SUPREMO TRIBUNAL DE JUSTIÇA

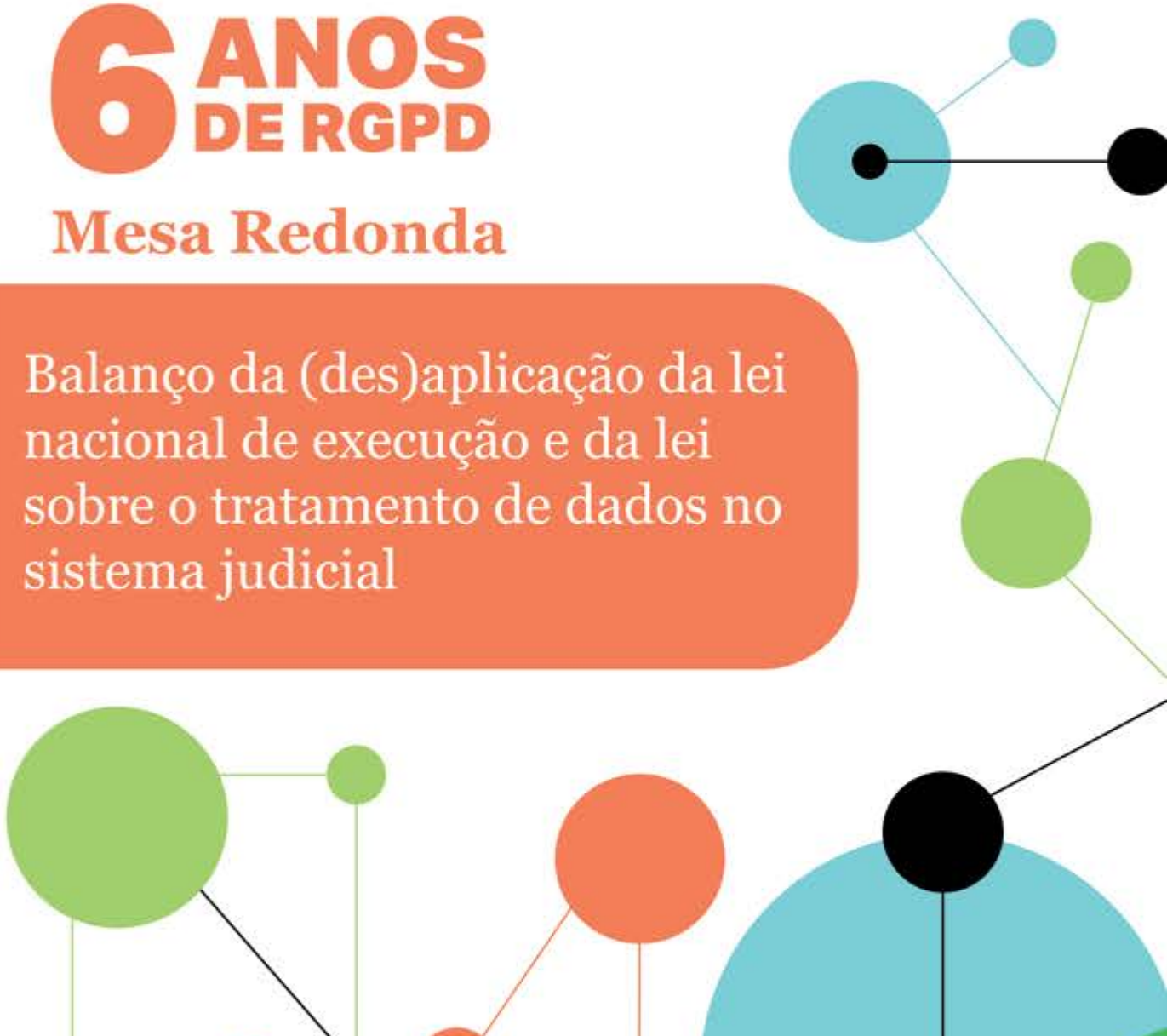
DIA DA PROTEÇÃO DE DADOS 2025

28 de Janeiro de 2025

6 ANOS DE RGPD

Mesa Redonda

Balanço da (des)aplicação da lei nacional de execução e da lei sobre o tratamento de dados no sistema judicial



COLEÇÃO LIVROS DIGITAIS DO SUPREMO TRIBUNAL DE JUSTIÇA

Esta coleção tem como objectivo principal coligir, de forma sistemática, os textos que resultem das comunicações levadas a efeito no Ciclo de Colóquios do Supremo Tribunal de Justiça e de outros eventos, atividades sistémicas inseridas no Plano de Atividades da atual presidência do Supremo Tribunal de Justiça.
Tem por escopo disponibilizar, a toda a comunidade jurídica, o acesso livre e gratuito dos conteúdos dos colóquios, de uma forma universal, potenciada pelo modo de divulgação/disponibilização digital.

Presidente do Supremo Tribunal de Justiça
Juiz Conselheiro João Cura Mariano

Chefe do Gabinete do Presidente do Supremo Tribunal de Justiça
Juíza Desembargadora Gabriela Cunha Rodrigues

Ficha Técnica

Coordenação institucional, coordenação editorial e produção executiva
Juíza Desembargadora Clarisse Gonçalves
Adjunta do Gabinete do Presidente do Supremo Tribunal de Justiça

Coordenação Executiva do Colóquio
Gabinete do Presidente do Supremo Tribunal de Justiça
Encarregado da Proteção de Dados do Supremo Tribunal de Justiça João Ferreira Pinto

Fotografia
Técnica especialista do Gabinete do Presidente Ana Coelho

Grafismo
Designer Ana Oliveira Pinto

Esta publicação não adopta o novo Acordo Ortográfico, deixando-se essa opção ao critério dos autores.

Edição Janeiro de 2026

ISBN 978-989-35696-8-9

Sempre que desejar voltar ao indíce, clique


VIRTVTIBVS
MAIORVM
VT. SIT. OMNIBVS. DOCVMENTO. P. P. D.

PRESIDENTE DO SUPREMO TRIBUNAL DE JUSTIÇA
Juiz Conselheiro
João Cura Mariano

É com grande sentido de compromisso que damos continuidade ao desenvolvimento da *Coleção Livros Digitais do Supremo Tribunal de Justiça*, um projeto iniciado pelo nosso antecessor com dedicação e visão estratégica.

Concebida para oferecer conteúdos acessíveis, universais, gratuitos, estruturados e dinâmicos, esta coleção abrange sobretudo áreas do direito, muito embora se possa estender a outras áreas do saber.

A nossa responsabilidade, neste momento, é consolidar e expandir este trabalho, garantindo que cada livro digital continue a ser uma ferramenta valiosa para o fortalecimento de uma cultura de conhecimento partilhado. A evolução tecnológica e as novas exigências educacionais desafiam-nos a inovar constantemente, incorporando novas abordagens e funcionalidades que acrescentem valor a esta iniciativa.

Expressamos o nosso reconhecimento a todos os que contribuíram para o progresso deste projeto, reconhecendo e valorizando todo o trabalho já realizado, e reafirmamos o nosso compromisso em dar-lhe continuidade com a mesma dedicação. Contamos com a colaboração de todos para reforçar e aperfeiçoar este trabalho, garantindo o seu impacto e relevância no futuro.

DISCURSO DE ABERTURA

PRESIDENTE DO SUPREMO TRIBUNAL DE JUSTIÇA
Juiz Conselheiro
João Cura Mariano

Celebramos hoje o Dia da Proteção de Dados neste encontro subordinado ao tema «Seis anos de RGPD – Balanço da (des)aplicação da lei nacional de execução e da lei sobre o tratamento de dados no sistema judicial».

É para mim um gosto e uma honra dar as boas-vindas a todos os intervenientes e a todos os que participam presencialmente e por via remota, num sinal do interesse que esta matéria desperta.

Num abrir e fechar de olhos decorreram mais de seis anos desde o início da aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD), a 25 de maio de 2018.

Entretanto, o recente Regulamento da Inteligência Artificial entrou para a família dos diplomas que protegem os direitos fundamentais dos cidadãos nos tempos modernos e desviou os olhares (e alguns orçamentos) das organizações.

Mas não afetou a relevância do RGPD.

Existe uma dialética clara entre os dados pessoais, enquanto permitem o desenvolvimento de sistemas de inteligência artificial e são também por estes gerados e trabalhados.

Os três «Vês» – volume, velocidade e variedade – caracterizam a explosão informacional dos nossos dias.

Surgem formas mais complexas de reprodução artificial da capacidade de raciocínio humano.

O acesso ao big data facilitou a aceleração desta evolução, com o predomínio da investigação centrada em algoritmos que, acedendo a tais informações, aprendem com base em exemplos, gerando o seu próprio conhecimento.

Há seis anos, a União Europeia deu este passo de gigante rumo à proteção da privacidade e dos dados pessoais.

O RGPD representou um marco de mudança de mentalidades e valores, obrigando ao cumprimento de regras mais rigorosas e uniformes de forma transversal pela Europa e até mesmo por todo o mundo.

E o que dizer da legislação nacional?

Segundo o artigo 97.º do RGPD, os Estados-Membros são obrigados a alterar ou revogar a legislação nacional em matéria de proteção de dados em conformidade com o Regulamento para assegurar a harmonização do Direito Europeu nesta matéria.

No que toca ao sistema judicial, o regime jurídico aplicável ao tratamento de dados, já havia sido aprovado pela Lei n.º 34/2009, de 14 de julho, anterior ao RGPD, pelo que tal diploma está naturalmente desatualizado e a carecer de uma revisão urgente, sendo uma peça de museu.

Com esse objetivo antes de terminar o período transitório previsto no artigo 99.º do RGPD, o Conselho Superior da Magistratura, o Conselho Superior dos Tribunais Administrativos e a Procuradoria-Geral da República subscreveram um documento conjunto em que adiantaram as linhas mestras das profundas alterações a efetuar àquele diploma.

Em 19 de junho de 2019 foi aprovada uma proposta de lei de alteração da Lei n.º 34/2009, a qual, contudo, previa inadmissíveis compressões do poder judicial.

Mas em 26 de julho de 2019, o Presidente da República, acolhendo a pronúncia do Conselho Superior da Magistratura e da Procuradoria Geral da República, exerceu o direito de veto, devolvendo sem promulgação este Decreto para que a Assembleia da República pudesse, nas palavras do Presidente, «proceder à sua reapreciação, ponderando as alterações que correspondam à garantia de não interferência nas áreas específicas de natureza jurisdicional e do Ministério Público, no exercício das suas funções e competências processuais».

Passados mais de 5 anos, em mais uma demonstração da inércia do poder legislativo não foi apresentada na Assembleia da República qualquer proposta de alteração que suprisse as deficiências apontadas no veto presidencial.

Durante este tempo de espera, o Conselho Superior da Magistratura decidiu constituir um Grupo de Trabalho com o objetivo de elaborar um projeto de alteração do referido regime jurídico.

O projeto acolheu os contributos do Conselho Superior dos Tribunais Administrativos e Fiscais, do Tribunal de Contas e da Procuradoria-Geral da República e foi aprovado, a 7 de novembro de 2023, pelo Plenário do Conselho Superior da Magistratura, tendo sido entregue a quem tem o poder de iniciativa legislativa.

Neste tempo de espera infinito importa irmos falando sobre a aplicação ou a desaplicação das Leis Nacionais sobre a proteção de dados pessoais, na esperança de que quem está em falta nos ouça.

E não só de leis, mas também da imperiosa mudança de "cultura" das organizações públicas e privadas, que se habituaram a fazer o que sempre foi feito, porque sempre foi feito assim.

E ainda do papel dos tribunais na importante tarefa de harmonizar o direito fundamental à proteção de dados com outros direitos fundamentais.

Dissipada a nuvem do não saber, há que assumir o desafio da conformidade com o RGPD não só como obrigação legal, mas como uma componente essencial da ética na era da inteligência artificial.

Espero que esta mesa-redonda seja proveitosa e seja mais uma pequena luz que no firmamento ilumine o caminho no sentido de uma segura e efetiva proteção dos dados pessoais. •

OS DESAFIOS DA COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (CNPD) ENQUANTO AUTORIDADE DE SUPERVISÃO

Paula Meira Lourenço
Presidente da Comissão Nacional de Proteção de Dados

Excelentíssimo Presidente do Supremo Tribunal de Justiça
Juiz Conselheiro João Cura Mariano
Excelência

Ilustres Oradores, Convidados e audiência aqui presente e remotamente, permitam-me que cumprimente todos Vós na pessoa de Sua Excelência o Senhor Presidente do Supremo Tribunal de Justiça, a quem agradeço, em meu nome e em nome da Comissão Nacional de Proteção de Dados, o honroso convite para celebrar o Dia da Proteção de Dados, aqui no Supremo Tribunal de Justiça (Tri-

bunal criado na década de 30 do século XIX, durante a guerra civil que opôs absolutistas e liberais, com a vitória destes últimos, há quase 2 séculos), com uma intervenção dedicada ao tema "**Os desafios da Comissão Nacional de Proteção de Dados (CNPD) enquanto Autoridade de supervisão**" em 2025.

Apresentar os desafios da Comissão Nacional de Proteção de Dados, que corresponde a apresentar os desafios da proteção de dados pessoais por cada um de nós, numa sociedade em acelerada e constante evolução, na qual as respostas e soluções para as questões que se colocam hoje, ficam de imediato desatualizadas e sem utilidade prática, sobretudo no que respeita à tentativa de assegurar a sua efetiva regulação e regulamentação normativa, constitui um grande desafio.

Talvez tenha sido esta, uma das razões pelas quais o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados - RGPD), marcou a passagem de um modelo de heteroregulação, para um modelo de autorregulação, mais condicente com o dinamismo e a flexibilidade que a permanente desadequação das soluções normativas impõe, com uma análise do risco decorrente das particularidades do caso concreto, com a complexidade de cada área e sector (saúde, económico, financeiro, etc..).

Atualmente, há uma autorregulação dinâmica em cada setor, que implica uma reflexão periódica e constante sobre os seus próprios desafios e oportunidades, ainda que sob a interpretação normativa uniformizadora do RGPD que assegura a equidade de soluções em sede de tratamento de dados pessoais das pessoas singulares, como se impunha quando se trata de proteger direitos humanos fundamentais, como tal previstos no n.º 1, do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, no n.º 1, do artigo 16.º do Tratado de Funcionamento da União Europeia, e no artigo 35.º da Constituição da República Portuguesa (CRP), o qual deve ser conjugado com outros princípios e direitos fundamentais conexos, como seja, os princípios da igualdade e não discriminação em razão de ascendência, sexo, raça, etnia, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual (artigo 13.º da CRP), o direito à reserva da intimidade da vida privada, à identidade pessoal, à identidade genética do ser humano, ao desenvolvimento da personalidade, ao bom nome, à reputação e à imagem (artigo 26.º da CRP), e bem assim o direito à liberdade (artigo 27.º da CRP) – direitos, liberdades e garantias constitucionais que assumem particular relevância em ambiente digital.

O RGPD permitiu ainda reforçar a cooperação entre os países do Espaço Económico Europeu no seio do Comité Europeu para a Proteção de Dados, em cujas reuniões a Comissão Nacional de Proteção de Dados e a Autoridade Europeia de Proteção de Dados, participam de forma muito ativa, sendo hoje crescente a utilização de instrumentos jurídicos de cooperação (assistência mútua e realização de operações conjuntas) no tratamento de casos transfronteiriços, para facilitar a obtenção de consensos, e bem assim os procedimentos de controlo da coerência, tendo em vista a interpretação e aplicação uniforme dos princípios e normas jurídicas previstas no RGPD.

E tendo em vista alcançar esse mesmo desiderato, a Comissão Nacional de Proteção de Dados tem ainda, ao nível europeu, participado ativamente no Comité de Supervisão Coordenada, para os sistemas de informação europeus, e na Conferência Europeia de Comissários de Proteção de Dados.

Destaco ainda que no dia 25 de junho de 2024, um dia após ter organizado a Conferência Internacional "*Proteção de Dados Pessoais: que futuro estamos a construir*", que se realizou na Sala do Senado da Assembleia da República, comemorativa do seu 30.º aniversário ao serviço de Portugal, de forma independente, isenta, objetiva, imparcial e transparente, assegurando o estrito cumprimento da lei, a Comissão Nacional de Proteção de Dados decidiu reforçar a cooperação institucional entre os Países de Língua Oficial Portuguesa, e lançou a **Rede Lusófona de Proteção de Dados,** com a assinatura da "Declaração de Lisboa", na sede da CNPD, entre as Autoridades Lusófonas de Proteção de Dados de Angola (Agência de Protecção de Dados de Angola – APD), do Brasil (Autoridade Nacional de Proteção de Dados do Brasil – ANPD), de Cabo Verde (Comissão Nacional de Proteção de Dados de Cabo Verde – CNPD), de Portugal (CNPD) e de São Tomé e Príncipe (Agência Nacional de Protecção de Dados Pessoais de São Tomé e Príncipe – ANPDP). A primeira reunião da Rede Lusófona de Proteção de Dados terá lugar em Cabo Verde, muito em breve.

Como a filosofia subjacente à autorregulação é mais responsabilizante para as organizações (públicas e privadas) que são as responsáveis pelo tratamento dos dados e os seus subcontratantes, e bem assim, para os Encarregados de Proteção de Dados, desde 2018 que assistimos à reorganização das instituições, que tiveram de se reinventar para corresponder aos objetivos da autorregulação, tendo designado os seus Encarregados de Proteção de Dados (artigo 37.º do RGPD), e os seus Responsáveis de Segurança da Informação (ou CISO – *Chief Information Security Officer*), porque ao fim de 6 anos de execução do RGPD, as organi-

zações responsáveis pelo tratamento dos dados compreenderam que é essencial investir mais em medidas preventivas, que possibilitem assegurar um nível de segurança adequado ao risco, nos termos impostos pelo artigo 32.º do RGPD, o que significa *(i)* proteger os dados pessoais, desde a conceção e por defeito (artigo 25.º do RGPD), e *(ii)* efetuar uma rigorosa avaliação de impacto sobre a proteção de dados (artigo 35.º do RGPD).

A CNPD, enquanto **Autoridade Nacional de Controlo** para efeitos de cumprimento e fiscalização do RGPD e da Lei n.º 58/2019, de 8 de agosto, também teve que se reinventar, pois passou a fazer uma regulação eminentemente *ex post*, uma vez que perdeu um conjunto significativo de competências legais em sede de autorização prévia (salvo situações previstas expressamente em sede de controlo prévio), e sem prejuízo de poder lançar mão de atribuições em sede de ação sancionatória, corretiva e cautelar, como seja, ordenar a suspensão de determinadas atividades, de que é exemplo a ordem da CNPD de suspensão de recolha de dados biométricos pela *Worldcoin Foundation*, de março de 2024.

Sublinhe-se que a missão da CNPD é focada na proteção de direitos fundamentais, direitos humanos, que emergiram há cerca de 50 anos com a democracia, com o eclodir do Estado de direito democrático, e que desde 1976 têm assento na Constituição da República Portuguesa – tendo Portugal sido pioneiro, a nível mundial, na sua consagração formal na nossa Lei Fundamental.

E quais os principais desafios, e oportunidades, da proteção de dados pessoais e, consequentemente, da CNPD?

1 | A necessidade de um Plano estratégico plurianual, flexível na sua execução

Em julho de 2023 a CNPD aprovou o seu **Plano Estratégico trienal**: o **Plano Plurianual de Atividades da CNPD para o triénio de 2024-2026**, no qual definiu 3 grandes objetivos e 20 vinte ações estratégicas:

> 1.º objetivo estratégico: o reforço da proteção dos dados pessoais dos cidadãos, através de uma maior divulgação ao público da missão da CNPD e dos direitos dos titulares dos dados;
>
> 2.º objetivo estratégico: o aprofundamento dos conhecimentos no domínio tecnológico e da inovação característicos da Era Digital, promovendo um enquadramento regulatório que previna e sancione más práticas, promovendo um permanente diálogo com os meios académicos, científicos e

empresariais;

3.º objetivo estratégico: o reforço da regulação dos dados pessoais através de mecanismos colaborativos e de cooperação com entidades nacionais e internacionais relevantes, e procedendo a uma reorganização dos serviços da CNPD, capacitando-a ainda mais para a resposta a novos desafios.

Permitam-me destacar algumas ações fundamentais para a missão da CNPD, dentro de cada objetivo.

No 1.º objetivo, assinalo, por um lado, o **lançamento do Plano Nacional de Formação em Proteção de Dados (PNFPD)**, em conjunto com os Pais e os Professores, e as crianças e jovens, tendo em vista um melhor entendimento do direito fundamental à proteção de dados por toda a população, envolvendo a Assembleia da República, o Governo (designadamente, o Ministério da Educação) e as autarquias locais.

E, por outro lado, destaco a **criação de um "Canal prioritário de interação"** no site da CNPD, que permita aos menores apresentarem as suas queixas online, que terão um tratamento urgente por parte da CNPD, quando se trate de disponibilização na Internet de conteúdos digitais de grande violência, sobretudo contra crianças e jovens mulheres, para que a CNPD possa ordenar a sua imediata eliminação, como medida cautelar (sem prejuízo da coordenação com o Ministério Público e os órgãos de polícia criminal).

A CNPD quer ter um papel proativo na defesa da proteção de dados das crianças e jovens em ambiente digital, e irá apresentar à Assembleia da República uma Proposta de Lei que consagre esta solução legislativa, que já provou funcionar em Espanha, onde há um procedimento administrativo cautelar, que vigora há 4 anos, no qual a Agência Espanhola de Proteção de Dados emite ordens de apagamento dos dados, que têm sido cumpridas pelas empresas reguladas em 100% dos casos e dentro do prazo definido (48 horas).

É minha convicção que há muito trabalho a fazer nesta matéria, e sublinho a recente recomendação do Governo para não utilização dos telemóveis nas Escolas, e a disponibilidade da CNPD para colaborar no projeto piloto relativo à literacia digital.

No 2.º objetivo, de aprofundamento da inovação tecnológica, característica da Era digital, saliento a criação de ferramentas eletrónicas que ajudem as entidades responsáveis pelo tratamento de dados (públicas e privadas), subcontratantes e os EPD, a cumprir as suas obrigações legais, de modo ágil, intuitivo e fácil.

O 3.º objetivo visa proceder à reorganização interna da CNPD tendo em vista a sua modernização administrativa, a agilização processual e maior eficácia; a capacitação dos recursos humanos da CNPD para a Era Digital, através de um quadro de pessoal com competências e conhecimentos técnicos relevantes para o exercício das suas atribuições legais em sede de proteção de dados pessoais no âmbito da regulação digital, da tecnologia de inteligência artificial; e o aumento da eficácia da ação sancionatória.

Estas ações estratégicas estão a ser concretizadas nos Planos de Atividades para os anos de 2024 e de 2025.

2 | A necessidade de harmonizar várias iniciativas legislativas da União Europeia entre si, e com a legislação nacional

A prolixidade legislativa da União Europeia merece uma especial atenção pois, por um lado, assiste-se à consagração de soluções desatualizadas relativamente a problemas muito complexos, carenciados de uma abordagem pluridisciplinar para a sua completa compreensão; e, por outro lado, exige-se uma especial aptidão por parte de cada Estado-Membro, e da cada Autoridade Nacional de Controlo, para proceder à articulação de todos estes instrumentos legislativos, quantas vezes só possível de alcançar com base na cooperação entre as várias Autoridades Reguladoras.

Foi isso mesmo que aconteceu com a Proposta de Lei n.º 32/XVI/1.ª, em apreciação na Assembleia da República, que visa assegurar a execução nacional do Regulamento dos Serviços Digitais (Regulamento (UE) n.º 2022/2065, do Parlamento Europeu e do Conselho, de 19 de outubro de 2022), cujo anteprojeto contou com a colaboração da CNPD no seio de um Grupo de Trabalho criado em fevereiro de 2024 (através do Despacho n.º 1747/2024, de 15 de fevereiro), no qual participaram várias Entidades Reguladoras, sendo justo destacar o trabalho desenvolvido pela Autoridade da Concorrência (AdC), pela Autoridade Nacional de Comunicações (ANACOM), como Autoridade competente e Coordenador dos Serviços Digitais em Portugal, pela Entidade Reguladora para a Comunicação Social (ERC) e pela Inspeção-Geral das Atividades Culturais (IGAC), entre outras.

Um excelente exemplo de cooperação institucional, que aproveito para publicamente assinalar.

Mas temos ainda o **Regulamento relativo à Governação Europeia de Dados** (Regulamento (UE) 2022/868, do Parlamento Europeu e do Conselho, de

30 de maio de 2022), a **Diretiva NIS 2** (Diretiva (UE) 2022/2555, de 14 de dezembro de 2022); ou o **Regulamento da Inteligência Artificial** (Regulamento (UE) n.º 2024/1689, do Parlamento Europeu e do Conselho, de 13 de junho de 2024).

3 | A regulação da Inteligência Artificial

O Regulamento da Inteligência Artificial constitui um marco regulatório decisivo de incontornável relevância do ponto de vista da geopolítica mundial, ao afirmar a Europa como o centro, o coração, da proteção dos direitos humanos e dos direitos fundamentais na era digital, dos valores éticos e jurídicos da União Europeia.

As tecnologias de IA podem trazer muitas vantagens para a Economia, benefícios para diferentes indústrias e áreas da vida (maior celeridade na execução de tarefas e poupança de encargos administrativos e financeiros). Mas é preciso garantir que essas inovações são feitas de forma ética, segura, em prol do ser humano, e onde os dados pessoais são protegidos e é cumprido o RGPD.

Como a IA envolve dados pessoais, onde há dados pessoais, a CNPD deve estar presente, e a CNPD pretende apoiar a inovação responsável da IA, garantindo o pleno respeito pela CRP, pelo RGPD e demais legislação relativa aos dados pessoais.

Mas também há riscos. Vou dar 6 exemplos de riscos evidentes da IA para a dignidade, a liberdade, e a própria identidade do ser humano, como bem demonstrou o escândalo conhecido por "Cambridge Analytics" (onde ocorreu um desvio de finalidade); a suspensão nos EUA do Projeto "COMPAS" (este sistema calculava a probabilidade de reincidência dos presos, a partir da análise de dados. Foi suspenso porque aconselhava sempre a liberdade condicional de pessoas caucasianas - e quase nunca de pessoas de raça negra -, concluindo-se que a discriminação em função da origem étnica pode ser repetida por estes sistemas IA, se os dados que analisam são racistas. O mesmo se diga de outro tipo de discriminação; sistemas de videovigilância através de registo biométrico (proibido pelo Regulamento da Inteligência Artificial); a exploração de emoções dos estudantes nas escolas (exames anulados se o sistema IA detetava determinados, como suor ou aceleração dos batimentos cardíacos; um mundo repleto de alucinações não intencionais dos sistemas de IA generativa (*deepfake*) e de riscos reputacionais (criação intencional de informação falsa e/ou difamatória); e ainda o facto de sistemas de IA já conseguirem analisar o nosso cérebro, o nosso comportamento consciente e inconsciente, e moldar a nossa forma de pensar (neurodados). Esta forma de manipulação psicológica, através de um sistema de IA, comporta um

risco elevado para a identidade humana.

Por isso, a CNPD está totalmente disponível para assegurar a regulação da IA, pois enquanto Autoridade Nacional independente, que assegura a proteção de direitos fundamentais, tem uma atuação transversal, algo fundamental para se regular uma tecnologia de uso amplo como a IA.

Esta é também a posição do Comité Europeu para a Proteção de Dados e da Autoridade Europeia de Proteção de Dados, expressa no Parecer conjunto 5/2021 do CEPD e da AEPD sobre a Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial), no qual bem frisaram que as Autoridades Nacionais de Proteção de Dados de cada Estado-Membro são as Autoridades vocacionadas para receber as competências legais em sede de IA, porque asseguram uma supervisão independente, com uma abordagem com base no risco (avaliações de impacto de proteção de dados), e já atentas à proibição de categorização das pessoas com base na biometria (ou seja, origem étnica, género, orientação sexual).

Mais recentemente, Comité Europeu para a Proteção de Dados aprovou a Declaração 4/2024 sobre o papel das Autoridades Nacionais de Proteção de Dados no quadro do Regulamento Inteligência Artificial, na qual se defende que estas Autoridades devem ser designadas as Autoridades competentes para efeitos do Regulamento Inteligência Artificial, e bem assim o Parecer 28/2024, de 17 de dezembro, sobre a utilização de dados pessoais para o desenvolvimento e a implantação de modelos de IA.

Por último, não é de admirar que no **Brasil, a Autoridade Nacional de Proteção de Dados tenha sido a Autoridade escolhida para a assegurar a regulação da IA** (Projeto de Lei em discussão) e na **Europa, a Autoridade Europeia de Proteção de Dados**[1] **tenha sido a Entidade escolhida para efeitos de execução do Regulamento de IA nas instituições europeias, e bem assim as Autoridades Nacionais da Holanda e de Malta** – porque a utilização da IA envolve riscos quanto à salvaguarda de princípios e direitos fundamentais, éticos, jurídicos que colocam em causa a identidade humana.

1. No dia 3 de junho de 2024, a Autoridade Europeia para a Proteção de Dados divulgou as "Orientações em sede de IA generativa: abraçar oportunidades e proteger as pessoas" (*Guidelines on generative AI: embracing opportunities, protecting people*) no seu papel de Autoridade de Controlo da proteção de dados da União Europeia (e não enquanto Autoridade Supervisora de IA ao abrigo do Regulamento de IA, papel que também assume). Trata-se de orientações muito relevantes, sobre as quais importa refletir.

Tendo presente a atual relevância da IA, a CNPD inseriu duas novas ações estratégicas no seu Plano de Atividades para 2025:

- **Ação 21** – Capacitação da CNPD para o exercício das suas atribuições legais em sede de proteção de dados pessoais no âmbito da regulação digital.
- **Ação 22** – Reforço da capacitação da CNPD em matéria de proteção de dados pessoais no âmbito da tecnologia de inteligência artificial.

4 | A necessidade de reorganização, modernização e rejuvenescimento da CNPD, para assegurar a eficácia da sua atividade

No final de 2023, o Instituto Kaizen entregou à CNPD o estudo intitulado "Visão de Melhoria para a Reorganização Interna", que constitui uma rigorosa análise e diagnóstico dos procedimentos e dos recursos humanos necessários a uma resposta célere e adequada por parte da CNPD, elaborada após um intenso trabalho com um âmbito alargado (análise da situação; formação e boas práticas Kaizen; desenho de soluções e mapeamento da situação futura em termos de eficiência e eficácia de processos, dimensionamento de recursos e adequação de sistemas e plataformas), utilizando uma metodologia participativa, em que todos foram convidados a dar o seu contributo (Presidente, os Vogais, a Secretária, e os trabalhadores da CNPD), quer na recolha e debate dos dados e procedimentos que sustentam a análise (que contou com múltiplas sessões de trabalho presenciais), quer na apresentação e discussão da análise preliminar, que precedeu a entrega final do estudo.

A "Visão de Melhoria para a Reorganização Interna" da CNPD contempla 6 (seis) iniciativas, sendo que uma delas assinala a necessidade de criação de uma nova estrutura (um novo organograma), e no qual se preveja um número adequado de Departamentos e respetivos dirigentes (comparando com as Autoridades de Espanha, França, Bélgica e Itália, por exemplo, verifica-se que apenas a CNPD não atualizou depois do RGPD a sua orgânica, só a CNPD não tem dirigentes nas suas Unidades), de coordenadores e de técnicos, tendo em vista uma maior agilidade, que se traduz num aumento de produtividade e melhoria do serviço ao cidadão; e uma outra iniciativa pretende assegurar o aumento da autonomia e da responsabilidades a líderes intermédios, para que os processos possam fluir com maior facilidade, aumentando a celeridade de resposta final da CNPD, através da redução do tempo da tramitação dos processos.

É ainda essencial continuar o processo de contratação de pessoas que permi-

ta o rejuvenescimento da Comissão, pois do conjunto dos 29 (vinte e nove) trabalhadores, apenas 18 são licenciados a trabalhar nos processos, a maioria tem idade igual ou superior a 50 anos, e 75,86% concentra-se no escalão etário dos 45 aos 64 anos, sendo inelutável propor a consagração de uma solução legislativa que permita contratar pessoas através de um regime atrativo e concorrencial de contratação, para atuar num mercado cada vez mais exigente e competitivo.

A integral execução destas relevantes iniciativas de melhoria interna sugeridas pelo Instituto Kaizen implica que se proceda à alteração legislativa da atual Lei de Organização e Funcionamento da CNPD, aprovada pela Lei n.º 43/2004 de 18 de Agosto, na redação dada pela Lei n.º 58/2019, de 8 de agosto, razão pela qual a CNPD apresentará junto dos órgãos de soberania com competência legislativa - Assembleia da República e Governo - uma Proposta de Lei que permita a respetiva implementação no âmbito da criação dos estatutos da CNPD coincidentes com os atuais desafios da Autoridade de Controlo Nacional em sede de proteção de dados pessoais.

Por último, a **Ação 23 – Aumento da eficácia da ação sancionatória** do Plano de Atividades da CNPD para 2025 visa assegurar um regime jurídico eficaz em sede de tramitação dos processos contraordenacionais, em conjugação com o RGPD, tendo presente a evolução legislativa ocorrida nos regimes contraordenacionais mais modernos, como seja, o regime jurídico das contraordenações económicas, aprovado pelo Decreto-Lei n.º 9/2021, de 29 de janeiro, ou o regime quadro das contraordenações do sector das comunicações, aprovado pela Lei n.º 99/2009, de 4 de setembro, na redação dada pela Lei n.º 16/2022, de 16 de agosto), que poderão servir de inspiração a um novo quadro jurídico das contraordenações na proteção de dados pessoais.

A CNPD apresentará uma Proposta de Lei junto dos órgãos de soberania com competência legislativa - Assembleia da República e Governo – tendo em vista uma tramitação num processo eletrónico, que permita *(i)* a eliminação de atos repetitivos e em suporte papel (como seja, a necessidade de os arguidos enviarem à CNPD, em suporte papel, os originais e duplicados dos atos processuais que praticam, quando a CNPD acaba por ter que digitalizar essas peças processuais, para as inserir no seu sistema informático, e que devolver um dos duplicados aos arguidos, com uma nota de boa receção – tarefas repetitivas e onerosas, que se eliminam com grande vantagem em sede de poupança de recursos humanos, custos administrativos, financeiros e ambientais); *(ii)* a redução do tempo de duração dos processos de contraordenação (que os processos eletrónicos sempre

permitem), compaginada com prazos mais dilatados de prescrição; *(iii)* e, em caso de impugnação judicial de uma decisão contraordenacional, a previsão clara de qual o tribunal competente (uma vez que a Lei n.º 58/2019, de 8 de agosto, tem originado dúvidas de interpretação e conflitos negativos de competência), e de que a CNPD pode intervir de forma autónoma (à semelhança de outras Entidades Reguladoras, como seja, a Autoridade Nacional de Comunicações, o Banco de Portugal ou a Comissão do Mercado de Valores Mobiliários).

Minhas Senhoras
Meus Senhores
Saudando, uma vez mais, Sua Excelência o Presidente do Supremo Tribunal de Justiça, pela iniciativa de celebração do Dia da Proteção de Dados com este evento, espero que esta comemoração permita assinalar, com esperança, audácia, coragem e determinação, e com uma visão prospetiva, adaptada aos atuais desafios e oportunidades, a incontornável relevância da proteção dos dados pessoais num mundo em constante mudança, e que precisa da ação de todas e de todos. •


SUPREMO TRIBUNAL DE JUSTIÇA
DIA DA PROTEÇÃO DE DADOS 2025
6 ANOS

MESA REDONDA

SEIS ANOS DE RGPD
BALANÇO DA (DES)APLICAÇÃO DA LEI NACIONAL DE EXECUÇÃO E DA LEI SOBRE O TRATAMENTO DE DADOS NO SISTEMA JUDICIAL

Susana Antas Videira
Diretora-Geral da Política de Justiça
Professora Associada da Faculdade de Direito da Universidade de Lisboa e da Universidade Europeia[1]

Há seis anos, quase sete, no dia 25 de maio de 2018, entrou em vigor o Regulamento Geral sobre a Proteção de Dados (RGPD).

Trata-se de um período temporal que nos permite, com segurança, efetuar uma avaliação consistente deste regime jurídico.

Aliás, ainda no ano passado, a Comissão Europeia procedeu, tal como previsto no artigo 97.º do RGPD, à avaliação do arco de tempo de vigência deste diploma estruturante.

Tal processo avaliativo foi seguido, com atenção, pela Direção-Geral da Política de Justiça (DGPJ), enquanto entidade do Ministério da Justiça com competência para o acompanhamento dos assuntos europeus.

E, por isso, gostaríamos de começar esta reflexão por partilhar algumas conclusões sobre a aplicação do RGPD a que quer o Conselho quer a Comissão chegaram e com as quais só podemos concordar.

Desde logo, como primeira nota, constata-se que, não obstante todos os desafios que colocou e que ainda convoca – e que vai, certamente, colocar no futuro –, o RGPD é, no essencial, um **caso de sucesso**, enquanto quadro jurídico adequa-

1. O presente artigo publica a nossa intervenção na Mesa Redonda da Conferência subordinada ao tema SEIS ANOS DE RGPD - BALANÇO DA (DES)APLICAÇÃO DA LEI NACIONAL DE EXECUÇÃO E DA LEI SOBRE O TRATAMENTO DE DADOS NO SISTEMA JUDICIAL, organizada pelo Supremo Tribunal de Justiça em 28 de janeiro de 2025, no Salão Nobre do Tribunal, para assinalar o Dia da Proteção de Dados 2025.

do para a proteção dos dados pessoais das pessoas singulares na União Europeia e um marco fundamental no reforço dos direitos fundamentais ao respeito pela vida privada e familiar, à privacidade do domicílio e das comunicações e à proteção dos dados pessoais.

Numa matéria com a sensibilidade tão própria dos direitos fundamentais e com a relevância que a privacidade e a proteção de dados adquiriram nas últimas décadas, numa ótica até quotidiana, o RGPD permitiu resultados significativos para as pessoas e para as empresas, harmonizando o direito da União Europeia e proporcionando aos cidadãos europeus o mesmo nível de proteção, independentemente do país em que se encontram.

Ao mesmo tempo, potenciou um maior controlo sobre o tratamento dos seus dados pessoais, enquanto impôs obrigações proporcionadas aos responsáveis pelo tratamento.

Os fundamentos do RGPD, alicerçados em princípios aplicados de forma combinada e flexível, prevendo direitos específicos para as pessoas singulares e obrigações também específicas para os responsáveis pelo tratamento dos dados e para os subcontratantes, tem-se revelado uma opção globalmente correta, eficaz na proteção dos direitos dos titulares dos dados e suscetível de se adaptar à evolução, às mudanças tecnológicas e a um mundo cada vez mais digitalizado.

Ao reforçar os direitos dos titulares dos dados, o RGPD contribui também (embora muito haja ainda a fazer neste âmbito, designadamente em Portugal) para ampliar, entre a opinião pública, o grau de consciência, o conhecimento e a compreensão dos direitos em matéria de proteção de dados.

Esse efeito positivo sobre a transparência e a capacitação dos titulares dos dados reflete-se, por sua vez, no aumento do exercício dos direitos dos titulares dos dados.

A este propósito e demonstrativo da consciencialização dos seus direitos, não deixa de ser relevante que os titulares dos direitos apresentem junto das várias autoridades nacionais de proteção de dados europeias um número crescente de reclamações por ano.

Simultaneamente, tanto os responsáveis pelo tratamento como os subcontratantes estão hoje mais conscientes das suas obrigações e das consequências do tratamento de dados que não esteja em conformidade com o RGPD.

Por outro lado, a responsabilidade das entidades a que se aplica o RGPD foi reforçada e os esforços de conformidade também tiveram um impacto favorável na governação dos dados nas diferentes organizações, contribuindo para uma

maior proteção dos dados pessoais das pessoas singulares.

Acresce que ao reforçar a confiança e a segurança jurídica, o RGPD veio, também, facilitar os fluxos transfronteiriços de dados na União Europeia, robustecendo outro dos seus grandes objetivos: a livre circulação de dados na União Europeia, o mercado interno e o desenvolvimento da economia digital, contribuindo para a criação de condições de concorrência equitativa entre empresas.

Ao mesmo tempo, o RGPD é uma das pedras angulares da estratégia da União Europeia para a transformação digital, estando os seus princípios básicos — tratamento lícito, leal, seguro e transparente dos dados pessoais, limitado nas suas finalidades e na sua conservação, minimizado e exato quanto aos dados utilizados — subjacentes a todas as políticas da União Europeia que envolvem o tratamento de dados pessoais.

De facto, desde a entrada em vigor do RGPD foram vários os instrumentos legislativos adotados a nível europeu que têm relevância no setor digital e que oferecem impacto a nível do tratamento dos dados pessoais, e que, por isso mesmo, reconhecem o tratamento e os princípios consagrados no RGPD.

Sem a preocupação de sermos exaustivos, convocam-se a este propósito, pela sua relação estreita com a proteção de dados pessoais e a título de exemplo, o Regulamento dos Mercados Digitais, o Regulamento dos Serviços Digitais, o Regulamento Governação de Dados – cumprindo referir, neste contexto, que, muito recentemente, no passado dia 23 de janeiro, foi publicado o Decreto-Lei n.º 2/2025, que executa este Regulamento – ou o Regulamento da Inteligência Artificial.

Ainda mais recente, aprovado há escassos dias, em 21 de janeiro, o Regulamento Espaço Europeu de Dados de Saúde serve o objetivo de melhorar o acesso das pessoas aos seus dados de saúde eletrónicos pessoais, permitindo ainda a reutilização de dados para fins de investigação e inovação. Estaremos, seguramente, perante uma afirmação da transformação digital também na área essencial da saúde.

Neste contexto, seguro é afirmar que o desafio a que todos somos convocados, desde os reguladores às entidades públicas e empresas, é garantir a coerência com o RGPD na aplicação de todos esses instrumentos.

As vantagens do RGPD refletem-se também no contributo que constitui para o reforço da cultura de proteção de dados não só na União Europeia mas também a nível mundial, porquanto esta é uma área onde o chamado "efeito Bruxelas", entendido como a capacidade de a legislação da União influenciar a legislação de

outras ordens jurídicas, se faz claramente sentir.

O RGPD tem sido, portanto, crucial para posicionar a União Europeia como referência internacional e é uma norma (diríamos mesmo, a norma) orientadora para a proteção de dados e da privacidade um pouco por todo o mundo.

No entanto, como antes assinalado, o RGPD continua a colocar inúmeros desafios.

Uma dessas instigações diz respeito ao esforço que ainda impõe quer às pequenas e médias empresas, quer a investigadores e a centros de investigação, por exemplo.

Estas são áreas que, como concluiu a Comissão Europeia, necessitam de orientações específicas, mais claras e úteis por parte das autoridades de proteção de dados, que permitam a interpretação, compreensão e aplicação em toda a União Europeia dos princípios, conceitos jurídicos e direitos previsto no RGPD, a fim de assegurar a coerência e a segurança jurídica.

Outro desafio que se coloca diz respeito à necessidade de um tratamento mais eficiente e harmonizado dos casos transfronteiriços em toda a UE, em especial tendo em conta as diferenças nos procedimentos administrativos nacionais e nas interpretações de conceitos no mecanismo de cooperação do RGPD, que existem e persistem, não obstante o sistema de balcão único previsto.

A este propósito, cumpre recordar que a Comissão Europeia apresentou em 2023 uma proposta de regulamento relativo às normas processuais, que completa o RGPD, estabelecendo regras pormenorizadas sobre as reclamações transfronteiriças, a participação do autor da reclamação, os direitos processuais das partes objeto de investigação e a cooperação entre as autoridades de proteção de dados.

Esta proposta, que tem sido acompanhada pela DGPJ no âmbito das suas competências em matéria comunitária, encontra-se, neste momento, a ser negociada entre o Conselho e o Parlamento Europeu, e acreditamos que contribuirá para agilizar e tornar mais eficaz a aplicação do RGPD pelas autoridades de controlo, ao mesmo tempo que assegura os direitos das partes.

Tal não significa, no entanto, que a aplicação do RGPD não esteja já a demonstrar resultados expressivos.

De facto, nos últimos anos registou-se um aumento das medidas tomadas pelas autoridades de proteção de dados, incluindo a aplicação de coimas substanciais em processos mediáticos contra «grandes empresas tecnológicas» multinacionais.

A aplicação destas medidas contribui, também, para que as empresas tenham em consideração, de forma séria, a proteção de dados e assumam, também de modo relevante, uma cultura de conformidade com esse desígnio.

Mas, outra necessidade que se coloca respeita à sensibilização das pessoas para o RGPD, algo que, particularmente no nosso país, justifica ainda um longo caminho a percorrer.

A este propósito, é significativo recordar que um estudo do Eurobarómetro realizado em março/abril de 2024 indica que se 72% dos inquiridos em toda a União Europeia afirma ter ouvido falar do RGPD, apenas 40% sabem em que consiste esse Regulamento.

E em Portugal, a percentagem de inquiridos que já ouviu falar do RGPD (73%) é até ligeiramente superior à média europeia, mas apenas 28% dos inquiridos afirma saber o que é, efetivamente, tal normativo.

Ora, não podemos exercer convenientemente os direitos que não sabemos existirem, pelo que é fundamental continuar a trabalhar para dar a conhecer a todos os direitos em referência.

Outro tópico que, nesta sede, cumpre explorar, de forma necessariamente perfunctória, tem que ver com a circunstância de, no espaço europeu, se começar a vislumbrar um "novo mandato" para o RGPD.

Falamos do início de um novo mandato porque será brevemente nomeada, para um novo ciclo, a Autoridade Europeia para a Proteção de Dados, que tem aumentado a sua influência ao nível da União Europeia pelo seu competente contributo para a definição de políticas neste domínio.

Ainda que não seja um colegislador, tem-se, pois, assumido como uma peça-chave na construção das regras da política digital europeia.

A este propósito, cumpre assinalar que há escassas semanas o Parlamento Europeu realizou audições com os quatro candidatos pré-selecionados para a próxima Autoridade e é interessante repararmos na preocupação subjacente às audições, porque demonstra, em termos bastantes, que o Parlamento Europeu, nesta recente composição, estará particularmente atento à forma como se irá lidar com a proteção de dados face à segurança, às novas tecnologias e à geopolítica.

A demonstrá-lo está o facto de as audições terem sido marcadas por questões relacionadas com o modo como deve ser encarado o equilíbrio entre a privacidade e os direitos fundamentais e a segurança, sobre como lidar com a pressão crescente dos "gigantes tecnológicos" e ainda quanto à postura a adotar face à inteligência artificial.

A propósito da inteligência artificial, permitam-nos referenciar o papel do Conselho Europeu de Proteção de Dados[2], que tem vindo a alertar para vários aspetos da proteção de dados relacionados com o processamento de dados pessoais no contexto de modelos de inteligência artificial.

A inteligência artificial é incontornável e está cada vez mais presente.

Mas, atendendo aos riscos que pode representar, reclama várias cautelas, sobretudo pelas significativas implicações para o futuro.

Inovação e responsabilidade, não temos dúvidas, têm de caminhar a *pari passu*…

Num dos mais recentes pareceres deste Conselho[3] foi destacada a inteligência artificial e os temas que especialmente suscita, de que salientamos, a título meramente ilustrativo:

- O cuidado com a **anonimização caso a caso**, considerando a probabilidade de extração de dados pessoais e a possibilidade de dados através de consultas, reduzindo a identificabilidade e impedindo a extração de dados.
- O **interesse legítimo como base jurídica**: o tratamento de dados no desenvolvimento e implementação de modelos de inteligência artificial deve ter como base jurídica o interesse legítimo, salvaguardando que este não deve ser sobreposto aos interesses dos titulares dos dados. Cabe aos responsáveis pelo tratamento de dados a implementação de um "teste" do interesse legítimo, de modo a concluírem que o tratamento dos dados é mesmo necessário e se existem ou não alternativas menos intrusivas.
- O **risco para os direitos fundamentais**: aqui não trazemos, certamente, novidades. O desenvolvimento e a implementação de modelos de inteligência artificial podem representar riscos para os direitos fundamentais. Seja pela natureza dos dados, do contexto em que são tratados ou até pelas expetativas razoáveis dos titulares dos dados, é essencial que reflitamos sobre medidas de mitigação do impacto do tratamento nos titulares dos dados.
- E por fim, naturalmente, não esqueçamos as consequências do **tratamento ilícito de dados pessoais**, desde a fase de desenvolvimento de um modelo de inteligência artificial, como no subsequente tratamento.

2. O *European Data Protection Board* (Conselho Europeu de Proteção de Dados), com a entrada em vigor do RGPD, substituiu o conhecido "Grupo de Trabalho do Artigo 29.º", que lidava, até então, com as questões relacionadas com a proteção da privacidade e dos dados pessoais.

3. Parecer n.º 28/2024, adotado em 17/12/2024.

Estas serão apenas algumas orientações para assegurar a aplicação consistente do RGPD no desenvolvimento e implementação de modelos de inteligência artificial, promovendo a inovação responsável a proteção dos dados pessoais dos cidadãos.

Vem a propósito a popular frase que compara os dados "*ao petróleo da era digital*" e, por isso, um dos recursos mais valiosos da atualidade.

Mas para além da analogia, importa não perder de vista a diferença: sem o devido processamento e sem a análise adequada, ou com um uso excessivo ou irresponsável, perde-se, inelutavelmente, o valor deste valioso "recurso".

Tomando como mote este uso excessivo, ilícito ou, no limite, irresponsável, permitam que atentemos, por escassos instantes, – ou não fosse este um dos temas desta nossa Mesa Redonda –, na Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD na nossa ordem jurídica e da sua parcial desaplicação por Deliberação da CNPD.

Conhecemos bem as dúvidas e até as críticas que este diploma suscita, bem como a posição adotada, na referida Deliberação, pela CNPD, que determinou desaplicar algumas das respetivas disposições, considerando o entendimento de contrariedade normativa face ao RGPD[4].

4. Referimo-nos concretamente à **Deliberação 2019/494**, pela qual a CNPD identificou e deliberou desaplicar várias normas da Lei n.º 58/2019, de 8 de agosto, por considerar que este normativo continha várias disposições que comprometem a aplicação uniforme do Regulamento Geral sobre a Proteção de Dados na União Europeia. As principais áreas onde a lei nacional portuguesa afeta a aplicação uniforme do RGPD incluem, no entendimento da CNPD:

1. **Âmbito de Aplicação Territorial**: o artigo 2.º da Lei n.º 58/2019 define o âmbito de aplicação da lei de uma forma que compromete a aplicação das normas procedimentais e a distribuição de competências entre as autoridades de controlo dos Estados-Membros em tratamentos transfronteiriços. A lei nacional aplica-se a tratamentos realizados em território nacional, mesmo que o estabelecimento principal do responsável esteja noutro Estado-Membro, o que é incompatível com o mecanismo de balcão único do RGPD. Além disso, a lei nacional limita a aplicação do RGPD a dados de cidadãos portugueses em postos consulares, contrariando a aplicação geral do RGPD em embaixadas e consulados portugueses;
2. **Direitos de Informação e Acesso:** O artigo 20.º, n.º 1, da lei nacional restringe os direitos de informação e acesso a dados pessoais quando a lei impõe um dever de segredo oponível ao titular dos dados. Esta restrição não está em conformidade com o RGPD, que apenas admite limitações específicas e justificadas, nos termos do artigo 23.º do RGPD, não cumprindo, assim, os requisitos de especificação de finalidade e proporcionalidade;
3. **Tratamento de Dados para Finalidades Distintas**: o artigo 23.º da lei nacional permite o tratamento de dados pessoais por entidades públicas para finalidades diferentes das que justificaram a recolha, desde que seja para prosseguir o interesse público. Contudo, o RGPD exige que tais desvios sejam devidamente especificados, proporcionais e necessários, o que não se verifica na generalidade da norma nacional. Esta disposição também contraria o princípio da limitação das finalidades;
4. **Consentimento do Trabalhador**: o artigo 28.º, n.º 3, alínea a) estabelece que o consentimento do trabalhador não é requisito de legitimidade para o tratamento de dados se resultar em vantagem jurídica ou económica para o trabalhador. Esta disposição restringe excessivamente a relevância do consentimento do trabalhador, contrariando o requisito de livre manifestação de vontade previsto no RGPD;
5. **Regime das Contraordenações**: os artigos 37.º, 38.º e 39.º da lei nacional definem um regime de contraordenações que contraria o estabelecido no artigo 83.º do RGPD. A lei nacional define sanções distintas com base na natureza dolosa ou negligente da conduta, o que não é permitido pelo RGPD. A lei também distingue a informação relevante da demais, o que não encontra respaldo no RGPD. Além disso, a lei define molduras sancionatórias distintas com base na dimensão das empresas e na natureza dos sujeitos, afastando os limites máximos definidos pelo RGPD. A lei também estabelece critérios adicionais para a determinação da coima e impõe uma advertência prévia para infrações negligentes, o que é incompatível com a discricionariedade conferida pelo RGPD às autoridades de controlo;

Nomeadamente – e aqui identificaremos dois aspetos que vão ao encontro do mote que lançamos – o **tratamento de dados para finalidades distintas**, presente no artigo 23.º da lei nacional[5] e o **regime das contraordenações**, consagrado nos artigos 37.º a 39.º da mesma lei.

Destacamos o tratamento de dados para finalidades distintas, mesmo que para uma fundamentada prossecução do interesse público (como parece ser a intenção da lei nacional), porque, de facto, parece-nos crucial que se pugne pelo respeito do **princípio da finalidade**, à luz do artigo 5.º do RGPD[6].

É à luz deste princípio que se promove a **transparência no tratamento de dados pessoais** e se garante que o tratamento é feito de forma responsável e dentro dos limites daquilo que é expetável para os titulares dos dados.

Naturalmente que o procedimento não pode deixar de passar pela obrigatoriedade de ponderação da reutilização de dados para outras finalidades, a par da devida informação aos titulares ou até à obtenção do seu consentimento. Por aqui acautelamos o uso excessivo (ou mesmo ilícito) dos dados.

Já em matéria de **contraordenações**, seja pelo *i)* afastamento da conduta por negligência[7] – que não resulta do RGPD –, *ii)* pela definição de molduras sancionatórias distintas em função da dimensão das empresas ou da natureza

---

6. Caducidade do Consentimento: o artigo 61.°, n.º 2 da lei nacional estabelece que o tratamento de dados é lícito até à cessação do contrato, caso a caducidade do consentimento seja motivo de cessação do contrato. Esta disposição confunde o consentimento com o contrato como fundamentos de licitude do tratamento de dados, condicionando a validade do contrato ao consentimento do titular;

7. Autorizações e Notificações à CNPD: o artigo 62.°, n.° 2 da lei nacional consagra que todas as normas que preveem autorizações ou notificações de tratamentos de dados à CNPD deixam de vigorar à data de entrada em vigor do RGPD, o que corresponde a 25 de maio de 2016, aplicando retroativamente o RGPD, em violação do fixado no n.° 2 do artigo 99.°. Em resumo, a CNPD identificou várias disposições da Lei n.° 58/2019 que impedem a aplicação uniforme do RGPD, levando à sua desaplicação em futuros casos concretos. A não aplicação destas disposições tem como consequência a aplicação direta das normas do RGPD que, na leitura da CNPD, estavam a ser restringidas ou contrariadas.

5. Cfr. artigo 23.°, n.° 1 da Lei n.° 58/2019: *O tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha tem natureza excecional e deve ser devidamente fundamentado com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado, nos termos da alínea e) do n.° 1, do n.°4 do artigo 6.° e da alínea g) do n.º 2 do artigo 9.° do RGPD*. A CNPD considera que este artigo viola o RGPD por não especificar finalidades de interesse público que podem justificar a reutilização, como impõe o n.° 4 do artigo 6.° do RGPD: "**Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.°**", caberá ao responsável pelo tratamento verificar se o tratamento para outros fins é ou não compatível com a finalidade para a qual os dados foram inicial e originariamente recolhidos (…).

6. V. artigo 5.°, n.° 1, al. b) do RGPD: os dados pessoais são "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»)".

7. A alínea a) do n.° 1 do artigo 37.° da Lei n.° 58/2019 consagra que constituem contraordenações muito graves "*os tratamentos de dados pessoais com inobservância **dolosa** dos princípios consagrados no artigo 5.° do RGPD*", mas o RGPD não distingue a natureza negligente ou dolosa da conduta, não permitindo aos Estados-Membros que alterem o elenco de infrações aí previstas (artigo 83.° do RGPD).

(coletiva ou singular) de quem trata os dados – que não resulta do RGPD –, ou mesmo *iii)* pela advertência do agente para cumprimento da obrigação omitida previamente à instauração de um processo de contraordenação, que como bem se lê na Deliberação da CNPD "esvazia o poder discricionário reconhecido pelo RGPD à autoridade de controlo" – que também não resulta do RGPD – urge restabelecer o alinhamento e harmonização com o RGPD, sob pena de não se alcançar, com êxito, o controlo e uma governação responsável dos dados.

Em primeira e última linha, a desconformidade entre a legislação nacional e a legislação europeia faz perigar o efeito direto dos regulamentos europeus, o primordial objetivo de uma aplicação uniformizada em todos os Estados-Membros e, constitucionalmente falando, o princípio do primado do direito da União.

Já quanto à aplicação do RGPD aos tribunais, é hoje por demais sabido e julgo que indiscutível que o RGPD se aplica aos tribunais, com as especificidades previstas na lei e em absoluta observância do **princípio da independência**, mesmo na sua função jurisdicional, tendo tal sido justamente reafirmado pelo Tribunal de Justiça da União Europeia, por exemplo no Acórdão emitido no âmbito do processo C-245/20[8].

E julgamos ser, de igual modo, consensual que os termos em que ocorre a aplicação do RGPD nos tribunais, através da Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, se encontra desatualizada e carecida de revisão.

E não precisamos de maiores argumentos para perceber uma primeira razão de ordem natural…

O RGPD é posterior a esta Lei e enquanto regulamento obrigatório e diretamente aplicável e, igualmente, por efeito do princípio do primado, deve refletir-se sobre uma revisitação deste normativo, sob pena de se entender que algumas normas se encontram automaticamente derrogadas por efeito do RGPD.

Trata-se, não obstante, de matéria complexa, que se enquadra no âmbito da competência, ainda que relativa, da Assembleia da República.

Mas o caminho já começou a ser trilhado, primeiro em 2019, com a proposta de lei que foi objeto de veto por S. Exa. o Presidente da República, e mais recentemente, com os trabalhos desenvolvidos [também] pelo Conselho Superior da Magistratura, que, mais uma vez, aproveitamos para saudar.

8. Este acórdão clarificou a aplicação do RGPD aos tribunais, definindo a amplitude com que deve ser interpretado o conceito de atuação no exercício da sua função jurisdicional. Neste processo discutiu-se a disponibilização a um jornalista de documentos dos autos de um processo judicial que continha dados pessoais.

Os motivos para esta revisitação são vários, permitindo-nos destacar como pontos basilares o respeito pela independência do poder judicial e, consequentemente, a garantia de não ingerência de entidades/autoridades administrativas no poder judiciário.

Estes pontos de partida refletem-se em outros, igualmente relevantes, designadamente:

- a necessidade de indicar expressamente quem são os responsáveis pelo tratamento dos dados pessoais nos processos judiciais;
- a necessidade de atualizar o elenco de dados que são, atualmente, tratados de forma estruturada pelos sistemas de informação dos tribunais
- o alargamento das entidades abrangidas; ou ainda,
- a necessidade de criar uma autoridade de supervisão das operações de tratamento de dados efetuadas pelos tribunais, que assegure, nos termos do já muito conhecido Considerando 20[9], o cumprimento das regras do RGPD, que reforce a sensibilização dos membros do poder judicial para as obrigações que lhe são impostas pelo Regulamento e que trate as reclamações relativas às operações de tratamento dos dados. E cuja composição permita ultrapassar as dúvidas constante do veto de Sua Excelência o Presidente da República em 2019.

Não obstante as limitações associadas à lei que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, importa, todavia, reconhecer que este normativo não tem impedido a aplicação do RGPD aos tribunais.

E a este propósito, gostaríamos de saudar o trabalho liderado pelo Conselho Superior da Magistratura, no qual a DGPJ teve a oportunidade de participar, relativamente ao Grupo de Trabalho referente à Fixação de Prazos para as Pu-

9. V. Considerando 20 do RGPD: *Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização os membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento dos dados.*

blicações na Internet de Dados Judiciais em Portais Públicos.

As conclusões do Grupo de Trabalho permitiram ao Conselho Superior da Magistratura aprovar a política de fixação de prazos para as publicações de dados judiciais em portais públicos, como o Portal Citius, o que constitui um marco significativo no âmbito da proteção dos dados pessoais nos tribunais.

Ao estabelecer prazos claros para a publicação de dados judiciais em todas as situações onde a lei não previa regras específicas, o Conselho Superior da Magistratura veio não apenas responder a uma necessidade efetivamente sentida nos tribunais e pelos cidadãos, mas também promoveu uma gestão mais transparente dos dados judiciais, conseguindo simultaneamente reforçar a proteção dos direitos dos titulares dos dados e conciliar esses direitos com o interesse público na publicação de informações em portais públicos.

Da parte da DGPJ, registamos com especial acuidade a referência à necessidade da legislação – processual e não só – ser mais precisa e desenvolvida sempre que prevê o tratamento de dados pessoais, nomeadamente para efeitos de publicações dos dados judiciais, assegurando que estão devidamente regulados os prazos de conservação, os dados pessoais a publicar e a finalidade da publicação.

Se antes esta já era uma preocupação da DGPJ, no âmbito das suas competências ao nível da política legislativa, as conclusões do Grupo de Trabalho vieram relembrar a importância destas questões e a necessidade de desenvolvermos esforços permanentes neste sentido. •

Sofia Wengorovius
Juíza de Direito
Encarregada da Proteção de Dados do Conselho Superior da Magistratura e dos Tribunais da Relação

RESUMO: A presente intervenção abordou, de forma breve, as contingências da aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD) à atividade dos tribunais, elencando algumas das iniciativas do Conselho Superior da Magistratura, a necessidade de alteração da Lei n.º 34/2009, de 14 de julho (regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial) e a proposta de alteração deste regime aprovada pelo CSM a que aderiram o CSTAF, o Tribunal de Contas e a PGR.

O tempo é demasiado curto para fazer um balanço sobre as inúmeras questões que o Conselho Superior da Magistratura (de ora adiante designado "CSM") tem tratado e iniciativas que impulsionado para a aplicação na atividade dos Tribunais do Regulamento (EU) n.º 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados (de ora adiante designado "RGPD").

Em virtude das atribuições constitucionais e legais do CSM, a implementação do RGPD deve ser efetuada a duas dimensões simultâneas, uma relativa aos dados judiciais – constantes dos processos judiciais e relativos a atividade dos tribunais – e a outra, aos dados pessoais depositados no próprio CSM – relativos a todos os magistrados judiciais e ao corpo de funcionários que nesse órgão prestam funções.

Quando fui nomeada Encarregada da Proteção de Dados do CSM ainda se discutia se o RGPD se aplicava à atividade dos tribunais e depois, já na certeza de que se aplicava passamos a discutir em que termos e quais as especialidades desta aplicação.

Face às especialidades constantes de algumas das normas do Regulamento quanto à sua aplicação aos Tribunais no exercício da sua função jurisdicional, a reflexão tem se centrado em como os Estados-Membros devem concretizar estas cláusulas de especificação (ou de abertura) consagradas nos artigos 9.º, n.º 2, alínea f), 23.º, n.º 1, alíneas d) e f), 37.º, n.º 1, alínea a) e 55.º, n.º 3, do RGPD. É neste âmbito e para cumprir a incumbência de concretização interna que se enquadra a necessidade de alteração da Lei 34/2009, de 14 de julho (regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial).

Ainda antes do início da aplicação do RGPD, o CSM, o Conselho Superior dos Tribunais Administrativos e Fiscais (adiante CSTAF) e a Procuradoria-Geral da República (adiante PGR) subscreveram um documento conjunto a consignar os pontos que consideravam essenciais sobre a aplicação interna no tratamento de dados pessoais realizados pelos tribunais, deste Regulamento e aquando da transposição da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

Neste documento subscrito por todos ficou prevista, designadamente, a necessidade de criação de um organismo independente específico, constituído exclusivamente por magistrados para supervisão do tratamento de dados pelos Tribunais; a possibilidade de em sede de especificação do Regulamento e de transposição da Diretiva (2016/680) serem previstas normas processuais para tutela incidental dos direitos dos titulares nos processos e o alerta de que a atividade dos magistrados nos tratamentos de dados realizados nos processos não se enquadra no conceito de responsável pelo tratamento.

Acontece que, em 8 de agosto de 2019, quando foram aprovadas a Lei n.º 58/2019, que assegura a execução na ordem jurídica nacional do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016 - e a Lei n.º 59/2019, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou

de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 -, foi também aprovada uma Proposta de Lei (apresentada sob o n.º 126/XIII) que visava alterar a Lei 34/2009, de 14 de julho, a qual não havia atendido a nenhum dos pontos que constavam da supra referida declaração conjunta.

Em 26 de julho de 2019, Sua Ex.ª o Presidente da República exerceu o direto de veto e devolveu o diploma (que após aprovação dera origem ao Decreto n.º 333/III/3ª) à Assembleia da República com indicação das razões do veto e estas são muitos claras. Desde logo, salienta Sua Ex.ª o Presidente da República que as garantias da proteção de dados no âmbito do sistema judiciário devem respeitar as áreas constitucionais do exercício das funções dos tribunais e do Ministério Público; que as responsabilidades que incumbem as autoridades de controlo devem assegurar o cumprimento do Regulamento e que esta deve ser independente e obedecer ao modelo previsto; e que nenhuma autoridade pode traduzir uma organização não conforme com a legislação europeia por sinal consonante com a CRP. Em consequência, devolveu o diploma para a Assembleia da República proceder à sua reformulação ponderando "*alterações que correspondam a garantia de não interferência nas áreas especificas de natureza jurisdicional e do Ministério Publico no exercício das suas funções e competências processuais*".

A verdade é que desde essa data não se conheceu mais nenhuma iniciativa legislativa.

Foi por essa razão que, em outubro de 2022 o CSM criou um grupo de trabalho com vista à elaboração de um projeto de alteração da Lei 34/2009, de 14 de julho. A proposta elaborada pelo grupo de trabalho foi aprovada na sessão Plenária Ordinária realizada em 07 de novembro de 2023. Posteriormente, esta proposta foi remetida ao Conselho Superior dos Tribunais Administrativos e Fiscais (de ora em diante designado por "CSTAF"), ao Tribunal Constitucional, ao Tribunal de Contas e à Procuradoria-Geral da República (de ora em diante designado por "PGR") para querendo se pronunciar. Todos, à exceção do Tribunal Constitucional, deram contributos para adequação do projeto que integrou estas alterações, tendo posteriormente sido também aprovado pelos respetivos órgãos decisórios.

É importante ter presente e foi isso que se pretendeu deixar claro logo em sede de fundamentação da proposta elaborada pelo grupo de trabalho que o RGPD se aplica à atividade dos tribunais e é este Regulamento que define os princípios e os conceitos aplicáveis quando há tratamento de dados pessoais.

O âmbito da Lei sobre o tratamento dos dados no sistema judicial (regime previsto na Lei n.º 34/2009) visa concretizar a margem que o Regulamento deixa

aos Estados-Membros para especificação das disposições que ressalvam a atividade dos tribunais no exercício da sua função jurisdicional para assegurar a independência do poder judicial e evitar a ingerência de uma autoridade administrativa no sistema judiciário.

É o caso das limitações do alcance dos direitos dos titulares ou obrigações dos responsáveis pelo tratamento para defesa da independência judiciária e dos processos judiciais previstas no artigo 23.º, n.º 1, al. f) do RGPD; ou a necessidade de criação do organismo específico de supervisão destas atividades de tratamento de que fala o Considerando (20) do RGPD e o artigo 8.º, n.º 3 da Carta de Direitos Fundamentais da União Europeia, o qual impõe que o cumprimento das regras sobre a proteção de dados fique sujeito a fiscalização por uma autoridade independente, face à exclusão da competência das autoridades de controlo nacionais, prevista no artigo 55.º, n.º 3 do RGPD.

Para concretização das mencionadas cláusulas de especificação, na proposta aprovada pelo CSM, pelo Tribunal de Contas, pelo CSTAF e pela PGR, destaco, designadamente:

- a previsão nos artigos 24.º e 25.º desta proposta da criação de um organismo para controlo das operações de tratamento realizadas nos termos desta Lei, designado Autoridade da Proteção de Dados Judiciais, prevendo-se no artigo 27.º a sua composição e no artigo 26.º as atribuições e competências;
- a previsão no artigo 29.º da possibilidade do titular de dados deduzir um incidente processual para tutela dos seus direitos (tutela incidental autónoma para exercício dos direitos do titular quanto o tratamento de dados se realiza no processo); ou reclamação hierárquica se o tratamento for realizado na fase em que o processo é da titularidade do Ministério Público;
- se o tratamento de dados for apreciado por decisão proferida pelo juiz do processo, o titular de dados pode reclamar para o tribunal imediatamente superior. Este incidente tem natureza urgente e é decidido pelo Presidente do Tribunal e em caso algum suspende a normal tramitação dos autos a que respeita, como se prevê nos n.ºs 4, 5 e 6 do artigo 29.º.

A proposta de alteração da Lei n.º 34/2009 aprovada pelo plenário do CSM foi remetida ao Ministério da Justiça ao abrigo do disposto no artigo 149.º, n.º 1, alínea j) do Estatuto dos Magistrados Judiciais, aguardando-se com expectativa o desencadear da necessária iniciativa legislativa, pressuposto da compatibilização do sistema interno com o Direito da União. •

Inês Oliveira[1]
Encarregada da Proteção de Dados da Autoridade Tributária (AT)
e Presidente da APDPO

SUMÁRIO: 1. Considerações introdutórias; 2. Análise da Deliberação 494/2019 da Comissão Nacional de Proteção de Dados; 2.1. Desaplicação do artigo 20.º, n.º 1, da Lei n.º 58/2019, de 8 de agosto; 2.2. Desaplicação do artigo 23.º da Lei n.º 58/2019, de 8 de agosto; 2.3. Desaplicação do artigo 28.º, n.º 3, alínea a), da Lei n.º 58/2019, de 8 de agosto; 2.4. Desaplicação dos artigos 37.º, n.º 1, alíneas a) e h), e 38.º, n.º 1, alínea b), da Lei n.º 58/2019, de 8 de agosto; 2.5. Desaplicação dos artigos 37.º, n.º 2, e 38.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto; 2.6. Desaplicação do artigo 39.º, n.º 1 e n.º 3, da Lei n.º 58/2019, de 8 de agosto; 2.7. Desaplicação do artigo 61.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto; 2.8. Desaplicação do artigo 62.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto; 3. Em especial, a responsabilidade contraordenacional do Encarregado de Proteção de Dados (EPD): outra norma nacional que merecia a desaplicação por parte da CNPD; 4. Notas conclusivas.

RESUMO: O presente artigo desenvolve a comunicação proferida pela signatária no evento subordinado ao tema "Seis anos de RGPD – Balanço da (des)aplicação da lei nacional de execução e da lei sobre o tratamento de dados no sistema judicial", realizado no Supremo Tribunal de Justiça no dia 28 de janeiro de 2025, visando uma leitura atualista e uma interpretação crítica da Deliberação 494/2019 da Comissão Nacional de Proteção de Dados.

PALAVRA-CHAVE: RGPD.

1. Licenciada (2008) e Mestre (2010) em Direito pela Faculdade de Direito da Universidade Nova de Lisboa. Membro do Observatório da Proteção de Dados Pessoais da Faculdade de Direito da Universidade Nova de Lisboa. Especialista em proteção de dados pessoais. Presidente da APDPO – Portugal.

ABSTRACT: This article develops the communication given by the author at the event entitled 'Six years of GDPR - Assessment of the (dis)application of the national implementing law and the law on data processing in the judicial system', held at the Supreme Court of Justice on 28 January 2025, with a view to an up-to-date reading and critical interpretation of Deliberation 494/2019 of the National Data Protection Commission.

KEYWORD: GDPR.

1 | Considerações introdutórias

A Deliberação 494/2019 da Comissão Nacional de Proteção de Dados (CNPD), a seguir Deliberação, concluiu pela desaplicação, na apreciação de casos concretos, de algumas normas da Lei n.º 58/2019, de 8 de agosto, lei que, recorde-se, assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Para os profissionais que diariamente aplicam o Regulamento Geral sobre a Proteção de Dados (RGPD), tal desaplicação causou estranheza e uma forte incerteza e insegurança.

Muitos dos profissionais de proteção de dados, que no dia-a-dia das organizações materializam as obrigações impostas pelo RGPD, não são juristas nem de áreas conexas com o Direito, pelo que o facto de uma entidade administrativa – subordinada à lei – deliberar desaplicar uma causou um abalo nas expectativas que a confiabilidade legal suporta.

E mesmo para os profissionais do RGPD juristas, uma desaplicação da lei causa surpresa e admiração, sobretudo aos mais legalistas, sendo o princípio da legalidade, previsto no artigo 3.º do Código do Procedimento Administrativo, muito claro: os órgãos da Administração Pública devem atuar em obediência à lei e ao direito, sendo – apenas e só – competência dos tribunais a apreciação da inconstitucionalidade, nos termos do artigo 204.º da Constituição da República Portuguesa.

Vejamos, pois, com mais detalhe, a Deliberação da CNPD.

2 | Análise da Deliberação 494/2019 da Comissão Nacional de Proteção de Dados

Na Deliberação que ora nos ocupa, a CNPD, destacando o carácter geral, obrigatório e diretamente aplicável do RGPD e, ao mesmo tempo, o dever de legislar que impõe aos Estados-Membros, sublinha que a legislação nacional não pode interferir na livre circulação de dados nem criar obstáculos nem colocar em perigo a aplicação direta, simultânea e uniforme do RGPD em toda a União Europeia, assim como não pode acrescentar condições adicionais às suas regras.

Reiterando que a legislação nacional em contradição com o RGPD não só viola o princípio do primado do direito da União como afeta o funcionamento adequado do mecanismo de coerência, e trazendo à colação a jurisprudência que entende que as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariam o direito da União Europeia, a CNPD entendeu que determinadas normas da Lei n.º 58/2019, de 8 de agosto, eram manifestamente incompatíveis com o direito da União e decidiu desaplicá-las em casos futuros que venha a apreciar[2].

A CNPD não perdeu a oportunidade para, nesta sede, lamentar a total desconsideração do seu Parecer n.º 20/2018, de 2 de maio de 2018, parecer esse emitido no âmbito do procedimento legislativo de execução do RGPD, que culminou com a aprovação da Lei n.º 58/2019, de 8 de agosto. Tendo sido, pois, uma ocasião perdida para levar em linha de conta o seu entendimento, e uma vez que a redação final desta lei não permite salvar as normas que então considerou violadoras do direito da União, a CNPD foi irredutível na afirmação da sua desaplicação no futuro, sublinhando que nem uma interpretação corretiva conforme ao direito da União seria viável.

Das normas ora desaplicadas pela CNPD, vamos atentar nas seguintes, que impactam no dia-a-dia dos profissionais da área.

2.1. Desaplicação do artigo 20.º, n.º 1, da Lei n.º 58/2019, de 8 de agosto

O artigo 20.º, no seu n.º 1, determina que os direitos de informação e de acesso a dados pessoais previstos nos artigos 13.º e 15.º do RGPD não podem ser exercidos quando a lei imponha ao responsável pelo tratamento ou ao subcontratante um dever de segredo que seja oponível ao próprio titular dos dados.

2. A CNPD deliberou desaplicar, nas situações de tratamento de dados pessoais que venha a apreciar, as seguintes normas da Lei n.º 58/2019, de 8 de agosto: i. Artigo 2.º, n.ºs 1 e 2; ii. Artigo 20.º, n.º 1; iii. Artigo 23.º; iv. Artigo 28.º, n.º 3, alínea a); v. Artigo 37.º, n.º 1, alíneas a), h) e k), e n.º 2; vi. Artigo 38.º, n.º1, alínea b), e n.º 2; vii. Artigo 39.º, n.ºs 1 e 3; viii. Artigo 61.º, n.º 2; ix. Artigo 62.º, n.º 2.

A CNPD é perentória na sua desaplicação e explica diferenciando os direitos em causa.

Quanto ao direito de informação, e apenas no caso de recolha indireta dos dados pessoais, a CNPD sublinha que é o próprio artigo 14.º do RGPD que define os casos em que este direito pode ser restringido e que este já prevê o dever legalmente previsto de segredo. Assim, quanto a este, como o RGPD já regula a restrição ao direito de informação perante um dever legal de segredo, o n.º 1 do artigo 20.º da nossa lei nacional nada acrescenta.

Quanto ao direito de informação no âmbito da recolha dos dados diretamente junto do titular, e uma vez que o artigo 13.º do RGPD não prevê nem legitima quaisquer limitações, o n.º 1 do artigo 20.º da nossa lei nacional não poderia criar uma tal restrição, pelo que a CNPD foi forçada a concluir pela sua desaplicação.

A igual conclusão se chega relativamente ao direito de acesso previsto no artigo 15.º do RGPD.

Ora, o direito de acesso é um dos mais exercidos pelos titulares dos dados – é isso que a experiência prática nos mostra. Esta desaplicação pela CNPD faz com tal direito seja absoluto, ou seja, nunca o responsável pelo tratamento o possa afastar, nem existindo um especial segredo como o sigilo fiscal ou o sigilo médico. Mas uma constatação é forçosa: quando o direito de acesso exercido pelo titular implica igualmente o acesso a dados de terceiros, então a confidencialidade que estes obrigam ditam necessariamente a restrição do direito de acesso exercido. Tal constatação merecia uma anotação especial da CNPD na Deliberação, estamos disso convictos.

2.2. Desaplicação do artigo 23.º da Lei n.º 58/2019, de 8 de agosto

O artigo 23.º, epigrafado de tratamento de dados pessoais por entidades públicas para finalidades diferentes, prevê dois casos que cumpre segregar.

Primeiro, quando há tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha, o artigo 23.º exige a natureza excecional de tal tratamento e obriga a que tal seja devidamente fundamentado com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado (artigo 23.º, n.º 1).

Em segundo lugar, antevê a transmissão de dados pessoais entre entidades públicas para finalidades diferentes das determinadas pela recolha, exigindo igualmente a natureza excecional de tal transmissão e obrigando também a que seja devidamente fundamentada, prevendo uma obrigação adicional, a saber que

seja objeto de protocolo, que estabeleça as responsabilidades de cada entidade interveniente, quer no ato de transmissão, quer em outros tratamentos a efetuar (artigo 23.º, n.º 2).

Para a CNPD, que – sublinhe-se – admite que a reutilização de dados é possível, a reutilização prevista no artigo 23.º da nossa lei nacional não especifica as finalidades de interesse público que podem justificar essa reutilização, procedendo, assim, a um alargamento inadmissível da referida possibilidade. A CNPD conclui que há um desvio das finalidades dos tratamentos inadmissível, por ser genérico e permanente, abstrato, não ponderado e não necessário, trazendo à colação a necessidade de respeito do princípio da limitação da finalidade. Para a CNPD, só um juízo concreto e ponderado de compatibilidade das finalidades (inicial e ulterior) justifica a reutilização de dados. Nunca seria possível uma norma abstrata prevê-la.

Ora, na prática, impactados pelo receio de recorrer ao artigo 23.º, desaplicado pela CNPD – a autoridade de controlo que fiscaliza e impõe sanções, os profissionais de proteção de dados têm vindo a afastar a sua invocação e aplicação, encontrando uma solução igualmente abstrata, permitimo-nos referir e destacar. E tal solução alternativa é para nós igualmente abstrata precisamente porque se baseia no recurso à legislação orgânica, em que as normas de competência e atribuições das entidades – gerais e genéricas – vão suportar o que o legislador do artigo 23.º pretendeu assegurar. Assim, neste quadro de desaplicação do artigo 23.º da Lei n.º 58/2019, de 8 de agosto, surgem, designadamente, protocolos, em que a lei habilitante para o tratamento de dados é a orgânica da entidade. Uma abstração concreta no caso? Parece que sim, mas o juízo de ponderação, que o citado artigo 23.º exige, assim como as avaliações de impacto sobre a proteção de dados, ficam, não raras vezes, por fazer.

2.3. Desaplicação do artigo 28.º, n.º 3, alínea a), da Lei n.º 58/2019, de 8 de agosto

Determina o artigo 28.º, n.º 3, alínea a), que, salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador.

A CNPD, não obstante admitir a natureza não paritária da relação laboral, entende que esta norma restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores, mesmo quando há condições para a sua manifestação sem risco

para os seus direitos e interesses.

Aliás, a CNPD recorda que o consentimento dos trabalhadores é lícito e legítimo, balizando que estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas.

Assim, acautelando a autodeterminação informacional dos trabalhadores e o controlo dos seus próprios dados, a CNPD, afastando a proteção que o legislador lhe quis garantir nesta norma, desaplica-a, considerando-a não adequada, desnecessária e excessiva, "para lá do que é necessário à salvaguarda dos direitos e interesses dos trabalhadores".

Na prática, tal gera incerteza quanto aos fundamentos de licitude para os tratamentos de dados que envolvam trabalhadores. Não há dúvida de que a maioria destes se baseia em obrigações legais e no próprio contrato de trabalho. Os demais, pelas dúvidas que o consentimento do trabalhador - enquanto parte mais frágil na relação contratual - podem gerar, levam os profissionais de proteção de dados a recorrer ao interesse legítimo do empregador como base de legitimidade, deixando-se este documentado para evidenciar a conformidade. Onde o legislador quis proteger, a CNPD pareceu não estar convencida de argumento bastante para tal discriminação positiva, estando a prática a contornar as dúvidas, com ferramentas e instrumentos que o próprio RGPD oferece.

2.4. Desaplicação dos artigos 37.º, n.º 1, alíneas a) e h), e 38.º, n.º 1, alínea b), da Lei n.º 58/2019, de 8 de agosto

O artigo 37.º, n.º 1, alínea a), indica que constitui contraordenação muito grave os tratamentos de dados pessoais com inobservância dolosa dos princípios consagrados no artigo 5.º do RGPD.

A CNPD é muito clara: o RGPD não distingue a natureza negligente ou dolosa da conduta, pelo que esta norma não pode afastar a suscetibilidade de sancionar a violação negligente, punindo apenas a dolosa, uma vez que o legislador nacional não tem o poder de definir normas que diminuam o elenco dos ilícitos suscetíveis de sanção.

Já a alínea h) do mesmo artigo 37.º, n.º 1, sanciona a não prestação de informação relevante, distinção e tipo este que o RGPD não categoriza e, por essa razão, de desaplicar para a CNPD, que afasta a aplicação do artigo 38.º, n.º 1, alínea b) pela mesma ordem de razão. Além disso, a CNPD chama a atenção que não é apenas a omissão de informação que deve ser sancionada: a informação

equívoca, errónea, incompleta, datada ou fora de prazo também deve ser sancionada. É mesmo isso que resulta do RGPD.

2.5. Desaplicação dos artigos 37.º, n.º 2, e 38.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto

As normas em apreço definem molduras sancionatórias distintas em função da dimensão das empresas e da natureza coletiva ou singular dos responsáveis pelo tratamento, normas que a CNPD contesta e desaplica, invocando, em primeiro lugar, o argumento de que os limites máximos definidos pelo RGPD não podem ser afastados pelo legislador e que cabe, apenas, à autoridade de controlo a determinação do valor das coimas nos casos concretos – e nunca ao legislador em abstrato. Sublinha ainda a CNPD que a fixação em abstrato, em lei nacional, de limites máximos inferiores aos previstos no RGPD constitui uma violação do mesmo.

Em segundo lugar, destaca a CNPD, o RGPD não abre espaço para a consideração autónoma da dimensão da empresa, pelo que o critério adotado pelo legislador nacional, de distinguir as pequenas e médias empresas para reservar o limite pecuniário máximo do RGPD para as grandes empresas, constitui em si mesmo uma violação do RGPD.

O mesmo se diga quanto à diferenciação das molduras sancionatórias para as pessoas singulares e para a fixação de limites mínimos, também desaplicados pela CNPD quando estão em causa as sanções previstas no RGPD.

2.6. Desaplicação do artigo 39.º, n.º 1 e n.º 3, da Lei n.º 58/2019, de 8 de agosto

O n.º 1 do artigo 39.º apresenta três critérios para a determinação em concreto da medida da coima, além dos estabelecidos no RGPD. Também aqui a CNPD é muito clara para a desaplicação: o RGPD não deixa espaço para que os legisladores nacionais venham definir outros critérios de ponderação.

O n.º 3 do artigo citado determina que, exceto em caso de dolo, a instauração de processo de contraordenação depende de prévia advertência do agente, por parte da CNPD, para cumprimento da obrigação omitida ou reintegração da proibição violada em prazo razoável. Por inexistir no RGPD esta advertência prévia, a CNPD vem afastá-la, precisamente porque nenhuma autoridade de controlo pode ficar sujeita à imposição de decidir por uma medida corretiva, em vez de aplicar logo uma coima, por exemplo. Para a CNPD, o seu poder de decidir o que fazer não pode ser objeto de legislação, resultando o seu poder diretamente do RGPD.

2.7. Desaplicação do artigo 61.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto

O artigo 61.º, epigrafado de renovação do consentimento, começa por determinar, no n.º 1, que, nos casos em que o tratamento dos dados pessoais em curso à data da entrada em vigor da lei se basear no consentimento do respetivo titular, não é necessário obter novo consentimento se o anterior tiver observado as exigências constantes do RGPD.

Já o n.º 2 do artigo em apreço prevê que, caso a caducidade do consentimento seja motivo de cessação de contrato em que o titular de dados seja parte, o tratamento de dados é lícito até que esta ocorra.

Para a CNPD, a norma constante deste n.º 2 parece ter sido introduzida pelo legislador para tentar resolver um problema antigo, que reside no facto de o contrato não ser fundamento de licitude adequado para legitimar o tratamento de dados de saúde, o que leva a que, em alguns setores de atividade, designadamente no segurador, falte base de licitude para o tratamento de dados necessários para a execução do contrato.

No entanto, a CNPD chama a atenção para o facto de esta norma ser estranha, encerrar uma contradição em si e levar à confusão de bases de licitude. Com efeito, para a CNPD o legislador confunde o consentimento e o contrato, admitindo que o consentimento no tratamento de dados pessoais seja condição da vigência de um contrato em que o titular seja parte. Sublinhe-se que o consentimento só é base de licitude para os tratamentos que não sejam necessários à execução do contrato, porque neste caso, em que é necessário, é o contrato que é a base de licitude. Aliás, solicitar consentimento no âmbito de um contrato nunca seria um verdadeiro consentimento, por não ser livre, antes condicionado pelo contrato. Ora, não se pode admitir o estabelecimento de uma relação de condicionalidade entre um e outro: tal condicionalidade é totalmente violadora do RGPD, nas palavras da CNPD.

2.8. Desaplicação do artigo 62.º, n.º 2, da Lei n.º 58/2019, de 8 de agosto

O artigo 62.º estabelece que as normas relativas à proteção de dados pessoais previstas em legislação especial se mantêm em vigor, em tudo o que não contrarie o disposto no RGPD e na lei que o executa, sem prejuízo de todas as normas que prevejam autorizações ou notificações de tratamento de dados pessoais à CNPD, fora dos casos previstos no RGPD e na lei de execução, deixarem de vigorar à data de entrada em vigor do RGPD.

Para a CNPD, ao fazer retroagir tais efeitos ao momento da entrada em vigor do RGPD, ou seja, a 25 de maio de 2016, o legislador nacional está a determinar a aplicação retroativa do RGPD, o que viola o RGPD e é inadmissível face ao direito da União. Outra não podia ser a conclusão, que não a desaplicação.

3 | Em especial, a responsabilidade contraordenacional do Encarregado de Proteção de Dados (EPD): outra norma nacional que merecia a desaplicação por parte da CNPD

Percorridos os trilhos da Deliberação 494/2019 da CNPD, trazemos à colação uma norma que não mereceu desaplicação por parte da autoridade de controlo, mas que, salvo melhor opinião, não poderá ser aplicável por também contrariar e violar o RGPD. Vamos, pois, debruçar-nos sobre a questão de saber se um Encarregado de Proteção de Dados (EPD) poder ser responsabilizado no âmbito de um processo contraordenacional e punido com uma coima[3].

Em primeiro lugar, parece-nos claro que o RGPD quis sancionar o incumprimento dos seus artigos 37.º a 39.º, atinentes ao EPD (cf. alínea a) do n.º 4 do artigo 83.º do RGPD).

Em segundo lugar, parece-nos óbvio que a sanção decorrente do incumprimento destes artigos visa o responsável pelo tratamento e o subcontratante, mas não – nunca – o EPD.

Com efeito, os artigos 37.º a 39.º do RGPD preveem várias obrigações para os responsáveis pelo tratamento e para os subcontratantes: a obrigação de designar um EPD nos casos em que tal é obrigatório; a obrigação de designar um EPD com as qualidades profissionais que o próprio RGPD impõe; a obrigação de assegurar as condições que o RGPD impõe para a posição do EPD, incluindo que não recebe instruções nem é colocado numa situação de conflito de interesses; a obrigação de atribuir ao EPD as funções de aconselhamento, formação do pessoal e controlo de conformidade; e a obrigação de facultar aos titulares dos dados o contacto direto com o EPD.

Ora, todas estas obrigações, cujo incumprimento a alínea a) do n.º 4 do artigo 83.º do RGPD sanciona, visam o responsável pelo tratamento e o subcontratante.

> "A interpretação literal da norma não deixa espaço para outras leituras: o que está em causa é a eventual aplicação de uma coima ao responsável pelo tratamento ou subcontratante. Ao arrepio desta norma, que – *ipsis verbis*

3. I. Oliveira e J. L. Dias, "O Encarregado da Proteção de Dados de entidades públicas", in D. Soares Farinho, F. Paes Marques e T. Fidalgo De Freitas, (coord.), *Direito da Proteção de Dados Perspetivas Públicas e Privadas*, Coimbra, Almedina, 2023, pp. 253-279.

> – identifica o agente como sendo o responsável pelo tratamento ou subcontratante, a Lei n.º 58/2019, de 8 de agosto, veio determinar que constitui contraordenação o incumprimento dos deveres previstos no artigo 39.º do RGPD, não identificando o agente da infração, isto é, a quem se aplicará a coima (alínea p) do n.º 1 do artigo 38.º da Lei n.º 58/2019, de 8 de agosto). Ora, não resultando da letra da lei nacional o agente a quem se aplicará a coima, parece-nos que a Lei n.º 58/2019, de 8 de agosto, visa punir com coima o EPD que incumpre as suas funções de informação e aconselhamento, sensibilização e formação do pessoal, controlo e auditoria"[4].

Assim, a alínea p) do n.º 1 do artigo 38.º da Lei n.º 58/2019, de 8 de agosto, sancionando o EPD, também deveria ter sido desaplicada pela CNPD: "o RGPD apenas pretende visar, no âmbito de processos contraordenacionais, a entidade e não o profissional que exerce as funções de EPD"[5].

4 | Notas conclusivas

A Deliberação 494/2019 da CNPD causou estranheza e trouxe incerteza e insegurança. Feita uma leitura atualista e uma interpretação crítica, porventura outros casos há que merecem a mesma desaplicação ora deliberada.

Terminamos com duas notas, convidando à devida ponderação: por um lado, constatamos que a Deliberação nunca mereceu revisitação por parte da CNPD, nunca tendo sido, pois, objeto de revisão. Por outro lado, verificamos que no último relatório de atividades da CNPD disponível para consulta[6] – referimo-nos ao Relatório de atividades de 2023 – não há qualquer referência, estatística ou indicador, sobre a desaplicação das normas nos casos concretos, referência que consideramos essencial para apurar o impacto da Deliberação que ora nos ocupou. •

4. Oliveira E Dias, Direito da Proteção de Dados, p. 278.

5. Oliveira E Dias, Direito da Proteção de Dados, p. 278.

6. Disponível em www.cnpd.pt, consultado no dia 26 de março de 2025.

OBSERVAÇÕES FINAIS

Juíza Desembargadora, Chefe do Gabinete do Presidente do SUpremo Tribunal de Justiça
Gabriela Cunha Rodrigues

I. Celebramos o Dia da Proteção de Dados num encontro dedicado ao tema "Seis anos de RGPD – Balanço da (des)aplicação da lei nacional de execução e da lei relativa ao tratamento de dados no sistema judicial".

Começo por saudar as Senhoras Oradoras Convidadas: a Professora Doutora Paula Meira Lourenço, Presidente da Comissão Nacional de Proteção de Dados; a Professora Doutora Susana Videira, Diretora-Geral da Política de Justiça; a Juíza de Direito Sofia Wengorovius, Encarregada da Proteção de Dados do Conselho Superior da Magistratura; e a Dra. Inês Oliveira, Encarregada da Proteção de Dados da Autoridade Tributária.

Agradeço profundamente a todas por terem enriquecido este Dia da Proteção de Dados com intervenções de elevadíssimo nível científico e técnico.

O Senhor Juiz Conselheiro Lopes da Mota, membro desta Casa, é um anfitrião por excelência, com uma carreira distinta, igualmente marcada por um contributo relevante e continuado numa área particularmente sensível do Direito.

II. Volvidos mais de seis anos desde a entrada em aplicação do RGPD, encontramo-nos num ponto da confluência de duas revoluções.

Depois do século do coração, as ciências biológicas avançam agora no desvendamento do cérebro e das emoções humanas.

Em paralelo, os progressos da ciência da computação tornaram possível uma capacidade de processamento de dados sem precedentes.

Neste contexto, torna-se imperiosa a aplicação efetiva do RGPD, bem como a sua articulação coerente com legislação em domínios como os da publicidade em linha, do microdirecionamento e da definição algorítmica de perfis, da clas-

sificação, disseminação e amplificação de conteúdos pelas plataformas digitais, e da cibersegurança.

O RGPD, que oferece as "linhas mestras" para a proteção dos dados pessoais e privacidade, não está isolado, como, aliás, o demonstram as recentes iniciativas legislativas da UE que, de uma forma ou outra, têm impactos na proteção de dados.

Disso são exemplos o Regulamento Governação de Dados (cf. o Decreto-Lei n.º 2/2025, de 23 de janeiro – execução do Regulamento), os Regulamentos dos Serviços Digitais (Digital Services Act) e do Mercado Digital (Digital Market Act), o Regulamento relativo à Privacidade nas Comunicações Eletrónicas (e-privacy) e o Regulamento da Inteligência Artificial (AI Act).

Os dados pessoais assumiram hoje a natureza de bens transacionáveis no mercado.

Entidades terceiras dedicam-se à sua recolha, mineração e análise, com o objetivo de os comercializar posteriormente.

A partir de volumes massivos de informação, são identificados padrões de comportamento e de preferências.

Perfis de dados pessoais, agregando informação relativa a múltiplos titulares, são adquiridos e utilizados para direcionar ofertas de bens e serviços ajustados a esses perfis.

Assim se podem também difundir as ideias políticas, ideológicas ou outras que se mostrem em sintonia com o público-alvo.

Em última instância, passamos a viver dentro de uma caixa informacional, moldada por dados e algoritmos.

E o problema não é tanto a questão da inteligência artificial em si mesma, mas o do impacto que ela possa ter na tutela dos dados pessoais.

O Direito não pode alhear-se.

Há que edificar uma tutela segura e efetiva dos dados pessoais.

A preocupação do jurista deve ser a de encontrar um equilíbrio necessário que garanta a salvaguarda do núcleo essencial dos diversos interesses e valores em presença.

III. Desde 2023, o Supremo Tribunal de Justiça tem vindo a assinalar o Dia da Proteção de Dados através de várias iniciativas.

Entre elas, destaca-se a divulgação anual, no seu *site*, de uma compilação de decisões judiciais relevantes em matéria de proteção de dados, proferidas desde

2020 pelo Tribunal Constitucional, pelo Supremo Tribunal de Justiça e pelos Tribunais da Relação.

No terceiro ano desta iniciativa nota-se uma evolução ao nível do número de decisões que tratam, ainda que de forma indireta, a problemática dos dados pessoais e a variedade das questões que são colocadas aos tribunais com enfoque neste tema[1].

Sem preocupação de exaustão, é possível agrupar as questões dirimidas pelos Tribunais nas seguintes temáticas:

A. No âmbito criminal/contraordenacional

- efeitos do Acórdão do Tribunal Constitucional n.º 268/22 ao nível do caso julgado e como (não) fundamento de revisão de sentença[2];
- efeitos da declaração de invalidade da Diretiva n.º 2006/24/CE como (não) fundamento de revisão de sentença[3];
- conservação e transmissão dos dados de tráfego e localização[4];
- preenchimento dos elementos constitutivos do crime de violação de normas relativas a ficheiros e impressos agravado p. e p. pelo artigo 43.º, n.º 1, da Lei n.º 37/2015, de 5 de maio[5];
- preenchimento do crime de acesso indevido (a dados pessoais)[6];
- preenchimento do crime de violação do dever de sigilo previsto no artigo 51.º, n.º 1, da Lei n.º 58/2019[7];

1. Texto com base na pesquisa de jurisprudência efetuada pela Juíza Assessora do Supremo Tribunal de Justiça, Dra. Cátia Santos, responsável pela publicação anual da coletânea de jurisprudência sobre proteção de dados pessoais.

2. **Acórdão do STJ de 31-1-2024**
www.jurisprudencia.csm.org.pt
Acórdão do STJ de 21-2-2024 www.juris.stj.pt

3. **Acórdão do STJ de 31-1-2024** www.juris.stj.pt

4. **Acórdão do TRL de 4-6-2024**
www.jurisprudencia.csm.org.pt
Acórdão do TRP de 21.2.2024
www.jurisprudencia.csm.org.pt
Acórdão do TRP de 16-10-2024
www.jurisprudencia.csm.org.pt
Acórdão do TRG de 23-1-2024
www.jurisprudencia.csm.org.pt
Acórdão do TRG de 19-3-2024
www.jurisprudencia.csm.org.pt

5. **Acórdão do STJ de 28-2-2024** www.juris.stj.pt
Trata-se de um caso interessante, em que o arguido é um advogado que, nessa qualidade, acedeu ao Certificado de Registo Criminal constante de um processo em que uma determinada pessoa era arguida e depois juntou esse certificado num outro processo em que aquela pessoa assumia a qualidade de assistente.
O STJ, mantendo o entendimento do Tribunal da Relação, entendeu que o arguido procedeu a uma operação de tratamento de dados pessoais, utilizando a informação que apenas poderia estar na disponibilidade do respetivo titular ou da autoridade judiciária. O arguido foi condenado pelo crime de violação de normas relativas a ficheiros e impressos agravado p. e p. pelo artigo 43.º, n.º 1, da Lei n.º 37/2015, de 5 de maio, na data dos factos por referência ao artigo 43.º, n.º 1, al. c), e n.º 2, da Lei n.º 67/98, de 26 de outubro.

6. **Acórdão do TRL de 23-2-2024**
www.jurisprudencia.csm.org.pt
Acórdão do TRP de 24-4-2024
www.jurisprudencia.csm.org.pt
Acórdão do TRG de 24-9-2024
www.jurisprudencia.csm.org.pt

7. **Acórdão do TRL de 5-11-2024**
www.jurisprudencia.csm.org.pt

- obtenção e utilização como prova de dados armazenados em equipamentos de segurança ou de ajuda ao condutor de veículos automóveis, v.g. GPS, ECall-SOS, Via Verde, etc.[8];
- obtenção de dados identificativos do titular de IP[9];
- sujeição do arguido a identificação fotográfica e lofoscópica ou a perícia psiquiátrica[10];
- recolha e forma de preservação de documentos apreendidos que possam conter dados pessoais[11];
- requisitos e autorizações no âmbito da instalação de câmaras de videovigilância[12].

B. No âmbito civil e laboral

- Junção/obtenção de documentos aos autos que contenham dados pessoais de terceiros e/ou cobertos por sigilo[13];

8. **Acórdão do Tribunal Constitucional n.º 506/2024, de 28-6-2024**
www.tribunalconstitucional.pt
a) não julgar inconstitucional a norma contida no artigo 125.° do CPP, quando interpretada no sentido de que é permitido valorar os dados recolhidos por um GPS instalado em veículo pelo respetivo proprietário, entregues por este a pedido da Polícia Judiciária para fins de investigação criminal; consequentemente,
(...) c) julgar inconstitucional a norma contida no artigo 125.° do CPP, quando interpretada no sentido de que a junção a um processo penal de dados recolhidos por um GPS instalado em veículo pelo respetivo proprietário, entregues por este a pedido da Polícia Judiciária para fins de investigação criminal, não carece de validação por um juiz, por violação do disposto nos artigos 26.º, n.° 1, e 18.°, n.° 2, da Constituição da República Portuguesa; consequentemente,
d) julgar procedente o recurso, no que respeita à inconstitucionalidade da norma referida na alínea anterior, e determinar a remessa dos autos ao Supremo Tribunal de Justiça, a fim de que este reforme a decisão em conformidade com tal juízo de inconstitucionalidade (...).
Acórdão do TRP de 11.12.2024
www.jurisprudencia.csm.org.pt

9. **Acórdão do Tribunal Constitucional n.º 533/2024, de 4-7-2024**
www.tribunalconstitucional.pt
Acórdão do TRC de 11-12-2024
O Tribunal considerou que os dados identificativos do titular de IP não são dados relativos a comunicações eletrónicas em si considerados, mas sim elementos contratuais com carácter permanente que podem ser obtidos independentemente de qualquer comunicação, pelo que a sua obtenção pelas autoridades judiciárias cai fora do âmbito da lei e da declaração de inconstitucionalidade feita pelo acórdão n.º 268/2022 do Tribunal Constitucional.
www.jurisprudencia.csm.org.pt
Acórdão do TRE de 5-3-2024
www.jurisprudencia.csm.org.pt

10. **Acórdão do Tribunal Constitucional n.º 852/2024, de 5-12-2024**
www.tribunalconstitucional.pt
Acórdão do TRC de 20-3-2024
www.jurisprudencia.csm.org.pt

11. **Acórdão do TRL de 9-1-2024** (p. 1526/19.8TELSB-F.L1-5)
www.jurisprudencia.csm.org.pt
Acórdão do TRL de 25-1-2024 (p. 1/21.5ICLSB-A.L1-9)
www.jurisprudencia.csm.org.pt
Acórdão do TRL de 21-11-2024 (p. 85/18.3TELSB-F.L1-9)
www.jurisprudencia.csm.org.pt

12. **Acórdão do TRL de 9-1-2024** (p. 152/22.9T9VLS.L1-5)
Neste acórdão distinguiu-se, por exemplo, o acesso às definições do sistema de CCTV do acesso aos dados pessoais recolhidos.
www.jurisprudencia.csm.org.pt

13. **Acórdão do Tribunal Constitucional n.º 426/2024, de 29-5-2024**
www.tribunalconstitucional.pt
Acórdão do TRL de 11-1-2024 (p. 4551/22.8T8FNC-A.L2-2)
Estava em causa a junção aos autos de extratos bancários para comprovar o pagamento de rendas. Constavam desses extratos menções a nomes de terceiros intervenientes nas transações.
O TRL considerou que:
- O RGPD não regula diretamente a junção aos autos de documentos que contêm dados tratados por terceiros e respeitantes a terceiros.
- O tribunal é um terceiro relativamente aos dados de terceiros que surgem nos extratos juntos aos autos nos

- o direito ao apagamento e esquecimento de dados previsto no artigo 17.º do RGPD[14];

termos da alínea 10) do artigo 4.º do RGPD;
- Os "dados" são meros nomes, comuns a um número indeterminado de pessoas, não suscetíveis de identificar, por si, sem outros elementos e, nesse contexto, não parecem "dados pessoais", ou se o são, não devem estar pseudonimizados (cf. alíneas 1) e 5) do artigo 4.º do RGPD).
- Mesmo sendo dados de terceiros, a Ré não tem legitimidade, nem interesse para suscitar o eventual tratamento indevido dos mesmos dados (nem isso é, mais uma vez, objeto deste processo);
- Mesmo que se tratasse de dados pessoais, o tratamento seria lícito, porque necessário para efeito dos interesses legítimos prosseguidos pelos Autores.

www.jurisprudencia.csm.org.pt

Acórdão do TRL de 9-5-2024 (p. 6308/22.7T8VNG-B.L1-6)
Decidiu-se que se o documento cuja junção se ordenou contiver indicações pessoais dos associados da autora, o tribunal deve determinar que o acesso ao processo seja limitado.
www.jurisprudencia.csm.org.pt

Acórdão do TRP de 3.6.2024 (p. 3326/22.9T8VFR-A.P1)
www.jurisprudencia.csm.org.pt

Acórdão do TRC de 5-3-3024 (p. 1337/22.3T8LRA-A.C1)
www.jurisprudencia.csm.org.pt
Neste processo discutia-se a admissibilidade de ser solicitada informação abrangente a entidades bancárias em ação que tinha por objeto o conluio entre marido, mulher e filha de modo a obviar uma execução sobre um determinado bem do marido.

Acórdão do TRP de 14-10-2024 (p. 2276/23.6T8MAI.P1)
www.jurisprudencia.csm.org.pt

Acórdão do TRP de 7-11-2024 (p. 1560/22.0T8OVR.P1)
www.jurisprudencia.csm.org.pt
Este acórdão trata da apresentação de documentos contendo dados de saúde entregues a uma seguradora no âmbito de um contrato de seguro.

Acórdão do TRE de 20-2-2024 (p. 2524/21.7T8PTM-F.E1)
www.jurisprudencia.csm.org.pt

Ac. TRG de 24-10-2024 (p. 4844/23.7T8BRG-A.G1)
www.jurisprudencia.csm.org.pt

14. **Acórdão do TRL de 25-1-2024** (p. 13467/21.4T8LSB.L1-2)
Neste acórdão estava em causa o eventual direito ao apagamento dos dados reativos a operações com o cartão de fidelização da FNAC nas lojas da 1.ª Ré, na aquisição de bilhetes. O TRL considerou que, assiste à 1.ª Ré o direito à conservação dos dados, operando o respetivo tratamento e que, ainda não tendo decorrido o prazo de conservação dos documentos fiscais, não assiste à Autora o direito ao apagamento.
www.jurisprudencia.csm.org.pt

Acórdão do TRL de 18-4-2024 (p. 28507/23.4 T8LSB.L1-8)
O Tribunal considerou que a divulgação de uma notícia/conteúdo respeitante a factos ocorridos há cerca de 20 anos, sobre um visado que não é uma pessoa com funções de exposição mediática ou papel decisório, não reveste qualquer interesse para o público atual e causa grave lesão aos direitos de personalidade do visado. Decidiu-se que a divulgação é absolutamente desnecessária ao exercício de liberdade de informação, prevalecendo o direito ao esquecimento, mediante a eliminação/apagamento da notícia/conteúdo.
www.jurisprudencia.csm.org.pt

Acórdão do TRL de 21-5-2024 (p. 3363/22.3T8OER.L1-7)
Embora não abordando o caso da perspetiva do RGPD, este acórdão decide que não é permitida a captação de imagens de figuras públicas, mesmo que se encontrem em locais públicos, se não estiverem a exercer funções direta ou indiretamente relacionadas com as que as tornaram conhecidas.
www.jurisprudencia.csm.org.pt

Acórdão do TRL de 24-10-2024
Discutiu-se o direito ao apagamento *vs* direito à liberdade de expressão
I. Ainda que a recorrida não constitua um órgão de comunicação social, tal não impede a mesma, nem lhe retira qualquer legitimidade, para indexar conteúdos que contribuam para o exercício da liberdade de expressão e de informação por parte dos cidadãos.
II. O direito ao apagamento, tal como se encontra previso no art. 17.º do Regulamento Geral sobre a Proteção de Dados (RGPD), não é aplicável caso existam interesses legítimos que prevaleçam, designadamente o exercício da liberdade de expressão e de informação, podendo estar em causa tanto os interesses do responsável, como de terceiros.
III. Para efetuar a ponderação entre o direito ao respeito pela vida privada e o direito à liberdade de expressão e de informação, deve ser tomado em consideração um determinado número de critérios pertinentes, como a contribuição para um debate de interesse geral, o grau de notoriedade da pessoa afetada, o objeto da reportagem, o comportamento anterior da pessoa em causa, o conteúdo, a forma e as consequências da publicação, o modo e as circunstâncias em que as informações foram obtidas, bem como a veracidade das mesmas.
IV. Porém, quanto à veracidade ou não há que distinguir entre afirmações de facto e juízos de valor, pois embora a materialidade das primeiras se possa provar, os segundos não se prestam a uma demonstração da sua exatidão.
V. Quando a pessoa visada desempenhe um papel na vida pública, essa pessoa deve demonstrar um grau de tolerância acrescido, dado que está inevitavelmente e com pleno conhecimento de causa exposta ao escrutínio público.
VI. No caso, as expressões usadas pelo autor do blog não podem sequer considerar-se, objectivamente, ofensivas da honra e bom nome do Recorrente, pois que, de acordo com o sentimento da generalidade da comunidade, não é razoável considerar-se que estas, no contexto em que foram proferidas, mereçam qualquer juízo de censura, antes consistindo meras opiniões.
www.jurisprudencia.csm.org.pt

Acórdão do TRC de 21-5-2024 (p. 2495/22.1T8LSB.L1-6)
Discutiu-se se o Autor declarado falido há 20 anos tem direito ao esquecimento das dívidas.
www.jurisprudencia.csm.org.pt

- Utilização de imagens captadas em sistema de videovigilância para efeitos criminais[15];
- utilização de imagens captadas por sistema de videovigilância em contexto laboral[16];
- controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral[17];
- realização de perícia vs acesso a dados de terceiros[18];
- proibição de tratamento de dados pessoais relativos à saúde[19];
- solicitação de informação a entidades terceiras para fixação do valor da causa[20];
- transmissão de dados pessoais a subcontratantes e outras entidades[21].

15. **Acórdão do TRP de 16-10-2024** (p. 112/20.4GAETR.P1)
www.jurisprudencia.csm.org.pt
Acórdão do TRP de 23-10-2024 (p. 1049/18.2JAPRT.P1)
www.jurisprudencia.csm.org.pt

16. **Acórdão do TRP de 28-2-2024** (p. 79/19.1T9AMR.P1)
www.jurisprudencia.csm.org.pt

17. **Acórdão do TRP de 9-9-2024** (p. 3958/21.2T8VNG.P1)
www.jurisprudencia.csm.org.pt

18. **Acórdão do TRC de 15-3-2024** (p. 2596/23.0T8VIS-B.C1)
www.jurisprudencia.csm.org.pt
Considerou-se que os dados pessoais dos clientes/pacientes da empresa terceira encontram-se protegidos nos termos constantes do RGPD pelo que, o acesso aos mesmos só pode ter lugar nos termos previstos no RGPD, mediante consentimento dos respetivos titulares.

19. **Acórdão do TRE de 6-6-2024** (p. 2500/23.5T8FAR.E1)
Pronunciou-se sobre o acesso ao exame de taxa de álcool no sangue para efeitos de junção a acção de direito de regresso da seguradora sobre um condutor.
www.jurisprudencia.csm.org.pt
Acórdão do TRE de 11-7-2024 (p. 1692/23.8T8STB-A.E1)
Discutiu-se a proibição de tratamento de dados de saúde de pessoa falecida.
1. Os dados relativos à saúde de pessoa falecida são protegidos nos termos do Regulamento Geral da Proteção de Dados (RGPD) e da Lei de execução nacional (Lei n.º 58/2019, de 8 de agosto) porque se integram nas categorias especiais de dados pessoais;
2. Deverão ser considerados dados pessoais todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental, o que inclui informações sobre a pessoa singular recolhidas em vida durante a prestação de serviços de saúde pelos centros de saúde ou instituições hospitalares – cfr. Considerando 35 do RGPD (fonte interpretativa);
3. Estes dados intrinsecamente pessoais, são no Considerando 51 do RGPD classificados de «dados sensíveis»;
4. Como tal o seu tratamento é proibido nos termos do artigo 9.º, n.º 1, do RGPD;
5. Assim não será se, o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, ou se, o tratamento for necessário (princípio da necessidade) à declaração, ao exercício ou à defesa de um direito num processo judicial ou, sempre que os tribunais atuem no exercício da suas função jurisdicional nos termos do artigo 9.º, n.º 2, do RGPD;
6. Porque a lei não distingue, a finalidade "defesa de um direito em processo judicial" tanto pode abranger um direito do titular dos dados, como um direito contra o titular dos dados.
7. O que importa atender é à efetiva necessidade de tratamento dos dados, devendo esta fazer-se de forma proporcional, restrita à finalidade que o justifica.

www.jurisprudencia.csm.org.pt
Acórdão do TRG de 8-2-2024 (p. 596/22.6T8VNF.G2)
Discutiu-se a proibição de tratamento de dados de saúde de pessoa falecida.
www.jurisprudencia.csm.org.pt

20. **Acórdão do TRG de 18-1-2024** (p. 743/23.0JAVRL-A.G1)
O Tribunal considerou ser manifesto que o interesse público atinente à acção da justiça e descoberta da verdade material se sobrepõe a qualquer constrangimento relacionado com a alegada intromissão da vida privada das entidades em causa ou protecção de dados pessoais protegidos. Estava em causa a notificação de entidades para virem indicar os valores recebidos pelos Autores a título de comissões pena "venda" de jogadores, para efeitos de fixação do valor da causa relativamente a pedidos não liquidados.
www.jurisprudencia.csm.org.pt

21. **Acórdão do TRG de 20-6-2024** (p. 1303/19.6T8BRG.G2)
Discutiu-se se em face da nulidade do contrato, o responsável pelo tratamento de dados carece de interesse legítimo para a transmissão dos dados do autor às sub-

Durante o ano de 2024 e em janeiro de 2025, o Tribunal de Justiça da União Europeia pronunciou-se sobre diversas questões relativas à proteção de dados pessoais.

Vejamos.

C. No recentíssimo Acórdão da 1.ª Secção de 9 de janeiro de 2025 (processo n.º 394/23, Association Mousse[22]), o Tribunal de Justiça teve oportunidade de esclarecer o alcance dos princípios da licitude e da minimização dos dados previstos no RGPD, no contexto do tratamento dos dados relativos ao género efetuado por uma empresa de transporte, para efeitos da personalização da sua comunicação comercial.

Estava em causa o seguinte:

Uma empresa comercializa títulos de transporte ferroviário através de um sítio na internet e de aplicações. Aquando da compra do título de transporte, os clientes são obrigados a preencher um campo com a menção "Senhor" ou "Senhora".

Foi apresentada uma reclamação à Comissão Nacional da Informática e Liberdades francesa, suscitando a violação dos princípios da licitude e da minimização dos dados e das obrigações de transparência e informação previstas no RGPD.

A referida Comissão considerou que o tratamento de dados efetuado pela empresa transportadora era lícito, tendo sido interposto recurso de anulação.

O órgão jurisdicional, *in casu* o Conselho de Estado francês, em formação jurisdicional, submeteu um pedido de reenvio prejudicial no sentido de saber se, para aferir da necessidade da recolha dos dados relativos ao género dos clientes efetuada pela empresa de transportes se pode ter em conta, por um lado, as práticas admitidas nas comunicações comerciais, civis e administrativas e, por outro lado, o facto de esses clientes poderem, após terem fornecido esses dados

contratantes, para que fossem incluídos na base de dados partilhada pelas empresas que oferecem redes e serviços de comunicações eletrónicas e, ainda, para tentativa de cobrança extrajudicial dos montantes imputados.
www.jurisprudencia.csm.org.pt
Acórdão do TRG de 27-6-2024 (p. 5232/19.5T8VNF-H.G1)
O Tribunal pronunciou-se, no âmbito de uma cessão de créditos, sobre a legalidade da cedência de dados pessoais do cedido ao cessionário.
www.jurisprudencia.csm.org.pt

22. Versão integral do acórdão:
www.curia.europa.eu
Resumo:
www.curia.europa.eu

ao responsável pelo tratamento, exercer o seu direito de oposição à utilização desses dados, por motivos relacionados com a sua situação particular.

Abordarei somente a primeira questão que me chamou a atenção.

O Tribunal de Justiça decidiu, em suma, que:

- O tratamento de dados só é necessário para a execução de um contrato se for objetivamente indispensável para realizar uma atividade que faça parte integrante da execução do contrato;
- No caso concreto, os dados foram recolhidos para personalização da comunicação comercial;
- A personalização da comunicação comercial com o cliente faz parte integrante da execução do contrato: a prestação do serviço implica comunicar com o cliente, nomeadamente para lhe remeter o título de transporte por via eletrónica, de prestar informações relativamente à viagem e efetuar contactos através do serviço de apoio aos clientes, utilizando-se fórmulas de cortesia demonstrativas do respeito para com o cliente;
- Contudo, essa comunicação não tem de ser personalizada em função da identidade de género do cliente visado;
- Considerando os serviços prestados pela empresa de transportes, a personalização da comunicação com fórmulas correspondentes à identidade de género, não é objetivamente indispensável nem essencial para a execução do contrato, podendo ser utilizadas formas de cortesia de carácter genérico;
- O artigo 6.º, n.º 1, primeiro parágrafo, alínea f), do RGPD não prevê a tomada em consideração dos usos e das convenções sociais para apreciar o caráter necessário do tratamento, devendo ser efetuada a uma interpretação restritiva deste preceito;
- O princípio da necessidade do tratamento para fins legítimos tem de ser analisado conjuntamente com o princípio da minimização: é necessário que o interesse legítimo não possa ser alcançado de forma razoável através de outros meios;
- Se o tratamento dos dados também tivesse como finalidade a adaptação dos serviços de transporte noturno, com vagões reservados a pessoas com a mesma identidade de género e para assistência a passageiros com deficiência, ainda assim, não estaria justificado o tratamento sistemático e generalizado dos dados relativos ao género;
- Tal tratamento violaria o princípio da minimização, sendo possível o tra-

tamento limitar-se aos dados dos clientes que pretendessem viajar no período noturno ou beneficiar da assistência personalizada em função de deficiência;

- Para efeitos de análise da eventual prevalência dos direitos/interesses do titular dos dados sobre o interesse legítimo do responsável do tratamento ou de terceiro, o órgão jurisdicional nacional deve ponderar as expectativas razoáveis do titular dos dados, o alcance e o impacto do tratamento dos dados sobre o titular dos mesmos em confronto com o interesse legítimo invocado, em especial, o risco de discriminação em função do género, incluindo da respetiva mudança de género.

IV. Nota final

O citado acórdão do Tribunal de Justiça da União Europeia de 9 de janeiro de 2025 reflete a complexidade atual da proteção de dados na era da inteligência artificial e plataformas digitais e gera alguma estranheza na ponderação que faz dos princípios da licitude e da minimização.

O direito à proteção de dados pessoais não é absoluto.

Deve ser ponderado em relação à sua função na sociedade e harmonizado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

O tratamento dos dados pessoais deve ser concebido para servir as pessoas.

Será caso para questionar se o Tribunal de Justiça não terá ido longe demais ao aplicar o princípio da minimização de forma tão estrita e desconsiderar a utilidade social das convenções de cortesia que humanizam e facilitam a interação comercial.

Perante as aporias da proteção de dados pessoais na era da inteligência artificial, há que ter a humildade de reconhecer que a perfeição é improvável e a mudança inevitável.

Muito obrigada pela atenção. •

OBSERVAÇÕES FINAIS

TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS NO SISTEMA JUDICIAL: OBSERVAÇÕES E PERSPETIVAS.

Juiz Conselheiro do Supremo Tribunal de Justiça
José Luís Lopes da Mota

Direito à proteção e tratamento de dados pessoais no sistema judicial – quadro legal

O direito à proteção de dados pessoais define-se muito sinteticamente como um direito autónomo de disposição e controlo sobre os «dados pessoais», entendidos estes como qualquer informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»). É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular [cfr. artigos 4..º do Regulamento Geral de Proteção de Dados («RGPD»)[1] e 3.º da Diretiva 2016/680[2]].

Na sua definição legal, importando restrições e ingerências no direito à proteção de dados e noutros direitos fundamentais, o «tratamento de dados» compreende quaisquer operações efetuadas sobre dados pessoais, consentidas pelo titular dos dados ou justificadas e autorizadas por lei, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, em ficheiros automatizados ou não automatizados (artigos 4.º do RGPD e 3.º da Dir680).

Um olhar retrospetivo sobre a génese, evolução e conteúdo deste direito evidencia uma densificação diretamente proporcional ao aumento dos riscos pelo

1. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) – Jornal Oficial da União Europeia («JOUE») L 119/1, de 4.5.2016.

2. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho – JOUE L 119/89, de 4.5.2016.

aprofundamento do grau de interferência na privacidade, em resultado do desenvolvimento e utilização das (novas) tecnologias de processamento (tratamento) «automático» de dados pessoais.

É o recurso aos sistemas informáticos de tratamento de dados que, definitivamente, justifica a edição de normas próprias neste domínio, como é reconhecido pela aprovação da Convenção 108 do Conselho da Europa, de 1981, o primeiro instrumento internacional de referência nesta matéria.

No sistema judicial, as atividades pelas quais se efetiva o «tratamento de dados», agora com o apoio de sistemas informáticos, não deixam de, no essencial, corresponder aos atos processuais (e não estritamente processuais, com eles conexos) que, antes do aparecimento dos computadores – sem que isso justificasse particulares preocupações de proteção da privacidade através de um subsistema normativo específico – se realizavam através de procedimentos manuais em processos organizados em papel («ficheiros manuais», como passaram a designar-se, por contraposição aos «ficheiros informáticos» ou «ficheiros automatizados», uns e outros atualmente sujeitos a idêntico regime[3]).

Embora não constituindo normas de proteção de dados «per se», as normas de direito processual – em particular as relativas à proteção da privacidade no âmbito da atividade dos tribunais –, regulando atos do processo («operações» sobre dados pessoais), sempre visaram finalidades semelhantes às de «tratamento de dados», sujeitas a princípios idênticos, nomeadamente aos princípios da necessidade, adequação, proporcionalidade e reserva de lei e do juiz (do tribunal), que, num Estado de Direito democrático, justificam a intervenção, restrição e compressão de direitos fundamentais[4].

3. Cfr., o artigo 35.º, n.º 7, da Constituição e os artigos 4.º, n.º 2, do RGPD, 3.º, n.º 2, da Diretiva 2016/680, e 2.º da Convenção 108 do Conselho da Europa (*infra*, 8), de 1981, na versão originária e na versão atual decorrente do Protocolo de 2018, que altera a Convenção (Convenção 108+).

4. Cfr, designadamente, os artigos 18.º, n.º 2 da Constituição (segundo o qual «a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos»), 8.º, n.º 2 da Convenção Europeia dos Direitos Humanos (CEDH, que dispõe que «não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros» e 8.º da Carta dos Direitos Fundamentais da União Europeia («proteção de dados pessoais»», que se baseia no artigo 8.º da CEDH (anotação ao artigo 8.º, das «Anotações relativas à Carta dos Direitos Fundamentais», do *Praesidium* da Convenção, JOUE C 303/17, de 14.12.2007) e 52.º Carta (Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros. (...) Na medida em que a presente Carta contenha direitos correspondentes aos direitos garantidos pela Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o sentido e o âmbito desses direitos são iguais aos conferidos por essa Convenção. Esta disposição não obsta a que o direito da União confira uma proteção mais ampla».

A evolução das tecnologias de informação e comunicação conduziu, nas últimas décadas, sobretudo a partir dos anos 90, à construção de um sistema de normas autónomo, ditado pelo aparecimento e explosão da *internet* e pelos *big data*, estruturado com base em princípios essenciais do Estado de Direito e de proteção dos direitos fundamentais, reconhecidos em instrumentos que integram o sistema de proteção internacional dos direitos humanos, com destaque para a Convenção Europeia dos Direitos Humanos, embora dotado de terminologia e conceitos próprios, de inspiração tecnológica.

A Convenção Europeia dos Direitos Humanos, numa interpretação dinâmica aberta à «evolução do sociedade», com o decisivo contributo da jurisprudência do Tribunal Europeu dos Direitos Humanos, inscreveu a proteção de dados pessoais no âmbito da tutela do «direito ao respeito pela vida privada e familiar, domicílio e correspondência» (art.º 8.º)[5], posteriormente desenvolvida na «Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal», assinada em 28 de janeiro de 1981[6], que marca o «Dia Europeu de Proteção de Dados» (convenção 108 do Conselho da Europa)[7].

É neste contexto que se desenha o reconhecimento do direito à «autodeterminação informativa»[8] e, mais recentemente, do direito à proteção de dados pessoais no âmbito da União Europeia (artigos 16.º do Tratado sobre o Funcionamento da União Europeia[9] e 8.º[10] e 52.º[11] da Carta dos Direitos Fundamentais da União Europeia), como direito fundamental autónomo, constitucionalmente protegido (artigo 35.º da Constituição).

O quadro jurídico atual estrutura-se e completa-se, no âmbito da União Europeia (UE), com o Regulamento (UE) 2016/679 (RGPD) do Parlamento Eu-

5. Artigo 8.º: «Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência».

6. Em vigor desde 1.10.1985. Toda a informação em: www.coe.int

7. Convenção ratificada pelo DPR n.º 21/93 e aprovada para ratificação pela RAR n.º 23/93, DR I-A, de 9.7.1993, completada pelo Protocolo Adicional de 2001 (DPR n.º 56/2006 e RAR n.º 45/2006, DR I-A, n.º 117, de 20/06/2006), que introduziu disposições sobre autoridades de controlo e fluxo transfronteiriço de dados de carácter pessoal para um destinatário que não está sujeito à jurisdição de uma Parte na Convenção, e modernizada (Convenção 108+) pelo Protocolo que Altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 2018 (DPR n.º 78/2023 e RAR n.º 107/2023, DR Série I, de 31.08.2023).

8. *Grundrecht auf Informationelle Selbstbestimmungsrecht*, na célebre sentença do Tribunal Constitucional alemão, de 1983.

9. Artigo 16.º TFUE: «1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. (…)».

10. *Infra*.

11. *Supra*, 4.

ropeu e do Conselho (Regulamento Geral sobre a Proteção de Dados), e com a Diretiva 2016/680 do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais[12], requerida pela Declaração 21 anexa ao Tratado de Lisboa[13] e transposta para o direito interno pela Lei n.º 59/2019, de 8 de agosto, e ainda, no âmbito do Conselho da Europa, com a Convenção 108+ do Conselho da Europa (2018)[14].

Na área penal e processual penal identificam-se ainda normas específicas, anteriores e posteriores, em vários instrumentos adotados no domínio da cooperação judiciária em matéria penal, a levar em conta, nomeadamente na Convenção de Aplicação do Acordo de Schengen de 14 de junho de 1985 (1990)[15], na Convenção de Auxílio Judiciário Mútuo (União Europeia, 2000)[16], no Segundo Protocolo Adicional (2001) à Convenção Europeia de Auxílio Judiciário Mútuo em Matéria Penal do Conselho da Europa, de 1959[17], na Decisão 2002/187/JAI relativa à Eurojust[18] e no seu regulamento interno (agora, nos Regulamentos UE 2018/1727[19] e 2018/1725[20]), na Convenção sobre o Cibercrime (Conselho da Europa, 2001[21]).

A Diretiva 95/46/CE, de 24.10.1995, adotada no âmbito do anterior «primeiro pilar» da UE[22], que vigorou até 2018, transposta para o direito interno pela Lei 67/98, de 26 de outubro, e revogada pela Lei 58/2019, de 8 de agosto, que

12. *Supra*, 1 e 2.

13. «21. Declaração sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial: A Conferência reconhece que, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições específicas sobre proteção de dados pessoais e sobre a livre circulação desses dados, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia.»

14. Convenção 108 atualizada para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal (cfr. "The modernised Convention 108: novelties in a nutshell", em www.coe.int – *supra*, 6.

15. Artigos 102.°-118.°.

16. Convenção elaborada pelo Conselho em conformidade com o artigo 34° do Tratado da União Europeia, relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia, artigo 23.°.

17. Artigo 26.°.

18. Decisão do Conselho de 28 de fevereiro de 2002 relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade, artigos 14.°-24.°.

19. Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), e que substitui e revoga a Decisão 2002/187/JAI do Conselho, artigos 26.º-46.º.

20. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE.

21. Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, disposições várias.

22. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

assegura a execução do RGPD, excluía as matérias de cooperação penal (do «terceiro pilar») do seu âmbito de aplicação[23].

Porém, por ocasião da transposição da diretiva, o n.º 7 do artigo 86.º do Código de Processo Penal, aditado pela revisão de 1998, inseriu uma norma de proteção de dados pessoais, embora de resultados pouco visíveis, de grande alcance na estrutura e dinâmica do processo e, em particular, nas relações com o princípio de publicidade do processo e com o segredo de justiça, do seguinte teor: «A publicidade não abrange os dados relativos à reserva da vida privada que não constituam meios de prova».

O artigo 8.º («Proteção de dados pessoais») da Carta dos Direitos Fundamentais da União Europeia estabelece que: «1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»[24]

Para o que agora interessa, importa levar especialmente em conta o n.º 20 do preâmbulo do RGPD: «(20). Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização dos membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento

23. Preâmbulo, nº 13, e artigo 3.º, nº 2.

24. O artigo 8.º da Carta baseia-se no artigo 286.º do anterior Tratado da Comunidade Europeia, na Diretiva 95/46/CE, no artigo 8.º da Convenção Europeia dos Direitos Humanos e na Convenção 108 do Conselho da Europa (cfr. Anotações à Carta dos Direitos Fundamentais, JOUE C 303, 14.2.2007).

dos dados». Bem como o artigo 55.º, n.º 3, que estabelece que a competência das autoridades de controlo «não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional».

No que respeita à justiça criminal há que ter em consideração a Diretiva 2016/680, que, com as especificidades próprias das matérias criminais, se aplica ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais (artigos 1.º e 2.º), nos termos da lei processual penal e demais legislação aplicável (artigo 2.º, n.º 1, da Lei n.º 59/2019), incluindo, pois, as autoridades judiciárias (juiz, juiz de instrução, Ministério Público) e órgãos de polícia criminal – artigo 1.º, als. b) e c), do Código de Processo Penal –, por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados (artigo 2.º, n.º 2, da Lei n.º 59/2019), área em que o RGPD é também aplicável em funções não necessariamente a executar para efeitos de investigação e repressão de infrações penais ou da execução de sanções penais, isto é, nos casos em que os dados são tratados para dar cumprimento a uma obrigação legal, mas não para os efeitos previstos na diretiva (n.º 11 do preâmbulo).

Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, é feito nos termos das regras nacionais aplicáveis aos processos judiciais (n.º 49 do preâmbulo).

A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais e pelo Ministério Público no exercício das suas competências processuais (artigo 43.º, n.º 2, da Lei n.º 59/2019), a fim de assegurar a independência dos juízes e dos tribunais no desempenho das suas «funções jurisdicionais» (na aceção da diretiva), sem prejuízo de o cumprimento das regras da diretiva ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta dos Direitos Fundamentais (n.ºs 80 a 82 do preâmbulo e artigo 43.º da Lei n.º 59/2019).

O direito a um tribunal independente, que o RGPD e a Diretiva 680 garantem, encontra consagração no artigo 47.º da Carta, com densificação na jurisprudência do Tribunal de Justiça da União Europeia (TJUE). No Acórdão de 27.2.2018, processo C-64/16 (Associação Sindical dos Juízes Portugueses), convocando jurisprudência consolidada, disse o Tribunal: «44. O conceito de in-

dependência pressupõe que a instância em causa exerça as suas funções jurisdicionais com total autonomia, sem estar submetida a nenhum vínculo hierárquico ou de subordinação em relação a quem quer que seja e sem receber ordens ou instruções de qualquer origem, e esteja, assim, protegida contra intervenções ou pressões externas suscetíveis de afetar a independência de julgamento dos seus membros e influenciar as suas decisões»

O conceito de «exercício da função jurisdicional», de crucial importância neste domínio, foi examinado e interpretado no Acórdão do TJUE de 24.3.2022, processo C-245/20[25]. Disse o Tribunal a este propósito que a referência às operações de tratamento efetuadas pelos órgãos jurisdicionais «no exercício da sua função jurisdicional» (artigo 55.º, n.º 3, do RGPD) deve ser entendida no sentido de que «não se limita aos tratamentos de dados pessoais levados a cabo pelos órgãos jurisdicionais no âmbito de processos concretos, mas sim no sentido de que visa, de maneira mais ampla, o conjunto das operações de tratamento efetuadas pelos órgãos jurisdicionais no âmbito da sua atividade judicial, pelo que estão excluídas da competência da autoridade de controlo as operações de tratamento cuja fiscalização é suscetível, direta ou indiretamente, de ter uma influência na independência dos seus membros ou de pesar nas suas decisões.[26]

O direito à proteção de dados pessoais inscreve-se, assim, no objeto do processo. Por definição, os atos processuais são "operações" de tratamento de dados, na sua definição legal: «recolha, registo, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou por qualquer outra forma de disponibilização, comparação ou interconexão, limitação, apagamento ou destruição».

O "tratamento" de dados é constituído por "operações" de interferência, de restrição ou compressão de direitos fundamentais que, como tal, têm de estar

25. Acórdão tendo por objeto o pedido de decisão prejudicial de interpretação do artigo 55.°, n.° 3, do RGPD, que dispõe: «As autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional». Repercutindo o mesmo princípio que, com as devidas adaptações, se aplica ao processo penal (artigo 45.° da Diretiva 680), os artigos 43.° a 45.° da Lei n.° 59/2019.

26. Estava em causa a disponibilização de informação de um processo a um jornalista, que mereceu a seguinte consideração: "o facto de um órgão jurisdicional disponibilizar temporariamente a jornalistas documentos dos autos de um processo judicial, que contêm dados pessoais, a fim de lhes permitir informar melhor sobre o desenrolar desse processo decorre do exercício, por esse órgão jurisdicional, da sua «função jurisdicional», na aceção desta disposição".

previstas na lei. Sendo necessário distinguir entre tratamento com fins jurisdicionais e tratamento com fins não jurisdicionais.

Inscrevem-se certamente na categoria de "tratamento com fins jurisdicionais" os atos processuais praticados pelas autoridades judiciárias (juiz, tribunal, Ministério Público), no âmbito de competências de autoridade na sua atividade processual, tal como definidas nas leis do processo. Nesta categoria se inscreverão também os atos de outros sujeitos (partes, arguidos, assistentes e advogados), dos órgãos de polícia criminal e de outros intervenientes processuais (v. g. testemunhas, peritos, consultores), preordenados à decisão do processo, bem como os atos de secretaria e de oficiais de justiça (preparação, execução, coadjuvação, apoio à decisão) e de outros agentes, que devam integrar-se no processo.

Por exclusão, inscrever-se-ão na categoria de "tratamento com fins não jurisdicionais" quaisquer outros atos, de magistrados, de secretaria, dos serviços, de outras entidades e interveniente, que, praticados no âmbito da atividade dos tribunais ou de serviços integrados no sistema judicial, não se incluem em processos para realização de uma finalidade processual.

Esta distinção é fundamental para se identificarem, definirem e clarificarem tarefas, papéis e responsabilidades definidas em conceitos funcionais, tal como definidos no RGPD e na Diretiva 680 – para identificação e reconhecimento, por exemplo, de responsáveis pelo tratamento, de subcontratantes ou de entidades e funções de controlo do tratamento[27].

Princípios do tratamento e direitos dos titulares dos dados no sistema judicial

As questões implicadas convocam necessariamente os princípios e as responsabilidades pelo tratamento dos dados pessoais.

Constituem princípios do tratamento, decorrentes da natureza das operações de tratamento definidas como atos de interferência em direitos fundamentais, sujeitos a critérios de proporcionalidade e a reserva de lei, os princípios da licitude, da lealdade e transparência[28], da limitação das finalidades da recolha, da exatidão, da minimização dos dados, da limitação da conservação e da integridade e confidencialidade (princípios consagrados nos artigos 5.º a 11.º do

27. Artigos 24.º e segs. do RGPD e 19 e segs. da Diretiva 680.

28. Esta com as restrições impostas pelo natureza dos dados, finalidades do tratamento e competências das autoridades judiciárias e órgãos de polícia criminal em matéria penal, nos termos da Diretiva 680 e da Lei n.º 59/2019.

RGPD e princípios relativos ao tratamento na área penal consagrados nos artigos 4.º a 11.º da Diretiva 680).

O «responsável pelo tratamento» é responsável pelo cumprimento do disposto no n.º 1 do artigo 5.º do RGPD e do n.º 1 do artigo 4.º da Diretiva 680, isto é, por que os dados pessoais sejam: a) objeto de tratamento lícito, leal e transparente em relação ao titular dos dados[29]; b) recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; c) adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados; d) exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora; e) conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; f) tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

O tratamento só é lícito se e na medida em que se verifique pelo menos uma das situações enumeradas no artigo 6.º do RGPD, nomeadamente se: o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas (al. a), o que no processo, sobretudo no processo penal, sofre severas restrições; o tratamento for necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito (al. c); o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento (al. e), como sucede com os tribunais.

Nos termos do artigo 5.º da Lei 59/2019 (que transpõe o artigo 8.º da Diretiva 680), o tratamento de dados pessoais no âmbito das investigações e do processo penal só é lícito se estiver previsto na lei e na medida em que for necessário para o exercício de uma atribuição da autoridade competente para os efeitos previstos nesta lei, que indica, pelo menos, os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento, sendo que, não estando previsto na lei, o tratamento dos dados pessoais apenas pode ser realizado se for necessário para a proteção dos interesses vitais do titular dos dados ou de outra pessoa singular.

29. Objeto de um «tratamento lícito e leal» (al. a), diz a Diretiva 680, dadas as restrições à transparência decorrentes das finalidades do tratamento no âmbito das investigações e do processo penal.

Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou do direito nacional que constituam uma medida necessária e proporcionada numa sociedade democrática, o «responsável pelo tratamento», a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta: a) qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; b) o contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) a natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) as eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e e) a existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização (artigo 6.º do RGPD).

O «responsável pelo tratamento», que, sublinhe-se, corresponde a um «conceito funcional» (como nota a Decisão 1/2010 do "Grupo de Trabalho do Artigo 29"[30]), é a entidade competente que determina as finalidades e os meios de tratamento ou a entidade indicada na lei, por si só ou conjuntamente com outros, que garante a aplicação dos princípios e assegura o exercício dos direitos dos titulares dos dados.

No caso da Justiça, tendo em conta a responsabilidade pela definição e aplicação de medidas técnicas e organizativas para garantir o cumprimento das normas de processamento e proteção de dados, atribuída ao «responsável pelo tratamento» (artigos 24.º a 26.º do RGPD e 20.º a 24.º da Lei n.º 59/2019, Diretiva 680) – que, para este efeito, não pode ser o juiz na sua atividade «jurisdicional» –, a complexidade do sistema impõe que se deva falar em «responsáveis conjuntos» pelo tratamento, em função da diversidade de intervenientes, papéis, competências e responsabilidades legalmente definidas, seja no que se refere à disciplina e gestão do processo, seja no que respeita à organização e funcionamento dos tribunais e serviços, à competência dos diferentes órgãos de gestão e às responsabilidades das várias entidades pelos recursos materiais, humanos e

30. "Grupo de Trabalho para a Proteção das Pessoas no que diz respeito ao Tratamento de Dados Pessoais", criado pelo artigo 29.º da Diretiva 95/46/CE , revogada pelo RGPD, substituído pelo Comité Europeu para a Proteção de Dados.

financeiros e pelos subsistemas de apoio à atividade judicial.

É também neste quadro que, em função das tarefas e responsabilidades atribuídas por lei, importa identificar os «encarregados do tratamento» («subcontratantes»)[31] e a sua participação na conceção, gestão e realização dos procedimentos de processamento de dados («operações de tratamento»), agindo sob a direção do «responsável pelo tratamento», nos termos dos artigos 28.º do RGPD e 22.º da Diretiva 680.

De acordo com a lei em vigor (artigo 23.º da Lei n.º 34/2009, de 14 de julho[32]), a responsabilidade pelo tratamento dos dados compete: a) aos responsáveis pela gestão dos dados, cujas competências são exercidas de forma coordenada através da Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial, prevista no presente capítulo; b) aos magistrados com competência sobre o respetivo processo, nos termos da lei.

Como é conhecido, esta Comissão não funciona e não parece que a lei (processual) em vigor garanta adequadamente o exercício dos direitos dos titulares dos dados e possibilite o exercício efetivo das competências dos magistrados enquanto responsáveis pelo tratamento face ao regime do RGPD e da Diretiva 680.

As leis de proteção de dados reconhecem e garantem um conjunto de direitos específicos, relacionados com o tratamento de dados pessoais (cfr. artigos 10.º a 13.º da Lei 67/98, de 26 de outubro), agora desenvolvidos no RGPD (artigos 12.º a 23.º) e na Diretiva 680 (artigos 12.º a 18.º).

Em síntese, são direitos dos titulares dos dados, designadamente, os direitos de acesso, retificação e apagamento; de limitação do tratamento (finalidades, minimização); de pedir o exercício dos direitos e verificação pela autoridade de controlo em caso de recusa; à segurança dos dados e à informação sobre violação de dados (artigos 32.º e 33.º do RGPD e 29.º a 31.º da Diretiva 680, incluindo medidas técnicas, organizativas, registos cronológicos); de obter intervenção humana do responsável pelo tratamento (no caso de decisões automatizadas, como limite à IA).

Compete ao responsável pelo tratamento assegurar os direitos dos titulares dos dados com a assistência de um encarregado de proteção de dados (artigos 39.º do RGPD e 34.º da Diretiva 680), sob fiscalização de uma ou várias auto-

31. "Subcontratantes", na terminologia da lei portuguesa; "encargado del tratamento" (esp.), "responsabile del tratamento" (it.), "processor" (ing.), «sous-traitant» (fr.), noutras versões linguísticas.

32. Lei que que «estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial».

ridades de controlo independentes (artigos 51.º e 52.º do RGPD e 41.º e 42.º da Diretiva 680), com as competências definidas nos artigos 55.º a 58.º do RGPD e 45.º a 47.º da Diretiva.

A Comissão Nacional de Proteção de Dados («CNPD»), que é a autoridade de controlo nacional para efeitos do RGPD (artigo 3.º da Lei n.º 58/2019)[33], não fiscaliza o tratamento de dados efetuado pelos juízes, tribunais e MP no exercício das suas competências processuais (tratamento no exercício de função jurisdicional).

As autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais e outras autoridades judiciárias, na área criminal, incluindo o Ministério Público, que atuem no exercício da sua função jurisdicional (artigos 55.º, n.º 3, do RGPD e 45.º, n.º 3, da Diretiva 680).

Questões em aberto

Tendo em conta o que vem de se expor, numa breve síntese e sem prejuízo de uma mais detalhada e demorada análise que a situação atual requer em diferente sede, pode identificar-se um conjunto de questões ainda em aberto que sistematicamente se relacionam com os seguintes temas:

a) *Adaptação da legislação processual penal aos princípios e regras de tratamento de dados pessoais*

Sendo a área de mais profunda interferência na privacidade e em outros direitos fundamentais, a atividade das autoridades judiciárias e dos órgãos de polícia criminal, bem como de outros intervenientes processuais, traduz-se, por definição, em atos («operações») de tratamento de dados pessoais necessários à realização das finalidades do processo, nas suas várias fases: (i) no âmbito de medidas cautelares e de polícia (artigos 248.ºss do CPP); (ii) no âmbito do inquérito, para investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher as provas, em ordem à decisão sobre a acusação (artigo 262.º, n.º 1, e 267.ºss do CPP); na instrução, para comprovação judicial da decisão de deduzir acusação ou de arquivar o inquérito em ordem a submeter ou não a causa a julgamento

33. Lei n.º 58/2019, de 8 de agosto, que «assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados».

(artigo 286.º, n.º 1, e segs. do CPP); (iii) no julgamento, para discussão e prova dos factos alegados pela acusação e pela defesa e dos que resultarem da prova produzida em audiência, tendo em vista as finalidades de decisão sobre a culpabilidade e sobre a sanção (artigos 339.º, n.º 4, 340.ºss, 368.º e 369.º do CPP), com elaboração do relatório social (artigo 370.º do CPP); (iv) para processamento e julgamento dos recursos (artigo 399.ºss CPP); (v) na fase de execução das penas, para execução das sentenças condenatórias (artigo 467.ºss do CPP e Código da Execução das Penas e Medidas Privativas da Liberdade[34]), incluindo, nomeadamente, as atividades destinadas (vi) à obtenção e produção de prova (art.ºs 124.º-195.º do CPP) e (vii) à aplicação de medidas de coação e garantia patrimonial (art.ºs 191.º-228.º do CPP) e, de modo geral, todos os atos processuais necessários.

Trata-se, em síntese, de um conjunto de disposições que respeitam à organização e disciplina do processo – que poderão exigir novas formas de organização do processo em função das suas diferentes fases e finalidades – e ao exercício de direitos processuais, em que, pela sua natureza e dos interesses em presença, se impõe a adequação do Código de Processo Penal e de outra legislação complementar à Lei n.º 59/2019, de modo a garantir-se a rigorosa observância dos critérios de limitação (material e temporária – artigo 5.º da Diretiva, segundo o qual devem ser previstas regras processuais que garantam o cumprimento dos prazos de apagamento e de avaliação periódica da necessidade de conservação[35]) e minimização dos dados e de operações e regras de tratamento em função das finalidades do tratamento com referência ao objeto da atividade processual em causa, e de necessidade, adequação e proporcionalidade, que conformam todo o processo, o qual, num Estado de direito democrático, deve garantir os direitos fundamentais de suspeitos e arguidos e de todos os intervenientes e participantes processuais.

34. Lei n.º 115/2009, de 12 de outubro.

35. Artigo 5.º (Prazos para a conservação e avaliação) da Diretiva 680: «Os Estados-Membros preveem prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar. Devem ser previstas regras processuais que garantam o cumprimento desses prazos.». Importaria também relembrar outras normas e princípios com reflexão nas normas processuais, como os artigos 6.º(Distinção entre diferentes categorias de titulares de dados), 7.º (Distinção entre dados pessoais e verificação da qualidade dos dados pessoais), 8.º (Licitude do tratamento), 9.º (Condições específicas do tratamento), 10.º (Tratamento de categorias especiais de dados pessoais), 11.º (Decisões individuais automatizadas) – cfr. artigos 4.º a 12º da Lei n.º 59/2019.

Na fase de inquérito, de limites indefinidos que só se fixam a final com a dedução da acusação, há que, designadamente, conjugar as normas de tratamento de dados, que diretamente respeitam aos princípios do tratamento e aos direitos dos titulares dos dados, com o regime da publicidade do processo e do segredo de justiça e com a limitações e restrições de acesso impostas pelo princípio "*need to know*", que comportam elevadas exigências ao nível do acesso e da proteção e segurança de dados.

A consideração destas exigências e o respeito pelos direitos fundamentais das pessoas sobre as quais são recolhidas informações (muitas delas sem interesse após o encerramento do inquérito) imporão, por exemplo, que devam equacionar-se alterações às regras processuais no sentido de limitar e impedir o acesso a dados que, findo o inquérito, não constituam objeto ou meio de prova, por pessoas que nisso não possam ter interesse (na decorrência do já estabelecido no n.º 7 do art.º 86.º do CPP). O que implicaria que o que não interessa para as fases seguintes permanecesse, em segurança, por tempo definido, à guarda do Ministério Público, sem prejuízo, obviamente, de ser facultado o acesso subsequente aos sujeitos interessados para satisfação de interesses legítimos, nomeadamente em matéria de produção de prova. O mesmo sucedendo, com as necessárias adaptações, relativamente às fases subsequentes do processo, a outros processos de natureza sancionatória e a processos de natureza não sancionatória (embora aqui o consentimento do titular dos dados assuma diferente relevância).

b) *Privacidade e publicação das decisões judiciais*

Proteção da privacidade e publicidade do processo são temas antagónicos que devem conciliar-se. A publicidade do processo, que justifica e impõe a audiência pública e a leitura pública da sentença, não se confunde com a publicação da sentença[36], que, em matéria penal, pode mesmo constituir uma sanção.

A publicação das decisões judiciais, requerida por razões de transparência numa sociedade democrática, nomeadamente através da inserção em bases públicas de jurisprudência, mesmo com «pseudonimização» – que, diferentemente da «anonimização», não impede a identificação da pessoa a que os dados respeitam –, constitui uma «operação» de tratamento de dados autónoma e distinta da finalidade da recolha (decisão do processo).

36. Como tem sublinhado o Tribunal Europeu dos Diretos Humanos em jurisprudência reiterada.

Se assim é, o princípio da licitude do tratamento requer a edição de normas legais próprias que regulem a publicação e minimização dos dados (nomeadamente mediante técnicas regulamentadas de «pseudonimização»). O que adquire considerável dimensão acrescida no domínio da publicação de sentenças criminais, em particular quando estão em causa dados relacionados com crimes contendo informações sobre dados pessoais particularmente sensíveis («tratamento de categorias especiais de dados pessoais», nomeadamente de dados relativos à saúde ou dados relativos à vida sexual – artigos 9.º do RGPD e 10.º da Diretiva 680 (artigo 6.º da Lei n.º 59/2019).

c) *Garantias dos direitos dos titulares dos dados*

Refiro-me aos direitos dos titulares dos dados conferidos pelo RGPD e pela Diretiva (bem como pela Convenção 108+, deve acrescentar-se).

Sendo os direitos de informação, acesso, retificação, apagamento e limitação do tratamento exercidos "nos termos da lei" processual e demais legislação aplicável, a questão em aberto é a de saber da necessidade de legislar para assegurar o exercício efetivo dos direitos dos titulares dos dados e a sua tutela jurisdicional efetiva, incluindo, se for caso disso, por via de reclamação ou de recurso.

O que significa que devam assegurar-se regras processuais próprias sobre exercício e garantia dos direitos dos titulares dos dados relativamente a atos de magistrados praticados na sua «função jurisdicional» (em que o magistrado é o «responsável pelo tratamento», em conjunto com outros responsáveis), quanto a atos do processo não praticados por magistrados (atos dos sujeitos e intervenientes processuais) e quanto a atos (operações de tratamento) praticados no âmbito dos tribunais, mas fora do processo (nomeadamente, atos de secretaria, de apoio, coadjuvação, comunicação e arquivo).

Haverá também que esclarecer quem detém as competências do «responsável pelo tratamento» relativamente a atos praticados fora da atividade jurisdicional. No rigor das coisas, tratando-se de atos judiciais, o respeito pela independência dos tribunais recomendaria que se devessem reconhecer competências neste domínio ao presidente do tribunal ou aos dirigentes das secretarias e serviços administrativos (secretário e administrador, em função das suas competências) com possibilidade de reclamação hierárquica para o presidente. O mesmo se aplicando quanto ao Ministério Público e aos respetivos serviços de apoio.

De qualquer forma, o que não se afigura conciliável com o princípio da independência dos juízes e dos tribunais é reconhecer estatuto e competências de responsável pelo tratamento de dados no exercício de «funções jurisdicionais» a órgãos de gestão das magistraturas, que não detêm competências jurisdicionais. Sendo os magistrados titulares dos processos os responsáveis pelo tratamento deste tipo de dados, o respeito pela independência da função só poderá assegurar-se pelas vias processuais próprias, de petição, reclamação ou recurso, ou de reclamação hierárquica no âmbito do Ministério Público.

Tudo isto sem prejuízo, como parece óbvio, do envolvimento e participação dos órgãos de gestão das magistraturas na definição de sistemas, procedimentos e critérios, em coordenação com os serviços e departamentos do Ministério da Justiça, no âmbito da competência destes. O que remete para a necessidade de se estabelecer um órgão ou órgãos dentro do sistema judicial que, assegurando a independência deste, como previsto no RGPD e na Diretiva 680, possam exercer funções de autoridade de controlo em colaboração com a Comissão Nacional de Proteção de Dados («CNPD»).

d) *Órgãos de controlo independente no sistema judicial*

A conceção, organização e exercício dos poderes de autoridade de controlo (independente), em colaboração com a CNPD, respeitando a independência do sistema judicial e convocando todos os serviços e entidades intervenientes, continua a ser uma das grandes questões em aberto, quer no que se refere às condições de tratamento de dados pelos magistrados no exercício de «funções jurisdicionais», quer no que diz respeito ao tratamento de dados «não jurisdicionais».

Não sendo esta a sede própria para se avançar em análises ou formulação de propostas com maior detalhe, que deverão envolver todas as entidades e serviços da Justiça no âmbito das competências legalmente definidas, importa sublinhar a urgência de intervir por via legislativa nestes domínios.

A situação atual evidencia uma insuportável carência de lei, em resultado da regulamentação incompleta do RGPD a nível interno (no que respeita ao tratamento de dados no sistema judicial) e da transposição, também incompleta, da Diretiva 2016/680.

Como é conhecido, a Proposta de Lei n.º 126/XIII/3.ª[37], de que resultou o

Decreto da Assembleia da República n.º 333/XIII[38], devolvido pelo Presidente da República à Assembleia da República, em 26.7.2019[39], para reapreciação, por suscitar questões relacionadas com a independência do controlo do tratamento de dados no sistema judicial, não mais teve sequência.

A Proposta de Lei visava completar o RGPD e a Lei n.º 59/2019, complementando a transposição da Diretiva 680, introduzindo, para isso, um conjunto de alterações à Lei 34/2009, dispondo sobre competências, responsabilidades e procedimentos de tratamento de dados, com respeito pelos princípios de tratamento e visando criar condições para o efetivo funcionamento da Comissão de Coordenação da Gestão da Informação do Sistema Judiciário.

Introduzindo um conjunto de normas quanto aos dados a tratar e ao objetivo e finalidade do tratamento e à conservação e segurança dos dados, e aprofundando e visando melhorar soluções anteriores, estabelecia que "são responsáveis pelo tratamento de dados os magistrados judiciais e do Ministério Público competentes, nos termos da lei do processo, relativamente aos dados tratados no âmbito e em atos do processo, no exercício da sua atividade processual e sob a sua direção ou autoridade". A expressão "nos termos da lei do processo", que já hoje se encontra no artigo 23.º da Lei 34/2009, requer, como já se notou, a avaliação da necessidade e a concretização de intervenções legislativas para assegurar o exercício de direitos dos titulares dos dados.

Para além disso, reconhecendo a complexidade da organização e funcionamento do sistema de justiça, organizava o exercício coordenado, como responsáveis do tratamento, das competências das entidades com responsabilidades na sua gestão e funcionamento (nomeadamente do Conselho Superior da Magistratura, do Conselho Superior dos Tribunais Administrativos e Fiscais, da Procuradoria-Geral da República e do Ministério da Justiça – Instituto de Gestão Financeira e Equipamentos da Justiça, Direcção-Geral da Administração da

37. Proposta de Lei n.º 126/XIII (3.ª), que «altera o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial», DAR II Série-A n.º 104, de 26.04.2018. cujo artigo 1.º (objeto) dispunha: « A presente lei procede à segunda alteração à Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, alterada pela Lei n.º 30/2017, de 30 de maio, adaptando o referido regime ao disposto no Regulamento (UE) n.º 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016, na Lei n.º [PL120/XIII], que assegura a sua execução na ordem jurídica interna, e na Lei n.º [Reg.ºPL74/2018], que transpõe para a ordem jurídica interna a Diretiva (UE) n.º2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016».

38. DAR II Série-A n.º 131, de 22-07.2019.

39. Veto (leitura) DAR I Série n.º 109, de 12.09.2019.

Justiça, Secretaria-Geral do Ministério da Justiça, Direção-Geral da Política de Justiça – artigos 24.º, 25.º e 26.º).

Há que, com a maior urgência, revisitar a anterior iniciativa legislativa e, por via legislativa, assegurar a proteção e o exercício de direitos fundamentais das pessoas que a Justiça tem o especial dever de garantir. •


DIA DA PROTEÇÃO DE DADOS 2025
6 ANOS
PROGRAMA