ALGORITMOS EM CONTEXTO EMPRESARIAL: VANTAGENS E DESAFIOS À LUZ DO DIREITO PENAL

Anabela Miranda Rodrigues
Susana Aires de Sousa

Sumário: I. Introdução; II. Em direção à digitalização empresarial; 1. Fatores externos: tecnológicos, económicos e políticos; 2. Fatores internos: eficiência, produtividade e *compliance*; 2.1 Eficiência e precisão; 2.2 Produtividade e criação de valor; 2.3 Regulação e cumprimento normativo; III. Consequências e desafios no plano criminal; 1. Automatização da empresa e *responsability gap*; 1.1 O problema da imputação; 1.2 O algoritmo perfeito: o fim do defeito de organização?; 2. Algoritmos, *compliance* agressiva e responsabilidade penal; IV. Conclusão.

Resumo: Este estudo toma como ponto de partida a digitalização empresarial para, a partir desta fundamental transformação do processo produtivo, discutir e analisar desafios e consequências que se colocam à responsabilidade penal em contexto empresarial, no plano substantivo e adjetivo. Atende-se, em particular, aos modelos legais de atribuição de responsabilidade coletiva, assentes no conceito de pessoa humana e jurídica, à distribuição de responsabilidade em contexto empresarial, ao controlo e vigilância digitais e ao aproveitamento para fins penais de informação recolhida por formas de monitorização "inteligente", mas à custa da compressão indevida de direitos fundamentais.

Palavras-chave: Digitalização empresarial; responsabilidade criminal da pessoa coletiva, *compliance* agressivo, vigilância empresarial.

Abstract: This paper addresses the main challenges that business digital transformation poses to criminal liability in a corporate context, both in the substantive and in the adjective legal level. The discussed issues are: the legal models of attribution of corporate criminal liability, based on the concept of human and legal person; the distribution of responsibilities; digital control and surveillance; and the use, for criminal purposes, of information collected by "smart" and aggressive compliance systems at the expenses of an undue compression of fundamental rights.

Keywords: Business digitalization; corporate criminal liability; aggressive compliance; corporate surveillance and control

I. INTRODUÇÃO

A descrição da "inteligência artificial" como uma espécie de *outsider*, por contraposição à inteligência biológica ou humana, talvez não capte inteiramente a essência do tempo presente. Os algoritmos estão em todo o lado, interagindo e complementando, em muitos momentos, a realização humana, nas suas várias

dimensões[1]. Esta presença algorítmica é, simultaneamente e quase sempre, pela sua natureza, invisível[2]. Diluindo-se a fronteira entre inteligências, os sistemas computadorizados complexos integram as decisões humanas quotidianas de muitos e diversos modos ainda que, por vezes, ausentes à imediata consciência humana: em indicações ou informações (meteorológica, gastronómica, geográfica, etc.) prestadas pelo *smartphone*; na geolocalização; na assistência virtual a encomendas, transporte e entregas de um bem ou à prestação de um serviço; na divulgação e gestão de publicidade adequada ao perfil pessoal; no jogo *online*; na concessão de crédito bancário; no sistema de orientação e de condução do carro; na enorme precisão do robô cirúrgico utilizado na intervenção cirúrgica¸ em *trading* de ações e produtos financeiros; na avaliação da mais-valia laboral de um trabalhador[3], entre muitas outras.

Esta capacidade de assessorar escolhas, refletida em exemplos quotidianos ou de maior complexidade, confere à tecnologia cognitiva, pelas suas vantagens, um enorme valor económico. A variedade de funções e de (concretas) aplicações dadas aos sistemas de IA, intensificada e potenciada pelo enorme desenvolvimento da computação e da comunicação cognitivas, está necessariamente ligada a uma nova etapa de industrialização — já chamada de quarta revolução industrial[4] — caracterizada por "combinar digitalização, conectividade, automatização, robotização e inteligência artificial"[5]. Não surpreenderá, por isso, a afirmação de que vivemos hoje uma nova realidade empresarial e industrial, possibilitada não só pelo enorme desenvolvimento computacional, mas sobretudo pela inovadora comunicação em rede dos próprios sistemas computacionais entre si — aquilo a que se chamou a "Internet das coisas" (*Internet of Things — IoT*) [6]. Um exemplo claro num futuro relativamente próximo é-nos sugerido por *Hilgendorf*[7] e diz

---

1 Sobre esta transformação, tecnológica, mas também cultural, Rodrigues, Anabela Miranda, «A justiça preditiva entre a americanização e a europeização», *A Inteligência Artificial no Direito Penal*, Almedina, 2020, p. 11 e ss.

2 Cf. Scopino, Gregory *Algo bots and the Law*, Cambridge University Press, 2020, 13.

3 No final de abril de 2021, vários meios de comunicação social noticiavam, no contexto do despedimento coletivo em curso na TAP, o uso por parte da empresa de um algoritmo desenvolvido por uma consultora norte-americana tendo por fim selecionar os trabalhadores (entre 435 e 500) que seriam dispensados.

4 A expressão é atribuída, na sua origem, como dá conta Barona Vilar, Silvina, *Algoritmización del Derecho y de la Jusicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, 2021, p. 58, a um projeto estratégico de alta tecnologia elaborado e proposto pelo governo alemão sobre "a fábrica inteligente", caracterizada pela comunicação entre máquinas automatizadas, pela integração de tecnologia avançada, com uma intensa capacidade de análise de dados, que permite realizar autodiagnósticos e tomar decisões mais eficientes.

5 Como bem sublinha Barona Vilar (nota 4), p. 58 e ss.

6 Sendo uma expressão antiga, com origem no final dos anos 90, atribuída a *Kevin Ashton*, cf. https://www.rfidjournal.com/that-internet-of-things-thing. Também Ashton, Matthew, «Debugging the Real World: Robust Criminal Prosecution in the Internet of Things», *Arizona Law Review*, Vol. 59, 2017, p. 807. Contudo, o desenvolvimento computacional e tecnológico com o aumento das "coisas" conectáveis e dos meios disponíveis para a sua ligação, levaria a uma reconfiguração e a uma necessária ampliação do conceito aplicável a "todas as coisas que se ligam, comunicam, acumulam ou transmitem informação, com ou entre elas, via Internet".

7 Hilgendorf, Eric, «Automated driving and the law», *Robotics, Autonomics and the Law*, Nomos, 2017, p. 173.

respeito a um sistema rodoviário, tecnologicamente desenvolvido, em que a condução automática se realiza por via da comunicação entre sistemas, com pouca ou limitada intervenção humana.

Num cenário deste tipo, as coisas — as máquinas e os sistemas — ligadas em rede comunicam e interagem entre si, mostrando-se capazes de, por exemplo, em contexto empresarial, *prever atos e processos produtivos de modo mais eficaz e eficiente ou de prevenir ou detetar erros prejudiciais à empresa.* O algoritmo apresenta-se, assim, com inúmeros benefícios, entre os quais a *vantagem de aumentar a segurança em contexto empresarial* prevendo, prevenindo e detetando atos lesivos de interesses juridicamente valiosos, vigiando e monitorizando o espaço e as pessoas que nele intervêm.

A transição digital favorece ainda a transferência de decisões em contexto empresarial para sistemas complexos computadorizados. Pelo menos parcialmente, várias opções assumidas ao longo do processo produtivo são já decididas pelas "coisas". Isto é, muitas das tarefas decididas, atribuídas e executadas anteriormente por humanos são hoje atribuídas, decididas e executadas pela máquina. Contudo, uma decisão errada do algoritmo, ligada a lesão de bens jurídicos, confronta criticamente um modelo de responsabilidade penal construído sobre a atuação de uma pessoa, humana ou jurídica.

Estas são as questões principais que norteiam as reflexões deste estudo: procura-se, num primeiro momento, esboçar o retrato da digitalização empresarial; para, num segundo momento, ensaiar como esta transformação digital das empresas se projeta nos modelos de prevenção, investigação e responsabilização da criminalidade empresarial.

II. EM DIREÇÃO À DIGITALIZAÇÃO EMPRESARIAL

1. Fatores externos: tecnológicos, económicos e políticos

A transição digital da economia e dos seus atores está em curso. A tecnologia — *machine learning*, processamento de linguagem, robótica, plataformas eletrónicas, computação cognitiva, computação quântica —, se bem que em estádios diferentes de desenvolvimento, integra já o contexto empresarial e industrial. São inúmeras as vantagens que a IA oferece às empresas: uma *função descritiva e de aconselhamento* sobre o que fazer; uma função de *diagnóstico s*obre um determinado acontecimento; uma função de *previsão* capaz de antecipar com forte probabilidade o que é incerto; uma *função decisória* capaz de tomar opções e de as implementar[8] e ainda uma função *criativa ou lúdica* apresentando soluções inovadoras e inesperadas. Assim, às capacidades descritiva e de previsão, há muito reconhecidas aos sistemas computadorizados, as novas técnicas de IA adicionam as capacidades preditiva e prescritiva.

---

[8] As quatro primeiras funções são elencadas por Giuffrida, Iria, «Liability for AI Decision-Making: some legal and ethical considerations», *Fordham Law Review*, Vol. 88., 2019, p (2019), p. 440.

A corrida à IA no setor empresarial e industrial está iniciada. Os pontos de partida diferem e estendem-se, desde as grandes empresas tecnológicas, como a *IBM*, a *Google* ou a *Microsoft*, até às *start-ups* de *software* de *FinTech* e *RegTech* ou a instituições financeiras tradicionais. Os pontos de chegada alargam-se ainda mais. O relatório divulgado pelo grupo de peritos em *FinTech* da Comissão Europeia[9], de dezembro de 2019, dá conta de que 19 das 161 grandes empresas comerciais e de retalho estão a implementar digitalização em grande escala. Espera-se que, nos próximos 10 anos, o mercado *FinTech* cresça substancialmente na Europa, potenciado pelo desenvolvimento do *cognitive computing*[10]. Esta transição digital reconforma mercados, alterando a sua arquitetura e o seu modo de funcionamento, com grande impacto no plano económico[11]. Do mesmo passo, numa economia globalizada, as políticas económicas seguidas pelos decisores políticos não são indiferentes a esta transformação.

Com efeito, a "transição digital" constitui um tópico de grande relevância no discurso político, nacional[12] e europeu, preocupado com o difícil equilíbrio regulatório exigido por uma "*global AI race*". No plano europeu, entre os grandes desafios, evidencia-se a preocupação com a transição digital das pequenas e médias empresas — aquelas que constituem a esmagadora maioria do cenário empresarial europeu. É, pois, compreensível a preocupação manifestada na comunicação da Comissão Europeia sobre uma estratégia das PME's para uma Europa sustentável e digital[13]: sendo estas empresas muito diferenciadas, na sua dimensão e nas atividades que desenvolvem, a sua competitividade revela-se essencial para o posicionamento económico da Europa à escala global. Isto é, para que a economia europeia possa ombrear tanto a ocidente (EUA), como a oriente (China).

Os desafios e dificuldades que as pequenas e médias empresas enfrentam na transição digital são, num certo sentido, superiores àqueles com que se deparam as empresas dotadas de maior dimensão, seja pelo investimento exigido, seja também por outras limitações ligadas à falta de conhecimento, informação e formação adequadas às novas técnicas e meios de produção "inteligentes", ou à diminuta influência junto dos órgãos decisores, ou ainda ao grau de dependência que ocupam na cadeia de fornecimento a grandes empresas. Espera-se,

---

9 *Final report of the Expert Group on Regulatory Obstacles to Financial Innovation: 30 recommendations on regulation, innovation and finance*, p. 22, disponível em https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf

10 Butler, Tom, «What's next in the Digital Transformation of Financial Industry», *IT Professional*, vol. 22, no. 1, Jan.-Feb. 2020, p.33.

11 Num relatório de janeiro de 2021, publicado pelo Parlamento Europeu, estimam-se os prejuízos económicos resultante da não intervenção a nível europeu em matéria de responsabilidade e proteção do uso da IA no sistema rodoviário e de transporte — um dos setores onde a IA mais impacto tem. Calcula-se que esta omissão de regulação poderá custar algo entre €231 097 a €275 287 milhões, cf. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/654212/EPRS_STU(2021)654212_EN.pdf

12 Em maio de 2021, a Lei nº 27/2021, de 17 de maio, publicou a *Carta Portuguesa dos Direitos Humanos na Era Digital*.

13 Cf. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0103

entretanto, destas empresas que se adaptem e integrem nos seus esquemas produtivos novas possibilidades tecnológicas, de acordo com o seu sector de atividade, *v. g.,* automatizando o seu processo produtivo (no setor agrícola), implementando soluções que permitem processar, analisar e selecionar informação de forma eficaz e segura (por exemplo, no setor dos serviços). Compreende-se, assim, que a Comissão Europeia tenha expressamente assumido, para a próxima década, como seu propósito, o favorecimento de uma transição digital das pequenas e médias empresas, através de propostas que reduzam o peso da regulação e incentivem o acesso à informação e a formas de financiamento[14].

A integração de sistemas computacionais, a inovação tecnológica e a automatização dos processos produtivos, sendo já uma realidade, revela-se, assim, uma inevitabilidade no futuro, estimulada e potenciada pelos decisores políticos e por uma concorrência económica globalizada.

Este processo de transição digital projeta-se no plano jurídico e convoca algumas inquietações no plano da responsabilidade em contexto empresarial. Se, por um lado, aumenta a eficiência e a segurança na empresa, diminuindo erros e riscos no processo produtivo, de outro lado, dificulta a atribuição de responsabilidade, quando os danos se associem a processos automatizados sem intervenção humana, como adiante se desenvolverá.

2. Fatores internos: eficiência, produtividade e *compliance*

2.1. *Eficiência e precisão*

A automatização dos processos produtivos não é inteira novidade no contexto empresarial e industrial. A introdução de novas tecnologias, seja por via de sistemas e máquinas robotizados, seja pela digitalização de serviços de auditoria de controlo de qualidade ou ainda pela monitorização dos circuitos produtivos e dos trabalhadores integra, desde há largos anos, a realidade empresarial. Entre as vantagens imediatamente identificáveis e comummente apontadas à digitalização empresarial está a diminuição dos custos, através de processos automatizados que reduzem substancialmente o erro humano, e o aumento da produtividade pela definição de estratégias empresariais de risco previsível. Contudo, a rápida evolução tecnológica, em paralelo com a digitalização e a massiva criação de dados e de informações digitais, favoreceram o aparecimento de algoritmos capazes de extrair e estruturar, a partir dos *big data*, informação relevante para a gestão empresarial[15]. Uma das aplicações mais comuns

---

[14] Entre as finalidades do processo de digitalização assume-se expressamente a "*Digital transformation of businesses*", com os seguintes propósitos para esta década: "*by 2030, three out of four companies should use cloud computing services, big data and Artificial Intelligence; more than 90% SMEs should reach at least basic level of digital intensity; and the number of EU unicorns should double.*": cf. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

[15] Na verdade, o algoritmo integra funções até agora atribuídas a trabalhadores, mas também funções de administração. É o caso de um programa de IA denominado VITAL (*Validating Investment*

assenta na enorme capacidade algorítmica de avaliação, gestão e controlo de risco empresarial. As soluções tecnológicas mais complexas, designadas de *deep learning*, ganham aqui especial importância pela enorme capacidade analítica e pela elevada capacidade de precisão e de antecipação que lhe são reconhecidas. A gestão do risco pela máquina abrange áreas tão distintas, como a gestão de trabalhadores, de produtos, de fornecedores ou mesmo de cumprimento das obrigações legais e regulatórias.

A concretização destas potencialidades depende, entre outros fatores, da área económica em que a empresa atua. Um setor económico onde a transição para uma digitalização se sente de forma muito intensa, com recurso a novos meios e técnicas de IA, é o setor financeiro, onde os bancos integralmente digitais são já uma realidade. Os termos *FinTech* (*Finantial Tecnhology*), *RegTech* (*Regulatory Technology*) e *SupTech* (*Supervisory Technology*)[16] materializam, no plano narrativo, esta transição digital, seja no setor bancário, seja no domínio do mercado de capitais, hoje profundamente alterados na sua arquitetura, estrutura, gestão e funcionamento por redes de sistemas computorizados que orientam inúmeras movimentações e transações digitais. A tecnologia financeira foi certamente uma das áreas que mais evoluiu na última década — basta pensar em novas formas de realização de pagamentos, de criação de investimento, de concessão de créditos ou de análise de risco. Consequentemente, foi um dos setores em que mais se investiu em sistemas tecnologicamente avançados[17].

O algoritmo, em constante e dinâmica evolução, não se restringe à análise de enormes quantidades de dados, mas, sobretudo, mostra-se capaz de os "compreender", encontrando padrões e estruturas inacessíveis ao intelecto humano. Esta especificidade confere às ferramentas de IA, desde logo, uma enorme capacidade de previsão e gestão do risco essencial à estratégia financeira. Movendo-se o setor financeiro por entre escolhas arriscadas que assentam em juízos de previsibilidade, cria-se o contexto propício às vantagens oferecidas por técnicas computacionais complexas, *v. g.,* na concessão de crédito de risco, em intervenções em mercados de risco ou na realização de operações de risco, calculando, medindo e identificando riscos e estratégias[18]. Uma análise de risco de operações e de agentes permite ainda a entidades financeiras, em

---

Tool for Advancing Life Sciences), nomeado para integrar o conselho de administração da *Deep Knowledge Ventures* em 2017.

16 Sobre a evolução destes conceitos, em particular depois da crise de 2008, Arner, Douglas W. / Barberis, Janos / Buckley, Ross P., «The Evolution of FinTech: A New Post-Crisis Paradigm?», *University of Hong Kong Faculty of Law Research Paper* No. 2015/047, *UNSW Law Research Paper* No. 2016-62, disponível em SSRN: https://ssrn.com/abstract=. Também Scopino, (nota 2), p. 177.

17 Aldridge e Krawciw referem que nos últimos anos o investimento em tecnologia financeira cresceu 201% em todo o mundo, cf. *Real-time risk: What investors should know about FinTech, high-frequency trading, and flash crashes*. Cf., também, Hoboken, NJ: Wiley*, apud* Monaco, E. «What Fintech can learn from high-frequency trading», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 52.

18 Sobre estas vantagens, com exemplos concretos, Aziz, Saqib / Dowling, Michael, «Machine Learning and AI for Risk Management», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 40 e ss.

cumprimento das obrigações impostas por reguladores, detetar ou mesmo evitar situações ilícitas ou de fraude financeira, "avaliando a melhor forma de proteger os sistemas, dados, e por último, os clientes"[19].

Os algoritmos oferecem a vantagem de conhecer previamente, com segurança, o grau de risco e, com isso, é a própria gestão do risco que se transfere para a máquina. A precisão — e o sucesso — do algoritmo está, contudo, dependente da disponibilidade de dados que lhe possam ser introduzidos. Os dados em si mesmo ganham valor, não sendo por isso de espantar a emergência de empresas que tomam como atividade empresarial a recolha, análise, tratamento e organização de dados, por distintas categorias e áreas de interesses, consoante a procura, recolhidos, por exemplo, nos percursos e experiências digitais quotidianos pertencentes a milhões de utilizadores mais ou menos anónimos da *internet*.

2.2. *Produtividade e criação de valor*

Para além das possibilidades já referidas, a transição digital cria ainda novos mercados e novas formas de criação de valor através de produtos financeiros inovadores, de que constituem exemplo a moeda e os ativos digitais, mas também por via da emergência de novas plataformas e meios de comunicação (por exemplo o *crowdfunding*) e ainda meios de transação de elevada segurança como é o caso da *blockchain* (*cadeia de blocos*)[20]. A plataforma *blockchain*, através da sua cadeia de códigos descentralizada (em que cada bloco contém a informação do anterior), possibilita, quer a realização transações seguras, quer o cumprimento automático de contratos, potenciando a figura dos "*smart contrats*". Os "contratos inteligentes" constituem configurações tecnológicas que permitem automatizar a execução e o cumprimento das condições e obrigações legais assumidas pelas contrapartes. O código em cadeia (em blocos encadeados) permite uma execução automática e segura das condições contratuais, trazendo enormes alterações em domínios como transações e pagamentos financeiros, empréstimos, transação de ações e valores mobiliários ou moeda digital[21].

Um outro exemplo de um mercado cada vez mais automatizado, onde a intervenção humana é cada vez mais reduzida e delegada em algoritmos[22], é o mercado de capitais, onde o desenvolvimento computacional trouxe novos sistemas de transação de base algorítmica, bem como ferramentas tecnoló-

---

19 Aziz, Saqib / Dowling, Michael (nota 18), p. 43.

20 Para uma definição e compreensão desta técnica e das suas implicações no plano legal, Szostek, Dariusz *Blockchain and the Law*, Nomos, 2019, p. 40 e ss.

21 Alguns autores têm vindo a sublinhar que a combinação da automatização da execução dos contratos combinada com segurança e imutabilidade das transações em *blockchain* pode contribuir para a emergência de novos modelos de negócios, verdadeiramente disruptivos, cf. Butler, Tom (nota 10), p. 31.

22 Sobre este tema, cf. a fundamental obra de Scopino, Gregory (nota 2).

gicas de aconselhamento ou assessoria como os *robot-advisers*. A transação algorítmica tende já a ser regra de *trading* em alguns mercados, pela intensidade de informação e pela velocidade que imprime às operações[23]. Entre estes novos *algobots,* destaca-se a negociação algorítmica de alta frequência (*High Frequency Trading — HFT*), definida pela Diretiva 2014/65/EU do Parlamento Europeu e do Conselho, de 15 de maio de 2014 (DMIF II), como um sistema de negociação "que analisa os dados ou sinais do mercado a alta velocidade e, em seguida, envia ou atualiza um grande número de ordens num período de tempo muito curto, em resposta a essa análise". Como esclarece a própria Diretiva, a "negociação algorítmica de alta frequência pode conter elementos tais como a abertura, geração, encaminhamento e execução de ordens que são determinados pelo sistema sem intervenção humana para cada transação ou ordem individual, um período curto para o estabelecimento e a liquidação de posições, uma elevada taxa de rotação da carteira, um elevado rácio ordens/transações intradiário e o encerramento de um dia de transações com uma posição nula ou próxima desse valor"[24]. Entre as características principais da HFT, conta-se a automação de *trading*, a elevada velocidade nas ordens de transação e de cancelamento e a intensidade (o número) de trocas. O sistema é veloz e capaz de trocar muito em pouco tempo, sem qualquer intervenção humana. Estudos sobre o impacto desta nova forma de negociação referem, com frequência, as mudanças estruturais no mercado de capitais, a diminuição de custos, o aumento de transações e de ordens, não obstante se associar, com frequência, a este tipo de transação um risco sistémico capaz de abalar a estabilidade do mercado[25].

Por sua vez, os *robots-advisers* — cada vez mais presentes no mercado digital — usam algoritmos e sistemas avançados de IA para encontrarem soluções de investimento pessoalizadas, adequadas ao perfil de determinado cliente. Como bem sintetiza *Scopino*, "*More specifically, robo-advisors use AI systems and related technologies for customer profiling, asset allocation, portfolio selection, trade execution, portfolio rebalancing, [and] tax-loss harvesting"*[26]. A transversalidade destas soluções manifesta-se no tipo de clientes que as procura, por regra, um público mais jovem de investidores, atraído pela facilidade de acesso e pelo menor custo que lhes está associado.

O impacto inovador de algoritmos inteligentes não se restringe ao mercado financeiro, mas antes fez-se já sentir em mercados mais clássicos. Ilustrativo exemplo advém do mercado automóvel, onde a automatização, nos seus diferentes níveis, constitui um dos grandes e atuais desafios mundiais e, evidentemente, no plano europeu, como se pode inferir do sugestivo título da Comunicação, de maio de 2018, da Comissão Europeia nesta matéria: *On the road to automated*

---

23 Scopino, Gregory (nota 2), p. 16; também Rodrigues, Anabela Miranda, «Uma leitura dos crimes de abuso de mercado praticados por agentes artificiais (o caso do *spoofing*)», neste volume.

24 Cf. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32014L0065, n.º 62.

25 Cf., sobre este impacto positivo e negativo Monaco, E. (nota 17) , p. 64 e s.; Rodrigues, Anabela Miranda (nota 23) e bibliografia aí citada.

26 Scopino, Gregory (nota 2), p. 179.

mobility: an EU strategy for mobility of the future[27]. São cada vez mais substanciais as modificações sentidas na indústria automóvel e do transporte, promovidas pelas grandes empresas tecnológicas, acompanhadas de perto pelas empresas que lideram o setor, por via da construção de veículos automatizados e cada vez mais autónomos[28].

2.3. *Regulação e cumprimento normativo*

Também no contexto do cumprimento normativo as soluções com base em sistemas de inteligência artificial apresentam diversas vantagens, para regulados e reguladores, na prevenção da fraude, na monitorização do funcionamento das empresas e dos seus trabalhadores, ou na redução dos enormes custos do "*regulatory compliance*"[29].

No horizonte da prevenção da fraude financeira, há vários exemplos concretos de aplicações práticas que têm vindo a ser desenvolvidas por instituições financeiras tendo por fim cumprir exigências impostas pelos reguladores, sobretudo em matéria de branqueamento de capitais. As soluções de IA prometem uma contínua monitorização da empresa, aliviando a empresa de custos com a autorregulação e facilitando, de outro lado, ao regulador, o acesso rápido a informação em caso de incumprimento[30]. Mas a *RegTech* garante ainda uma outra enorme vantagem, como referem Arner *et. al.*[31]: a contínua monitorização da empresa permite identificar problemas e resolvê-los antecipadamente, prevendo "*compliance breaches*", e, com isso, evitando que o regulado (a empresa) tenha que responder perante o regulador e outras autoridades judiciárias. Mais do que *know your customer*, evolui-se para *know your data*! E com isso, como sublinham *Aziz* e *Dowling*, à medida que a organização e a análise dos dados se tornam mais orientadas e focadas através da AI, a informação em tempo real permitirá antecipar os próprios riscos e chegar ao santo graal de um sistema de *compliance inteligente*: "ser capaz de, com exatidão, conhecer antecipadamente os riscos, sejam eles da empresa, do mercado, operacionais ou de crédito"[32].

---

27 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0283

28 A Alemanha aprovou, em maio, legislação que permitirá a circulação de carros autónomos, em 2022, em determinadas regiões, abrindo a porta a táxis autónomos e a veículos de entrega (nível 4 de autonomia, que significa que o carro pode desempenhar todas as funções atribuídas a um condutor humano). Cf. https://www.bundestag.de/dokumente/textarchiv/2021/kw20-de-autonomes-fahren-840196

29 Cf., de forma desenvolvida, Butler, Tom / O'Brien, Leona, «Artificial intelligence for regulatory compliance: Are we there yet?», *Journal of Financial Compliance*, Vol. 3, N 1, 2019, p. 44.

30 Butler /O'Brien referem-se mesmo a uma revolução capaz de transformar a "*risk and compliance monitoring into a predictive process*": cf. nota 29, p. 45.

31 Arner, Douglas W. / Barberis, Janos / Buckley, Ross P., «The emergence of RegTech 2.0: from know your customer to know your data, *Journal of Financial Transformation 79, disponível em https://ssrn.com/abstract=3044280*

32 Aziz, Saqib / Dowling, Michael (nota 18), p. 47.

Não surpreende, por isso, o elevado investimento em formas de *compliance* "inteligente", seja por *bic-tech corporations*, por reguladores ou por instituições financeiras. Veja-se o caso da infraestrutura de IA, fundada e criada pelos grandes bancos nórdicos, inicialmente designada por *KYC Utility* e, a partir de 2019, como *IVIDEM*, com o propósito de congregar informação precisa e adequada ao cumprimento da exigência de "conhecer e diagnosticar o cliente" (*Know Your Customer*)[33].

Ao enorme investimento do setor bancário na implementação de novas tecnologias, a partir de algoritmos inteligentes, liga-se, ainda, no plano das vantagens, a possibilidade de uma enorme redução dos custos que as entidades bancárias suportam com as obrigações de *compliance*. Como dão conta *Aziz* e *Dowling*, o BBVA, o segundo maior banco espanhol, tem 8000 de cerca de 130 000 trabalhadores em *compliance*, vindo a investir nos últimos anos em soluções de cumprimento inteligente como forma de reduzir este custo base[34]. Também *Buttler* e *O'Brien*, de forma muito clara, identificam os principais fatores que favorecem o investimento em sistemas de IA tendo por fim a regulação e *compliance* financeiros: os enormes custos do cumprimento normativo — os custos de cumprimento com o *Dodd Frank Act* superavam, em 2019, $ 36 biliões e com a DMIF II mais de €2.5 biliões, esperando-se ainda o seu incremento —, o volume e a complexidade de normas, orientações e regras, bem como a velocidade a que são emitidas — a DMIF II gerou cerca de 30.000 páginas em textos conexos e o *Dodd Frank Act* americano originou mais 22.000 páginas de orientações — e a dificuldade sentida pelas entidades financeiras em compreender (aceder) e corresponder às exigência regulatórias, tanto no exercício da sua atividade como na resposta aos consumidores. Os sistemas de IA oferecem a poderosíssima vantagem de modelar toda esta informação, tornando-a acessível e compreensível[35].

Contudo, a concretização destas promessas e vantagens de eficiência tecnológica na regulação e *compliance* não se faz sem dificuldades, entre as quais se tem vindo a destacar uma necessária harmonização semântica e conceptual que mitigue o risco de se transferir para o plano digital o caos regulatório. Atente-se que um sistema inteligente e automatizado de *compliance* e de regulação financeira dependerá sempre da transformação de normas e orientações regulatórias em comandos capazes de serem apreendidos e compreendidos pelo algoritmo, questão que tem merecido a atenção, quer da indústria, quer de regulados e reguladores[36].

O combate à fraude financeira passa ainda pela aplicação das novas técnicas de IA como garantes da segurança e integridade do sistema financeiro, impe-

---

33 Aziz, Saqib / Dowling, Michael (nota 18), p. 44.

34 Aziz, Saqib / Dowling, Michael (nota 18), p. 47. Dados mais recentes podem ser encontrados em https://www.bbva.com/en/corporate-information/#bbva-due-diligence

35 Butler, Tom / O'Brien, Leona, «Understanding RegTech for Digital Regulatory Compliance», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 86 e ss.; também, dos mesmos autores, nota 29, p. 44 e ss.

36 Butler, Tom / O'Brien, Leona (nota 35), p. 95 e ss.

dindo ciberataques e sinalizando situações ilícitas ou criminosas (por exemplo, indícios de branqueamento de capitais). O mercado de *software* crítico capaz de impedir e detetar fraude está em expansão, sendo cada vez maior o número de empresas que se dedicam à oferta destes produtos. Veja-se o caso da *Feedzai*, uma *start-up* portuguesa de tecnologia financeira, especializada na deteção de fraude e na prevenção do cibercrime no setor financeiro e bancário, utilizando técnicas de IA e de *machine learning*[37].

As vantagens, entre promessas futuras e benefícios presentes, da digitalização empresarial são, assim, de diversa natureza e permitem compreender e explicar o processo de digitalização de serviços e de atividades empresariais já ocorrido em alguns setores económicos — como a área financeira — ou em vias de se realizar, a vários ritmos, em conformidade com o setor de mercado, a dimensão da empresa ou seu âmbito de atuação geográfico.

III. CONSEQUÊNCIAS E DESAFIOS NO PLANO CRIMINAL

O processo de digitalização empresarial tem, contudo, uma outra face, mais oculta, mas que se expõe problematicamente quando, através e por causa dos sistemas computorizados complexos, se ponham em causa interesses protegidos pela ordem jurídica. É o caso da lesão de bens jurídicos-penais por decisão do algoritmo em contexto empresarial, ou ainda o uso de técnicas agressivas de monitorização da atividade empresarial, a gestão de dados privados recolhidos pela empresa ou a utilização de informação armazenada ou criada pelo sistema para fins penais. É sobre estes pontos que nos debruçaremos em seguida.

1. Automatização da empresa e *responsability gap*

A transformação digital das empresas determina que muitas das decisões tomadas em contexto empresarial são (ou serão) automatizadas, tomadas pela máquina ou com base em informação por si gerada. Facilmente se intui um conjunto de dificuldades, no plano da responsabilidade, quando daquela decisão ou da atuação do algoritmo resulte a lesão de interesses e de modo particular, no plano penal, se ofendam bens jurídicos-penais[38]. Em palavras simples, quem responde quando a máquina atua incorretamente, *v. g.*, não reconhecendo um

---

37 A empresa mereceu a atenção dos meios de comunicação social pela avaliação internacional em cerca de mil milhões de dólares, atribuindo-lhe o estatuto de "*start-up unicórnio*". Em 2018, a *Feedzai* tinha sido considerada uma das 50 empresas mais promissoras na área da tecnologia financeira pela *Forbes*, tendo recebido várias distinções internacionais. Cf. https://feedzai.com/about-us/

38 Sobre este ponto, de forma desenvolvida, Sousa, Susana Aires de, «"Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial», *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Almedina, 2020, p. 59 e ss.

sinal de trânsito, favorecendo uma transação ilegítima ou discriminando um cliente ou um trabalhador?

A pluralidade de intervenientes, entre humanos e não humanos, aumenta a complexidade na atribuição de responsabilidade. Entre os primeiros, os humanos, contam-se, desde logo, os programadores de IA, os que recolhem dados e treinam os algoritmos, aqueles que produzem as máquinas, os seus proprietários, aqueles que as introduzem no processo produtivo, etc.[39] Do lado dos intervenientes não humanos temos a máquina e a empresa, a pessoa jurídica. Num contexto de acelerada digitalização empresarial, a responsabilidade da empresa pelos danos causados pelo algoritmo constitui uma questão nuclear.

É sabido que na europa continental, contrariando a teoria clássica de um direito penal em torno do agente individual, se vem afirmando e expandido uma responsabilidade criminal dos entes coletivos em resposta à criminalidade empresarial[40]. Em Portugal, a responsabilidade criminal da pessoa coletiva é conhecida desde há muito, destacando-se, na evolução desta forma de controlo da criminalidade empresarial, o DL 28/84, de 20 de janeiro (Regime Jurídico dos Crimes contra a Saúde Pública e contra a Economia), que, no seu artigo 3º, prevê uma modelo de responsabilização dos entes jurídicos[41]. No plano europeu, cabe ainda destacar a lei penal francesa de 1994 e a lei belga de 1999. Contudo, esta solução político-criminal modificar-se-ia, progressivamente, de um regime tido como excecional e extravagante, para merecer acolhimento nos códigos penais, mesmo em países tradicionalmente avessos a uma responsabilidade criminal desta natureza, como ocorreu, em 2010, no âmbito do Código Penal espanhol. A abertura à responsabilização penal da pessoa coletiva foi-se alargando, para além dos ordenamentos jurídicos já referidos, a países como a Áustria, Dinamarca, Estónia, Eslovénia, Eslováquia, Holanda, Finlândia, Hungria, Irlanda, Luxemburgo ou a Suíça. Do outro lado, procurando manter a fidelidade ao princípio *societas delinquere non potest* e recusando, pelo menos formalmente, uma responsabilidade criminal dos entes coletivos, encontram-se a Bulgária, a Grécia, a Itália, ou a Lituânia e, por enquanto, com perspetivas de mudança em pouco meses, a Alemanha, onde se discute atualmente a inclusão na legislação penal desta responsabilidade através da *Verbandssanktionengesetz*[42].

A questão da imputação do facto criminal à pessoa coletiva está naturalmente ligada à sua capacidade de, enquanto agente abstrato, poder agir e poder fazê-lo com culpa. Isto é, à determinação dos pressupostos e condições para *lhe* atribuir um facto com relevância criminal sem incorrer em uma responsabilidade

---

39 Cf. Giuffrida, Iria (nota 8), p. 443.

40 Sobre esta tendência e as suas razões, Sousa, Susana Aires de *Questões Fundamentais de Direito Penal da Empresa, Livraria Almedina*, 2019, p. 82 e ss.

41 Sobre a evolução do regime legal da responsabilidade das pessoas coletivas em Portugal cf. Sousa, Susana Aires de (nota 40), p. 99 e ss., e bibliografia aí citada.

42 Cf. Sousa, Susana Aires de, «As diferentes faces dos progamas de compliance», *Legitimidade e efetividade dos programas de compliance* (org. Adán Nieto Martin / Eduardo Saad Diniz), Tirant lo blanch, 2021, p. 29 e ss.

puramente objetiva pelo dano causado. A literatura penal sobre este tópico é extensa, quase inabarcável, bem como as distintas propostas doutrinárias nela descritas[43]. Ainda assim, no que diz respeito à imputação do facto criminal à pessoa coletiva, é possível identificar dois grandes modelos de imputação: de um lado, o modelo de heterorresponsabilidade ou vicarial, que fundamenta a responsabilidade da pessoa jurídica no facto praticado por pessoas físicas individuais organicamente ligadas ao ente coletivo e que, como seus representantes ou trabalhadores, atuam em seu nome e no seu interesse; de outro lado, um modelo de autorresponsabilidade ou responsabilização direta, que procura construir a responsabilidade criminal da pessoa coletiva de forma autónoma, baseada em pressupostos próprios e distintos da responsabilidade individual das pessoas singulares que a ela se ligam[44].

No primeiro, a atuação da pessoa individual é o substrato de atuação e de vontade da pessoa coletiva. Já, no segundo, o facto é da pessoa coletiva, plasmando-se uma imputação direta, tanto no plano da ação como da culpa. A atribuição objetiva e subjetiva do facto sustenta-se num defeito de organização da empresa que permitiu a realização do facto criminoso: censura-se o agente coletivo por esta falha estrutural que permitiu a lesão de bens jurídicos. Trata-se, assim, de uma responsabilidade coletiva por defeito na organização, iniciada no pensamento de *Klaus Tiedemann* e posteriormente concretizada e desenvolvida em várias propostas doutrinárias.

Ambos os modelos, vicarial e direto ou autónomo, descritos nas suas linhas essenciais, são colocados à prova pela digitalização empresarial e, de modo particular, pela introdução de algoritmos com algum grau de autonomia no contexto da empresa. Os desafios despontam tanto no plano da exclusão da responsabilidade como no plano da sua atribuição, muito embora com razões e argumentos de distinta natureza e substância. De um lado, no plano da atribuição de responsabilidade, a natureza dinâmica do algoritmo, que se ajusta continuamente, criando o seu próprio modelo através da aprendizagem e da identificação de padrões que lhe permitem tomar decisões, desafia os modelos de imputação da ofensa, quer a pessoas jurídicas quer a pessoas humanas. De outro lado, entre as vantagens que se reconhece ao algoritmo está a capacidade

---

43 Fundamental para a compreensão das propostas doutrinárias mais representativas é a obra coordenada por Gómez-Jara Díez, Carlos, *Modelos de Autorresponsabilidade Penal Empresarial. Propuestas Globales Contemporáneas*, Cizur Menor: Editorial Aranzadi, 2006.

44 Cf. Bacigalupo, Silvina, *La Responsabilidad Penal de las Personas Jurídicas*, Barcelona: 1998, p. 148 e ss., Feijoo Sánchez, Bernardo, *Derecho Penal de la Empresa e Imputación Objetiva*, Madrid: Editorial Reus, 2007, p. 131 e ss., Tiedemann, Klaus, *Wirtschaftsstrafrecht*, Munique: Carl Heymanns Verlag, 2007, p. 136 e s.; entre nós, por todos, Silva, Germano Marques da, *Responsabilidade Penal das Sociedades e dos seus Administradores e Representantes*, Lisboa: Verbo, 2009, p. 174 e s., com referências adicionais; Magalhães, Tiago Coelho, «Modelos de imputação do facto à pessoa colectiva em direito penal: uma abordagem do pensamento dogmático (e de direito comparado) como tentativa de compreensão do discurso legislativo», *RPCC 25*, p. 145 e ss., Sousa, Susana Aires de (nota 40), p. 89 e ss. e Rodrigues, Anabela Miranda, *Direito Penal Económico. Uma Política Criminal na Era Compliance*, 2ª ed., Almedina, 2020, p. 110.

de eliminar o erro humano e, com isso, de libertar a pessoa jurídica dos defeitos de organização, constituindo um meio por excelência para que ela cumpra o direito e varra do seu âmbito qualquer responsabilidade pelo facto criminoso.

1.1. *O problema da imputação*

Caberá, neste contexto, distinguir dois tipos situações com base no grau de dificuldade que cada uma coloca ao juízo de imputação da ofensa a interesses jurídicos. Em primeiro lugar, as situações em que a máquina é pré-programada e orientada para a realização de terminada tarefa criminosa (*deterministic robots*) e, de outro lado, os casos de algoritmos "inteligentes", tecnologicamente complexos, capazes de autonomamente fazerem opções qualificáveis como criminosas, mas que não foram pré-programados nesse sentido ou sequer tais decisões eram previsíveis para o programador (*cognitive robots*)[45]. Será essencialmente neste último caso que as dificuldades em atribuir a responsabilidade pelos danos causados aumentam significativamente.

Com efeito, a criação e a utilização de meios informáticos, mais ou menos sofisticados, para fins de natureza ilícita não constitui novidade. Em muitos ordenamentos jurídicos, o cibercrime esteve na origem de legislação especial que procura responder ao abuso ilícito de mecanismos informáticos e tecnológicos[46]. Também os sistemas autónomos de inteligência artificial têm estado ligados a situações com relevância criminal, designadamente quanto a atos de manipulação da informação do mercado de valores mobiliários, criando situações fraudulentas que determinam a alteração dos preços de mercado, designadamente através de ordens de compra fantasma *(spoofing)*[47]. Como exemplo, pode apontar-se o caso *U. S. v. Coscia*[48], que resultou na primeira condenação criminal por *spoofing* de um intermediário financeiro pelo uso de um algoritmo de HFT. *Michael J. Coscia* e a empresa *Panther Energy Trading LLC* foram acusados pela *Commodity Futures Trading Comission* (CFCT), em 2011, de empregarem um algoritmo de alta frequência para, de forma ilícita, influenciarem os preços de mercado dos valores transacionados. Analisando este caso em pormenor, *Gregory Scopino*[49] dá conta de condenações (não criminais) proferidas pelas entidades reguladoras por manipulação do mercado. Em causa estava o recurso

---

45 Sobre esta distinção, de forma clara no contexto dos robôs, o *Report of COMEST on Robotic Ethics*, 2017, p. 48, disponível em https://unesdoc.unesco.org/ark:/48223/pf0000253952

46 Tome-se, como exemplo, no ordenamento jurídico português, os crimes previstos nos artigos 3.º a 8.º da Lei 109/2009, de 15 de setembro, construídos em torno da proteção da integridade do sistema de informação.

47 Cf. Rodrigues, Anabela Miranda (nota 23).

48 A decisão está disponível em: https://law.justia.com/cases/federal/appellate-courts/ca7/16-3017/16-3017-2017-08-07.html. Também Copler, Catriona, «The Anti-Spoofing Statute: Vague As Applied to the 'Hypothetically Legitimate Trader'», *American University Business Law Review*, Vol. 5, No. 2, 2016, p. 268 e ss.

49 Scopino, Gregory (nota 2), p. 355 e ss.

a um algoritmo de alta frequência, *ab initio* criado para gerar significativas ordens de transação de um lado do mercado, canceladas milissegundos após a entrada de pequenas ordens do outro lado do mercado. Com as primeiras, criava-se um cenário de aparente interesse e liquidez financeira sobre os produtos, que favorecia de forma artificial a sua transação a preços mais elevados. A obtenção de ganhos por práticas de *spoofing* está dependente da velocidade e da intensidade da transação. Se a intensidade é necessária para que possam ser lançadas grandes ordens, a velocidade é fundamental para que o algoritmo crie uma janela de tempo que permita a transação a preços favoráveis, aproveitando-se da aparência por si criada, antes que o mercado — e os algoritmos que nele operam — corrijam a inflação ou deflação, eliminando as condições de lucro[50]. O regulador aplicou a *Coscia* e à empresa *Panther* uma sanção pecuniária no valor de $2.8 milhões[51]. Contudo, para além desta sanção, *Coscia* e a empresa de intermediação financeira enfrentariam também um processo de natureza criminal por violação das leis federais contra a fraude ao mercado mobiliário. Em 2014, o Departamento de Justiça norte-americano anunciou uma investigação criminal por violação das leis federais que proíbem o *spoofing,* que avançaria para julgamento em outubro de 2015. Para a convicção dos jurados e para a sua rápida deliberação, seriam decisivas as declarações prestadas pelo programador, que teria recebido instruções específicas e concretas sobre o tipo de algoritmo pretendido: um algoritmo desenhado para lançar um largo volume de ordens, cuja execução seria cancelada imediatamente a seguir (milissegundos depois) ou por via da execução de pequenas ordens entretanto cumpridas[52]. Em novembro de 2015, *Coscia* seria condenado em 36 meses de prisão, tornando-se a primeira condenação criminal pelo uso de algoritmo capaz de determinar o autocancelemanto de ordens por si dadas. Não obstante o recurso interposto pelo arguido, pondo em causa a constitucionalidade da norma incriminadora com fundamento na indeterminabilidade e no carácter aberto da incriminação, o tribunal superior confirmaria a condenação criminal[53].

Importa salientar que, neste caso concreto, a imputação do ilícito à pessoa jurídica e à pessoa física fundamentou-se nas declarações prestadas pelo programador. A hipótese a considerar é, neste contexto, a de que, se a máquina é programada na sua origem para explorar os limites das orientações legais, seja em matéria de *trading* seja para outros fins, como os de branqueamento de capitais, haverá lugar a responsabilidade penal.

Todavia, a resposta sobre a responsabilidade criminal, designadamente em empresas com alguma dimensão e estrutura organizativa, complica-se quando o algoritmo tenha capacidade para, perante um *input* que lhe é dado, produzir,

---

50 Cf. Olychyk, Abram, «A Spoof of Justice: Double Jeopardy Implications for Convictions of Both Spoofing and Commodities Fraud for the Same Transaction», *American University Law Review*, Vol. 65., 2015, p. 143.

51 Scopino, Gregory (nota 2), p. 355.

52 Scopino, Gregory (nota 2), p. 361.

53 Em pormenor, Scopino (nota 2), p. 366 e s.

com autonomia, informação nova, não previsível nem programada. A novidade está então no facto de a máquina ser programada para aprender, chegando a um resultado novo que é, num certo sentido, seu. Particularmente relevante, por ser nesse contexto que se identificam as questões mais difíceis de responsabilidade, é o caso dos *cognotive computers*, enquanto *"máquinas que aprendem"*[54]. Enquanto sistema de inteligência artificial, uma "máquina que aprende" não se confunde com um complexo processador de dados, isto é, não se limita a calcular a melhor opção de entre os milhares de dados que lhe foram introduzidos, análise inacessível ou muito difícil para o humano (como por exemplo, optar por uma das inúmeras possibilidades de jogada num jogo de estratégia como o xadrez). Antes, o algoritmo, alimentado com dados, ajusta-se continuamente, por forma a diminuir o erro e criar a sua própria jogada. É esta natureza dinâmica da máquina — que alguns qualificam como autonomia — que desafia a atribuição de responsabilidade às pessoas que estão por detrás da máquina, sejam pessoas físicas sejam pessoas jurídicas.

Com isto, alcança-se aquele que parece ser o problema principal que os *softwares* computacionais complexos colocam ao regime de imputação do facto à pessoa coletiva: em que medida a autonomia da máquina perturba o nexo de imputação, objetivo e subjetivo, à agente pessoa coletiva? Instala-se assim a dúvida sobre se aquela ofensa pode ainda ter-se como uma conduta da pessoa coletiva ou a imputação é interrompida pela autonomia da máquina. Dúvidas que ganham vigor reforçado se se atender aos modelos legais e aos respetivos pressupostos de responsabilização dos entes coletivos. Um sistema vicarial de imputação faz assentar a responsabilidade da pessoa jurídica numa ação ou omissão de uma pessoa física: o administrador, o gerente, ou mesmo o trabalhador. As decisões e ações criminalmente relevantes realizados pela máquina sem qualquer intervenção humana cumprem este requisito? À luz da norma-texto, a resposta dificilmente pode ser positiva, evidenciando-se, desde logo, na maioria dos ordenamentos jurídicos, um forte obstáculo fundado no princípio da legalidade criminal. Tomando como exemplo o regime legal português previsto no artigo 11º do Código Penal, a imputação do crime ao ente coletivo assenta em atos ou omissões realizados por *pessoas* que atuam em nome da empresa ("pessoas que nelas [pessoas coletivas] ocupem uma posição de liderança").

As exigências próprias de um modelo vicarial constituiriam, à partida, um argumento favorável a modelos de responsabilização direta, tomando-se o acontecimento criminal como um facto autónomo da pessoa coletiva. Contudo, uma tal responsabilidade direta ou autónoma assenta numa censura dirigida à pessoa coletiva por não se ter organizado de forma a prevenir a prática do crime. Isto é, em causa está uma deficiente auto-organização da pessoa coletiva que veda a possibilidade de controlar um risco que era *ab initio* previsível, porque ligado

54 Sobre este tipo de tecnologia e as dificuldades que levanta no plano da imputação, com adicionais referências bibliográficas, Sousa, Susana Aires de (nota 38), p. 65 e ss.

à sua organização. Porém, também por esta via persistem as dificuldades na exata medida em que o "defeito" do algoritmo não seja passível de ser conhecido e, como tal, prevenido e evitável. A capacidade cognitiva da máquina torna-a imprevisível, capaz de reagir ao inesperado, retirando a sua decisão do domínio da previsibilidade do programador. É esse espaço de liberdade da máquina, explorando as suas capacidades de aprendizagem, que não pode ser determinado (ou impedido). O "defeito" do algoritmo não existe; está no futuro e, por isso, escapa à auto-organização ... do algoritmo... e por aqui da empresa! Pelo menos em abstrato, 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.

No momento presente, a digitalização e a automatização empresariais não eliminarão decisões erradas tomadas por *softwares* inteligentes, de que constituem exemplos comprovadas opções discriminatórias na contratação ou no despedimento de trabalhadores, situações de combinação de preços, ou transações financeiras fantasmas. Na verdade, esta transformação evidencia uma patente desconformidade entre a evolução tecnológica das empresas e os modelos legalmente previstos para aferir da sua responsabilidade penal. Desconformidade que, por sua vez, é fonte de uma lacuna já identificada por alguma literatura.

As propostas de integração dessa lacuna, sendo diversas, reclamam uma extensão ou reconfiguração dos pressupostos de responsabilidade penal. Perante a manifesta dificuldade em fazer responder a pessoa humana, as soluções apresentadas oscilam entre a modificação e atualização dos pressupostos da responsabilidade das empresas, até soluções mais radicais que admitem a responsabilidade da máquina.

Referindo-se especificamente a esta problemática, *Mihailis Diamantis*, procura a solução do lado da responsabilidade da empresa. Para tal, explora um modelo que consiste na adaptação ao contexto empresarial da "*extended mind thesis*"[55]: desta perspetiva, no processo de automatização da empresa, os algoritmos integram a forma como a empresa pensa e decide e, assim, constituem uma extensão do seu estado mental e da sua vontade, vinculando-a criminalmente.

De outro lado, a suposta insuficiência dos esquemas jurídicos clássicos de atribuição de responsabilidade penal constituiu um impulso decisivo para o surgimento de propostas teóricas defensoras de uma *personalidade jurídica eletrónica*, no plano civil, e de uma consequente responsabilização criminal direta da máquina como resposta ao *responsability / accountability gap*. Defende, por exemplo, *Gabriel Hallevy* a ideia aparentemente simples de que, estando verificados os pressupostos da responsabilidade criminal numa entidade, ela deve ser responsabilizada, seja ela um ente físico, um ente coletivo ou um ente

---

[55] Diamantis, Mihailis E., «The Extended Corporate Mind: When Corporations Use AI to Break the Law», 98 *N.C. L. Rev.* 893 (2020); também Bryson / Diamantis/ Grant, «Of, for, and by the people: the legal lacuna of synthetic persons», *Art. Intelll Law* (2017), p. 273 e ss.

artificial[56]. Numa clara compreensão utilitarista da responsabilidade penal, a extensão do direito penal às máquinas autónomas e inteligentes não exigiria, na visão do autor, grandes modificações aos pressupostos exigidos por esta responsabilidade[57], sendo possível identificar, na atuação da IA, os elementos externos (*actus reus*) e mentais (*mens rea*) exigidos por uma responsabilização penal[58].

1.2. *O algoritmo perfeito: o fim do defeito de organização?*

A digitalização empresarial com recurso a algoritmos cognitivos representa um potencial enorme para as empresas, orientadas para a maximização da sua eficiência e produtividade, em condições de maior controlo e segurança, sendo a sua implementação uma tendência crescente em alguns setores do mercado, como anteriormente se desenvolveu. A tecnologia constitui um meio importante para melhorar a resposta empresarial ao cumprimento de obrigações legais e, com isso, é um poderoso instrumento para excluir a responsabilidade da empresa em situações de ofensa a interesses juridicamente protegidos. Representa também, num contexto empresarial complexo que envolve humanos e não humanos, uma ferramenta que permite uma ampla recolha de elementos capazes de esclarecer as circunstâncias e as causas da ofensa e, com isso, facilita a deteção e a atribuição do erro.

A tecnologia de IA aplicada ao cumprimento normativo e à regulação do mercado financeiro tornou-se não só num produto procurado como motivou uma resposta, rápida e intensa, do lado da "oferta" por um conjunto crescente de empresas tecnológicas. O "génio da *RegTech* foi libertado" e, com ele, uma diversidade de soluções de *Fintech* e *RegTech*, de titularidade empresarial privada, e uma variedade de modelos, tecnologicamente pouco transparentes, de *compliance* digital. Como bem assinalam *Buttler* e *O'Brien*, as instituições financeiras que adquirem estes serviços tecnológicos deparam-se frequentemente com verdadeiras soluções *black-box*, opacas, e com inerente risco de incumprimento caso uma norma não tenha sido, por exemplo, devidamente codificada[59]. O sucesso dos algoritmos inteligentes, no contexto de autorregulação regulada, dependerá de várias circunstâncias, desde a simplificação e criação de uma linguagem comum e partilhada por humanos e sistemas até uma cooperação entre regulados, reguladores e *stakeholders* que permita uma digitalização mais

---

56 Hallevy Gabriel, «The Criminal Liability of Artificial Intelligence Entities — From Science Fiction to Legal Social Control», *Akron Intellectual Property Journal* Vol. 4, Issue 2 (2010), p. 199. Uma análise crítica em Cappellini, Alberto, «Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale», *Criminalia* 2018, p. 499 e ss.

57 Hallevy, Gabriel, *Liability for crimes involving artificial intelligence systems*, Springer, 2015, p. 61.

58 Para uma apreciação crítica da construção deste autor, Sousa, Susana Aires de (nota 38), p. 77 e ss. Em sentido crítico também Rodrigues, Anabela Miranda (nota 1), p. 52 e s.

59 Buttler / O'Brien (nota 35), p. 100.

universal, contrariando uma certa atomização de algoritmos de regulação e de cumprimento normativo.

Contudo, uma "empresa inteligente", capaz de atuar em comunicação contínua e sem falhas de organização — na medida em que tais defeitos seriam antecipadamente corrigidos pelo algoritmo, e com isso, excluída uma sua eventual responsabilidade — é ainda uma visão situada num futuro incerto. Um sistema de *compliance* de base algorítmica que automatize a empresa no cumprimento das obrigações impostas por reguladores, sendo um desafio em curso, prosseguido por algumas empresas, está por concretizar. Em ordenamentos jurídicos que consagrem modelos em que a imputação do facto criminoso à pessoa jurídica se sustenta num defeito de organização, como acontece em Itália ou em Espanha, os *softwares* "inteligentes" de *compliance* apresentam-se com a promessa de serem uma poderosa ferramenta para excluir de responsabilidade a pessoa jurídica, facilitando, desde logo, a prova de que a empresa se auto-organizou para cumprir o direito. Do lado da empresa, as vantagens de um sistema inteligente de *compliance* revestem assim, à primeira vista, uma dupla natureza, tangível e normativa: a primeira, concretizada na mitigação ou eliminação do erro e no consequente aumento da segurança; a segunda, aproximando a atividade empresarial de um estrito cumprimento normativo apto a excluir a empresa de qualquer responsabilidade. Contudo, do outro lado do espelho, o complexo processo de realização de um tal sistema inteligente de cumprimento normativo terá um custo elevado, pelos direitos fundamentais que sacrifica, no plano substantivo e processual[60].

2. Algoritmos, *compliance* agressiva e responsabilidade penal

Os programas de *compliance* conheceram nos últimos anos uma enorme extensão[61], que foi alcançando de forma progressiva o direito criminal. O *criminal compliance* tornou-se uma expressão comum, incorporando fins e categorias próprios da linguagem e do procedimento punitivos, no que se designou, na expressão de Todd Haugh[62], por *criminalization of compliance*. De facto, temos vindo a assistir a um endurecimento dos programas de *compliance*, concretizado na implementação de mecanismos cada vez mais fortes e agressivos, apostados em detetar, denunciar, investigar, punir e até dar publicidade à punição (*shaming*). Com isto, o risco é o de termos um direito penal da pessoa jurídica

---

60 Uma apreciação crítica, sublinhando os elevados custos da compliance digital, *Christoph Burchard* na sua intervenção oral "*Digital Compliance: on the potentials and pitfalls of AI*" no âmbito do Colóquio *IA no setor económico: prevenção e responsabilidade,* organizado no contexto do Projeto Exploratório IA e responsabilidade empresarial, pelo Instituto Jurídico da Universidade de Coimbra, em 2021.

61 Desenvolvidamente, Laufer, William S., «A Very Special Regulatory Milestone», *20 Univ. Pa. J. Bus. Law* 391 (2018). Também Rodrigues, Anabela Miranda (nota 44), p. 83 e ss.

62 Haugh, Todd "The Criminalization of Compliance*", Notre Dame L. Rev.,* Vol. 92. (2017), p. 1215 e ss. Sobre este ponto Sousa, Susana Aires de (nota 42), p. 29.

que se transfere para um direito de *compliance* de natureza privada, menos societário e mais punitivo[63].

Importa salientar que esta sobreposição entre o público e o privado, acelerada pela digitalização empresarial e pelas vantagens que ela proporciona, não se faz sem custos no plano dos princípios que regem a afirmação de uma responsabilidade criminal. É nosso propósito dar visibilidade a alguns desses "custos", elencando-os, na tentativa de que essa sua identificação possa contribuir para o ensaio de soluções mais equilibradas.

A digitalização potencia uma maior eficácia na deteção, na investigação e na consequente responsabilização da pessoa humana que, na empresa, cometeu o erro. A falha humana escapa com grande dificuldade à vigilância da máquina. A contínua monitorização dos trabalhadores facilita a identificação do erro e, sobretudo, facilita que se aponte aquela falha individualizada como causa do acontecimento criminoso. E, com isso, transfere-se para aquela conduta individual, identificada e indicada pelo algoritmo, uma *presunção de responsabilidade*. Esta reflexão sugere-nos duas breves inquietações: a primeira do lado substantivo, a segunda do lado processual.

Quanto à primeira, a digitalização, sob a forma de contínua monitorização dos trabalhadores, promove uma dupla transferência de responsabilidade da empresa para as pessoas individuais, e, entre estas, dos administradores para os quadros intermédios ou mais baixos da empresa (*top-down*). Com efeito, o algoritmo tem a capacidade de identificar com precisão o momento do erro, desconsiderando o contexto e o "filme do acontecimento»[64].

Este aspeto prende-se com um outro de grande relevância ao nível do princípio da presunção de inocência. A "fotografia" do erro alivia a empresa e sobrecarrega a defesa do trabalhador. O algoritmo permite que a empresa supere, com facilidade, o teste da adequação abstrato-concreta do programa de cumprimento, aumentando a possibilidade de excluir a sua responsabilidade à custa da presunção de culpa do trabalhador[65].

Ainda do lado processual, ocorrendo no exercício da atividade empresarial um facto com relevância criminal, por exemplo, um pagamento indevido ligado a um ato de corrupção ou uma manipulação defeituosa do produto ou, ainda, uma alteração das contas societárias, em que termos se pode aproveitar a informação acumulada pelo algoritmo? A digitalização na empresa cria um novo fluxo informacional, um conjunto de dados útil ao esclarecimento do acontecimento criminoso, cabendo indagar do seu aproveitamento probatório na investigação

---

63 Sobre este ponto Sousa, Susana Aires de (nota 42), p. 29. Num movimento contrário ao que defende para o *compliance* um sentido socializador, apontando-o como a socialização dos tempos modernos para os agentes empresariais, cf. Rodrigues, Anabela Miranda (nota 44), p. 98 e ss.

64 O chamado "filme dos acontecimentos, cf. Rodrigues, Anabela Miranda (nota 44), p. 112, nota 229.

65 Sobre esta questão de particular relevância em modelos autónomos de responsabilidade criminal das empresas, Rodrigues, Anabela Miranda (nota 44), p. 112 e ss. Também, «Compliance programs and corporate criminal compliance», *Polar — Portuguese Law Review,* Vol. 2, January 2018, n.º 1, p. 5 e ss.

penal[66]. O algoritmo transforma-se agora num meio de obtenção da prova, de criação privada, gerando-se, assim, um conjunto de questões, não só ligadas ao seu enquadramento processual e ainda ao exercício do contraditório e do direito de defesa, mas também atinentes à supressão de um conjunto de direitos, essencialmente dos trabalhadores, como o direito à imagem, à palavra ou à intimidade da vida privada[67].

De facto, a digitalização empresarial, associada a um discurso securitário (de controlo) de prevenção da criminalidade empresarial, potencia a imolação de direitos fundamentais, sobretudo de trabalhadores, obnubilando entre as suas vantagens um custo elevado, quase invisível, porém irreversível[68]. Há um lado mais obscuro da monitorização "inteligente" da atividade empresarial que tem vindo a merecer a atenção da doutrina. A introdução da tecnologia em contexto empresarial conduz a uma rede invisível de vigilância, capaz de reunir informações e dados privados daqueles que interagem com a empresa ou que atuam no espaço empresarial, designadamente dos trabalhadores. Num extenso estudo sobre esta matéria, *Richard Bales* e *Katherine Stone* elencam diversos mecanismos digitais hoje utilizados por diversas empresas, em distintos momentos e com distintas finalidades: contratação, evolução e avaliação do desempenho do trabalhador, cumprimento das obrigações laborais e manutenção da segurança do trabalhador. Alguns destes instrumentos, contudo, ao mesmo tempo que favorecem, por exemplo, a segurança do trabalhador, permitindo-lhe ampliar o seu campo de visão (*computer vision*) ou diminuir a carga e o esforço físico (exosqueletos), recolhem informações pessoais (sobre a sua localização, características físicas ou mesmo resultantes de monitorização de sinais e reações biológicos) que alimentam algoritmos capazes de prever a *performance* individual, a ética laboral, a personalidade, a lealdade à empresa, futuros custos médicos ou mesmo a permanência na empresa. Cabendo assinalar que, do lado do aproveitamento probatório destas informações para fins de responsabilidade criminal, sempre sobrariam, no ordenamento jurídico português, os limites inultrapassáveis à sua validade resultantes do disposto no artigo 32º, n.º 8, da Constituição, e no artigo 126º, do Código de Processo Penal.

---

66 Sobre este problema, em geral, Gless, Sabine, «AI in the courtroom: a comparative analysis of machine evidence in criminal courts», *Georgetown Journal of International Law*, Vol. 51, 2020, p. 197 e ss.

67 Sobre a utilização das novas realizações tecnológicas como prova digital e do perigo que ela representa para alguns direitos fundamentais, em geral, Fidalgo, Sónia, «A utilização de inteligência artificial no âmbito da prova digital — direitos fundamentais (ainda mais) em perigo», *A Inteligência Artificial no Direito Penal*, Almedina, 2020, p. 137.

68 Em geral, sobre o modelo de *compliance* perspetivado para a vigilância e controlo, Rodrigues, Anabela Miranda (nota 44), p. 105.

IV. CONCLUSÃO

Este estudo congrega algumas reflexões sobre o processo de digitalização empresarial, acelerado por fatores externos e internos às empresas. Foram identificados, entre as circunstâncias externas que estimulam esta digitalização, fatores económicos e políticos. Do lado endógeno, fizeram-se sobressair razões de eficiência e de produtividade, de cumprimento normativo e de prevenção da criminalidade financeira e empresarial (*compliance*).

Entretanto, a automatização digital das empresas tem uma outra face, menos positiva e mais oculta, que se projeta no plano criminal. A delegação de decisões em sistemas computadorizados complexos, capazes de decidir com algum grau de autonomia, gera dificuldades de imputação de ofensas criminalmente relevantes. O *responsability gap* resulta, desde logo, da falta de adequação dos modelos legais de atribuição de responsabilidade, estruturados em torno do conceito de *pessoa*, humana e jurídica. Para além disso, nos casos em que o erro resulta de uma atuação humana, a monitorização e a vigilância digitais da atividade empresarial promovem a transferência de responsabilidade da organização para os quadros mais baixos ou intermédios da empresa. Acresce que o controlo digital é feito, em alguns casos, à custa da compressão indevida de direitos fundamentais. Do lado processual, faz-se notar como a emergência de novos elementos probatórios produzidos por algoritmos, de titularidade e propriedade privada, desafiam, entre outros, princípios, como o da presunção e inocência, ou colocam em causa o exercício de direitos, como o do contraditório.