COMPLIANCE DIGITAL: TRANSPARÊNCIA E CONFORMIDADE ALÉM DE DATA LEX; UM CAMINHO PREVENTIVO DE SOLUÇÃO DE CONFLITOS

Digital compliance: Transparency and compliance beyond data lex; a preventive way to resolve conflicts

Patrícia Cardoso Dias[1]

Universidade Autónoma de Lisboa "Luís de Camões"

Catarina Jerez Gomes Farran[2]

Universidade Autónoma de Lisboa "Luís de Camões"

DOI: https://doi.org//10.62140/PDCF3552024

Sumário: 1.Law Enforcement e Compliance: Redundância ou complementaridade; 2.Digital compliance programs como projetos éticos com dupla finalidade: cumprimento normativo e cumprimento normalizado voluntário; 3.Compliance Digital; 4.O RGPD como ato jurídico compliance friendly; 4.1.Princípio da responsabilidade ou accountability; 4.2.Privacy by design e by default; 4.3.Registo de atividades de tratamento de dados pessoais e notificação de violação de dados pessoais; 4.4.Códigos de conduta e certificação; Considerações finais a respeito a metodologia de solução de conflitos e o compliance digital

Resumo: A expressão jurídica original do termo *compliance* significa «*the fact of obeying a particular law or rule, or of acting according to an agreement*»[3], ou seja, numa tradução prática e despretensiosa para o português do verbo "*to comply*", trata-se de estar em conformidade e fazer cumprir normas e regulamentos, internos e externos, que se impõem às atividades das organizações públicas ou privadas[4].

É uma expressão que progressivamente se tornou indissociável da já conhecida "*law enforcement*" (aplicação efetiva do Direito), por um lado em virtude de nenhuma lei garantir por si só a sua boa aplicação e por outro lado da crescente perceção das organizações em relação à necessidade de adotarem objetivos éticos e de boas práticas internas de forma a reduzirem os riscos inerentes à prossecução das suas atividades a um mínimo razoável que não comprometa as suas atividades e

[1] Patrícia Cardoso Dias – Professora Assistente Convidada na Universidade Autónoma de Lisboa " Luís de Camões", Investigadora do Ratio Legis [Projeto: Cultura de Paz e Democracia]; L.L.M. Universidade Autónoma de Lisboa "Luís de Camões"; Investigadora do CIDEP – Centro de Investigação Baiano sobre Direito, Educação e Políticas Públicas, vinculado ao PPGD/UniFG; Professora Convidada no ISPA – Instituto Superior de Psicologia Aplicada, Ciência ID: DE1B-C26C-6EA3; ORCID ID: 0000-0002-8564-8839, padias@autonoma.pt

[2] Catarina Gomes Jerez Farran: Finalista 2023/2034 do curso de licenciatura em Direito da Universidade Autónoma de Lisboa "Luís de Camões"

[3] CAMBRIDGE Dictionary – **Dictionary.** [Em linha]. Disponível em https://dictionary.cambridge.org/dictionary/english/comply.

[4] Cláudio Carneiro distingue no emprego material dos programas de conformidade o *Compliance* no contexto das pessoas coletivas de direito privado e Integridade no contexto das pessoas coletivas de direito público. Cfr. CARNEIRO, Claúdio – A Era do *Compliance* no Século XXI. In ***Compliance*: Perspetivas e Novas Dinâmicas**. P. 21; CARNEIRO, Cláudio; SANTOS JÚNIOR, Milton de Castro – **Gestão de Riscos em Compliance.** P. 2 Introdução.

que assegure uma estratégia competitiva de mercado através de sistemas de controlo efetivo interno.

O *compliance* emerge, enquanto atividade que visa mitigar os riscos de incumprimento legal e regulamentar do exercício das atividades empresariais, intrinsecamente associado ao desenvolvimento de uma consciência ética da pessoa coletiva como instrumento ao serviço da sociedade em que se insere e que a ultrapassa.

Palavras-chave: *Compliance*, Resolução de Conflitos; Programas de Conformidade; *Accountability*

Abstract: The original legal expression of the term compliance means «the fact of obeying a particular law or rule, or of acting in accordance with an agreement», that is, in a practical and unpretentious translation into Portuguese of the verb "to comply", it is about comply with and enforce internal and external rules and regulations that apply to the activities of public or private organizations.

It is an expression that has progressively become inseparable from the already known "law enforcement" (effective application of the Law), on the one hand due to the fact that no law alone guarantees its good application and on the other hand due to the growing perception of organizations in relation to need to adopt ethical objectives and good internal practices in order to reduce the risks inherent in the pursuit of their activities to a reasonable minimum that does not compromise their activities and that ensures a competitive market strategy through effective internal control systems.

Compliance emerges, as an activity that aims to mitigate the risks of legal and regulatory non-compliance in the exercise of business activities, intrinsically associated with the development of an ethical awareness of the legal person as an instrument at the service of the society in which it operates and beyond it.

Keywords: Compliance, Conflict Resolution; Compliance Programs; Accountability

1. ***Law Enforcement*** **e** ***Compliance*****: Redundância ou complementaridade**

A expressão jurídica original do termo *compliance* significa «*the fact of obeying a particular law or rule, or of acting according to an agreement*»[5], ou seja, numa tradução prática e despretensiosa para o português do verbo "*to comply*", trata-se de estar em conformidade e fazer cumprir normas e regulamentos, internos e externos, que se impõem às atividades das organizações públicas ou privadas[6].

É uma expressão que progressivamente se tornou indissociável da já conhecida "*law enforcement"* (aplicação efetiva do Direito), por um lado em virtude de nenhuma lei garantir por si só a sua boa aplicação e por outro lado da crescente perceção das organizações em relação à

[5] CAMBRIDGE Dictionary – **Dictionary.** [Em linha]. Disponível em https://dictionary.cambridge.org/dictionary/english/comply.

[6] Cláudio Carneiro distingue no emprego material dos programas de conformidade o *Compliance* no contexto das pessoas coletivas de direito privado e Integridade no contexto das pessoas coletivas de direito público. Cfr. CARNEIRO, Claúdio – A Era do *Compliance* no Século XXI. In ***Compliance*****: Perspetivas e Novas Dinâmicas**. P. 21; CARNEIRO, Cláudio; SANTOS JÚNIOR, Milton de Castro – **Gestão de Riscos em Compliance.** P. 2 Introdução.

necessidade de adotarem objetivos éticos e de boas práticas internas de forma a reduzirem os riscos inerentes à prossecução das suas atividades a um mínimo razoável que não comprometa as suas atividades e que assegure uma estratégia competitiva de mercado através de sistemas de controlo efetivo interno.

O *compliance* emerge, enquanto atividade que visa mitigar os riscos de incumprimento legal e regulamentar do exercício das atividades empresariais, intrinsecamente associado ao desenvolvimento de uma consciência ética da pessoa coletiva como instrumento ao serviço da sociedade em que se insere e que a ultrapassa.

A vocação dos dois termos (*law enforcement* e *compliance*) não é por isso redundante, mas sim complementar[7], encontrando o denominador comum na progressiva tomada de consciência das organizações de que litígios, sanções ou restrições regulatórias poder-se-iam evitar ou mitigar com a adoção de programas de cumprimento normativo voluntário (*compliance programs*) que genericamente defendem os interesses dos *stakeholders* (e demais interessados), reduzindo as possibilidades de responsabilização civil, contraordenacional ou criminal[8].

O emprego de verbos transitivos como mitigar, reduzir, minimizar não é por isso inócuo de sentido no contexto da abordagem a programas de *compliance* uma vez que se trata de um instrumento de autorregulação das organizações tendente a evitar a prática de ilícitos e não a afastar responsabilidades (individuais ou coletivas) ou atenuar sanções[9].

A consecução de um programa de *compliance* não é, assim, um expediente de exoneração de responsabilidades, o que não significa, todavia, que ainda que para as autoridades de controlo independentes a existência de um programa de conformidade seja um evento inócuo, ponderada a existência de um programa de *compliance*, a efetividade do programa, a identificação de medidas adequadas e implementadas contra omissões que podem promover ou facilitar a prática de

[7] «(…) o cumprimento normativo voluntário por parte das empresas só pode melhorar se tiver devidamente em conta os poderes de regulamentação, supervisão e aplicação de sanções administrativas por parte das autoridades independentes, assim como as competências de investigação e acusação do Ministério Público em matéria penal», cfr. MENDES, Paulo de Sousa – *Law Enforcement & Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal.** P. 12.

[8] MENDES, Paulo de Sousa – *Law Enforcement & Compliance*. In ***Estudos sobre Law Enforcement, Compliance e Direito Penal.*** P. 11-12.

[9] Observam-se, contudo, duas tendências evolutivas no que concerne ao *compliance* de que são exemplo a Ley Organica 1/2015, de 31 de março no ordenamento jurídico espanhol que o prevê como circunstância de possível afastamento ou diminuição da responsabilidade penal da pessoa coletiva, e o Capítulo VIII *United States Setencing Comission Guidelines Manual* de 2015, onde se prevê um *culpability score* que vai diminuindo em função das práticas funcionais concretamente adotadas pela organização em sede de *compliance* e a cooperação com as autoridades. No mesmo sentido, MARQUES JÚNIOR, Filipa; MEDEIROS, João – A elaboração de Programas de *Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal.** P. 127-128.

infrações e a identificação, avaliação e controlo do risco, aquele não venha a ter impacto na avaliação da responsabilidade (coletiva ou individual) e na determinação da sanção aplicável[10] [11].

Um programa de *compliance* visa, sobretudo, assegurar a adequação e o regular funcionamento dos sistemas de controlo interno das organizações, mitigando os riscos[12] de acordo com a complexidade da atividade desenvolvida[13] [14], numa lógica sobretudo preventiva e não de réplica, observando-se por isso quatro vetores fundamentais num programa efetivo de conformidade: a) a antecipação (identificação de riscos e vulnerabilidades); b) prevenção (adoção de medidas de proteção relativamente aos riscos e vulnerabilidades detetados); c) deteção (adoção de instrumentos e mecanismos que permitam detetar possíveis indícios de ilícitos e violação de regras); d) reação (criação de mecanismos que permitam uma reação eficaz quando detetados indícios daquelas irregularidades).

2. ***Digital compliance programs*** **como projetos éticos com dupla finalidade: cumprimento normativo e cumprimento normalizado voluntário**

Originariamente os programas de *compliance* surgem ligados às políticas de combate à criminalidade económica, sendo catalisador da promoção destes o escândalo *Watergate* que conduziu à promulgação do *Foreign Corrupt Practices Act*[15] em 1977 pelo Governo dos Estados

[10] MENDES, Paulo de Sousa – *Law Enforcement & Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal**. P. 14.

[11] Encontram-se, aliás, no nosso modesto entendimento, alguns afloramentos no Regulamento Geral sobre a Proteção de Dados Pessoais das duas tendências evolutivas em sede de *compliance*, e por isso tendente à objetivação da diminuição da culpa em função do nível de *compliance* em concreto observável e o nível de cooperação com as autoridades de controlo, v.g. alíneas b), c), d), f), j) k) do n.º 2 do artigo 83.º.

[12] «Assim, de entre tais riscos destacam-se, desde logo, os riscos legais (riscos a que a empresa está sujeita em virtude da desconformidade com as normas aplicáveis à sua actividade, incluindo os riscos regulatórios e legislativos), reputacionais (e que afetam, desde logo, a imagem da empresa), bem como os riscos financeiros (com impacto financeiro na empresa)», cfr. MARQUES JÚNIOR, Filipa; MEDEIROS, João – A elaboração de Programas de *Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal.** P. 124-125.

[13] «O grau de abrangência e detalhe de uma política consistente de compliance é mais exigente quando se tratar de uma empresa que desenvolve a sua atividade em setor regulado. (…) a teia legal e regulamentar nesses setores é sempre mais ampla, e também mais densa e minunciosa, do que nos restantes setores de atividade, para além de ser mais propensa à evolução e revisão do respetivo quadro normativo (muitas vezes, como sucede entre nós, em resultado da transposição de instrumentos da União Europeia), cfr. MENDES, Paulo de Sousa – *Law Enforcement & Compliance*. In ***Estudos sobre Law Enforcement, Compliance* e Direito Penal.** P. 18.

[14] MARQUES JÚNIOR, Filipa; MEDEIROS, João – A elaboração de Programas de *Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal.** P. 124.

[15] O texto original está disponível para consulta em https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2012/08/29/corruptrpt-95-213.pdf.

Unidos da América[16] que por sua vez, intercedendo junto das principais organizações internacionais para a promoção dos princípios nele previstos, culminou na celebração, apenas para elencar duas das mais significativas[17], da "*Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*" da OCDE (Organização para a Cooperação e Desenvolvimento Económico)[18] e da "*Convention against Corruption*" da ONU (Organização das Nações Unidas)[19] [20].

Este primeiro esforço internacional de criação de um padrão ético-normativo homogeneizante foi progressivamente ampliado a outros domínios, observando-se hoje um consenso alargado relativamente à importância de um *friendly system* de gestão de risco incorporado em programas de *compliance* que avoque não só as soluções legislativas internas e internacionais, mas bem assim boas práticas e códigos éticos[21] [22] que permitam colocar as organizações numa posição competitiva num mercado global densificado e ampliado pela era digital.

A organização internacional não governamental e independente, International Organization for Standardization (ISO)[23], fundada em 1946, e contando atualmente com representantes de 165 países[24], é um exemplo significativo do profícuo resultado alcançável da complementaridade entre a *hard law* e a *soft law*. A ISO reúne especialistas que contribuem para o desenvolvimento e fixação de padrões universais de sistemas de cumprimento normativo

[16] OBERHEIDEN, Nick – 10 Reasons Why FCPA Compliance Is Critically Important for Businesses. **The National Law Review.** Vol. XI, Number 39. [Em linha]. Disponível em Why FCPA Compliance Is Important for Businesses (natlawreview.com)

[17] Outros acordos Internacionais com relevância para o combate à criminalidade económica podem ser consultados em UNITED States Department of Justice – **International Agreements.** [Em linha]. Disponível em https://www.justice.gov/criminal-fraud/international-agreements

[18] OCDE - **Convention on Combating Bribery of Foreign Public Officials in International Business Transactions** (1997). [Em linha]. Disponível em 210X297 (oecd.org)

[19] ONU - **Convention Against Corruption** (2003). [Em linha]. Disponível em https://www.unodc.org/pdf/corruption/publications_unodc_convention-e.pdf.

[20] Ainda, a título de exemplo e com relevância, a Convenção OEA contra a Corrupção (Organização dos Estados Americanos), disponível em http://www.oas.org/juridico/portuguese/treaties/b-58.htm e o United Kingdom Bribery Act (2010), disponível em https://www.legislation.gov.uk/ukpga/2010/23/contents

[21] «Se engrosó el glosario de términos del Derecho Penal, con un goteo constante de menciones a la gestión del riesgo, el gobierno corporativo, la responsabilidad social corporativa o los códigos de conducta. Precisamente estos últimos se han convertido en la antesala de los denominados *compliance programs* o programas de cumplimiento normativo. Esta expresión englobaría la prevención de riesgos en la empresa ante posibles incumplimientos». Cfr. GUTIÉRREZ PÉREZ, Elena – Los *Compliance Programs* o la vuelta al *No Body to Kick*, *No Soul to Dam*. In **Propuestas Penales: Nuevos Retos y Modernas Tecnologías**. P. 381.

[22] Numa aproximação à dimensão de uma cultura ética de responsabilidade corporativa a Novartis substituiu a anterior designação de Código de Conduta para Código de Ética em setembro de 2020. Cfr. NOVARTIS – **Code of Ethics**. [Em linha]. Disponível em https://www.novartis.com/our-company/corporate-responsibility/reporting-disclosure/codes-policies-guidelines

[23] Informações pormenorizadas da ISO disponíveis em https://www.iso.org/about-us.html

[24] O Instituto Português de Qualidade (IPQ) é o órgão representativo português no campo da qualidade a nível internacional.

voluntário (v.g. ISO 19.600 – *Compliance Management Systems – Guidelines*[25]), evidenciando-se a tendência corporativa internacional à adesão de programas de conformidade que tendencialmente mitiguem o risco de incumprimento legal e regulamentar desde o início da atividade da organização de forma espontânea. Os sistemas de gestão de risco são, evidentemente, enunciados de forma a harmonizarem-se com outros sistemas de normas de cumprimento voluntário que no seu conjunto visem a consecução de um objetivo no contexto do exercício da atividade da organização (v.g. ISO 19.600 e ISO 27.001[26] [27]).

A tendência internacional para a adesão a programas de conformidade efetivos e funcionais tem vindo a beneficiar de um conjunto de instrumentos legais que impulsionam a abordagem baseada no risco, com um acentuado caráter autorregulador, impondo a realização de uma *due diligence* sustentada na análise do risco da própria organização, favorecendo uma política ética e de transparência de cultura organizacional das empresas no contexto económico atual.

Sendo certo que vivemos numa sociedade praticamente dependente das tecnologias digitais, o recurso crescente às tecnologias de informação e comunicação convocou inúmeros riscos e vulnerabilidades que a maior parte das pessoas desconhece, não obstante os inestimáveis benefícios que trouxe para as esferas da vida hodierna.

«Na atual sociedade em rede, de sistemas de informação e comunicação digital, a posse de dados sensíveis sobre qualquer cidadão é cada vez mais uma fonte de poder. O armazenamento em larga escala de informação pessoal, de dados sensíveis sobre a vida particular de cada um, sobre os seus hábitos e comportamentos, nas mãos de um número restrito de entidades, pode ser problemático, como problemática pode ser a implícita capacidade, sem precedentes, de autoridades estatais e de entidades várias, públicas e privadas, para controlar e monitorizar dados, comunicações e movimentos de qualquer pessoa ou organização. O receio aumenta quando o cidadão recorre à assinatura eletrónica para certificar os seus documentos, ou quando leva a cabo transações financeiras com recurso ao *e-banking*, ou quando troca informações confidenciais através de meios

[25] A ISO 19.600 enuncia orientações para estabelecer, desenvolver, implementar, avaliar, manter e melhorar um sistema de gestão de conformidade eficaz e responsivo dentro de uma organização e é orientada pelos princípios de boa governança, proporcionalidade, transparência e sustentabilidade. Disponível em https://www.iso.org/standard/62342.html

[26] ISO 27.001 é dedicada à tecnologia da informação, técnicas de segurança, sistemas de gerenciamento de segurança da informação e requisitos aplicáveis. Disponível em https://www.iso.org/management-system-standards-list.html

[27] «A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da organização», cfr. CENTRO Nacional de Cibersegurança – **Quadro Nacional de Referência para a Cibersegurança**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

eletrónicos. Numa outra perspetiva, também ela eticamente relevante, levanta-se a questão de saber até que ponto o acesso aos benefícios potenciados pela tecnologia, bem como a exposição aos seus riscos, se encontram devidamente distribuídos»[28].

Neste sentido, os últimos anos vieram acentuar a necessidade do reconhecimento de uma cultura universal de cumprimento normativo voluntário com uma imanente dimensão ética. Esta dimensão foi recebida na Resolução N.º 57/239 da Assembleia Geral das Nações Unidas que a incluiu nos elementos estruturantes de uma cultura de cibersegurança, em função da presença global dos sistemas e redes de informação das sociedades modernas, mobilizando todos os participantes (governos, empresas, organizações e utilizadores individuais) a respeitar os interesses legítimos de terceiros e a desenvolver programas éticos e de conduta orientados pelo paradigma de que os atos e omissões poderiam representar sérios riscos para as sociedades democráticas, acentuando assim o carácter essencial dos programas de *compliance*, enquanto linha crítica de proteção do cidadão face a ameaças a direitos e valores fundamentais à vida em democracia.

Na verdade, os códigos de conduta ou ética são os percursores dos programas de *compliance* digital face ao manifesto desencontro entre o direito objetivo e a tecnologia, que tem desde logo dificuldade em incorporar na letra da lei o transitório léxico das novas tecnologias, optando-se no que em particular diz respeito ao Direito da União Europeia, pela redação de atos jurídicos que passem no teste do polimorfismo da evolução digital através da técnica legislativa de neutralidade tecnológica[29], donde resulta a necessidade da iniciativa de autorregulação no contexto específico do ecossistema digital da organização, sustentado numa cultura de conformidade preventiva que congregue os eixos da transparência, confiabilidade, responsabilidade e respeito pelos direitos fundamentais.

3. *Compliance* Digital

[28] OBSERVATÓRIO de Cibersegurança – **Relatório Cibersegurança em Portugal: Ética & Direito**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriocibersegurancа_cncs.pdf

[29] «(…) uma das técnicas legislativas encontradas, em particular no Direito da União Europeia, tem sido a de redigir uma lista de definições relevantes para um determinado diploma (…) O desafio que se coloca é, então, o de encontrar conceitos e definições suficientemente abstratos para resistir ao polimorfismo da evolução tecnológica e, ao mesmo tempo, suficientemente concretos, para que a leitura do texto legal se torne acessível», cfr. OBSERVATÓRIO de Cibersegurança – **Relatório Cibersegurança em Portugal: Ética & Direito**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriocibersegurancа_cncs.pdf

O *compliance* digital é, nestes termos, um segmento do quadro mais amplo dos programas de conformidade, dedicado especificamente à integridade digital, ou seja, à implementação de um programa sustentado em políticas de integridade que incluam a área da tecnologia e da informação na sua governação.

Trata-se de um programa de conformidade que parte da conceptualização de ciberespaço como «metáfora para descrever o espaço não físico criado por redes de computadores, nomeadamente pela internet (…)»[30] e que «consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação»[31], orientado para a adoção de um «conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem»[32].

Com efeito, quando se aborda o tema do *digital compliance*, em bom rigor, estamos a falar de um programa de conformidade setorial que compreende as infraestruturas críticas e os serviços essenciais (v.g. setor da energia – incluindo eletricidade e gás, transportes, bancário e mercado financeiros, saúde, fornecimento e distribuição de água potável, infraestruturas digitais – pontos de troca de tráfego, prestadores de serviços de *domain name system*), o cibercrime e a prova digital, as comunicações eletrónicas, o comércio eletrónico, os pagamentos eletrónicos e identificação eletrónica, a propriedade intelectual, a própria transição digital da Administração Pública e a proteção de dados, entre outros.

O RGPD é, desta forma, um exponente num programa de *compliance* digital que, necessariamente, é suportado numa análise de risco inicial, entendida como um processo de identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, relativa à probabilidade e impacto de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos, bem como a circunstância ou um evento,

[30] CENTRO Nacional de Cibersegurança – **Glossário**. Em linha]. Disponível em https://www.cncs.gov.pt/recursos/glossario/
[31] N.º 1, 3.º parágrafo da Resolução do Conselho de Ministros n.º 92/2019, **Diário da República** N.º 108/2019, Série I de 2019/06/5. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized
[32] N.º 1, 4.º parágrafo da Resolução do Conselho de Ministros n.º 92/2019, **Diário da República** N.º 108/2019, Série I de 2019/06/5. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized

razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação[33].

4. O RGPD como ato jurídico *compliance friendly*

A rápida evolução tecnológica e a globalização económica convocaram novos desafios para a proteção de dados pessoais e assim, não obstante os princípios fundamentais consagrados na Diretiva 95/46/CE ainda se mantivessem válidos e enquadrados no âmbito da prossecução do processo de integração europeia (proteção dos direitos e liberdades fundamentais – em especial o direito à proteção de dados pessoais, bem como a realização de um mercado interno – em especial a livre circulação desses dados), a Comissão Europeia concluiu pela necessidade de uma reforma e modernização do regime jurídico nesta matéria, impondo-se à UE o desenvolvimento de uma abordagem global e coerente que garantisse o respeito pelo direito fundamental das pessoas singulares à proteção dos dados pessoais tanto no ordenamento jurídico europeu como fora dele[34].

O *kick off* da Comissão Europeia em 2010 levou à adoção do Regulamento (UE) 2016/679 (RGPD), cujo quadro de reforma foi assumido como componente essencial da "Estratégia para o Mercado Único Digital na Europa"[35], visando simultaneamente harmonizar as normas de direito interno dos Estados Membros (EM) em matéria de proteção de dados e consolidar a posição de liderança global da Europa no contexto da economia digital.

A manifesta digitalização da economia mundial determinou que a União Europeia (UE) em 2015 promovesse a criação de um Mercado Único Digital, considerando desde logo que o setor das tecnologias da informação e das comunicações (TIC) se encontrava na base de todos os sistemas económicos modernos inovadores e que a internet, bem como as tecnologias digitais, compreendiam um potencial transformador individual (na vida de cada pessoa, na forma de trabalhar) e coletivo (nas empresas e nas comunidades) que necessariamente deveria ser

[33] CENTRO Nacional de Cibersegurança – **Glossário**. Em linha]. Disponível em https://www.cncs.gov.pt/recursos/glossario/

[34] COMISSÃO Europeia – **Uma abordagem global da proteção de dados pessoais na União Europeia.** COM (2010). (01-11-2010). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52010DC0609&from=pt

[35] COMISSÃO Europeia - **Estratégia para o Mercado Único Digital na Europa**. COM (2015). (06-05-2015). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192

aproveitado simultaneamente com a profunda integração em todos os setores da economia e da sociedade[36].

A reforma do regime jurídico de proteção de dados pessoais surge assim neste contexto como um elemento fundamental desta estratégia pretendendo reforçar a confiança nos serviços digitais uma vez que prossegue uma ampla proteção das pessoas singulares no que se refere ao tratamento de dados pessoais, designadamente, através da declarada preocupação com a cibersegurança enunciada como princípio geral subjacente ao tratamento de dados pessoais como segurança da informação, integridade e confidencialidade[37].

O Regulamento Geral sobre a Proteção de Dados[38] é uma evidência da relevância de programas de *digital compliance* no âmbito dos sistemas internos das organizações, elevando o paradigma da autorregulação a um nível mais exigente de *corporate governance* por via da consagração dos princípios da responsabilidade e de *data protection by design* e *by default*, bem como o estabelecimento de novas medidas organizativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes das organizações que oferecem os seus serviços no mercado europeu[39].

Caraterística deste ato jurídico é a consolidação do paradigma de autorregulação, especialmente orientado para a adesão ao cumprimento normativo voluntário através de "*compliance programs*" em privacidade, proteção de dados e cibersegurança, materializadores do *law enforcement* em proteção de dados pessoais orientado para uma economia digital.

O princípio da autorregulação subjacente ao RGPD, vertido em *compliance programs*, endereça medidas mais rigorosas de responsabilidade e governança para as organizações, imediatamente dirigidas aos responsáveis pelo tratamento e aos subcontratantes, bem como um

[36] COMISSÃO Europeia - **Estratégia para o Mercado Único Digital na Europa**. COM (2015). (06-05-2015). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192

[37] OBSERVATÓRIO de Cibersegurança – **Relatório Cibersegurança em Portugal: Ética & Direito**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriociberseguranca_cncs.pdf

[38] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. **Jornal Oficial da União Europeia**. [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

[39] «As ciberameaças são um problema sem fronteiras e têm um impacto negativo na (…) economia, [bem como] nos direitos fundamentais dos cidadãos e na sociedade em geral. O número crescente de infrações (por exemplo, interceção de dados, fraudes em pagamentos em linha, usurpação de identidade, roubo de segredos comerciais) está a resultar em perdas económicas significativas. Estas traduzem-se frequentemente em perturbações nos serviços e em violações de direitos fundamentais e minam a confiança dos cidadãos nas atividades em linha». Cfr. COMISSÃO Europeia - **Estratégia para o Mercado Único Digital na Europa.** COM (2015). (06-05-2015). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192

modelo de abordagem baseado no risco considerando o potencial ou real efeito adverso avaliado numa escala de amplitude abrangente que compreende não só o impacto na perspetiva do titular dos dados, bem como o impacto geral coletivo.

Trata-se de uma abordagem baseada no risco[40], que não se cinge à abordagem centrada nos danos, impondo aos responsáveis pelo tratamento e subcontratantes a adoção de medidas práticas e concretas que assegurem a eficácia do regime jurídico de proteção de dados, concretizando o princípio da responsabilidade ou *accountability*, que vertido num programa de *compliance* digital é desenhado numa perspetiva de melhoria contínua e não de uma utilização estática das práticas, mas, sim, evoluir de acordo com a maturidade da organização e o seu contexto particular.

4.1. Princípio da responsabilidade ou *accountability*

Uma das principais caraterísticas do RGPD é precisamente a consagração do princípio da responsabilidade ou *accountability* (n.º 2 do art.º 5.º), cujo objetivo é reafirmar e reforçar a responsabilidade primária do responsável pelo tratamento[41], considerando que o regime jurídico anterior (não obstante já o propugnasse) se encontrava insuficientemente vertido em medidas práticas e concretas que cumprissem os princípios de proteção de dados e que traduzissem a vinculação dos responsáveis ao cumprimento das obrigações decorrentes do regime jurídico de proteção de dados.

«Este princípio assume, portanto, um papel fundamental como instrumento de compliance, ao promover a implementação, por parte do responsável pelo tratamento, das garantias necessárias ao cumprimento das regras de proteção de dados e a respetiva demonstração, tanto a nível interno como externo»[42].

Não se trata de um princípio absolutamente novo, mas reveste-se do efeito compulsório necessário à adoção de medidas práticas e funcionais (medidas técnicas e organizativas) que assegurem o cumprimento dos princípios consagrados no art.º 5.º, tendo como premissa o efetivo cumprimento com suporte numa abordagem baseada no risco, que poderá ser variável em termos

[40] Que não era totalmente desconhecida na Diretiva 95/46/CE, v.g. por via da referência ao tratamento de dados pessoais sensíveis que representassem maior risco para os titulares, à segurança do tratamento ou ao controlo prévio das autoridades de controlo (agora estabelecido noutros moldes no RGPD).
[41] LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no âmbito do novo Regulamento. In **Anuário da Proteção de Dados 2018.** P. 52-53.
[42] LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no âmbito do novo Regulamento. In **Anuário da Proteção de Dados 2018.** P. 55.

de probabilidade e gravidade, considerando a natureza, o âmbito, o contexto e as finalidades do tratamento de dados.

Extrai-se ainda do princípio a necessidade de um comportamento pró-ativo (*compliance friendly*) por banda do responsável pelo tratamento quanto à obrigação de demonstrar o cumprimento do regime jurídico, designadamente, no que concerne à adoção de mecanismos que permitam a avaliação das medidas técnicas e organizativas antes da ocorrência de qualquer incidente de violação de dados pessoais (daqui resulta, de igual forma, a importância da realização de uma avaliação de impacto).

4.2. *Privacy by design e by default*

Intrinsecamente ligado ao princípio da responsabilidade o art.º 25.º do RGPD vem consagrar dois princípios que devem presidir às operações de tratamento de dados pessoais em toda a extensão do seu ciclo de vida: a proteção de dados desde a conceção e a proteção de dados por defeito.

Estes princípios foram ensaiados por Ann Cavoukian em 2009[43] e a sua natureza fundamental no regime jurídico atual eleva-os a princípios norteadores de quaisquer processos de tratamento de dados pessoais.

4.3. Registo de atividades de tratamento de dados pessoais e notificação de violação de dados pessoais

Visando prosseguir o objetivo de comprovar a observância do RGPD, o responsável pelo tratamento e o subcontratante, conservem registos das atividades de tratamento de dados pessoais desenvolvidas sob sua responsabilidade. A disponibilização dos registos de atividades de tratamento é, aliás, umas das vias de cooperação com as autoridades de controlo, se para o efeito de fiscalização aqueles forem solicitados (n.º 4 do art.º 30.º).

Não obstante a derrogação prevista no n.º 5 do art.º 30.º, para as micro, pequenas e médias empresas, quanto à conservação deste registo para as organizações com menos de 250

[43] CAVOUKIAN, Ann – **Privacy by Design: The 7 Foundational Principles**. [Em linha]. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

trabalhadores, a obrigação mantém-se se as operações de tratamento implicarem um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou seja dedicado a dados pessoais sensíveis.

4.4. Códigos de conduta e certificação

Ainda no Capítulo IV, dedicado ao responsável pelo tratamento e subcontratante, a Secção V relativa aos Códigos de Conduta e Certificação promove a criação de mecanismos de autorregulação de conformidade com o RGPD que, se por um lado constituem um instrumento de demonstração do cumprimento das obrigações do responsável pelo tratamento (n.º 3 do art.º 24.º do RGPD), por outro apresentam-se como fator atenuante na determinação da coima aplicar no caso de uma violação de dados pessoais (alínea j) do n.º 2 do art.º 83.º do RGPD).

A natureza jurídica dos códigos de conduta é, pois, endereçada a *soft law* uma vez que não apresentam natureza coercitiva, sendo que a inobservância dos preceitos meramente indicativos deles constantes em nada releva relativamente aos responsáveis pelo tratamento e subcontratantes, uma vez que o cumprimento das obrigações constantes do RGPD não é prejudicado pela não adesão a um eventual código de conduta.

Considerações finais a respeito a metodologia de solução de conflitos e o compliance digital

Em resultado da interseção das novas tecnologias com o Direito, foi considerada a importância de adesão voluntária a programas de conformidade que visem criar um sistema multidisciplinar, transversal e interdisciplinar que vise em primeira instância a criação de uma cultura empresarial assente num princípio de transparência e integridade da matriz fundante que sustenta o desenvolvimento da atividade.

Este desiderato convoca a perceção organizacional do modelo preventivo de conflitos que podem resultar do não cumprimento de programas de conformidade, gerando custos económicos, financeiros e de projeção social para a organização e para os particulares que com aquela se relacionem de forma direta ou indireta. Configura-se, por conseguinte, um modelo preventivo de solução de conflitos que pode colaborar ou coadjuvar aos métodos de solução de adequados de

conflitos e reforçar a base de interação e harmonização dos conflitos apresentados, *v.g.* a mediação, a conciliação ou a arbitragem nas circunstâncias em que sejam os mesmos cabíveis.

Os meios de resolução extrajudicial de litígios são uma solução de justiça acessível, célere e simples que apresentam as mesmas garantias que os tribunais, enquanto alternativa a estes, representam a consolidação de uma instância que se quer menos litigiosa que a tradicional administração da justiça, menos informalizada e que tende a diminuir a conflitualidade, conforme é desiderato dos programas de *compliance digital*.

É, neste sentido, uma via a ser ponderada desde a academia em direção ao terreno jurídico, modelando um sistema integrado que assente na promoção do acesso ao direito e à justiça sustentado na prossecução prévia de um modelo de adesão voluntária que se encontre para além da necessidade de adequação às normas sancionatórias e que vise salvaguardar as posições de todos os intervenientes (direitos e indiretos) no âmbito dos programas de *compliance* digital.

REFERÊNCIAS BIBLIOGRÁFICAS:

CAMBRIDGE Dictionary – **Dictionary.** [Em linha]. Disponível em https://dictionary.cambridge.org/dictionary/english/comply.

CARNEIRO, Claúdio – A Era do *Compliance* no Século XXI. In ***Compliance*: Perspetivas e Novas Dinâmicas**.
CARNEIRO, Cláudio; SANTOS JÚNIOR, Milton de Castro – **Gestão de Riscos em Compliance.**

CAVOUKIAN, Ann – **Privacy by Design: The 7 Foundational Principles**. [Em linha]. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

CENTRO Nacional de Cibersegurança – **Glossário**. Em linha]. Disponível em https://www.cncs.gov.pt/recursos/glossario/

CENTRO Nacional de Cibersegurança – **Quadro Nacional de Referência para a Cibersegurança**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

COMISSÃO Europeia - **Estratégia para o Mercado Único Digital na Europa.** COM (2015). (06-05-2015). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192

COMISSÃO Europeia – **Uma abordagem global da proteção de dados pessoais na União Europeia.** COM (2010). (01-11-2010). [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52010DC0609&from=pt

LOPES, Teresa Vale – Responsabilidade e Governação das Empresas no âmbito do novo Regulamento. In **Anuário da Proteção de Dados 2018.**

MARQUES JÚNIOR, Filipa; MEDEIROS, João – A elaboração de Programas de *Compliance*. In **Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal.** P. 124.

MENDES, Paulo de Sousa – *Law Enforcement & Compliance*. In ***Estudos sobre Law Enforcement, Compliance* e Direito Penal.**

OBERHEIDEN, Nick – 10 Reasons Why FCPA Compliance Is Critically Important for Businesses. **The National Law Review.** Vol. XI, Number 39. [Em linha]. Disponível em Why FCPA Compliance Is Important for Businesses (natlawreview.com)

OBSERVATÓRIO de Cibersegurança – **Relatório Cibersegurança em Portugal: Ética & Direito**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriocibersegurancacncs.pdf

OBSERVATÓRIO de Cibersegurança – **Relatório Cibersegurança em Portugal: Ética & Direito**. [Em linha]. Disponível em https://www.cncs.gov.pt/content/files/relatorio_etica.direito2020__observatoriocibersegurancacncs.pdf

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. **Jornal Oficial da União Europeia**. [Em linha]. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

Resolução do Conselho de Ministros n.º 92/2019, **Diário da República** N.º 108/2019, Série I de 2019/06/5. Disponível em https://dre.pt/home/-/dre/122498962/details/maximized