COMPLIANCE CRIMINAL DIGITAL — O ORÁCULO DA ERA DA INTELIGÊNCIA ARTIFICIAL

Digital Criminal Compliance: The Oracle of the Artificial Intelligence Era

Anabela Miranda Rodrigues
Professora Catedrática, Faculdade de Direito, Universidade de Coimbra, Portugal
Professora Adjunta, Faculdade de Direito, Universidade de Macau

Resumo: Na atual sociedade do risco e da inteligência artificial, os desafios regulatórios são múltiplos. No âmbito de uma criminalidade económico-financeira, protagonizada por grandes entidades coletivas multinacionais, onde sobressai o *compliance* como estratégia de aplicação da lei, discute-se, neste estudo, à luz dos seus mais recentes desenvolvimentos no sentido cooperativo de dupla via, as vantagens e os riscos que comporta a digitalização do *compliance*. Analisa-se, neste contexto, a questão do *overcompliance* e da sua repercussão no aspeto nevrálgico da *efetividade* do *compliance.* Por fim, chama-se a atenção para a mudança de paradigma do direito penal na abordagem do controlo do crime que o *compliance* - sobretudo quando potencializado pela digitalização – deixa antever, ao transformar um *modelo preventivo indireto* por um *modelo preventivo direto* de repressão da criminalidade.

Palavras-Chave: *Compliance*; *compliance* digital; *compliance* cooperativo de dupla via; *overcompliance*; justiça penal preditiva.

Abstract: In the current society of risk and artificial intelligence, the regulatory challenges are multiple. In the context of economic-financial crime, carried out by large multinational collective entities, where compliance stands

out as a law enforcement strategy, this study discusses, in the light of its most recent developments in a dual-track cooperative sense, the advantages and the risks that the digitalization of compliance entails. In this context, the issue of overcompliance and its impact on the neuralgic aspect of compliance effectiveness is analyzed. Finally, attention is drawn to the change in the paradigm of criminal law in the approach to crime control that compliance - especially when enhanced by digitalization - allows us to foresee, by transforming an indirect preventive model into a direct preventive model of crime repression.

Keywords: Compliance; digital compliance; dual-track cooperative compliance; overcompliance; predictive criminal justice.

1. Introdução

Progresso técnico-científico e risco caraterizam o momento histórico que vivemos. Volvidas quase quatro décadas sobre a publicação de *Ulrich Beck*, em 1986,[1] a propósito da sociedade do risco, em que captou com apurada sensibilidade a insegurança inerente ao projeto da sociedade industrial da modernidade, o seu diagnóstico não perdeu atualidade e está hoje reforçado. A OCDE referia-se, muito recentemente, em fevereiro de 2023, ao *global mood* como estando longe de ser otimista.[2] Ainda mal refeitos da pandemia, os governos mundiais têm de encarar novos conflitos em cenário de guerra, sob o pano de fundo das alterações climáticas, da disrupção de sistemas económico-financeiros e digitais e de uma crise generalizada de confiança. Os avanços alcançados na promoção dos direitos humanos, na consolidação da democracia e do Estado de direito, a crença na ciência e na técnica e nas suas possibilidades ilimitadas deram lugar a um risco existencial perante os problemas sociais, económicos, de saúde pública, ambientais - de segurança *humana*[3] - que, no novo milénio, colocam a humanidade no fio da

1 A referência é a BECK, Ulrich, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Suhrkamp, Frankfurt a. M., 1986, *passim*. O Autor definiu a «sociedade do risco» como aquela que, juntamente com os progressos da civilização, apresentava a contrapartida da produção de novos riscos conaturais àqueles progressos, por exemplo, perigos ambientais ou nucleares.

2 *Embracing Innovation in Government: Global Trends 2023*, *passim.*

3 Sobre o que se segue, cf. RODRIGUES, Anabela Miranda e MACHADO, Jónatas, «Segurança humana, globalização e desenvolvimento. Desafios para o Século XXI», *Liber Amicorum Manuel Simas Santos*, Coordenação André Paulino Piton/Ana Teresa Carneiro, REI dos Livros, 2016, p.109s; RODRIGUES, Anabela Miranda, «A política criminal no Estado de Direito do Século XXI – os desafios da segurança», *Revista Brasileira de Ciências Policiais,* v.11, n.º 1, jan/abr 2020, Brasília, p. 19 s; id., «Criminalidade económica empresarial e direitos humanos – boa

navalha. Estamos nos antípodas do otimismo das *Luzes*, em que o percurso de domínio do Mundo pelo Homem está comprometido por um percurso de conquista ilimitada. O coro de *Antígona* deveria hoje ser dito sob o signo da «inquietação», que o retorno dos mitos de *Frankenstein* ou do *Aprendiz de Feiticeiro* traduzem.

Nesta sociedade do risco ou «sociedade invisível» - como a apelida *Daniel Innerarity*[4] -, confrontada com transformações avassaladoras, como é o caso da entrada nas nossas vidas da Inteligência Artificial (IA), não admira que o conceito de segurança tenha vindo a assumir uma centralidade inusitada e se apresente como um conceito em mudança. Nas últimas décadas, observou-se uma tendência no sentido de ampliar as fronteiras semânticas do conceito. Ele incorpora também a noção de *safety*, que traduz uma segurança que implica a observância de normas científicas e técnicas e padrões de cuidado adequados à diminuição dos riscos associados à fruição de bens, serviços, equipamentos e instalações, e aproxima-se do sentido de *welfare* e *well-being*. Abrange-se, aqui, a proteção de direitos das pessoas - designadamente, de consumidores ou de trabalhadores, mas não só -, reforçada pela ideia de que alguns destes direitos devem ser considerados direitos humanos, já que, no atual cenário de globalização, algumas empresas são atores económico-sociais de primeira linha – são os novos atores da política num novo espaço, que desempenham um papel chave, não só na configuração das relações económicas, mas na sociedade no seu conjunto, mais poderosas e potencialmente mais perigosas e danosas do que muitos Estados.[5] O problema vem sendo discutido com particular intensidade no confronto entre utilizadores de bens e serviços, por um lado, e grandes grupos empresariais transnacionais, por outro, em setores variados, que podem ir do farmacêutico, passando pelo das utilidades, v. g. água ou energia, até, mais recentemente, ao financeiro e tecnológico e da IA. Pode dizer-se, na verdade, que os desafios da segurança humana vão hoje da segurança do consumidor, passando pela segurança económica e social, alimentar, sanitária,

---

governança e *compliance* ao serviço da política criminal», *Estudos em Homenagem ao Professor Doutor Wladimir Brito*, coord. Mário Ferreira Monte, Joaquim Freitas da Rocha e Maria da Assunção do Vale Pereira, Almedina, dezembro de 2020 a), p. 135 s.

4 Assim, INNERARITY, Daniel, *A sociedade invisível*, Editorial Teorema, 2009 (primeira publicação: 2004), p. 57 s.

5 Sobre o que se segue, RODRIGUES, Anabela Miranda, «Criminalidade económica empresarial, *Governance* e *Compliance* – para uma nova política criminal à distância», *Nuevos Desafíos frente a la criminalidad organizada transnacional y el terrorismo*, Laura Zúñiga Rodríguez (Directora)/ Julio Ballesteros Sánchez (Coordinador), Dykinson, OCOT, Madrid, 2021, p. 129 s (p. 130); *id*., «O último cocktail – criminalidade económico-financeira, responsabilidade penal empresarial, *Compliance* e Inteligência Artificial», *Homenaje al Professor Ignatio Berdugo Gómez De La Torre, Liber Amicorum Derechos Humanos y Derecho Penal,* Tomo II, Ediciones Universidad de Salamanca, 2022, p. 272 s.

ambiental e eletrónica, até à segurança pública, nacional e global.

Este é um cenário em que não admira que a *regulação* assuma uma importância crescente – fala-se de um mundo *luhmanianamente* mais complexo, em que são ineficientes muitas das técnicas clássicas de intervenção estadual. Está em causa enfrentar desafios regulatórios e propor soluções inovadoras orientadas para responder às exigências de proteção de bens jurídicos, também penais, e de direitos das pessoas.

Identificamos, a este respeito, um universo teórico, de que queremos destacar três núcleos problemáticos.

Em primeiro lugar, somos remetidos para uma reflexão sobre o risco e a sua projeção sobre o direito, também no âmbito penal, que leva à consideração de um direito preventivo e de normas que visam evitar a produção de riscos de diferente natureza. No mundo jurídico, em geral, este paradigma emergiu para responder a diversos problemas sociais com que atualmente se confronta a *segurança humana*, no plano global. Não faltam propostas, em múltiplos domínios, de aplicação da lógica da prevenção para responder àquelas exigências de segurança. O paradigma de direito preventivo[6] teria por base a recolha e o processamento da máxima informação disponível, utilizando-a em seguida na identificação dos comportamentos individuais e coletivos e dos processos naturais e técnico-científicos potencialmente perigosos ou lesivos para o ser humano e a natureza, e na fundamentação da atuação preventiva, de forma a conseguir ganhos na redução do risco e do dano e, assim, da incerteza e da insegurança, nos planos fáctico e jurídico. O direito preventivo escora-se em ideias fundamentais como análise de riscos, identificação e discussão de problemas jurídicos, planeamento, preparação, prontidão e atuação preventiva, antes de os danos fácticos e jurídicos se materializarem. Entretanto, muitos aspetos da sociedade do risco global dos nossos dias ligam-se a um novo progresso científico que, se destrói velhas certezas e cria outras, gera incertezas no momento de pronunciar-se sobre as causas e as condições dos novos riscos globais. A reclamar um princípio da precaução como princípio orientador da regulação para lidar com estas incertezas científicas – o seu controlo é um desafio, especialmente evidenciado quando está em causa a proteção de bens jurídicos coletivos, de que já são exemplos clássicos a saúde pública ou o ambiente e, mais recentemente, com os desenvolvimentos da IA, a *essência* da humanidade. É a diferença entre risco e perigo que justifica a passagem para um paradigma de precaução, baseado sobre uma presumível, mas não segura, fonte de risco. De acordo com um paradigma de prevenção, o desenvolvimento científico

6 Vide, para uma reflexão sobre os paradigmas da prevenção e da precaução, GARCÍA ALFARAZ, Ana Isabel, *Princípio de precaución. Seguridad alimentaria y delito*, Tirant lo blanch, Valencia, 2022, p. 79 s.

identifica a causa do perigo que se pretende evitar. Já no enquadramento de um paradigma da precaução, a ciência salienta a incerteza sobre a causa que pode levar à produção (materialização) do risco – está-se perante um perigo incerto. Neste caso, a resposta do direito deve ter em conta, por um lado, a incerteza científica, que supõe a projeção do saber científico sobre a regulação e que dá conteúdo ao risco; e, por outro lado, os resultados que podem produzir-se, no caso de o risco também se produzir (materializar).

Em segundo lugar, e nesta mesma linha, deve ser clarificado o papel a desempenhar pelos sistemas de regras e princípios, o grau de flexibilidade desejado ou tolerado. Mais concretamente, deve ser debatido o papel a desempenhar pelo direito penal, pelo direito civil e pelo direito administrativo e de mera ordenação social, com os seus mecanismos de intervenção *ex post facto* ou *ex ante*. Assim, embora não se abdique de constituir o direito penal como *ultima ratio*, há que redefinir o seu lugar na nova *sociedade de segurança*, preservando-se da consideração da segurança como bem jurídico-penal. Que, adverte-se, abre a via para a utilização generalizada do direito penal para evitar riscos e ao fenómeno da sua expansão e transformação em um *ordenamento de segurança* em prejuízo da sua configuração como um *ordenamento de liberdade*.[7] A questão pode equacionar-se à luz da determinação do nível do paternalismo admissível na atividade regulatória do Estado no seio de uma *sociedade de segurança*. Numa sociedade livre e pluralista, haverá sempre uma razoável dose de liberdade para a adoção de comportamentos prejudiciais e geradores de risco e insegurança para os próprios indivíduos e para terceiros. A liberdade de escolha é um valor intrínseco, ainda que algumas escolhas sejam erradas e desaconselhadas, do ponto de vista dos seus efeitos individuais e coletivos. Na linha dos estudos da psicologia e da economia do comportamento, reconhece-se que, por razões endógenas e exógenas, pessoais e contextuais, os indivíduos e os grupos nem sempre tomam as decisões mais racionais do ponto de vista da maximização das suas preferências a médio e longo prazo, podendo por isso haver alguma margem para os poderes públicos tentarem induzir o seu comportamento, com formas de paternalismo *soft*, embora protegendo o essencial da sua liberdade de escolha[8].

De um modo geral, este equilíbrio e esta margem de manobra dos poderes públicos têm sido encontrados na noção de uma ordem constitucional livre e democrática, baseada na dignidade da pessoa humana e na autonomia individual, em que a liberdade é a regra e a limitação à liberdade é a exceção. Embora

---

7 Nesta linha, em determinados domínios do direito penal, RODRIGUES, Anabela Miranda (nota 3, 2020 e 2020 a)).

8 HAINES, Fiona, «Regulatory Failures and Regulatory Solutions: A Characteristic Analysis of the Aftermath of Disaster», February 2009, https://doi.org/10.1111/j.1747-4469.2009.01138.x

se admitam restrições à autonomia individual em nome de bens jurídicos da comunidade e do Estado constitucionalmente protegidos, existe uma predisposição *prima facie* do direito constitucional contra perspetivas unilateralmente libertárias ou paternalistas. Quando muito, admite-se que o Estado assegure uma escolha livre e esclarecida, eventualmente acompanhada de uma estrutura de incentivos favoráveis a uma determinada alternativa considerada socialmente mais desejável, embora sem pôr em causa a possibilidade real de escolha e sem afetar dimensões fundamentais da dignidade e da autonomia individual.[9] Este paternalismo regulatório, em nome de um conceito amplo de segurança humana, não deixa de ter os seus perigos. Por um lado, também os decisores políticos e os reguladores são afetados pelas falhas racionais, cognitivas e comportamentais que facilmente atribuem aos indivíduos que pretendem ajudar. Por outro lado, esse paternalismo prepara os cidadãos para aceitarem medidas cada vez mais intrusivas e restritivas da sua liberdade (*hard paternalism*), podendo minar os fundamentos da ordem constitucional livre e democrática a médio prazo[10].

Em último e terceiro lugar, assomam aqui novas estratégias regulatórias. No quadro da regulação[11], devem aqui ser reequacionadas as vantagens comparativas da *hétero-regulação*, da *autorregulação* e da *autorregulação regulada*, bem como o recurso a instrumentos mais ou menos formalizados de *soft regulation* ou à chamada *hard regulation*, com os seus mecanismos *de comando, controlo e sanção*. Relevante é a discussão sobre o movimento de *metarregulação* ou «regulação da autorregulação»[12], em que múltiplas e díspares atividades são reconduzidas ao mesmo esquema regulatório para a prossecução de objetivos. O regulador cria regras gerais, mais ou menos prescritivas, e define certos objetivos que devem ser alcançados; por seu turno, a entidade regulada mantém a sua discricionariedade na opção de formulação, implementação e controlo e aperfeiçoamento dos planos e processos - os programas de *compliance* -[13] necessários para alcançar os objetivos relevantes. O âmbito financeiro configura um domínio expressivo desta tendência de uma autorregulação cada vez mais hétero-regulada, em que

9 Richard H. THALER, Richard H., SUNSSTEIN, Cass R., "Libertarian Paternalism Is Not an Oxymoron", 70 *University of Chicago Law Review*, 2003, p. 1159 ss.

10 RIZZO, Mario J., WHITMAN,Douglas Glen, "Little Brother Is Watching You: New Paternalism On The Slippery Slopes", 51 *Arizona Law Review,* 2009, p. 685 ss.

11 RODRIGUES, Anabela Miranda, *Direito penal económico – uma política criminal na era compliance*, Almedina, 2.ª edição, 2020, p. 83 s.

12 Cf. COLIN, Scott, «Regulating Everything: From Mega- to Meta-Regulation», *Administration*, Vol. 60, 2012, p. 57 s.

13 Sobre este modelo de elaboração de programa de compliance em três colunas, delineado por *Marc Engelhardt*, cf. RODRIGUES, Miranda Anabela, (nota 11), p. 102 s.

a metarregulação se difundiu de forma tão relevante que se tornou um modelo: manifesta-se na evolução dos acordos de capital a partir de *Basileia I*, onde uma abordagem comum a todas as instituições bancárias foi adotada, sem prejuízo de existir na sua base um processo de interação com a própria instituição.

É sobre este pano de fundo que avanços tecnológicos poderosíssimos marcam a sociedade contemporânea, com a entrada da IA no nosso quotidiano. E em que o direito e o sistema de justiça em geral e, especificamente, o direito e a justiça penais[14] são interpelados por esta prodigiosa mudança cultural – um «facto social total»[15] -, que atinge os fundamentos da vida coletiva.

Neste estudo, confrontamo-nos com a mais atual política de prevenção e luta contra a criminalidade económico-financeira, que, protagonizada sobretudo por grandes entidades coletivas multinacionais, se nutre de um arcaboiço legal onde sobressai o *compliance* – um *compliance*, sublinhe-se, cada vez mais digital e inteligente. Destaca-se, de um lado, a questão da efetividade que o acompanha e interroga-se esta mudança na aplicação do direito no seu significado para o direito penal.

2. O *compliance* – luzes sobre o *compliance* digital

Uma política de autorregulação regulada tem sido concebida, generalizadamente – apontando-se os domínios da criminalidade ligada ao branqueamento, à corrupção ou às agressões ambientais -, de acordo com um modelo em que a responsabilidade pela criação do controlo interno (*compliance*) assentava nos ombros do setor privado, que, de forma autónoma, devia estabelecer programas de *compliance* eficazes, integrados por múltiplos deveres de controlo – os deveres de *compliance* -, concebidos «à medida», de acordo com uma abordagem de prevenção de riscos, baseada na sua identificação, deteção, avaliação e redução, por forma a prevenir a prática de ilícitos ou de atividades criminosas.

Com o tempo, no entanto, verificou-se que esta abordagem não se revelava uma tarefa simples. A este propósito podem elencar-se uma série de razões. Desde logo, refiro-me à complexidade do ambiente em que as entidades privadas em geral atuam, não só de desenvolvimento tecnológico sofisticado e de

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

15 GARAPON, Antoine/LASSÈGUE, Jean, *Justice digitale*, Presses Universitaires de France/ Humensis (PUF), 2018, p. 83, apelando a *Marcel Mauss*, que o define como um fenómeno que «met en branle la totalité de la societé et de ses institutions» (*Sociologie et anthropologie*, Paris, PUF, 1973, p. 274).

novos riscos emergentes bem como de aplicação extraterritorial de leis nacionais. Depois, a resposta a estas – e outras – dificuldades e a um crescente sentimento de inefetividade do modelo que se tinha posto em funcionamento desencadeou uma hiper-regulação – ao ponto de, relativamente a certos fenómenos criminológicos, se dizer que a prevenção e luta contra eles enfrenta uma *selva regulatória*[16] – de elevada abstração e complexidade por parte das entidades públicas.

Na verdade – convém lembrar -, o nascimento da ideia de *compliance*[17], cujo epicentro geográfico originário se localiza no mundo anglo-saxónico e que rapidamente influenciou o mundo continental, tem as suas raízes em novas dinâmicas da sociedade e da economia, que se evidenciaram no protagonismo das empresas, em particular das multinacionais e no caráter transnacional e dificilmente controlável da sua atuação, também ao nível da prática de crimes, e na produção de riscos, que, em certos domínios, rapidamente evoluíram para catastróficos para as populações e para o ambiente. E que reclamavam, assim, uma reorientação da governança empresarial, acompanhada da responsabilidade direta da entidade coletiva pelos comportamentos ilícitos e criminosos cometidos no seu seio e através dela. Neste cenário, o *compliance* surge como uma estratégia organizacional de avaliação e gestão de riscos, a que dedicaram particular atenção os principais fóruns internacionais, como a OCDE, ONU, União Europeia, Conselho da Europa, o G20, o G7, o Banco Mundial ou a Organização Internacional do Comércio. De um ponto de vista político-ideológico, é típica do modelo de Estado regulador – o *Regulatory State* –, que se posiciona historicamente entre o Estado liberal oitocentista, que acreditou que podia transformar o lobo em cordeiro, e o *Welfare State ou Wohlfahrtsstaat* de novecentos, cuja capacidade de intervenção se erodiu com a crise fiscal, a industrialização e, por fim, com a globalização. Pode perspetivar-se o *compliance* como um sistema em que se acentua mais o *controlo interno*[18] ou pode atribuir-se-lhe um significado, comum no domínio empresarial, que implica o controlo sobre as contrapartes comerciais (*know your counterparty*), que se alarga e abrange o controlo sobre a cadeia de fornecedores globais das empresas multinacionais, tendo em vista prevenir o cometimento de ilícitos e violações de direitos humanos – falo, agora, de *compliance* no sentido de *due diligence*.

No contexto da questão de uma *persistente* crise de efetividade do

16 CASSANI, Ursula/VILLARD, Katia Anne, «The Changing Face of Money Laundering Regimes», *Révue Internationale de Droit Pénal*, 90, 2019, n.º 2, p. 159 s (p.167).

17 Cf., RODRIGUES, Miranda Anabela (nota 11), p. 83 s.

18 Seguindo uma metodologia estabelecida pelo Relatório COSO (*Committee of Sponsoring Organizations*) da *Treadway Commission*, que teve recentemente, em 2023, a sua última edição, com o 2023 ICSR (*Internal Control Sustainability Report* de 2023.

compliance, interessa-me destacar um seu aspeto que se prende com o caráter mais vinculativo ou mais flexível da intervenção dos legisladores e dos reguladores na autorregulação. O setor financeiro e bancário surge como um bom exemplo de uma *enforced self-regulation* ou *compliance cogente*. Acrescentando, ainda, que a este aspeto se liga normalmente uma hétero-regulação minuciosa e invasiva, quase asfixiante, ou hiper-regulação a que já me referi. A autorregulação do setor continua a ser um objetivo, mas nos limites de uma metarregulação ditada pelo legislador e pelos reguladores. Este enorme impulso regulatório experimentado diminuiu, na prática, o espaço de intervenção da *soft law*, que - sem ser eliminada e mantendo a sua influência -, cedeu o lugar, numa medida significativa, à abordagem de *hard law*.

De uma forma geral, isto significa que o quadro regulatório enfatiza cada vez mais o papel do setor público. Isso é visível em diferentes domínios legais relativos à prevenção e luta contra a criminalidade económico-financeira e tem uma justificação evidente. Sobretudo depois da crise financeira e económica de 2007-2008, os legisladores preocuparam-se cada vez mais em assegurar que interesses pessoais e fins lucrativos prosseguidos pelas entidades privadas não se sobrepusessem à prevenção e luta contra os fenómenos criminais em causa, de elevada danosidade social. Em última análise, os regimes jurídicos que a este propósito se foram estabelecendo refletiam uma evolução da compreensão do *compliance* com tendência para o ver menos como um instrumento de gestão, servindo a satisfação dos interesses próprios da entidade privada e o êxito da sua atividade, designadamente dos seus sócios, e mais como constituindo um instrumento a utilizar pela organização tendo em vista respeitar interesses públicos e, assim, interesses alheios a ela e indisponíveis por ela - e, por isso, constituindo *o compliance* um domínio de autorregulação cada vez mais imperativo e (hétero-) regulado.

Foi-se, assim, assistindo à expansão da regulação pública num quadro de autorregulação regulada. Em suma: *more regulation is better regulation* – talvez seja a melhor expressão do *Zeitgeist* em matéria de *compliance*.

É aqui que a prodigiosa evolução tecnológica que vivemos se faz sentir, ao favorecer o aparecimento de algoritmos capazes de extrair e estruturar, a partir dos *big data*, informação relevante para a gestão (*governance*) empresarial. Uma das suas aplicações mais comuns assenta na enorme capacidade de avaliação, gestão e controlo de risco empresarial. As soluções tecnológicas mais complexas de *deep learning* e com base em sistemas de IA ganham uma especial importância pela enorme capacidade analítica e pela elevada capacidade de precisão e de antecipação que lhe são reconhecidas. *Buttler e O'Brien*[19] referem-se a uma revolução capaz

19 Butler, Tom/O'Brien, Leona, «Artificial Intelligence For Regulatory Compliance: Are We There

de transformar a «*risk and compliance monitoring into a predictive process*». A gestão do risco pela «máquina» abrange áreas tão distintas como a monitorização do funcionamento das empresas - atuando no âmbito da gestão de produtos e de fornecedores ou de cumprimento das obrigações legais e regulatórias - e dos seus trabalhadores e a prevenção e luta contra a fraude, sendo-lhe reconhecidas diversas vantagens na redução dos enormes custos do "*regulatory compliance*".

A contínua monitorização da empresa através do algoritmo permite identificar problemas e resolvê-los antecipadamente, prevendo "*compliance breaches*" e, com isso, evitando que o regulado tenha que responder perante o regulador e outras autoridades judiciárias. À medida que a organização e a análise dos dados se tornam mais orientadas e focadas através da IA, a informação em tempo real permitirá antecipar os próprios riscos e, em última análise, chegar ao Santo Graal de um sistema de *compliance* inteligente[20].

Para além disto, a digitalização da empresa potencia a transformação do local de trabalho num *digital work place*, permitindo a criação de uma rede invisível de vigilância capaz de reunir informação e dados sobre aqueles que atuam no espaço empresarial, designadamente os trabalhadores, e também daqueles que interagem com a empresa. Estão muito difundidos instrumentos de *electronic performance monitoring* de trabalhadores, que podem assumir diversas formas de controlo, de acordo com o nível de monitorização – da organização, do departamento ou pessoal - ou consoante o objeto a controlar – o desempenho, o trabalho ou o indivíduo – ou ainda as tecnologias utilizadas[21]. De qualquer forma, reconduzem-se a formas de vigilância direta e de exercício de poderes de polícia preditiva privada sobre «dependentes» da empresa[22].

No horizonte da prevenção e luta contra a fraude, um setor económico onde a transição digital 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*) materializam, no plano narrativo, esta transição digital, seja no setor bancário, seja ainda no domínio do mercado de valores mobiliários, hoje profundamente alterados

---

Yet?», *Journal of Financial Compliance*, Vol. 3, n.º 1, 2019. p. 45.

20 Como sublinham AZIZ, Saqib/DOWLING, Michael, «Machine Learning and AI for Risk Management», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 47.

21 Cf. KALISCHKO, Thomas/RIEDL, René, «Electronic Performance Monitoring in the Digital Workplace: Conceptualization, Review of Effects and Moderators, and Future Research Opportunities», *Frontiers in Psychology,* Volume 12 – 2021, p. 1-15.

22 Sobre isto, cf. MORGANTE, Gaetana/FIORINELLI, Gaia, «Promesse e rischi della compliance penale digitalizzata», *Archivio Penale,* n.º 2, 2022, p. 1 s (p. 28).

na sua arquitetura, estrutura, gestão e funcionamento por redes de sistemas computorizados que orientam movimentações e transações digitais[23]. A tecnologia financeira foi certamente uma das áreas que mais tem evoluído - 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. 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 das entidades bancárias, aliviando-as de custos com a autorregulação e facilitando, de outro lado, ao regulador, o acesso rápido a informação em caso de incumprimento. Pode mesmo dizer-se que o setor bancário, que foi sempre um utilizador intensivo de inovações técnicas e tecnológicas, está na primeira linha do aproveitamento de aplicações de IA para a sua atividade. A particular adequação das utilidades fornecidas por sistemas de IA a este setor explica a significativa atenção que entidades, reguladas ou reguladoras, lhe têm dedicado, sendo o *compliance* uma das áreas da atividade das entidades bancárias que mais apetência evidencia pela sua utilização. Estando cada vez mais submetidas a deveres de *Know Your Customer* (*KYC*), o seu cumprimento pode revelar maior efetividade, se a informação puder ser cruzada com diferentes fontes - a começar pela que é fornecida no *on boarding* pelo próprio cliente – num curto período temporal ou mesmo instantaneamente. Com a revolução digital, do *KYC* evoluiu-se para o *Know Your Data* (*KYD*) – *Data is King*[24]! A partir do momento em que as instituições de crédito possuem um crescente volume de dados que têm o dever de utilizar adequadamente – a começar pela avaliação da sua qualidade e autenticidade até à sua atualização -, as soluções tecnológicas tornaram-se cruciais. O modelo tem na automatização (*automation*) um aspeto fulcral. Os procedimentos são levados a efeito por sistemas autónomos e em que pode haver alguma intervenção humana. Entretanto, o setor tem amplo espaço para a aplicação do potencial da IA, dada a utilização de enormes bases de dados para a identificação de padrões de branqueamento e subsequente deteção de operações similares ou de novos padrões destas operações. São geralmente apontados cinco

23 Sobre o que se segue, cf. RODRIGUES, Miranda Anabela/AIRES de SOUSA, Susana, «Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal», Coordenação: Anabela Miranda Rodrigues, *A Inteligência Artificial no Direito Penal,* Vol. II, Almedina, 2022, p. 11 s (p. 16 s) e bibliografia aí citada; RODRIGUES, Miranda Anabela, «*Compliance* inteligente e prevenção e luta contra o branqueamento», *op.ult. cit.,* p. 207 s (p. 215 s).

24 ARNER, Douglas W./BARBERIS, Janos Nathan/BUCKLEY, Ross P., "The emergence of RegTech 2.0: from know your customer to know your data", *Journal of Financial Transformation,* vol. 44, 2016, p.16 s.

domínios de aplicação da IA à prevenção e luta contra o branqueamento, para além da avaliação do risco e da descoberta de padrões - a priorização de casos, a análise visual e o apoio à decisão -, em três áreas principais: prevenção, deteção e investigação.

Um outro exemplo de um mercado cada vez mais digitalizado, onde a intervenção humana é cada vez mais reduzida e delegada em algoritmos, é o mercado de capitais, onde um impressionante avanço tecnológico se faz sentir[25], com a introdução de programas algorítmicos capazes de negociar autonomamente, acelerando as transações, em número, eficiência e liquidez. Num mercado em que a informação e a velocidade das transações são elementos essenciais, a IA modificou não só a génese da informação e a velocidade a que é transmitida, como também alterou, de forma disruptiva, o próprio funcionamento dos mercados, que passou a ser «frequentado», senão dominado, por novos operadores - agentes artificiais. A colonização do mercado por estes agentes artificiais é tecnológica, com origem na potência do *hardware* e no elevado grau de sofisticação do *software* de *trading.* Os operadores algorítmicos de alta frequência caraterizam-se, então, por uma particular velocidade operativa, que os distingue dos *traders* algorítmicos identificados simplesmente por serem baseados em instruções operativas de tipo matemático. A velocidade é a pedra-de-toque da negociação algorítmica de alta frequência (*High Frequency Trading* - HFT).

É no contexto de imprevisibilidade do sistema de HFT que avulta a dimensão de *compliance* na regulação dos mercados financeiros, comportando uma série de deveres de cuidado na definição dos limites da permissibilidade do risco. A reflexão sobre os riscos de atuação dos operadores algorítmicos começou com o *flash crash* do índice *Dow Jones*, em 6 de maio de 2010, a que outros se seguiram. O risco da ocorrência deste tipo de fenómenos, que têm natureza mecânica, independente de fatores económicos reais, está associado ao modo como a negociação de alta frequência se relaciona com a informação, que não atende aos fundamentos económicos do título negociado. A correta formação dos preços nos mercados pode, assim, ser prejudicada. Encontram-se relatos do *flash crash* de 23 de abril de 2013, ocorrido nos mercados financeiros norte-americanos na sequência da notícia falsa, lançada na conta *twitter* da *associated press*, de um atentado a *Barack Obama*, em que os operadores algorítmicos processaram a notícia antes de qualquer outro operador físico, prevendo um efeito de descida nos mercados e, portanto, não só antecipando a verificação deste efeito, mas também amplificando

25 Sobre o que se segue, RODRIGUES, Anabela Miranda, «Os crimes de abuso de mercado e a 'Escada Impossível' de *Escher* (o caso do *spoofing*)», *A Inteligência Artificial no Direito Penal*, Coordenação: Anabela Miranda Rodrigues), Vol. II, Almedina, 2022, p. 245 s e bibliografia aí citada.

exponencialmente o seu alcance. Em geral, os estudos sobre o impacto desta nova forma de negociação referem, normalmente, 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. De qualquer modo, há uma polarização em torno do juízo sobre o efeito dos operadores algorítmicos, provavelmente a refletir um conhecimento ainda relativamente parco da HFT.

3. O *compliance* e o critério da efetividade

Subjacente a estes desenvolvimentos está a preocupação desde há muito manifestada, com a efetividade do *compliance*[26]. Não é de agora a denúncia de que pode utilizar-se como uma operação cosmética ou encobrir uma burocratização estéril da atividade da empresa, caraterizada mais pela prossecução do cumprimento formal de regras, de acordo com uma abordagem *tick-the-box*, do que pela atuação eficaz do seu sistema de prevenção e repressão da criminalidade[27]. Em geral, definir pela positiva o que é um *compliance* efetivo sempre foi o seu calcanhar de Aquiles. Desde logo[28], o *compliance* não se expressa em uma relação binária de cumprimento/não cumprimento, mas antes em graus de conformidade entre expetativas da regulação e esforço colocado pela entidade obrigada na satisfação dessas expetativas. O que quer dizer que a avaliação (da efetividade) do cumprimento não é nem simples nem objetiva. Depois, e em face deste cenário, as entidades obrigadas não estão motivadas para investir esforços e dinheiro adicionais em relação ao conhecimento *normal* – e em muitos casos *simplificado* – de quem interage com elas. Na verdade, não só poderão não ser avaliados pelos reguladores no esforço de obtenção de melhores resultados, como

---

26 Cf., designadamente, LAUFER, William, «Illusions of Compliance and Governance», *Corporate Governance*, Vol. 6, n.º 3, p. 239 s.

27 AMICELLE, Anthony/LAFFOLA, Vanessa, «Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing», *The British Journal of Criminology*, Vol 58, Issue 4, July 2018, 845-863 (855-857).

28 MANACORDA, Stefano, The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal World", MANACORDA, Stefano/CENTONZE, Francesco, *Corporate Compliance on a Global Scale*, Springer, 2022, p. 67 s. (p. 73). Especificamente, sobre a dificuldade da avaliação da efetividade da prevenção e luta contra o branqueamento, POL, Ronald F., «Anti-money laundering: The world's least effective policy experiment? Together, we can fix it», *Policy Design and Practice,* 2020, 3:1, p. 73 s. (p. 80); e DASSAN, Pedro, «O overcompliance na prevenção do branqueamento de capitais», em curso de publicação, *Revista Portuguesa de Ciência Criminal*.

inclusivamente apostam em que um cumprimento «medíocre» lhes pode oferecer a garantia de um cumprimento «suficiente» na avaliação dos reguladores. Para além disso – por último –, a dificuldade em densificar o critério da efetividade desencadeia um fenómeno de *overcompliance*[29], que, numa certa faceta se traduz numa prática de *over-reporting*, também conhecida por *crying wolf*[30]. O que está em causa com este fenómeno é um desfasamento entre os riscos valorados por reguladores e regulados. Os primeiros, avaliam o risco de infração e as entidades reguladas valorizam o risco de serem sancionadas por uma violação de um dever de *compliance* – a que, sublinhe-se, dão mais peso do que ao risco real e concreto de infração numa determinada situação, mais difícil e mais exigente de avaliar na prática.[31] Diga-se, de resto, que as entidades supervisoras e judiciárias fazem um juízo *ex post*, retrospetivo e, nessa medida, enviesado (*hindsight bias*) sobre a eventual violação de um dever, diferentemente do que acontece com os responsáveis de *compliance*, que fazem juízos *ex ante*, isto é, prospetivos. Como as sanções por violação de deveres de *compliance* são aplicadas no caso de não serem comunicadas informações que posteriormente se demonstrou serem suspeitas de infrações – os falsos negativos – e não no caso de comunicações de operações que posteriormente se vieram a demonstrar como lícitas – os falsos positivos -, as entidades privadas reguladas tendem a aumentar a comunicação de relatórios de atividades suspeitas para evitar sanções por falsos negativos. Ou seja, no final, esta prática traduz-se no aumento da quantidade de comunicações que são simultaneamente falsos positivos. O *over-reporting* é, ainda, alimentado pelos reguladores. E, assim, por uma cada vez maior pressão por parte destes sobre os regulados em relação à comunicação de relatórios, sem que exista uma noção clara da parte de qualquer dos lados acerca do que deve constituir a grandeza adequada das comunicações; e, ainda, por uma ausência de *feedback* daqueles (reguladores) em relação aos relatórios comunicados, que caem numa espécie de «buraco negro», por não haver retorno quanto à sua utilidade[32]. O que

---

29 Para uma aproximação ao problema do *overcompliance*, em geral, cf. MANACORDA, Stefano (nota 27), p. 73 s; e, para o domínio do branqueamento, AZEVEDO de MOURA, Miguel, «O *overcompliance* e o princípio da proporcionalidade na aplicação de normas relativas à prevenção e combate ao branqueamento de capitais e financiamento do terrorismo», *Vida Judiciária*, janeiro/fevereiro, 2020, p. 40 s (p. 40 e 41) e DASSAN, Pedro (nota 28).

30 TAKÁTS, Előd, «A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement», 2007 International Monetary Fund, IMF WP/07/81.

31 LAUFER, William S., «Corporate Liability, Risk Shifting, and the Paradox of Compliance», *Vanderbilt Law Review*, Vol 52, Issue 5, 1999, p. 1340 s (p. 1402 s).

32 MAXWELL, Winston / BERTRAND, Astrid /VAMPARYS, Xavier, «Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?», ICML *Law and Machine Learning Workshop*, 2020, *Hal -02884824v3*, p.1 s (p.19).

acontece, no final, é que o *over-reporting*, por um lado, pode ocasionar, por parte das entidades (públicas) destinatárias das informações (e comunicações) falhas na identificação das que são realmente relevantes como indicando suspeita de infração – «o que é de facto importante torna-se difuso»[33] -, desta forma associando-se ao fenómeno da captura regulatória; e, por outro lado, como reverso da moeda, gera, da parte dos regulados, a produção de uma enorme quantidade de informações (e de comunicações) que, para além de poderem ser inúteis (os falsos positivos), originam a criação de enormes bancos de informações/dados.

4. *Compliance*, *compliance* cooperativo de dupla via e *compliance* digital

A lógica do *compliance* inspira, como é reconhecido, a política criminal atual e os mais recentes quadros regulatórios de prevenção e luta contra a criminalidade económico-financeira como técnica de intervenção e de gestão de riscos. Quer seja cogente, motivada ou voluntária, rígida ou flexível, baseia-se, em qualquer caso, em sistemas de controlo interno que podem experimentar os benefícios, em termos de efetividade, da digitalização.

Para além disto, todavia. O que agora se quer sublinhar é que o *compliance digital* pode ser especialmente vantajoso, em face dos desenvolvimentos que, tendo (também) em vista a efetividade, vem conhecendo o *compliance* no sentido cooperativo de *dupla via*.[34] É isto que se observa, por referência especificamente ao fenómeno do branqueamento[35], onde a cooperação na partilha de informações entre os setores público e privado implica a necessidade de partilhar informações estratégicas e mais direcionadas, passando a centrar-se num fluxo (de informações) bidirecional, isto é, não só das entidades reguladas para as autoridades públicas reguladoras e de investigação criminal, mas também destas para as privadas. O objetivo do reforço do *compliance* mediante o duplo sentido da partilha de

33 Cf. DASSAN, Pedro (nota 28).

34 Cf. MORGANTE, Gaetana/FIORINELLI, Gaia (nota 22), p. 26, salientando, ainda, as potencialidades da digitalização face a um *compliance integrado*, ao agilizar as sinergias da interação entre os diversos sistemas de *compliance* adotados num ente coletivo e entre estes e a função de *governance*.

35 Cf. VOGEL, Benjamin, «Potentials and Limits of Public-Private Partnerships Against Money Laundering and Terrorism Financing», EUCRIM, 2022/1, p. 52 s; VOGEL, Benjamin/MAILLART, Jean-Baptiste (eds.), *National and International Anti-Money Laundering Law Developing the Architecture of Criminal Justice, Regulation and Data Protection,* Intersentia, 2020, 911 s, 924s, 930 s, 1021 s; MAXWELL, Nick, «A Survey and Policy Discussion Paper: 'Lessons in private-private financial information sharing to detect and disrupt crime'. Future of Financial Intelligence Sharing (FFIS) research programme», 2022, p. 26 s.

informações é capacitar o setor privado para o melhor cumprimento dos seus deveres de *compliance* para prevenir a circulação e descobrir ativos provenientes da prática de crimes e, dessa forma, favorecer a efetividade do *compliance*. Está em causa promover a *qualidade* da informação partilhada, sem simultaneamente negligenciar a sua *quantidade*,[36] capacitando, por sua vez, o setor público para o seu eficaz aproveitamento.

Importa acentuar que a expansão e o apertar da malha da rede do *compliance* – favorecendo, de resto, o florescimento de uma *indústria do compliance*[37] –, que privilegia, apenas, a consagração de cada vez mais deveres de *compliance* para um número cada vez maior de entidades obrigadas – ou alimenta, inclusivamente, um aspeto ligado ao *compliance* que é a tentação de fazer recair sobre os particulares, feitos «bodes expiatórios» do fracasso dos sistemas de controlo, as responsabilidades, administrativas (ou contraordenacionais) e mesmo penais, quando um caso de fraude ocorre -, não tem trazido, mesmo na sua feição digital, os ganhos de efetividade pretendidos. Estudos efetuados no domínio da prevenção e luta contra o branqueamento demonstram que, se a informação produzida pelas entidades reguladas desencadeou, inicialmente, um efeito de aumento exponencial de comunicações de operações suspeitas, com elevada percentagem de investigações efetuadas na sua base, seguiu-se, todavia, um aparente decréscimo de eficácia (utilidade) da informação fornecida e armazenada, mesmo em face do número total crescente de comunicações que a digitalização propiciou. Isto tem a ver com a persistente desadequação de dados, em quantidade e qualidade, que criam problemas à sua análise, também por sistemas autónomos e inteligentes,[38] suscitando especial atenção.

---

36 Assim, é fácil entender que, no caso em que a informação partilhada pode acrescentar valor às investigações criminais, a sua qualidade é de particular importância e, portanto, a principal preocupação do sistema é reduzir os falsos positivos. Já se a sanidade do sistema (económico-) financeiro é enfatizada pelo modelo de prevenção e luta contra o branqueamento, uma regulação que suscite um elevado número de informações (a quantidade) é positivamente valorada, na medida em que pode fornecer uma imagem mais nítida das situações de risco potencial de práticas de branqueamento e, deste modo, melhorar a capacidade de análise do apetite de risco das entidades obrigadas individualmente consideradas e, consequentemente, de identificação de operações ou negócios de risco elevado.

37 Cf., designadamente, BLANCO CORDERO, Isidoro, «Eficacia del sistema de prevención del blanqueo de capitales: estudio del cumplimiento normativo (compliance) desde una perspectiva criminológica», *Eguzkilore: cuaderno del Instituto Vasco de Criminologia,* 23, 2009, p.123 s.

38 Cf. AGAPITO, Leonardo Simões/MIRANDA, Matheus de Alencar/JANUÁRIO, Túlio Felippe Xavier, «On the Potentialities and Limitations of Autonomous Systems in Money Laudering Control», *Révue International de Droit Pénal,* Gert Vermeulen, Nina Persak and Nicola Recchia (Eds.), *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, Vol. 92 issue 1, 2021, p. 87 s (p. 93 s), para o sistema financeiro brasileiro.

Aqui chegados, é particularmente importante acentuar como a qualidade da informação é um dos principais desafios colocados à efetividade da regulação concebida de acordo com um princípio de *compliance*. Com efeito, se a efetividade do modelo se joga hoje no tabuleiro do desenvolvimento tecnológico e de sistemas de IA, ela não pode perder de vista o melhoramento e reforço do *compliance* que implica ter em conta, por um lado, a interdependência entre a regulação assim concebida e informação – sem informação que a regulação torna disponível não há resultados – e sua qualidade e, de outro lado, a relação de confiança entre reguladores e regulados em que assenta, quanto a informações prestadas por estes àqueles, que devem alimentar uma base de dados confiável. Pelo lado do setor privado, isto significa contrariar práticas de *over-reporting* e de informação maliciosa ou enviesamento de informação e um compromisso com o cumprimento não meramente formal de deveres de *compliance* e, do lado do setor público, uma cooperação pró-ativa com o setor privado, que tem em vista apoiar as entidades privadas e – fundamentalmente – fornecer-lhes informações que possam responder às dificuldades experimentadas e auxiliá-las no cumprimento dos deveres de *compliance*. Trata-se de uma compreensão do *compliance* que, por sua vez, acentuando a efetividade, beneficia da digitalização, não só do setor privado, mas também pelo que se refere ao setor público, exatamente na medida em que as autoridades públicas estabelecem uma relação de cooperação dinâmica e continuada – pró-ativa – e não de mera vigilância com as entidades privadas na atuação do controlo interno. Está em causa melhorar e potenciar a atividade de controlo das entidades públicas na relação que instituem com o setor privado, por forma a alcançarem um desempenho positivo e contrariarem a captura regulatória a que estão sujeitas por parte do setor privado. Designadamente, colocando ao seu serviço a tecnologia, nas suas manifestações mais evoluídas, para acompanhar e responder aos correspondentes e prodigiosos avanços desse cariz que experimentou e experimenta quotidianamente o sistema financeiro[39] e, além disso e simultaneamente, criando um melhor ambiente para a utilização de IA, tendo em vista evitar o enviesamento de dados e melhorar a sua qualidade. Isto pode ser feito através de auditorias proactivas por parte dos reguladores[40]. As inspeções *in loco* - mediante o livre acesso de agentes públicos a computadores e arquivos físicos da entidade e o contato direto com os trabalhadores -, sendo um

---

39 Cf. *PERRONE, Andrea, «La nuova vigilanza. RegTech e capitale umano», Banca Borsa e Titoli di Credito, IV, 2020, p. 516 s (p. 526), apontando para «uma evolução da relação entre vigilância e RegTech num sentido marcadamente cooperativo»; referindo-se a um «paradigma de vigilância cooperativa data-driven» (com referências bibliográficas),* MORGANTE, Gaetana/FIORINELLI, Gaia (nota 22), p. 26.

40 Sobre as vantagens e os inconvenientes das auditorias proactivas, cf. AGAPITO, Leonardo Simões/MIRANDA, Matheus de Alencar/JANUÁRIO, Túlio Felippe Xavier (nota 37), p. 100.

método relativamente simples, podem ter efeitos positivos ao nível da fiabilidade dos dados, ao passarem pela «materialização» institucional e a «colaboração» dos empregados. Designadamente, estes podem sentir-se mais seguros para colaborar desta forma do que através dos canais formais instituídos. Uma outra forma de verificação de qualidade dos dados é a experimentação *sandbox*. As *regulatory sandboxes* são já usadas por entidades financeiras, designadamente UIF's, para desenvolver respostas regulatórias adequadas a novos utensílios tecnológicos no âmbito financeiro. Uma abordagem *sandbox* (*sandbox approach*) permite avaliar dados concretos produzidos, tendo em vista conhecer o seu potencial, vulnerabilidades e oportunidades; e, assim, eventualmente validar os sistemas institucionais de controlo ou a mineração de dados. Em geral, este tipo de abordagem tem a colaboração das entidades financeiras, que, em troca, recebem uma certificação das UIFs. Além disso. No âmbito da prevenção e luta contra o branqueamento, designadamente, o desenvolvimento de um *compliance inteligente* exige, para que os dados sejam cruzados com êxito, a sua «maturação» pelas entidades bancárias, mediante a verificação das operações, de acordo com um sistema complexo de condições e caraterísticas. Importante é, também, de acordo com *Zengan Gao* e *Mao Ye*[41], que as informações prestadas sejam baseadas em «casos», tendo em conta que o branqueamento não é uma operação isolada e envolve uma complexa cadeia de trocas, devendo ser utilizada uma técnica de mineração de dados que pode somar informações de clientes, contas, produtos, tempo e geografia por análise de vetores. A verificação de condições deste tipo é essencial à qualidade dos bancos de dados construídos, propiciando a sua melhor utilização por sistemas autónomos e de IA.

5. O *compliance* – sombras sobre o *compliance* digital

A transição digital económico-financeira e dos seus atores está em curso. Não é novidade, no contexto empresarial e industrial, a automatização dos processos produtivos. A introdução de novas tecnologias, seja pela via de máquinas robotizadas, pela digitalização de serviços de controlo de qualidade ou ainda pela monitorização de circuitos produtivos e dos trabalhadores, integra, desde há largos anos, a realidade empresarial. Entre os benefícios imediatamente identificáveis e comummente apontados estão a diminuição de custos, designadamente ao permitir reduzir substancialmente o erro humano, e o aumento da produtividade, através da definição de estratégias empresariais de risco previsível. O algoritmo oferece

41 GAO, Zengan/YE, Mao, «A Framework for data mining-based anti-money laundering research», *Journal of Money Laudering Control*, Vol.10, n.º 2, 2007, p. 170 s (p. 171).

a vantagem de determinar previamente graus de risco, e, com isso, é a própria gestão do risco que se transfere para sistemas autónomos e de IA. Que, agora, acrescentam às capacidades descritiva e de previsão, há muito reconhecidas aos sistemas computadorizados, as capacidades preditiva e prescritiva.

Do mesmo passo, numa economia globalizada, as políticas económico-financeiras seguidas pelos decisores políticos não são indiferentes a esta transformação. A "transição digital" constitui, aos vários níveis, internacional, europeu e nacional, um tópico de grande relevância no discurso político, preocupado com o difícil equilíbrio regulatório exigido por uma *global AI race*. O processo de transição digital projeta-se no plano jurídico e suscita atenção em vários planos.

O contexto do *compliance* é expressivo do que está em causa. Neste campo, as soluções com base em sistemas de IA apresentam, para regulados e reguladores, diversas vantagens, não surpreendendo, por isso, o elevado investimento em formas de *compliance* "inteligente" nos vários domínios económico-financeiros. Entre benefícios presentes e promessas de benefícios futuros, compreende-se e explica-se o processo de digitalização de serviços e de atividades empresariais em alguns setores – como o setor bancário ou na área financeira – já ocorrido ou em vias de se realizar, a vários ritmos, em conformidade com a especificidade de mercados, dimensão das empresas ou o seu âmbito geográfico de atuação.

De qualquer modo, a promessa de efetividade do *compliance* digital não se concretiza 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. Um sistema automatizado e inteligente de regulação económico-financeira de *compliance* 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.

Outras questões estão, todavia, para além disto.

O processo de digitalização empresarial tem uma 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 ou colocação em perigo de bens jurídicos, também penais, por decisão do algoritmo em contexto empresarial ou, ainda, do uso de técnicas agressivas de monitorização da atividade empresarial, do tratamento de dados privados recolhidos pela empresa ou da utilização de informação armazenada ou criada pelo sistema para fins penais – para só enunciar alguns problemas.

No primeiro caso, os desafios colocam-se face a questões de atribuição e de exclusão da responsabilidade em contexto empresarial, quer a pessoas

coletivas quer a pessoas físicas (humanas)[42]. A digitalização empresarial e, de modo particular, a introdução de algoritmos "inteligentes", tecnologicamente complexos, capazes de autonomamente fazerem opções qualificáveis como ilícitas ou criminosas, mas que não foram pré-programados nesse sentido ou sequer tais decisões eram previsíveis para o programador (*cognitive robots*), coloca à prova os tradicionais modelos de imputação, vicarial ou autónomo, de responsabilidade jurídica. A novidade está então no facto de a máquina ser programada para aprender, chegando a um resultado novo que é, num certo sentido, seu. 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. Antes, o algoritmo, alimentado com dados, ajusta-se continuamente, por forma a diminuir o erro e criar a sua própria decisão. É esta natureza dinâmica da máquina – que alguns qualificam como autonomia - que desafia a responsabilidade das pessoas, que estão por detrás da máquina, sejam naturais sejam jurídicas. A preferência por um modelo de responsabilidade direta autónoma da pessoa coletiva, assente numa deficiente auto-organização da pessoa coletiva que impede o controlo de um risco que era *ab initio* previsível, porque ligado à sua organização, não resiste inteiramente às dificuldades, que persistem, 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 atribuir a responsabilidade ao ente coletivo por não evitar um risco que não podia conhecer.

Ligado a esta dificuldade, um feixe de problemas emerge. Assim, em ordenamentos jurídicos que consagrem modelos em que a imputação do facto criminoso à pessoa coletiva 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 melhorar, como vimos, a resposta da entidade coletiva ao cumprimento de deveres de *compliance* e, assim, para excluir ou atenuar a sua responsabilidade, em situações de ofensa a bens

42 A este respeito, cf. RODRIGUES, Miranda Anabela, «A Empresa Inteligente o os seus Crimes – onde está o Responsável?», *Livro de Homenagem ao Professor Augusto Teixeira Garcia*, em curso de publicação.

juridicamente protegidos, facilitando, desde logo, a prova de que se auto-organizou para cumprir o direito. Da sua perspetiva, 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, aproxima a sua atividade de um (estrito) cumprimento normativo, apto a exclui-la de qualquer responsabilidade, ou, em certos casos, de a atenuar. Contudo, o sistema inteligente de *compliance* terá um custo elevado, pelos direitos fundamentais que sacrifica. Representa, também, num contexto coletivo complexo que envolve humanos e não humanos, uma ferramenta que permite uma ampla recolha de elementos capazes de esclarecer as circunstâncias e as causas das ofensas a bens jurídicos e, com isso, facilita a deteção e a atribuição das falhas ocorridas. Com efeito, a digitalização potencia uma maior eficácia na deteção, na investigação e na consequente responsabilização da pessoa humana que, na entidade coletiva, 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 ilícito ou criminoso. E, com isso, transfere-se para aquela conduta individual, identificada e indicada pelo algoritmo, uma *presunção de responsabilidade*. Sob a forma de contínua monitorização dos trabalhadores, a digitalização promove uma dupla transferência de responsabilidade, da pessoa coletiva para as pessoas individuais, e, entre estas, dos administradores e diretores para os quadros intermédios ou mais baixos de uma organização empresarial (*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». No âmbito penal, este aspeto prende-se com o princípio da presunção de inocência. A "fotografia" do erro alivia a empresa e sobrecarrega a defesa do trabalhador. O algoritmo permite que uma empresa, por exemplo, 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. Em última análise, toca-se aqui o fenómeno conhecido da *criminalização do compliance*[43]. Que, de uma certa perspetiva, se analisa no endurecimento dos programas de *compliance*, concretizado na implementação de mecanismos cada vez mais 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 coletiva que se transforma em um *direito de compliance de natureza privada,* menos societário e mais punitivo – um *novo direito quase-penal e intrinsecamente privado*. Para além disso,

43 Assim cunhado por HAUGH, Todd, «The Criminalization of Compliance, *Notre Dame Law Review*, Vol.92, 2017, p. 1215 s.

assiste-se à crescente configuração como crime de muitas violações de deveres de *compliance* a concorrer para a descaraterização dos programas de *compliance* como instrumentos de socialização.

Além disto e como se referiu, não devem, ainda, perder-se de vista dois domínios particularmente sensíveis: um, em matéria de proteção de dados pessoais; o outro, contende com os direitos de arguidos em processos penais.

Pelo que diz respeito ao tratamento de dados pessoais[44] por parte das entidades obrigadas e por entidades públicas, tendo em conta que pode dar origem a processos penais, é conveniente ter em conta que, com a digitalização crescente, os dados fornecem informações cada vez mais detalhadas sobre a vida pessoal e quaisquer atividades dos cidadãos. Acrescente-se que, pelo que se refere a instituições financeiras, por exemplo, estas utilizam diferentes mecanismos de mineração de dados para conhecer os seus clientes e, neste contexto «tecnológico», encorajadas pelos reguladores - configurando um procedimento de *gold plating* -, podem conhecer os seus clientes muito para além do que lhes é legalmente exigido. O princípio da proporcionalidade assume aqui um papel fulcral, implicando um equilíbrio entre a necessidade de limitações de direitos das pessoas à privacidade e de direitos sobre os dados pessoais e a realização do objetivo tido em vista com a recolha e o tratamento de informações. Assim, designadamente, quando são criados perfis de risco, os perigos da categorização das pessoas verificam-se, na medida em que as expõem à estigmatização em atividades comerciais - e, por aqui, à violação de princípios da igualdade e da não discriminação - e à possibilidade de serem sujeitas a medidas repressivas. Deste modo, ocorrendo, no exercício da atividade do coletivo, um facto com relevância criminal, por exemplo, um pagamento indevido ligado a um ato de corrupção ou uma manipulação defeituosa de produto ou, ainda, uma alteração de contas societárias, coloca-se a questão de saber em que termos se pode aproveitar a informação acumulada pelos algoritmos. A digitalização na empresa cria um novo fluxo informacional, um banco de dados útil ao esclarecimento do acontecimento criminoso, cabendo indagar do seu aproveitamento probatório no processo penal. O algoritmo transforma-se num meio de obtenção da prova, de criação privada, gerando-se um conjunto de questões ligadas ao seu enquadramento processual e ao exercício do contraditório e do direito de defesa.[45] De facto, a digitalização,

---

44 Cf. RODRIGUES, Miranda Anabela (nota 23), p. 223 s; VOGEL, Benjamin (nota 35), p. 56 s.

45 Sobre a utilização das novas realizações tecnológicas como prova digital e o perigo que representa para alguns direitos fundamentais, em geral, cf., FIDALGO, Sónia, «A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo», *A Inteligência Artificial no Direito Penal*, Coordenação: Anabela Miranda Rodrigues, Almedina, 2020, p. 137.

associada a um discurso de controlo na prevenção da criminalidade em contextos coletivos, potencia a imolação de direitos fundamentais, de trabalhadores, mas não só, tais como o direito à imagem, à palavra ou à intimidade da vida provada, para só referir alguns exemplos, obnubilando entre as suas vantagens um custo elevado, quase invisível, porém irreversível. Cabendo assinalar que, do lado do aproveitamento probatório destas informações para fins de responsabilidade criminal, no ordenamento jurídico português há que perspetivar os limites à sua validade, resultantes da Constituição (Artigo 32.º, n.º 8) e do Código de Processo Penal (Artigo 126.º). Sendo que a questão da limitação de direitos fundamentais que se pode verificar recrudesce, na medida em que as autoridades judiciárias públicas poderão efetivamente controlar (o tratamento d)os bancos de informações/dados das entidades obrigadas e de entidades públicas de controlo, como as Unidades de Informação Financeira (UIF's).

Já particulares preocupações são suscitadas pela partilha de informações quando a circulação da informação se faz a partir das autoridades de investigação criminal para entidades obrigadas, com o objetivo de estas controlarem as operações/transações/atividades de suspeitos sob investigação criminal. A atividade de *due diligence* em relação aos seus clientes levada a efeito pelas entidades obrigadas *transforma-se,* desta forma, em atividade de vigilância e produz inteligência financeira. As questões aqui implicadas vão para além da proporcionalidade[46]. Desde logo, na medida em que as informações obtidas no âmbito da *due diligence*, fora do processo penal, têm em vista ser partilhadas em processos penais em curso, sem que, todavia, a atividade que esteve na origem da produção/obtenção destas informações se tenha submetido aos princípios e às regras processuais penais, por exemplo, a emissão de uma autorização judicial. O risco de violação de direitos de defesa das pessoas envolvidas no processo penal torna-se manifesto, tanto mais evidente se se pensar na regra de proibição de divulgação de comunicações entre entidades obrigadas e entidades públicas de controlo, designadamente UIF's[47], que não permite, em geral, aos visados, agora arguidos em processos penais, entender como foram produzidas contra si certas provas incriminatórias. Há que equacionar, em última análise, a i/legitimidade de uma «im/possível» restrição ao princípio *nemo tenetur se ipsum accusare* de

46 Cf. *European Data Protection Supervisor. Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing*, n.º 44.

47 Cf. Artigo 39.º, n.º 1, Diretiva 2015/849, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo.

que gozam os arguidos em processo penal[48]. Além do mais, na medida em que um circuito de dupla via - que induz uma entidade privada a obter informações sobre as atividades de um cliente no decurso de um processo penal contra ele, eventualmente solicitando-lhas diretamente – pode colocar a entidade privada na condição de um «agente encoberto» das autoridades de investigação, sem que a sua atuação esteja enquadrada legalmente, e que pode, assim, atuar sem controlo judicial ou outro de natureza independente.

6. O *compliance* digital entre luzes e sombras (o fim do paradigma do direito penal repressivo?)

A revolução digital do *compliance* tem a ver com a efetividade que ele pode trazer à aplicação dos programas de *compliance*, em comparação com as tradicionais modalidades humanas, analógicas, de gestão e controlo das entidades coletivas, designadamente empresariais. O contributo do digital para a prevenção de ilícitos e de crimes faz-se sentir, como já vimos, na medida em que a tecnologia é utilizada como instrumento de monitorização, controlo e identificação, em tempo real, de sinais de alarme, anomalias e potenciais violações de deveres de compliance. Neste contexto, para ilícitos e crimes em que a conformidade/não conformidade possa ser codificada em termos numéricos, como é o caso quando se utilizam valores-limite, verificações de património ou quantificação de fluxos financeiros, as novas tecnologias permitem auxiliar ou substituir as tradicionais funções de controlo interno. Os domínios, onde, desta perspetiva, pode ser utilizada digitalização do compliance são os mais diversos e vão desde o ambiental, do branqueamento, da corrupção, dos mercados financeiros ou da prevenção do risco de insolvência empresarial. Sublinha-se[49] como esta *smart data analytics* significa, para o *compliance* das entidades coletivas, passar de uma abordagem «estático-reativa» para um seu funcionamento «dinâmico-preventivo», permitindo uma intervenção antes do efetivo cometimento do ilícito ou do crime. Outra forma de contribuir para a prevenção de ilícitos e de crimes que o digital aplicado ao *compliance* permite tem a ver com o rastreio e registo contínuos que possibilita de todas as operações e fluxos de informação, criando uma espécie de

48 Sobre a questão aqui implicada, ANDRADE, Manuel Costa, «*Nemo tennetur se ipsum accusare* e direito tributário. Ou a insustentável indolência de um acórdão (n.º 340/2013) do Tribunal Constitucional», *Revista de Legislação e Jurisprudência*, Ano 144.º, n.º 3989, 2014, p.121 s.

49 BURCHARD, Christoph, «Digital Criminal Compliance», *Festschrift fur Ulrich Sieber zum 70. Geburtstag*, Herausgegeben von Marc Engelhart, Hans Kudlich und Benjamin Vogel, Teilband I, Duncker & Humblot, Berlin, 2021, p. 741 s (p. 746).

«caixa negra», não só da atividade da pessoa coletiva, mas também do sistema de *compliance*. Esta utilização do digital facilita a demonstração e a prova em tribunal do efetivo funcionamento do *compliance*, não deixando, todavia, de se salientar[50] como o *compliance* digital não está, por sua vez, imune a vícios ou a possíveis «erros/fugas fraudulento(a)s», podendo, por exemplo, os *intranei* beneficiar das «debilidades» do sistema digital (*oracle attacks*). Finalmente, a utilização de instrumentos de *compliance* digital para «desenhar estruturas de comportamentos» humanos e, assim, potencialmente prevenir em tempo real eventuais violações de deveres, para além de enfrentar a crítica da precariedade das generalizações preditivas sobre o comportamento desviante do membro da organização coletiva[51], pode permitir uma prevenção *direta* de ilícitos e de crimes à custa de formas de vigilância (direta) sobre pessoas concretas que trabalham na organização. A introdução da tecnologia em contexto coletivo 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, mas, pelo que agora queremos destacar, dos trabalhadores, em distintos momentos e com distintas finalidades: contratação, evolução e avaliação do seu desempenho, cumprimento das obrigações laborais e manutenção da sua segurança. Ao mesmo tempo que alguns destes instrumentos 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, todavia, 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.

Uma primeira questão que se coloca toca a própria legitimidade do *compliance* digital, em face do uso de instrumentos de polícia preditiva (*predictive policing*) no âmbito de prerrogativas de autotutela preventiva por parte de entidades privadas. Que transformam o local de trabalho num *digital work place* a que já nos referimos e vão para além do controlo interno da entidade coletiva enquanto tal e permitem a monitorização eletrónica do desempenho dos trabalhadores. Exige-se, assim, a definição de limites, em face dos poderes de investigação agora disponíveis dos empregadores, procurando o equilíbrio entre razões *compliance* e direitos fundamentais das pessoas visadas. A questão passa por equacionar quais são as novas exigências de proteção que derivam especificamente da digitalização

50 BURCHARD, Christoph (nota 49), p.750.

51 Cf. CENTONZE, Francesco, « The Imperfect Science: Structural Limits of Corporate Compliance and Co-regulation», *Corporate Compliance on a Global Scale: Legitimacy and Effectiveness*, S. Manacorda, F. Centonze, co-eds., Springer, 2021, p. 45 s (p. 50).

do *compliance*. E pode conter-se no âmbito de uma taxinomia dos controlos baseada numa teoria de círculos concêntricos[52], que, em termos invasivos, parte do anel mais externo como o menos invasivo, relativo, por exemplo, ao controlo das comunicações dos trabalhadores, passando pelo círculo intermédio, em que aqueles são monitorizados diretamente, em tempo real, até ao círculo interno – o mais problemático -, onde os sistemas de *compliance* digital podem compreender uma espécie de polícia preditiva (*predictive policing*) privada e pessoal, que integra e potencia o modelo organizacional com uma valoração preventiva e preditiva do risco individual de cometimento de violações do modelo e de crimes[53]. Isto representa um salto conceitual, na medida em que se *individualiza* o risco a gerir, que não tem apenas a ver com a atividade do ente coletivo, mas reside sobretudo no trabalhador individualmente considerado, que se constitui ele próprio como fator de risco. Identifica-se, aqui, um «desvio» para um «paradigma de desconfiança» no interior do contexto coletivo[54].

Uma segunda questão prende-se com o facto de que a digitalização do *compliance* não acrescenta nada da perspetiva da *produção* de regras, mas sim da sua *aplicação*. Com efeito, a codificação, em sentido digital, de uma norma jurídica e a automatização da sua aplicação, em certo sentido, acabam por alterar a relação entre a realidade e o direito. Observa-se[55], de forma acutilante, que a norma, num contexto de *regulation by code*, não retira a sua eficácia da ameaça com as consequências previstas – multas ou privação de liberdade –, mas, antes, de uma espécie de «restrição física» (*physical constraint*).: «*the rule is applied to an individual through a kind of physics»,* um *«physical constraint*». Como já evidenciámos a outros propósitos, com apoio em *Garapon* e *Lassègue*[56]*,* estamos perante uma «transformação interna da normatividade», onde ressalta a diferença entre a simbolização do direito, que se realiza através da «escrita alfabética, a qualificação jurídica e o ritual», e a digitalização, vale por dizer, a codificação do real mediante a «escrita digital». Assim, no contexto de um modelo de organização

52 Cf. MORGANTE, Gaetana/FIORINELLI, Gaia (nota 22), p. 29 s.

53 Cf. BURCHARD, Christoph (nota 49), p. 748.

54 Cf. BURCHARD, Christoph (nota 48), p. 751.

55 Cf. LESSIG, Lawrence, *Code version 2.0*, New York, 2006, p. 81s e 120 s («*the rule is applied to an individual through a kind of physics»,* a *«physical constraint*»). Vide, também, BURCHARD, Christoph, «Artificial Intelligence as the End of Criminal Law? On the Algorithmic Transformation of Society», *Artificial Intelligence in the Economic Sector. Prevention and Responsibility*, Editors: Maria João Antunes/Susana Aires de Sousa, Instituto Jurídico da Universidade de Coimbra, 2022, p. 165 s (p. 191s).

56 Cf. RODRIGUES, Anabela Miranda, «Justiça Penal e Inteligência Artificial – a (nossa) opção entre uma justiça *fitness* e uma justiça *fair*», *Estudos em Homenagem ao Professor Doutor Fernando Alves Correia*, Vol. I, Almedina, 2023, p. XXX.

digital, a atuação conforme ao direito torna-se ela própria *a única realidade possível*, exatamente em virtude da capacidade do digital de «internalizar» a regra e de a tornar, ao mesmo tempo, *imediatamente* e *inevitavelmente* executiva. Desta forma, evidencia-se como o *compliance* digital torna esfumados os limites entre prevenção e repressão[57], atuando coativamente sobre os comportamentos, não sequencialmente e, portanto, de uma perspetiva repressiva, mas antes de um ponto de vista preventivo. Um modelo de *self enforcement* digital pode revelar-se perversa e perniciosamente inflexível, até ao ponto de se tornar ele próprio um fator de risco.

Em última análise, a transição digital do *compliance* assume um significado mais profundo, que vai para além do âmbito limitado do *compliance*, revelando uma mudança de paradigma na abordagem estadual do controlo do crime de sentido securitário. Está em causa, em termos de legitimação e eficácia, o clássico modelo repressivo até agora estabelecido, baseado na prevenção através da ameaça da aplicação de penas (modelo de *prevenção indireta*). Mediante a «conformação tecnológica» dos comportamentos, permite-se a constante e difusa vigilância das pessoas e um modo de prevenção de atividades ilícitas ou criminosas por parte destas, que, progressivamente, substitui o modelo repressivo de *prevenção indireta* por um modelo de *prevenção direta*, que busca o controlo total dos comportamentos e a eficácia plena da regulação, também penal.

Uma estratégia securitária de controlo da criminalidade tem conhecido uma implantação progressiva nas nossas sociedades do medo. As razões profundas e as causas desta alteração são múltiplas. Estamos num tempo em que «governar» já não significa garantir a segurança, mas gerir perigos e riscos. Este processo – à semelhança do que é descrito por *Shoshana Zuboff* como um projeto global de modificação do comportamento que ameaça transformar a natureza humana no século XXI[58] - não pode ser visto unicamente pelas lentes dos penalistas. Na era *compliance* e da inteligência artificial, os caminhos da política criminal são sinuosos. É tentador deslizar para o aumento e a mecanização do controlo. À função socializadora e de responsabilidade do *compliance* contrapõe-se um modelo de vigilância, em que a imagem é a de um Arquiteto Digital Omnipresente – de novo, *Zuboff*.

É a política – não é à governança ou à tecnologia –, no caso, a orientação política criminal em que estas se inscrevem que é responsável por criar um direito e um sistema de justiça penais de controlo e securitário. Transformar este

---

57 Cf. BURCHARD, Christoph (nota 55), p. 184 s.

58 Cf. ZUBOFF, Shoshana, *A Era do Capitalismo da Vigilância. A Disputa por um Futuro Humano na Nova Fronteira do Poder*, Relógio D'Água, 2019, passim, que se refere à ameaça de um «arquitecto digital omnipresente» na sociedade do século XXI.

sistema e esta justiça é uma tarefa política. Com orientação e poder políticos[59], o *compliance*, que abre caminho a uma sociedade de vigilância que nos exige, «qual gato doméstico, precisão de movimentos por entre cristais»[60] para garantir o controlo em que nos compromete, pode ter um contraponto num *compliance*, também digital, de feição ética, com uma dimensão de responsabilidade social que deve impregnar a ação coletiva.

59 Cf. OLIVEIRA, José Carlos/AGAPITO, Leonardo Simões/MIRANDA, Matheus de Alencar, «O modelo de 'autorregulação regulada' e a teoria da captura: obstáculos à efetividade no combate à lavagem de dinheiro no Brasil», *Questio Iuris*, vol. 10, n.º 1, Rio de Jnaeiro, 2017, p. 365 s (p. 130), que se referem à ação de *policymakers* por contraposição à dos *stakeholders*.

60 A imagem é de ZAFFARONI, Eugenio Raúl, *El enemigo en el derecho penal*, Editorial Ibáñez y la Universidad Santo Tomás, Bogotá, 2006, p. 56 s.