entidades supervisores para monitorizar e regular os agentes económicos. Neste sentido, se as novas tecnologias potenciam a prática de crimes, não deixa de ser verdade que podem (e devem), ao mesmo tempo, ser aproveitadas e

desenvolvidas novas formas de os combater[312]. O *criminal compliance* "inteligente" como figura análoga à *RegTech* é exemplo disto através da prevenção criminal.

Concretamente, *SupTech* (*Supervisory Technology*) corresponde à utilização de tecnologia por entidades reguladoras e de supervisão para auxiliar as suas funções de forma mais eficaz[313]. Em termos funcionais, auxilia as entidades supervisores a informatizar os processos, facilitando a monitorização do risco e das funções do *compliance* regulatório no setor financeiro.

Como já se afirmou, a interligação do sistema financeiro com as novas tecnologias não é recente. Foi, desde sempre, o setor mais disponível à introdução da inovação, tanto como consequência de imposições normativas, tanto por sua iniciativa para aumentar a eficiência dos seus processos que, em função da tecnicidade do setor, podem ser morosos e de elevada complexidade. Este é, como vimos, o terreno fértil para a aplicação da inteligência artificial. Isto porque, a possibilidade de análise de uma vastidão de dados por forma a tornar os processos mais céleres, menos dispendiosos e mais eficientes é o que define as potencialidades da inteligência artificial[314].

Concretamente, diversas instituições bancárias incluíram já perfeitamente sistemas de inteligência artificial no seu quotidiano, seguindo uma abordagem de *sandbox*[315], para que possam testar num ambiente seguro os sistemas que pretendem implementar. O *Bank of England* e a *Financial Conduct Authority* do Reino Unido (FCA) são exemplos pioneiros neste contexto, utilizando atualmente sistemas de *data analysis*, *machine learning*, *perceptual* e *semantic computing* para auxiliar a deteção de fraude no mercado (manipulação do mercado ou *insider trading*)[316]. Um outro exemplo relevante decorre da criação de uma base de dados europeia (EuReCA) criada pela Autoridade Bancária Europeia (EBA), que

---

[312] RAMOS, José Ricardo Marcondes, *Op. cit.*, p. 89.

[313] *Supra* nota 60. Mais desenvolvido, BROEDERS, Dirk / PRENIO, Jermy, «Innovative technology in financial supervision (SupTech): the experience of early users», Bank for International Settlements, Financial Stability Institute, Insights on Policy Implementation No. 9, 2018.

[314] RAMALHO, Inês Palma, «SupTech e Regtech: o futuro da supervisão portuguesa?», *InforBanca – Revista do Instituto de Formação Bancária*, n. º 116, jun. 2019, p. 45 («As vantagens de dispor de ferramentas adequadas de *suptech* e da *regtech* são inúmeras tanto para o supervisor como para o supervisionado: desde resolver problemas de *templates* regulatórios, detetar e completar elementos em falta, erros e inconsistências, dispensar (uma morosa) validação humana, diminuir os custos de *compliance* e *reporting* e permitir refocar o negócio, etc.»).

[315] *Supra*, nota 283.

[316] BUTLER, Tom / O'BRIAN, Leona, «Artificial Intelligence for regulatory compliance: Are we there yet?», *Op. cit.*, p. 52. Com mais exemplos de instituições financeiras que utilizam soluções "inteligentes", JUNG, John Ho Hee, *Op. cit.*, p. 271 e ss.

visa centralizar os dados sensíveis relevantes em sede de prevenção de branqueamento de capitais e financiamento do terrorismo e identificar riscos e alertas precoces de ameaças emergentes na União Europeia. Através destes dados, os sistemas das autoridades supervisoras produzirão relatórios digitais, aumentando a eficácia de todos os sistemas a nível europeu, graças a centralização dos dados estruturados e padronização das condutas, que facilitará a prevenção e deteção destas através das capacidades preditivas dos sistemas dotados de *machine learning*[317]. No caso de Portugal, os passos são pequenos, mas estão a ser dados, pelo que diversas estruturas de supervisão e fiscalização estão já a implementar estes sistemas, ou em processos disso[318]. Deste modo, «(é) inegável que a inovação tecnológica vem acompanhada de toda uma nova gíria que o supervisionado (e, em geral, o mercado) se tem visto forçado a aprender só para conseguir perceber (quanto mais acompanhar) a tendência. Parece existir pouca margem para o supervisor não o fazer também»[319].

Numa palavra, são já várias as instituições reguladoras que utilizam (ou pretendem utilizar) sistemas "inteligentes" para dinamizar os seus processos de atuação, adotando uma *data-driven* e *risk-based approach*[320], aproveitando as enormes vantagens e capacidades que a inteligência artificial lhes pode trazer: seja no melhoramento das capacidades de deteção de crimes económico-financeiros, na eficiência de processos de *compliance* e também no aprimoramento dos dados colhidos e geridos nas diversas áreas por forma a garantir eficácia aos processos[321].

---

[317] European Bank Authority, *EBA launches today 'EuReCA', the EU's central database for anti-money laundering and counter-terrorism financing*, 31 jan. 2022.

[318] O Banco de Portugal está a implementar uma ferramenta que permite «avaliar automaticamente o cumprimento de alguns requisitos legais e regulamentares que as instituições supervisionadas devem observar nas minutas dos contratos de crédito que venham a celebrar com os clientes bancários» Cfr. https://clientebancario.bportugal.pt/pt-pt/noticias/banco-mundial-destaca-iniciativa-de-suptech-do-banco-de-portugal; para além disto tem promovido o Portugal FinLab, enquanto plataforma de comunicação entre entidades reguladoras portuguesas e *start-ups* de FinTech que permite o desenvolvimento de soluções inovadoras na área. Também a CMVM tipificou como prioridade para o ano de 2022 a criação de grupos para o desenvolvimento de soluções no âmbito da inteligência artificial e outras novas tecnologias, tendo lançado uma consulta pública sobre este tema por forma a encontrar soluções benéficas na prossecução das suas funções. Cfr. https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20220607n.aspx. Ainda o Tribunal de Contas pretende implementar e desenvolver algoritmos para fiscalizar contratos públicos. Cfr. https://eco.sapo.pt/2021/10/19/tribunal-de-contas-recorre-a-inteligencia-artificial-para-fiscalizar-contratos-publicos/

[319] RAMALHO, Inês Palma, *Op. cit.*, p. 46.

[320] *Ibid.*, p. 45.

[321] Sobre, em geral, o uso de *SupTech* como instrumento para melhorar a supervisão e integridade do mercado, e, em especial, sobre os benefícios desta tecnologia, OCDE, «The use of SupTech to enhance market supervision and integrity», *OECD Business and Finance Outlook 2021: AI in Business and Finance*, Ch. 5, 2021, §5.3.

Nesta medida, se é verdade que a inteligência artificial no sistema financeiro torna possível realizar análises de riscos e detetar crimes em tempo real (seja através de sistemas de *RegTech* ou do *criminal compliance* "inteligente"), facilmente este consubstancia o Santo Graal tanto das empresas como dos próprios reguladores[322] e, em termos amplos, do Direito Penal. Daí que CRISTOPH BRUCHARD questione se a inteligência artificial não ditará o fim do Direito Penal como o conhecemos[323].

É precisamente neste ponto que surge a indagação da possibilidade da utilização destes sistemas por parte do Ministério Público e órgãos de polícia criminal. Certamente esta é, para já, uma indagação hipotética, mas que tem que ser levada em consideração dadas as potencialidades que uma medida como esta poderia trazer para os sempre atuais problemas de celeridade processual, recursos humanos e custos de investigação por parte do titular da ação penal.

Hipoteticamente, pense-se num sistema "inteligente" ao dispor do Ministério Público e dos órgãos policiais que esteja interligado, por exemplo, por *cloud computing*, aos *criminal compliance* "inteligentes" das empresas e que automaticamente emita "alertas" (*red flags*) assim que eles ocorram. Estes "alertas" seriam ambivalentes, ou seja, dispor-se-iam tanto para a empresa como para o Ministério Público, podendo a empresa resolvê-lo (se for possível). Caso não o resolva, essa informação seria relevante para desencadear uma investigação (se houver fundamento para tal), mas não poderia ser usada como meio de prova, uma vez que as *red flags* são meramente indiciárias e não garantem a consumação ou tipificação de qualquer crime. Para além disto, mecanismos de cooperação judiciária internacional em matéria penal poderiam ser incluídos neste processo, por forma a aumentar a eficiência e veracidade das *red flags*, onde uma harmonização das procuradorias a nível europeu centralizasse dados relevantes, incluindo-se, por exemplo, em iniciativas como a da supracitada Autoridade Bancária Europeia. Do lado empresarial, apenas com o consentimento das respetivas empresas seria possível aderir a esta interligação com o Ministério Público[324]. Neste contexto, como forma de incentivo à adesão a esta rede

[322] AZIZ, Saqib / DOWLING, Michael, *Op. cit.*, p. 47.
[323] Interrogação esta feita diretamente no título, mas desenvolvida ao longo do artigo, BURCHARD, Cristoph, *Op. cit.*, p. 184 e ss.
[324] Em linha com o art. 13.º da Carta Portuguesa de Direitos Humanos na Era Digital, que estabelece o "direito ao esquecimento".

colaborativa, as empresas poderiam beneficiar, casuisticamente, de certas atenuações ou vantagens processuais no crime em questão[325].

Uma opção como estas, enquanto opção político-criminal, não estaria isenta de riscos, devendo estes ser estritamente ponderados em função dos perigos inerentes impostos pela inteligência artificial. Inevitavelmente teremos que associar esta ideia à Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais. Esta disposição veio identificar e alertar o Conselho e a Comissão para um conjunto de considerações que devem ser relevadas num futuro instrumento legislativo europeu, sendo apresentadas algumas preocupações quanto à utilização destas tecnologias pelas autoridades judiciárias e policiais, principalmente, pelas potenciais lesões irreversíveis aos direitos fundamentais previstos na Carta dos Direitos Fundamentais da União Europeia.

Com uma solução destas, tanto supervisores como o Ministério Público ficam com o acesso a uma infinitude de dados onde, certamente, se integrarão dados sensíveis das empresas e dos trabalhadores destas. Deste modo, seria sempre necessário respeitar os direitos de privacidade de todos os envolvidos, devendo, por exemplo, «regular fornecedores de *SupTech* ou *RegTech*» para que seja possível «assegurar a confidencialidade e segurança dos elementos que recolha/receba nas mais diversas áreas de risco em que possam estar enquadrados»[326]. Ademais, a vertente do erro algoritmo não pode nunca ser afastada (desde logo por que há algum tipo de intervenção humana), importando também para este propósito a qualidade dos dados em causa (*data quality*)[327].

Para obstar a este problema, deverá promover-se uma "normalização" dos conceitos por forma a tornar os dados unívocos em todos os sistemas[328], mas também deverá limitar-se a

[325] De certa forma, no caso do crime de branqueamento de capitais e financiamento do terrorismo este processo já acontece, mas de forma descentralizada. Isto é, no âmbito da Lei n. º 83/2017, de 18 de agosto, as entidades obrigadas têm que cumprir um conjunto de deveres, nomeadamente, o dever de comunicação e de colaboração, que lhes impõe a obrigação de reporte às entidades autoridades judiciárias e policiais quando saibam, suspeitem ou tenham razões para suspeitar que certos fundos provêm de atividades criminosas ou estão relacionados com financiamento do terrorismo (art. 43.º). Para além disto, o agente poderá beneficiar de uma atenuação especial da pena de auxiliar na recolha de provas decisivas para a identificação ou captura dos responsáveis pela prática de factos ilícitos de onde provieram as vantagens (art. 368.º-A/11 do Código Penal).
[326] RAMALHO, Inês Palma, *Op. cit.*, p. 47.
[327] *Id., Loc. cit.* E também, OCDE, *Op. cit.*, §5.4.1.
[328] *Id., Loc. cit.* Quanto a este problema da "Torre de Babel digital", *supra* nota 75.

função destas ferramentas ao auxílio da tomada de decisão do supervisor humano, pois só desse forma se consegue triar a qualidade dos dados e agir de forma eficaz[329].

Outra relevante preocupação com a introdução destes sistemas diz respeito, mais uma vez, à potencial lesão dos direitos processuais dos investigados. Neste contexto, este respeito deve ser efetivado através de uma admissibilidade destes sistemas de forma proporcional, isto é, que, nos termos do princípio da proporcionalidade em sentido amplo, a utilização dos dados obtidos com estes sistemas seja proporcional às finalidades da investigação, tornando possível a não discriminação, não adulteração, transparência, explicabilidade da decisão, permitindo uma igualdade de armas entre Ministério Público e arguido[330].

Por fim, para garantir tecnicamente uma certa fiabilidade da decisão e do sistema, devem as entidades supervisoras e o Ministério Público estreitar relações, promovendo esforços conjuntos entre si, mas também com outros setores da Administração e da sociedade, nomeadamente, cientistas de dados, programadores, investigadores[331].

Em suma, percebe-se que a evidência do futuro são os problemas de hoje. E assim deve ser, para que os estes não se prolonguem na decorrência do tempo. Esta discussão deverá ser ainda mais premente num setor como é o processo penal, onde o conflito é inevitável. Neste prisma, o processo penal é o campo de debate teleológico, mas onde ambas as partes devem ceder e compatibilizar-se. Daí que as finalidades do processo penal sejam conflituantes, mas harmonizáveis. Mais ainda quando se fale em inteligência artificial, que, por si só, pode destabilizar a balança em favor da realização da justiça. É aqui que deve entrar a regulação: para limitar os excessos e prevenir lesões irreversíveis.

Deste modo, como já aludido, não será aconselhável falar neste âmbito (e no setor judicial em termos amplos) de uma verdadeira inteligência artificial, mas antes de uma inteligência aumentada, isto é, uma extensão e auxílio à inteligência humana com soluções

---

[329] Neste sentido, segundo a Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais, P9_TA (2021)0405, §E («a tecnologia de IA deve ser desenvolvida de forma antropocêntrica, ser digna de confiança pública e estar sempre ao serviço dos seres humanos»).

[330] Sobre isto, OCDE, *Op. cit.*, §5.4.1., relembrando que na admissibilidade de buscas e apreensões de discos rígidos ou servidores para investigação torna-se possível que os dados adquiridos nesse processo contenham informações pessoais e irrelevantes para a investigação. E também, *idem*, §5.4.2. («Where evidence has been located using AI across large data sets, it could be imperative for defendants to have access to the same data sets and possibly the AI technology itself, particularly where they could not afford this themselves (equality of arms issue) »).

[331] Releva-se aqui a importante e louvável iniciativa do DCIAP do Ministério Público com a criação do grupo de reflexão Think Tank. Este grupo consiste num fórum de discussão multidisciplinar tendo em vista a procura de soluções de prevenção de fraudes na utilização de recursos financeiros da União Europeia.

(teoricamente) mais eficientes que contribuam para a resolução dos problemas de celeridade processual e custos de investigação, sem nunca ir além da proteção garantística assente no ordenamento jurídico em favor dos arguidos (mas também de terceiros). Partindo desta base, deve, em primeiro lugar, o legislador tornar possível adaptações do sistema processual penal às novas realidades para que, em segundo, o Ministério Público e os órgãos policiais possam acompanhar o desenvolvimento tecnológico dos agentes económicos, se possível, numa lógica de cooperação ou, não sendo, numa perspetiva antagónica, mas com semelhantes capacidades.

Conclusões

Chegados aqui, caberá fazer corresponder e concretizar as expectativas deixadas em aberto nas considerações iniciais que, esperamos nós, tenham sido mediatamente atendidas ao longo do percurso. Desde início, sabíamos que a tarefa de procurar responder a todas as questões tinha tanto de complexo como de ambicioso. Desde logo porque a temática em causa implica uma interdisciplinaridade não só dogmática, como problemática. Para além disto, esta interdisciplinaridade implica a realização de juízos preditivos do que será o futuro da inteligência artificial e da sua interconexão com o Direito Penal. Ora, como vimos, nós humanos não fomos "programados" para esse fim. Ainda para mais numa ciência *constituenda* como é a inteligência artificial. Não obstante, em função das suas úteis e apetecíveis funções, procurou-se abrir as hostilidades relativamente aos problemas gerados pela inclusão de algoritmos em sistemas de prevenção criminal empresariais.

Para tal, em primeiro lugar, procurou-se identificar qual a relevância jurídica da inteligência artificial e porque é importante o Direito (e o Direito Penal) estar na vanguarda das inovações (e desta especificamente). Em concreto, as tecnicidades descritas quanto à programação algorítmica viriam, mais tarde, a relevar para a discussão não só das utilidades, mas principalmente dos riscos que estes sistemas geram; e, especialmente, no apuramento de responsabilidade penal quando um crime seja praticado ou permitido por um sistema de inteligência artificial. Posteriormente, constatou-se que no âmbito empresarial são vários os setores que beneficiam com a introdução de algoritmos, nomeadamente, na gestão empresarial (nos recursos humanos e numa perspetiva económica de redução de custos e valorização económica), no setor financeiro (com soluções otimizadas de gestão e análise de risco em tempo real e de forma precisa, dando respostas às exigentes obrigações regulatórias e elevados custos de implementação) e no setor do mercado dos valores mobiliários (com a utilização de instrumentos de investimento que, utilizados de forma responsável, aumentam a eficiência dos mercados). Não obstante, a ponderação terá que ser feita com os riscos correspondentes, concretamente, com a possibilidade inerente aos algoritmos de falibilidade (pelo que é de extrema importância a qualidade dos dados inseridos) ou de enviesamento e discriminação (que podem gerar decisões injustas), com potenciais lesões à privacidade digital de vários intervenientes, ou ainda, de forma mais notória e transversal a toda discussão, a opacidade e inexplicabilidade algorítmica, carreadas pelo *black box problem*. Estes são dois *handicaps* no que concerne à plena adoção destes

sistemas, uma vez que dificultam, concretamente no âmbito da responsabilidade penal, os juízos de previsibilidade nos quais toda a doutrina do facto punível se sustenta.

Para além da relevância jurídica da inteligência artificial, foi necessário proceder ao ponto de situação no que concerne à já não tão inovadora dogmática do *compliance*. Desde logo, partiu-se para uma conceitualização deste em função do caos terminológico que hoje existe. Em função disto, distinguiu-se o *compliance* (enquanto termo aglutinador de todas as outras subconceitualizações), de programas de *compliance*, de *compliance* regulatório e de *criminal compliance*. Quanto a este último, até pela incidência da temática, foi dada especial autonomia formal e conceitual, pois, de facto, esta representa uma concretização da prevenção criminal, ou seja, representa a ideia «do último convidado», neste caso, em sede de delimitação do risco permitido e prevenção do incumprimento no âmbito empresarial. Aqui, analisou-se a função primordial e respetivas subfunções do *criminal compliance* de prevenção, deteção e repressão, sendo a partir da aferição da eficácia destas que se torna possível extrair os efeitos concretos deste mecanismo. Em termos amplos, distinguiram-se dois tipos de efeitos de um *criminal compliance* eficaz, os efeitos processuais e económicos, percebendo-se a sua relevância processual na aferição de responsabilidade (com a potencial atenuação ou isenção de responsabilidade, mormente, no plano da sanção ou como instrumento de negociação processual), mas também em sede de maximização do lucro (com vantagens competitivas ou diminuição de custos). Ainda assim, constatou-se que os atuais modelos de imputação do facto criminal às pessoas coletivas relevam diferentemente um *criminal compliance* eficaz. Ademais, examinou-se esta mesma realidade no ordenamento jurídico português, uma vez que recentemente, com a entrada em vigor do Regime Geral de Prevenção da Corrupção e das consequentes alterações ao Código Penal e de Processo Penal, o nosso legislador penal optou por, meritória e finalmente, atribuir relevância substantiva e adjetiva a estes mecanismos de autocontrolo, tornando-os obrigatórios em determinadas situações. Por fim, em jeito conclusivo, levantaram-se algumas questões quanto à concreta eficácia de um *compliance* cada vez mais "agressivo", aplicado numa estrita ligação com o Direito Penal e se isso não poderia ter o efeito reverso, potencializando mais a criminalidade empresarial com racionalizações internas, segundo um prisma de uma "vontade coletiva" e de influência de grupo. Mais a mais, relevou-se que a visão de um *criminal compliance* deve ir além de ponderações estritamente económicas e de racionalizações de responsabilidade, primando pelo seu concreto objetivo de prevenção do incumprimento através da promoção

de um cumprimento ético-legal. Nestes termos, é de facto um instrumento útil tanto para a própria pessoa coletiva (numa ideia de não ver contra si um processo penal), mas também, logicamente, para o Estado. O tempo dirá se será esta a melhor abordagem.

Quanto ao segundo capítulo, a autonomização deste ponto justifica-se na necessidade que encontrámos de estabelecer a ponte entre o *criminal compliance* e a inteligência artificial, uma vez que, por mais que não aparente, são duas realidades que se irão encontrar e interligar (julgamos nós). Encontrámos semelhanças com o já existente conceito de *RegTech*, todavia, distinguem-se na mesma medida em que o *criminal compliance* se distingue do *compliance* regulatório, ou seja, pela densidade axiológica das condutas que visam prevenir ou regular. Por conseguinte, sustentou-se aqui pela primeira vez (de algumas) a importância de salvaguarda do controlo humano em setores de risco, como é o setor de prevenção criminal, quando em causa estejam sistemas de inteligência artificial. Isto graças às caraterísticas e ao risco inerente aos algoritmos. Deste modo, antecipa-se que a função de *Chief Compliance Officer* do futuro não será extinta, mas aprimorada com a utilização destes sistemas, nomeadamente, com o melhoramento das qualificações daqueles que exercem esta função, em especial, com conhecimentos necessários para o controlo do sistema (e.g. informática ou ciência de dados). Ulteriormente, a concreta interligação da inteligência artificial com o *criminal compliance* faz valorizar economicamente a empresa, deixando este de ser visto como um custo para ser um investimento. A isto se acrescenta que, aliando as capacidades da inteligência artificial a estes mecanismos, idealiza-se uma maior eficiência nos processos, melhorando a prevenção, deteção e repressão de atos juridicamente desvaliosos no domínio empresarial. Contudo, estes efeitos são consequenciais do nível de desenvolvimento dos sistemas, pelo que se procedeu à concreta ligação dos conceitos técnicos acima explanados à realidade específica da prevenção criminal nos seus diversos elementos.

Em última instância, terminou-se, novamente, com o levamento de relutâncias quanto à manutenção e fomento da ética corporativa, enquanto conceito essencial ao *criminal compliance*. Isto porque a mecanização dos processos apenas os torna mais eficientes, não conseguindo introduzir o cunho ético-legal nas suas funções. Daí que se preveja que um sistema de IA poderá não responder da forma mais ética quando se depare com situações de conflito, julgando-se competente para prosseguir única e exclusivamente

o objetivo para o qual foi programado. É por esta razão que se reforça a ideia de controlo humano dos processos com o auxílio da máquina.

Por último, o terceiro capítulo representa a súmula das preocupações geradas com a introdução destes sistemas no âmbito empresarial: a possibilidade dos sistemas falharem e gerarem resultados imprevisíveis que facilitem ou pratiquem crimes (os chamados «*Hard AI Crimes*»). Perante esta situação coube esclarecer potenciais respostas *de jure condendo*, tanto substantiva como adjetivamente, para auxiliar o legislador penal na regulação futura. Na perspetiva da factualidade típica, o problema foi abordado na vertente omissiva (nas situações de falha do *criminal compliance* "inteligente") e nos delitos de ação (procurando responder ao *AI accountability gap*). Como tal, formulou-se um caso hipotético que abarcasse estas duas possibilidades e se pudesse discorrer a partir deste como exemplo. Quanto à primeira situação, coube analisar como seria valorada a falha do sistema na responsabilidade de uma empresa que praticou um crime, alegando a confiança nesse sistema de prevenção que falha. A questão maior que estava aqui em causa era saber se os deveres de garante inerentes à função do responsável pelo cumprimento poderiam ser transferidos para um sistema de inteligência artificial programado para a prevenção criminal. Chegou-se aqui à primeira divergência doutrinal, considerando os adeptos da teoria que chamámos disruptiva (por irromper com os bases dogmáticas do Direito Penal), que o algoritmo tem capacidade para agir e para agir com culpa, podendo ser responsabilizado diretamente pela sua falha. Ora, percebeu-se através de diversos argumentos que uma visão como estas é ficcional e inoperante, devendo-se antes olhar para agentes penalmente cognoscíveis, nomeadamente, as pessoas coletivas. Como tal, sendo estas os principais programadores e utilizadores de algoritmos, devem sobre estas impender certos deveres, em concreto, o dever de precaução (na programação e na utilização do algoritmo). Deste modo, não podem as empresas alegar a transferência de deveres a algoritmos (pois estes são produtos), sendo estas ainda titulares dos deveres originários, respondendo pela falta com eles. Assim, é através da prova do cumprimento dos respetivos deveres de precaução que se poderá pensar numa relevante influência na falha do sistema para a empresa delinquente. Esta, porque responderá sempre pelo crime, poderá ter uma atenuação nas situações em que fique provado que a sua utilização foi responsável e que a falha não dependeu da utilização que deu ao algoritmo, mostrando que atuou daquela forma, pois tivera confiado na não falibilidade do sistema. Para mais, caso fique provado que o dever de precaução na

programação não foi cumprido, poderá também ser chamado a responder o produtor. No reverso do problema, como excurso, procurou-se auxiliar na resposta para o *accountability gap* nos delitos de ação. Isto é, nas situações em que algoritmos de forma inexplicável e indesejável praticam crimes. De igual forma, surge um debate doutrinal análogo ao acima deposto: aqueles que defendem uma responsabilização direta do algoritmo (novamente, a teoria disruptiva) e aqueles que consideram este um problema de legalidade que o nosso ordenamento jurídico tem a capacidade para preencher sem deturpar bruscamente o *status quo* (a teoria clássica). Replicam-se os argumentos acerca da impossibilidade de responsabilização direta dos algoritmos, mas agora de forma especifica na inaplicabilidade das penas, por falta de eficácia, incapacidade moral de algoritmos as entenderem e desvirtuação da axiologia penal. Por outro lado, soluções mais moderadas se enaltecem como a tese do controlo-benefício ou a responsabilidade penal pelo produto "inteligente", que visam encontrar soluções através de respostas já existentes, mas revisitadas, pois, os tradicionais modelos de imputação do facto tornam-se obsoletos com esta nova realidade. Em jeito de compatibilização, parece-nos a solução mais equilibrada a opção pela responsabilização pelo produto "inteligente", incluindo-se aqui o utilizador que tenha tido influência no processo de atuação do algoritmo, dado que estes possuem, na maioria dos casos, capacidade de aprendizagem através da experiência.

Como último ponto de discussão, tocou-se na relevância póstuma do *criminal compliance* "inteligente" no processo penal, por um lado, enquanto meio de obtenção de prova, indagando-se essa admissibilidade tendo em conta os riscos acrescidos que a inteligência artificial poderá gerar; e por outro, numa visão futurista, no aproveitamento de mecanismos de colaboração e investigação por parte do Ministério Público e órgãos de polícia criminal, assemelhando-se ao que já acontece no âmbito das entidades supervisoras no sistema regulatório (*SupTech*). Concluiu-se que uma visão positiva acerca destas inovações apenas poderá ser de admitir caso as garantias processuais e demais direitos fundamentais não sejam lesados bruscamente, numa lógica de proporcionalidade à qual terá o legislador que atender.

Numa palavra final, factualmente, o Direito (especialmente o Direito Penal) foi feito por e para o Homem se regular e regular as suas relações subjetivas na e com a comunidade. Deste modo, a esfera de controlo da ordem jurídica não poderá nunca ir além do controlo por parte deste. Caso isso aconteça, a ordem jurídica deixa de ser o local de realização do

Homem na sua dignidade, passando a uma anarquia de agentes jurídicos que se fazem substituir a este ao ponto de se tornar dispensável. Não quer isto dizer que deve o legislador limitar o desenvolvimento tecnológico da inteligência artificial. Quer dizer, por outro lado, para fazê-lo de forma consciente e responsável, por forma a ser sempre possível estar o Homem no controlo da máquina e deixar em aberto a possibilidade de carregar no botão "*off*" sempre que for necessário. Neste contexto, ao longo de todo o nosso discurso, sempre que se falou em inteligência artificial, pensou-se numa existência harmoniosa de uma inteligência artificial controlada e controlável, sendo possível explicar as decisões que toma, torná-las transparentes e, ao mesmo tempo, poder usufruir de todas as utilidades e benefícios socioeconómicos para a comunidade.

Deixaremos esta tarefa de controlo e do contrabalanço entre o necessário desenvolvimento tecnológico e a regulação desse desenvolvimento ao legislador, mantendo-nos por cá para criticar ou auxiliar na descoberta de novas soluções para estes novos problemas.

Bibliografia

ABBOT, Ryan / SARCH, Alex, «Punishing Artificial Intelligence: Legal Fiction or Science Fiction», *University of California Davis Law Review*, Vol. 53, 2019, p. 323 – 384.

ANAND, Vikas *et al.*, «Business as usual: the acceptance and perpetuation of corruption in organizations», *The Academy of Management Executive*, Vol. 19, n. º 4, 2005, p. 9-23.

ANDRADE, Manuel da Costa, «*Nemo tenetur se ipsum accusare* e direito tributário. Ou a insustentável indolência de um acórdão (n.º 340/2013) de Tribunal Constitucional», *Boletim de Ciências Económicas*, LVII/I, 2014, p. 385 - 451.

ANTUNES, Maria João, *Direito Processual Penal*, 2.ª Ed., Coimbra: Almedina, 2019.

_____, «Privatização das investigações e *compliance* criminal», *Revista Portuguesa de Ciência Criminal*, ano 28, 2018, p. 119 – 127.

ARNER, Douglas W. / BARBERIS, Jànos / BUCKLEY, Ross, «The Evolution of FinTech: a New Post-Crises Paradigm?», *University of Hong Kong Faculty of Law*, Research paper n. º 2015/047, UNSW Law Research paper n. º 2016-62, 2015, p. 1 – 43.

ASARO, Peter. M. «A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics», *in* Robot Ethics: The Ethical and Social Implications of Robotics, Chapter 11, 2012, p. 169–186.

AZIZ, Saqib / DOWLING, Michael, «Machine Learning and AI for Risk Management», *in* LYNN, Theo *et al. (eds.), Disrupting Finance: FinTech and Strategy in the 21st Century*, Palgrave Studies, Cap. 3, 2018, p. 33 – 50.

BALES, Richard A. / STONE, Katherine V. W., «The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance, Under the Labour Laws», *Berkeley Journal of Employment and Labour Law*, Vol. 41, n. º 1, UCLA School of Law, Public Law Research Paper, n. º 19 - 18, 2020, p. 1 – 62.

BARBOSA, Mafalda Miranda, «Dos Expert Systems aos Data Systems AI: impacto ao nível da proteção de dados», *Revista JULGAR*, n. º 45, Almedina, 2021, p. 13 – 33.

_____, «Inteligência artificial, *e-persons* e direito: desafios e perspetivas», *Revista Jurídica Luso-Brasileira,* Ano n. º 3, n. º 6, 2017, p. 1475 – 1503.

BARTNECK, Christoph / LÜTGE, Christoph / WAGNER, Alan / WELSH, Sean, *An Introduction to Ethics in Robotics and AI,* Springer Nature, 2021.

BATHAE, Yavar, «The artificial intelligence black box and failure of intent and causation», *Harvard Journal of Law & Technology*, Vol. 31, 2018, p. 889 – 938.

BRAITHWAITE, John, «Enforced Self-Regulation: A New Strategy for Corporate Crime Control», *Michigan Law Review*, Michigan: Vol. 80, issue 7, 1982. p. 1466 – 1507.

BRAVO, Jorge Reis, *Direito Penal dos Entes Coletivos: Ensaio sobre a Punibilidade de Pessoas Colectivas e Entidades Equiparadas*, Coimbra: Coimbra Editora, 2008.

BRITO, Teresa Quintela de, «*Compliance, cultura corporativa e culpa penal da pessoa jurídica», in Estudos sobre Law Enforcement, Compliance e Direito Penal.*, coord. PALMA, Maria Fernanda *et al.*, 2.ª Ed., Almedina, 2018, p. 57 – 100.

_____, «Relevância dos mecanismos de compliance na responsabilização penal», *Anatomia do Crime – Revista de Ciências Jurídico-Criminais*, N. º 0, jul.-dez. 2014, p. 75 – 91.

BROEDERS, Dirk / PRENIO, Jermy, «Innovative technology in financial supervision (suptech): the experience of early users», Bank for International Settlements, Financial Stability Institute, Insights on Policy Implementation No. 9, 2018, p. 1 – 26.

BURCHARD, Cristoph, «Artificial Intelligence as the End of Criminal Law? On the Algorithmic Transformation of Society», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 165 – 205.

BUSATO, Paulo César, «O que não se diz sobre o *criminal compliance*», *in Estudos sobre Law Enforcement, Compliance e Direito Penal,* coord. M. Fernanda Palma *et al.*, 2.ª Ed., Coimbra: Almedina, 2018, p. 21 – 55.

BUTLER, Tom / O'BRIAN, Leona, «Artificial Intelligence for regulatory compliance: Are we there yet?», *Journal of Financial Compliance*, Vol. 3, N. º 1, Henry Stewart Publications, 2019, p. 44 – 59.

_____ / _____, «Understanding RegTech for Digital Regulatory Compliance», *in* LYNN, Theo, et. al (eds.), *Disrupting Finance: FinTech and Strategy in the 21st Century*, Palgrave Studies, Cap. 6, 2018, p. 85 – 102.

CAPPELLINI, Alberto, «*Machina delinquere non potest*? Bervi appunti su inteligenza artificiale e responsabilità penale», Criminalia, 2018, p. 499 – 520.

COFFEE, JR., John C., *Corporate Crime And Punishment: The Crisis of Underenforcement*, Berret-Koelher Publishers, Inc., p. 44 – 49.

COSTA, Ernesto / SIMÕES, Anabela, *Inteligência Artificial: fundamentos e aplicações*, 3.ª Ed., FCA Editora, 2008.

CUNHA, Paulo Ferreira da, *Crimes & Penas: Filosofia Penal*, Almedina, 2020.

DAVENPORT, Thomas H. / RONANKI, Ranjeev, «Inteligência artificial para o mundo real», *Harvard Business Review, in* DAVENPORT, Thomas H. *et al.*, *Inteligência Artificial Análise de Dados e a Nova Era das Máquinas*, trad. Alexandra Cardoso, Actual Editora, 2021, p. 9 – 29.

DIAMANTIS, Mihailis E., «Algorithms Acting Badly: A Solution from Corporate Law», *The George Washington Law Review*, Vol. 89, N. º 4, 2021, p. 802 – 855.

_____, «Algorithmic Harm as Corporate Misconduct», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 135 – 164.

_____, «The Extended Corporate Mind: When Corporations use AI to Break the Law», *North Carolina Law Review*, Vol. 98, N. º 4/6, 2020, p. 894 – 930.

_____, «Vicarious Liability for AI», *in* JOHNSON, Kristin Johnson / REYES, Carla (eds.), *Cambridge Handbook of AI and Law*, 2022, University of Iowa Legal Studies Research Paper No. 2021-27, p. 1 – 18.

DIAS, Jorge de Figueiredo, *Direito Penal, Parte Geral*, Tomo I, colab. M. J. Antunes *et al.*, 3.ª Ed., Coimbra: GESTLEGAL, 2019.

DU, Zhihui / HE, Ligang / CHEN, Yinong / XIAO, Yu / GAO, Peng / WANG, Tongzhou, «Robot cloud: bridging the power of robotics and cloud computing», *Future Generation Computer Systems*, n. º 74, 2017, p. 337 – 348.

EMMANUEL, Isitor / STANIER, Clare, «Defining Big Data», *in Proceedings of the International Conference on Big Dta and Advance Wireless Technologies (BDAW)*, Association for Computing Machinery, New York, Article 5, 2016, p. 1 – 6.

ENDENMÜLLER, Horst, «*Robot's Legal Personality*», University of Oxford, Faculty of Law, 8 mar. 2017, disponível em: https://www.law.ox.ac.uk/business-law-blog/blog/2017/03/robots%E2%80%99-legal-personality

ENGELHART, Marc, *The Nature and Basic Problems of Compliance Regimes*, Max-Planck-Institut für ausländisches und internationales Strafrecht, Forschungsgruppe "Architektur des Sicherheitsrechts"(ArchiS), 2018.

ENRIQUES, Luca, «Financial supervisors and Regtech: Four roles and four challenges», *Revue Trimestrielle de Droit Financier* n. º 53, 2017, p. 1 – 9.

ESAYAS, Samson / MAHLER, Tobias, «Modeling compliance risk: a structured approach», *Artificial Intelligence and Law*, n. º 23, 2015, p. 271 – 300.

FIDALGO, Sónia, «A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo», *in A Inteligência Artificial no Direito Penal*, coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 129 – 161.

FRIEDMAN, Milton, «The social responsibility of business is to increase its profits» *in* ZIMMERLI, Walter Ch. / RICHTER, Klaus / HOLZINGER, Markus (eds.), *Corporate Ethics and Corporate Governance*, Springer, Berlim, Heidelerg, 2007, p. 173 – 178.

GIUFRIDDA, Iria, «Liability for AI Decision-Making: Some Legal and Ethical Considerations», *Fordham Law Review*, Vol. 88, 2019, p. 439 – 456.

GLESS, Sabine, «AI in the courtroom: a comparative analysis of machine evidence in criminal trials», *Georgetown Journal of International Law*, Vol. 51, n. º 2, 2020, p. 195 – 253.

_____ / SILVERMAN, Emily / WEIGEND, Thomas, «If robots cause harm, who is to blame? Self-driving cars and criminal liability», *New Criminal Law Review*, Vol. 19, N. º 3, 2016, p. 412 – 436.

GRACE, Katja, *et al.*, «When will AI exceed human performance? Evidence from AI experts», *Journal of Artificial Intelligence Research*, n. º 62, 2018, p. 729-754.

HALLEVY, Gabriel, *Liability for Crimes Involving Artificial Intelligence Systems*, 1st Ed., Springer, 2015.

_____, «Virtual Criminal Responsibility», *Original Law Review*, Vol. 6, n. º 1, 2010, p. 6 – 27.

HAUGH, Todd, «The Criminalization of Compliance», *Notre Dame Law Review*, Vol. 92, issue 3/5, 2018, p.1215 – 1268.

HILDEBRANDT, Mireille, «Algorithmic regulation and the rule of law», *Philosophical Transactions of the Royal Society A*, Vol. 376, Issue 2128, p. 1 – 11.

JOHNSON, Deborah G., «Computer systems: moral entities but not moral agents», *Ethics and Information Technology*, n. º 8, 2006, p. 195 – 204.

JUNG, John Ho Hee, «RegTech and SupTech: the future of compliance», *in* MADIR, Jelena (ed.), *FinTech*: Law and Regulation, 2nd Ed., UK: Edward Elgar Publishing, Chapter 12, p. 291 – 316.

LAMBSDORFF, Johann Graf, «Preventing corruption by promoting trust: insights from behavioral science», *Passauer Diskussionspapiere-Volkswirtschaftliche Reihe*, Vol. 69, n. º 15, 2015, p. 1 – 16.

LASCURAÍN, Juan Antonio, «Los programas de cumplimiento como programas de prudencia penal», *Revista Portuguesa de Ciência Criminal*, ano 25, n.º 1 a 4, IDPEE, Coimbra, jan.-dez., 2015, p. 95 – 115.

LAUFER, William S., «Corporate Liability, Risk Shifting and the Paradox of Compliance», *Vanderbilt Law Review*, Vol. 52, Issue 5, Art. 9, 1999, p. 1343 – 1420.

_____, «Corporate prosecution, cooperation, and the trading of favors», *Iowa Law Review*, Vol. 87, 2001, p. 643 – 667.

LIMA, Dafni, «Could AI agents be held criminally liable? Artificial intelligence and the challenges for criminal law», *South Carolina Law Review*, Vol. 69, 2018, p. 677 – 694.

LIN, Tom C.W., «Compliance, Technology, and Modern Finance», *Brooklyn Journal of Corporate Financial & Commercial Law*, Vol. 11, Issue 1, Art. 6, 2016, p. 159 – 182.

LUCA, Michael / KLEINBERG, Jon / MULLAINATHAN, Sendhil, «Os algoritmos também precisam de gestores» *Harvard Business Review*, *in* DAVENPORT, Thomas H. *et al.*, *Inteligência Artificial Análise de Dados e a Nova Era das Máquinas*, trad. Alexandra Cardoso, Actual Editora, 2021, p. 43 – 53.

MAIA, Pedro «*Compliance* Bancário na Era da Inteligência Artificial – uma breve introdução», *Revista JULGAR*, n. º 45, Almedina, 2021, p. 159 – 191.

_____, «Intelligent Compliance», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 3 – 50.

MARQUES, Mário Reis, Introdução ao Direito, Vol. I, 2.ª Ed., Coimbra: Almedina, 2012.

MARTÍN, Adan Nieto, «Problemas fundamentales del cumplimiento normativo en el derecho penal», *in Temas de Derecho Penal Económico: Empresa y Compliance - Anuario de Derecho Penal 2013-2014*, p. 172 – 200.

MARTINS, Alexandre Soveral, «Algo-trading», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 51 – 84.

MASCHMANN, Frank «Compliance y derechos del trabajador", *in* KUHLEN, Lothar *et al.*, *Compliance y Teoria del Derecho Penal*, Marcial Pons, 2013, p. 147 – 168.

MATTEN, Dirk / MOON, Jeremy, «Pan-European Approach. A Conceptual Framework for Understanding CSR» *in* ZIMMERLI, Walter Ch. / RICHTER, Klaus / HOLZINGER, Markus (eds.), *Corporate Ethics and Corporate Governance*, Springer, Berlim, Heidelerg, 2007, p. 179 – 199.

McCARTHY, John, *What is AI? / Basic Questions*, University of Standford, 2007, p. 1 -15.

MEIJER, Albert / WESSELS, Martijn, «Predictive policing: review of benefits and drawbacks», *International Journal of Public Administration*, Vol. 42, Issue 12, 2019, p. 1031 – 1039.

MENDES, Paulo de Sousa, «A problemática da punição do autobranqueamento e as finalidades de prevenção e repressão do branqueamento de capitais no contexto da harmonização europeia», *Católica Law Review*, Vol. 1, n. º 3, 2017, p. 127 – 156.

_____, «*Law Enforcement & Compliance*», *in Estudos sobre Law Enforcement, Compliance e Direito Penal*, coord. PALMA, Maria Fernanda *et al.*, 2.ª Ed., Almedina, 2020, p. 13 – 24.

MUELLER, Tim / SISWICK, James, «How Can Artificial Intelligence Augment the Investigative Process?», *in Corporate Investigations* 2020, International Comparative Legal Guides, 4th ed., Chap. 3, 2020, p. 15 – 20.

OSMANI, Nora, «The Complexity of Criminal Liability of AI Systems», *Masaryk University Journal of Law and Technology*, Vol. 14, N. º 1, 2020, p. 53 – 82.

PACKIN, Nizan Geslevich, «RegTech, Compliance and Technology Judgment Rule», *Chicago-Kent Law Review*, Vol. 93, Issue 1: *FinTech's Promises and Perils*, Art. 7, 2018, p. 193 – 218.

PAGALLO, Ugo / QUATTROCOLO, Serena, «The impact of AI on criminal law, and its twofold procedures» *in Research Handbook on the Law of Artificial Intelligence*, Cheltenham, UK: Edward Elgar Publishing, Chapter 14, 2018, p. 385 – 409.

PAIS, Ana, «Os programas de *compliance* e o risco da privatização do processo penal, em especial, a problemática da "prova emprestada" e o princípio *nemo tenetur se ipsum accusare*», *Estudos em Homenagem ao Prof. Doutor Manuel da Costa Andrade* (coord. José de Faria Costa *et al.*), Stvdia ivridica Vol. II, Coimbra: Universidade de Coimbra, 2017, p. 663 – 686.

PINTO, Carlos Alberto da Mota, *Teoria Geral do Direito Civil*, 4.ª Ed., António Pinto Monteiro e Paulo Mota Pinto (eds.), Coimbra: Coimbra Editora, 2012.

RAMALHO, Inês Palma, «SupTech e Regtech: o futuro da supervisão portuguesa?», *InforBanca – Revista do Instituto de Formação Bancária*, n. º 116, jun. 2019, p. 44 – 48.

RAMOS, José Ricardo Marcondes, «The use of Big Data and Artificial Intelligence to prevent and detect fraud», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 85 – 115.

RAUB. McKenzie, «Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices», *Arkansas Law Review*, Vol. 71, n. º 2, art. 7, dec. 2018, p. 529 – 570.

RUSSELL, Stuart / NORVIG, Peter, *Artificial Intelligence: a modern approach*, 3rd Edition, Pearson, 2016.

RODRIGUES, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização» *in A Inteligência Artificial no Direito Penal,* coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 11 – 58.

_____ / SOUSA, Susana Aires de, «Algoritmos em Contexto Empresarial: Vantagens e Desafios à Luz do Direito Penal», *Revista JULGAR*, n. º 45, Almedina, 2021, p. 193 – 214.

_____, *Direito Penal Económico*: *Uma Política Criminal na Era Compliance*, 2.ª Ed., Coimbra: Almedina, 2020.

_____, «A justiça preditiva entre a americanização e a europeização», *in A Inteligência Artificial no Direito Penal,* coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 11 – 58.

_____, «Os crimes de abuso de mercado e a "Escada Impossível" de Escher (o Caso do Spoofing)», *Revista JULGAR*, n. º 45, Almedina, 2021, p. 65 – 86.

_____, «The Last Cocktail – Economic and Financial Crime, Corporate Criminial Responsibility, Compliance and Artificial Intelligence» in.: ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the Economic Sector: Prevention and Responsibility*, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. 120 – 133.

RODRIGUES, André Alfar, *Manual Teórico-Prático de Compliance*, Coimbra: Almedina, 2022.

ROTSCH, Thomas, «Criminal Compliance», InDret, n.º 1, 2012, p. 1 – 11.

SALIGER, Frank, «Grundfragen von Criminal Compliance», *Rechtswissenschaft, Zeitschrift für rechtswissenschaftliche Forschung*, Heft n. º 3, 2013, p. 263-291.

SCHEMMEL, Alexander / DIETZEN, Alexandra, «"Effective Corporate Governance" by Legal Tech & Digital Compliance, *in* BREIDENBACH, Stephan / GLATZ, Florian, *Rechtshandbuch Legal Tech*, C.H. Beck, München, 2017, p. 137 – 153.

SIAU, Keng / WANG, Weiyu, «Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI», *Journal of Database Management*, Vol. 31, issue 2, Missouri University of Science and Technology, 2020, p. 74 – 87.

SILVA, Germano Marques da, *Responsabilidade penal das sociedades e dos seus administradores e representantes*, Lisboa: Editorial Verbo, 2009.

SIMMLER, Monika / MARKWALDER, Nora Mark, «Guilty Robots? – rethinking the nature of culpability and legal personhood in an age of artificial intelligence», *Criminal Law Forum*, n. º 30, 2019, p. 1 – 31.

SLYE, Ronald C., «Corporations, Veils, and International Criminal Liability», *Brooklyn Journal of International Law*, Vol. 33, 2008, p. 955 – 973.

SOLUM, Lawrence B., «Legal Personhood for Artificial Intelligences», *North Carolina Law Review*, Vol. 70, N. º 4, art. 4, 1992, p. 1231 – 1287.

SOLOMON, Robert C., «Introduction to Ethics» *in* ZIMMERLI, Walter Ch. / RICHTER, Klaus / HOLZINGER, Markus (eds.), *Corporate Ethics and Corporate Governance*, Springer, Berlim, Heidelberg, 2007, p. 11 – 36.

SOUSA, Susana Aires de, «A colaboração processual dos entes coletivos: legalidade de oportunidade ou "troca de favores?», *Revista do Ministério Público*, n. º 158, abril – junho 2019, p. 9 – 36.

_____, «As diferentes faces dos programas de compliance», *in Legitimidade e efetividade dos programas de compliance* (org. Adan Nieto Martin / Eduardo Saad Diniz), Tirant lo blanch, 2021, p. 29 – 38.

_____, *A responsabilidade criminal pelo produto e topos causal em direito penal: contributo para uma proteção penal de interesses do consumidor*, 1.ª Ed., Coimbra: Coimbra Editora, 2014.

_____, «Introduction – AI in the economic sector: prevention and responsibility», *in* ANTUNES, Maria João / SOUSA, Susana Aires de (eds.), *Artificial Intelligence in the*

Economic Sector: Prevention and Responsibility, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, dezembro de 2021, p. ix - xvi.

_____, «Não fui eu, foi a máquina», *in A Inteligência Artificial no Direito Penal*, coord. Anabela Miranda Rodrigues, Coimbra: Almedina, 2020, p. 59 – 93

_____, «Um Direito Penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial» *Revista da Defensoria Pública da União*, n. º 14, 2020, p. 21 – 37.

_____, *Questões Fundamentais de Direito Penal da Empresa*, Coimbra: Almedina, 2019

STONE, Peter *et. al., Artificial Intelligence and Life in 2030 - One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford, Stanford University Press, 2016, p. 1 – 52.

TIEDEMANN, Klaus, *Wirtschafstrafrecht*, 5. Auflage, Freiburg: Verlag Franz Vahlen, 2017.

TURING, Alan M., «Computing Machinery and Intelligence», *Mind*, Vol. LIX, n. º 236, 1950, p. 433-450.

VARELA, João de Matos Antunes, *Das Obrigações em Geral*, Vol. I, 10.ª Ed., Coimbra: Almedina, 2017.

VECCHIO, Fabrizio Bon / VIEIRA, Débora Manke, «Compliance Programs and Artificial Intelligence», *Studia Prawnicze: rozprawy i materiały*, Issue 1 (28), 2021, p. 61 – 69.

WARREN, Danielle E. / GASPAR, Joseph P., / LAUFER, William S., «Is Formal Ethics Training Merely Cosmetic? A Study of Ethics Training and Ethical Organizational Culture», *Business Ethics Quarterly*, Vol. 24, n. º 1, 2014, p. 85 - 117.

WILSON, H. James / DAUGHERTY, Paul R., «Inteligência colaborativa: seres humanos e IA estão a unir forças», *Harvard Business Review, in* DAVENPORT, Thomas H. *et al.*,

Inteligência Artificial Análise de Dados e a Nova Era das Máquinas, trad. Alexandra Cardoso, Actual Editora, 2021, p. 161 – 180.

ZEDNIK, Carlos, «Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence», *Phiolosophy & Technology*, Vol. 34, 2021, p. 265 – 288.

ZHENG, Nan-ning, *et al.*, «Hybrid-augmented intelligence: collaboration and cognition», *Frontiers Information Technology & Electronic Engineering*, n. º 18**,** 2017, p. 153–179.

Documentos, legislação e outras fontes:

ADAMS, Zachary / CHALK, Richard, «The Rise of AI in Corporate Investigations», Law360, New York, Set. 2017, disponível em: https://www.law360.com/articles/956749?utm_source=LexisNexis&utm_medium=LegalNewsRoom&um_campaign=articles_search

ANTUNES, Maria João, *Canais de Denúncia e Investigações Internas,* V Curso de Especialização de Compliance e Direito Penal, 14 de novembro de 2020, organizado pelo Instituto de Direito Penal Económico e Europeu (IDPEE) da Faculdade de Direito da Universidade de Coimbra.

BGH 5StR 394/08, 17/07/2009, disponível em: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=48874&pos=0&anz=1

BOSTROM, Nick, «What happens when our computers get smarter that we are?», TED Talks, 27. abr. 2015, acessível em: https://www.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_smarter_than_we_are

Comissão Europeia, *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19.2.2020, COM (2020) 65 final, 2020. Disponível em: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf

DASTIN, Jeffrey, «Amazon scraps secret AI recruiting tool that showed bias against women», *Reuters*, 11 Out. 2018, acessível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

Deloitte, «Compliance modernization is no longer optional: How evolved is your approach?», disponível em: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-compliance-modernization.pdf

DURO, Pedro, «O Compliance nas áreas aparentemente não reguladas – a propósito do art. 11.º do Código Penal», Youtube - Conselho Regional de Lisboa OA, 3 de julho de 2020, disponível em: https://www.youtube.com/watch?v=Pz590xhEe54&t=332s

EBA, *EBA launches today 'EuReCA', the EU's central database for anti-money laundering and counter-terrorism financing*, 31 jan. 2022, disponível em: https://www.eba.europa.eu/eba-launches-today-eureca-eus-central-database-anti-money-laundering-and-counter-terrorism-financing

Estratégia Nacional Anticorrupção 2020-2024, acessível em: https://justica.gov.pt/Portals/0/Ficheiros/Organismos/JUSTICA/ENAC010421.pdf

Estratégia Nacional de Inteligência Artificial (AI Portugal 2030), acessível em: https://www.incode2030.gov.pt/ai-portugal--2030

FRIDMAN, Lex, «MIT 6.S091: Introduction to Deep Reinforcement Learning (Deep RL)», 2019, YouTube, disponível em: https://www.youtube.com/watch?v=zR11FLZ-O9M&t=101s

Grupo de reflexão ThinkTank: https://thinktank-fundosue.ministeriopublico.pt/

IMF Staff Discussion Note, «Corruption: Costs and Mitigating Strategies», mai. 2016, disponível em: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf

KAKU, Michio, «3 mind-blowing prediction about the future», *BigThink*, acessível em: https://bigthink.com/the-future/prediction-michio-kaku/

KPMG, «Intelligent automation in financial crimes: forging an innovative compliance strategy for the future», disponível em: https://advisory.kpmg.us/articles/2017/intelligent-automation-in-financial-crimes.html

McKinsey & Company, *Global Survey: The state of AI in 2021*, mai. - jun. 2021, disponível em: https://www.mckinsey.com/business-functions/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021

Mecanismo de Recuperação e Resiliência, disponível em: https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_pt

National Transportation Security Board, Preliminary Report Highway HWY18MH010, 2018, disponível em: http://online.wsj.com/public/resources/documents/NTSBuber.pdf

OECD, «The use of SupTech to enhance market supervision and integrity», *OECD Business and Finance Outlook 2021: AI in Business and Finance*, Ch. 5, 2021, disponível em: https://www.oecd-ilibrary.org/sites/d478df4c-en/index.html?itemId=/content/component/d478df4c-en#chapter-d1e11426

Report of World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) on Robotics Ethics, *SHS/YES/COMEST -10/17/2 REV*, 2017, disponível em: http://unesdoc.unesco.org/images/0025/002539/253952e.pdf.

Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)), disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html#title1

Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais, P9_TA (2021)0405, disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html

The European Commission's High-Level Expert Group on Artificial Intelligence, «A definition of AI: Main capabilities and scientific disciplines», dez. 2018, disponível em: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

_____, «Ethics Guidelines for trustworthy AI», abr. 2019, disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

The Greens/EFA, «The Costs of Corruption across the EU», dez. 2018, disponível em: https://www.greens-efa.eu/files/doc/docs/e46449daadbfebc325a0b408bbf5ab1d.pdf

WILLIE, Rob, «A Venture Capital Firm Just Named An Algorithm To Its Board Of Directors — Here's What It Actually Does», *Bussiness Insider*, 13 de maio de 2014, disponível em: https://www.businessinsider.com/vital-named-to-board-2014-5?IR=T

Jurisprudência

Ac. do STJ de 12 de abril de 2000, proc. nº 141/2000-3ª; SASTJ, nº 40. 48, disponível em: www.dgsi.pt

Ac. TC n. º 340/2013, disponível em: https://files.dre.pt/2s/2013/11/218000000/3311633121.pdf

Ac. TC n. º 279/2022, de 26-04, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20220279.html

Caso *Bărbulescu v. Romania* (processo n.º 61496/08) do Tribunal Europeu dos Direitos Humanos de 5 setembro de 2017, acessível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}

STS n.º 2844/2014, disponível em: https://www.poderjudicial.es/search/AN/openCDocument/cac2ec927df2ac24a0bb78e44820713e35038df6f53826db

United States. v. Coscia, 08-07-2017, n. º 1:14-cr-00551-1, United States District Court for the Northern District of Illinois, Eastern Division, disponível em: https://law.justia.com/cases/federal/appellate-courts/ca7/16 3017/16-3017-2017-08-07.html

Holbrook v. Prodomax Automation Ltd. et al., 09-20-2021, 1:17-cv-2019, United States District Court, Western District of Michigan, Southern Division, diponível em: https://www.courthousenews.com/wp-content/uploads/2017/03/RobotDeath.pdf