MACEDO VITORINO

COMPLIANCE

RGPD: OITO ANOS DEPOIS, UM BALANÇO NA ERA DA INTELIGÊNCIA ARTIFICIAL

Cláudia Fernandes Martins e Joana Fuzeta da Ponte

INTRODUÇÃO

Em 2026, o Regulamento Geral sobre a Proteção de Dados (RGPD) já não é uma novidade. Passaram oito anos desde a sua aplicação, em 25 de maio de 2018, e dez anos desde a sua entrada em vigor, em 24 de maio de 2016. Este enquadramento temporal é relevante: o balanço que hoje se impõe já não é o de uma fase inicial de adaptação, mas o de uma década de maturidade regulatória e de transformação da governação dos dados nas organizações.

A questão que se coloca hoje é, por isso, mais exigente do que em 2018: as organizações incorporaram efetivamente a proteção de dados nos seus processos de decisão ou permanecem alinhadas com o RGPD apenas no plano formal? A conformidade documental continua a ser necessária, mas há muito deixou de ser suficiente.

A experiência prática revela uma evolução assinalável na sensibilização das empresas e dos seus colaboradores. Ainda assim, subsistem fragilidades relevantes: escolha inadequada do fundamento de licitude, recurso excessivo ao consentimento, prazos de conservação demasiado amplos ou inexistentes, dificuldade em distinguir responsável pelo tratamento e subcontratante, controlo insuficiente de transferências internacionais de dados e resposta pouco estruturada a violações de dados pessoais.

A esta realidade acresce um novo fator de complexidade: a utilização crescente de sistemas de inteligência artificial (IA). A IA não suspende o RGPD nem cria uma zona de exceção à proteção de dados. Pelo contrário, sempre que um sistema de IA trate dados pessoais, o RGPD continua a aplicar-se em pleno, agora em articulação com o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (doravante «Regulamento da IA»).

1. O IMPACTO INICIAL DO RGPD NAS ORGANIZAÇÕES

A aplicação do RGPD representou uma alteração estrutural na forma como as empresas recolhem, utilizam, conservam, partilham e eliminam dados pessoais. O seu impacto foi particularmente sentido nas áreas de recursos humanos, marketing, videovigilância, tecnologias de informação, cibersegurança, gestão financeira e gestão contratual. Mais do que impor políticas de privacidade ou modelos de consentimento, o RGPD consolidou uma lógica de responsabilidade proativa: definição de finalidades e fundamentos de licitude, manutenção de registos de atividades de tratamento, *privacy by design* e *by default*, avaliação de riscos, realização de avaliações de impacto, controlo de subcontratantes, resposta a pedidos dos titulares dos dados e gestão de incidentes de segurança.

A entrada em aplicação do RGPD desencadeou uma mobilização intensa nas organizações. Numa primeira fase, muitas empresas concentraram-se na revisão de políticas de privacidade, cláusulas contratuais, formulários de consentimento, contratos com subcontratantes e procedimentos internos. Esse esforço foi indispensável, embora tenha ficado, com frequência, centrado numa lógica de regularização documental.

Nos primeiros anos, a conformidade foi, em muitos casos, entendida como um projeto com início e fim: atualizar documentação, recolher consentimentos, designar interlocutores internos e criar canais para o exercício de direitos. O tempo veio demonstrar, porém, que o RGPD exige uma disciplina permanente de governação, monitorização e prova. Cada organização tem de conseguir demonstrar, em qualquer momento, não apenas que formalizou políticas e procedimentos, mas que decide, executa e controla os tratamentos de dados em conformidade com o que documentou.

2. PRINCIPAIS DESAFIOS APÓS UMA DÉCADA DE VIGÊNCIA

Passados oito anos de aplicação e dez de vigência do RGPD, a maioria das organizações reconhece que a proteção de dados é um processo continuado. O desafio deslocou-se da adaptação inicial para a integração efetiva do RGPD na gestão corrente: desenvolvimento de novos produtos e serviços, contratação de tecnologia e utilização de ferramentas digitais, gestão de colaboradores, marketing baseado em dados e partilha de informação dentro de grupos empresariais.

O aumento dos ciberataques e dos incidentes de segurança tornou particularmente visível a importância das medidas técnicas e organizativas. Não basta aprovar políticas: é necessário testar controlos, rever acessos, aplicar os princípios da minimização e da necessidade, formar colaboradores,

documentar decisões e assegurar mecanismos de deteção, resposta e notificação de violações de dados pessoais dentro dos prazos legais.

A atuação das autoridades de controlo, incluindo a Comissão Nacional de Proteção de Dados (CNPD), contribuiu também para uma maior perceção do risco regulatório. As coimas e decisões sancionatórias deixaram claro que o incumprimento do RGPD pode gerar consequências financeiras, reputacionais e operacionais, tanto no setor privado como no público.

A pandemia, a expansão do teletrabalho e a generalização de ferramentas colaborativas aceleraram a digitalização das empresas e expuseram novos pontos de tensão: controlo da atividade dos trabalhadores, monitorização da produtividade, videovigilância, utilização de dispositivos pessoais, armazenamento em cloud e transferência de dados para fora do Espaço Económico Europeu. A conformidade passou, assim, a depender de uma articulação mais estreita entre as áreas jurídica, de recursos humanos, de TI, de segurança da informação e de gestão de risco.

Apesar das dificuldades, o balanço é globalmente positivo. O RGPD elevou o nível de consciência sobre a importância dos dados pessoais, reforçou a confiança de trabalhadores, clientes e parceiros, reduziu riscos reputacionais e obrigou as organizações a conhecer melhor os seus fluxos de informação. Nas empresas que o levaram a sério, o RGPD foi menos um obstáculo burocrático e mais um instrumento de qualidade, segurança e maturidade digital.

O novo ciclo de conformidade será marcado pela inteligência artificial. Sistemas de seleção e avaliação de candidatos, ferramentas de scoring, assistentes virtuais, soluções de análise preditiva, modelos generativos, sistemas de deteção de fraude e aplicações de monitorização comportamental podem envolver tratamentos intensivos de dados pessoais, criação de perfis, decisões automatizadas ou riscos acrescidos para direitos fundamentais. É precisamente nesse ponto que a articulação entre o RGPD e o Regulamento da IA se torna decisiva.

3. O RGPD E O REGULAMENTO DA IA

O Regulamento da IA introduz uma abordagem baseada no risco, classificando determinados sistemas como proibidos, de risco elevado ou sujeitos a obrigações específicas de transparência. A sua aplicação é faseada: as proibições relativas a práticas de IA e os deveres de literacia em IA produzem efeitos desde 2 de fevereiro de 2025; as regras de governação e as obrigações aplicáveis a modelos de IA de finalidade geral são aplicáveis desde 2 de agosto de 2025; e o regime geral torna-se aplicável já em 2

de agosto de 2026. Na sequência do acordo político de maio de 2026 sobre a simplificação do Regulamento da IA, prevê-se ainda um calendário específico para sistemas de risco elevado: 2 de dezembro de 2027 para determinados domínios de risco elevado e 2 de agosto de 2028 para sistemas integrados em produtos regulamentados. Este calendário significa que as empresas devem preparar-se já, e não apenas quando o regime estiver plenamente aplicável.

A articulação entre os dois regulamentos deve ser feita de forma prática. Antes de implementar ou contratar um sistema de IA, a organização deve mapear os dados utilizados, verificar se há tratamento de dados pessoais, confirmar a licitude do tratamento, avaliar necessidade e proporcionalidade, reduzir os dados ao mínimo indispensável, definir prazos de conservação, assegurar transparência perante os titulares e ponderar a realização de uma avaliação de impacto sobre a proteção de dados (AIPD), sempre que o tratamento seja suscetível de implicar um risco elevado para os direitos e liberdades dos titulares. Quando o sistema se enquadre como IA de risco elevado, acrescem exigências próprias do Regulamento da IA, incluindo governação dos dados, documentação técnica, supervisão humana, robustez, segurança e gestão de riscos.

O ponto essencial é simples (mas nem sempre fácil): a conformidade em IA começa, em larga medida, pela conformidade em dados. Uma empresa que não conhece os seus dados, não controla os seus subcontratantes, não documenta decisões e não gere riscos dificilmente conseguirá cumprir o Regulamento da IA. O RGPD torna-se, assim, o alicerce jurídico e organizativo, em matéria de dados pessoais, de uma utilização responsável, segura e fiável da inteligência artificial.

4. CONCLUSÃO

O RGPD deixou de ser uma novidade e passou a constituir uma componente central da governação empresarial. O seu verdadeiro valor mede-se hoje pela capacidade de as organizações integrarem a proteção de dados na estratégia, na tecnologia, nos processos internos e na cultura dos colaboradores.

O balanço deste primeiro ciclo é, por isso, exigente, mas positivo. As organizações evoluíram, os titulares dos dados estão mais atentos e a proteção de dados tornou-se um assunto de administração, risco e confiança. Persistem, todavia, desafios relevantes, sobretudo quando a inovação tecnológica avança mais rapidamente do que os processos internos de controlo.

A inteligência artificial tornará este equilíbrio ainda mais complexo. O Regulamento da IA não afasta o RGPD: complementa-o. As empresas que melhor se prepararem serão as que tratarem a proteção de

dados, cibersegurança, governação tecnológica e ética da IA como dimensões integradas de uma mesma política de compliance.

Mais do que cumprir formalmente, o desafio passa agora por demonstrar, de forma contínua, que os dados pessoais são tratados com rigor, proporcionalidade e responsabilidade. Na próxima década, a maturidade das organizações medir-se-á não apenas pela capacidade de inovar, mas por inovar com confiança.

SOBRE A MACEDO VITORINO

A MACEDO VITORINO é uma prestigiada sociedade de advogados. Assessoramos clientes portugueses e estrangeiros num amplo leque de setores de atividade, incluindo banca, distribuição, indústria, energia, tecnologia, media e telecomunicações. Temos ainda estado envolvidos em projetos e em processos de reestruturação de empresas.

Somos conhecidos pela nossa abordagem profissional e empresarial aos assuntos mais complexos e difíceis.

A MACEDO VITORINO mantém relações de correspondência e parceria com algumas das mais prestigiadas sociedades de advogados internacionais da Europa, Estados Unidos, Brasil e Ásia, o que nos permite prestar aconselhamento em operações internacionais de forma eficiente.

Se pretende saber mais sobre a MACEDO VITORINO, visite o nosso site www.macedovitorino.com.

INFORMAÇÃO IMPORTANTE

Esta informação é de caráter genérico, não devendo ser considerada aconselhamento profissional. Caso necessite de aconselhamento jurídico sobre estas matérias, deve contactar um advogado. Se for cliente da MACEDO VITORINO, pode contactar-nos por email para: mv@macedovitorino.com.