A SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS NO JUDICIÁRIO, EM PORTUGAL E NO BRASIL[1]-[2]

SECURITY IN THE PROCESSING OF PERSONAL DATA IN THE JUDICIAL BRANCH IN PORTUGAL AND BRAZIL

Manuel David Masseno[3]

RESUMO

Prima facie, os regimes previstos para o tratamento de dados pessoais pelo Poder Judiciário no Regulamento Geral sobre Dados Pessoais da União Europeia (RGPD) e na Lei Geral sobre Proteção de Dados Pessoais (LGPD) brasileira são muito semelhantes, incluindo a previsão da especificidade da Justiça criminal. Porém, para além da persistente omissão do legislador brasileiro no referente à "LGPD Penal", as profundas divergências quanto ao enquadramento legislativo relativamente à autonomia normativa e administrativa do Poder Judiciário em Portugal e no Brasil resultam em realidades muito distintas, mormente no que se refere à responsabilidade relativa à segurança no tratamento

[1] Este texto constitui uma versão do escrito para a Obra coletiva em homenagem ao Ministro Ricardo Villas Bôas Cueva, por ocasião dos 13 anos que completou no Superior Tribunal de Justiça em junho de 2024, devendo ter por referência peças processuais ou trabalhos académicos dele, *in casu* o estudo "Segurança da informação e proteção de dados pessoais" In FRANCOSKI, Denise de Souza Luiz & TASSO, Fernando Antonio (coord.). *A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado: LGPD*. São Paulo: Thomson Reuters / Revista dos Tribunais, 2021. pp. 539-550. A Obra *de qua* é coordenada por Ana Frazão *et al*. e está em vias publicação pela editora Juristas.

[2] A redação de este estudo contou com o apoio de vários Colegas que contribuíram para o mesmo com conteúdos não disponíveis publicamente e / ou com leituras preliminares como Alexandre Sousa Pinheiro, Cleórbete Santos, José Joaquim Martins, Karine Borges de Liz e Valéria Reani Rodrigues Garcia, aos quais deixo os devidos agradecimentos, tal como aos organizadores da Obra pelo honroso convite. Obviamente, todos os erros e omissões são da minha exclusiva responsabilidade.

[3] Em Portugal, é Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, onde também pertence às Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo Investigador [*i.e.*, Pesquisador] Colaborador do CEG-UAb – Centro de Estudos Globais da Universidade Aberta e Membro Convidado do CDPC – Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, ambas de Lisboa. Desde há mais de uma década, leciona sobre matérias de Proteção de Dados Dados no MESI do IPBeja, no Curso Avançado em Proteção de Dados: Regulamento Geral de Proteção de Dados, Diretivas da UE e Legislação Nacional do Instituto de Ciências Jurídico-Políticas e no Curso de Pós-Graduação Avançada em Direito da Proteção de Dados do Centro de Investigação de Direito Privado, ambos da Faculdade de Direito da Universidade de Lisboa, assim como nos Cursos de Especialização em Direito da Proteção de Dados e em Direito da Comunicação do Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra. Além de ter integrado e integrar várias Comissões de Direito Digital da Ordem dos Advogados do Brasil, é Consultor da Comissão de Direito à Privacidade e Proteção de Dados Pessoais da Subseção de Campinas da OAN e faz ainda parte da EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência da União Europeia para a Cooperação Policial. Para contacto: masseno@ipbeja.pt.

dos dados. O presente artigo analisa, detalhada e criticamente, ambos regimes, sobretudo aplicando a metodologia própria do Direito Comparado.

Palavras-chave: Brasil; Comparação; Poder Judiciário; Portugal; Proteção de Dados Pessoais.

ABSTRACT

Prima facie, the legal regimes of personal data processing by the Judiciary at the General Data Protection Regulation of the European Union (GDPR) and the Brazilian General Personal Data Protection Law (LGPD) are quite similar, including a specific regime for the processing for law enforcement. However, notwithstanding the enduring omission of the Brazilian legislative regarding the "Criminal LGPD", the deep differences regarding the regulatory and administrative autonomy of the Judiciary in Portugal and in Brazil led to very diverse realities, mostly concerning the responsibilities related to security in data processing. This paper analyses, in a detailed and critical manner, both legal regimes, mainly applying the methodologies of Comparative Law research.

Keywords: Brazil; Comparison; Judiciary; Personal Data Protection; Portugal.

1 A SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS PELO PODER JUDICIAL / JUDICIÁRIO EM PORTUGAL E NO BRASIL, QUESTÕES PRELIMINARES[4]

Começando por uma pré-compreensão dos problemas[5], inclusive antecipando as conclusões, podemos adiantar que os dois Ordenamentos partem de referências comuns e têm passado por vicissitudes semelhantes. Embora seguindo vias paralelas, sobretudo por força dos distintos contextos institucionais, e sendo problemática a sua convergência.

Efetivamente, tanto um quanto o outro assentam nos regimes gerais aplicáveis à Proteção de Dados Pessoais, embora prevejam também disciplinas suscetíveis de melhor responderem às diferentes necessidades sociais a serem satisfeitas através do exercício da judicatura.

[4] Nota do editor-chefe RED&TI: procurou-se preservar o modo de escrita do Prof. Manuel David Masseno, ajustando-se, formalmente, o mínimo possível às regras da revista.

[5] Para um enquadramento transversal das questões relativas à Proteção de Dados pela Justiça, além das considerações presentes na generalidade dos estudos referidos neste texto, têm um especial interesse as reflexões de Doneda (2022), produzidas por solicitação da UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura.

Assim, relativamente a tais tratamentos, se em Portugal vigora o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, *relativo à proteção das pessoas singulares* [físicas] *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*) – o *RGPD*[6], complementado pela Lei n.º 58/2019, de 8 de agosto; no Brasil, é aplicável a Lei n.º 13.709, de 14 agosto de 2018, *Lei Geral de Proteção de Dados Pessoais* – a *LGPD*[7].

Do mesmo modo, em ambos os casos é feita uma diferenciação entre os dados tratados pela Justiça no exercício da sua função administrativa e os tratados no da jurisdicional, em sentido estrito (Artigos 2.º n.º 1 e 9.º n.º 1 f), 23.º n.º 1 f), i) e j), 37.º n.º 1 a) e 55.º n.º 3 do *RGPD*, assim como, Artigos 1º, 7.º VI e 23.º *caput* da *LGPD*). Embora essa destrinça seja objetivamente difícil de estabelecer, como mostrou o Acórdão do TJUE – Tribunal de Justiça da União Europeia (Primeira Secção), de 24 de março de 2022, no Processo C-245/20 – X e Z contra *Autoriteit Persoonsgegevens*[8], além de ser de difícil efetivação quanto à segurança dos dados, sobretudo por razões de ordem técnica.

---

[6] Concretamente, o *Considerando* (20) do *RGPD* explicita, que, "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.". A este propósito, são de atender as considerações breves de Castro (2020, 11-13), de Martins (2022, 114-117) e de Wengorovius (2023, 448-449).

[7] A propósito do sentido e das especificidades da aplicabilidade da *LGPD* ao Poder Judiciário enquanto "Poder Público", têm muito interesse as considerações de ROCHA (2021), de SANTOS (2021, 94 e 99-101) e de Baião & Teive (2022). O que é hoje incontroverso, como mostram as iniciativas do próprio Judiciário, a serem abordadas, assim como o "Guia Orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público", da ANPD – Autoridade Nacional de Proteção de Dados, publicado em junho de 2023, cuja versão 2.0 está acessível, https://bit.ly/3QWN1iY. Ainda que extravasando manifestamente o objeto de este estudo, é de acrescentar que esta questão não é confundível com a relativa aos fundamentos de legitimação do tratamento (Artigo 7º da LGPD), como ocorre em parte da Doutrina brasileira.

[8] Como concluiu o TJUE, "O artigo 55.º, n.º 3, do [*RGPD*] deve ser interpretado no sentido de que 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

Igualmente, dos correspondentes âmbitos objetivos ficou excluída a Justiça Criminal (Artigos 2.º n.º 2 c) do *RGPD* e 4º III d), este *a contrario*, da *LGPD*). Com efeito, para o tratamento de tais dados estão previstas disciplinas diferenciadas, atendendo aos direitos dos titulares dos dados e às finalidades em causa. Em Portugal, a correspondente previsão foi efetivada através da Lei n.º 59/2019, de 8 de agosto, 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, *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*

desta disposição.". O que decorre de entender que, "(33) […] a preservação da independência do poder judicial pressupõe, de maneira geral, que as funções jurisdicionais sejam exercidas com total autonomia, sem que os órgãos jurisdicionais estejam submetidos a vínculos hierárquicos ou de subordinação nem recebam ordens ou instruções seja de que origem for, estando assim protegidas de qualquer intervenção ou pressão externa suscetível de prejudicar a independência de julgamento dos seus membros e de influenciar as suas decisões. O respeito das garantias de independência e de imparcialidade exigidas pelo direito da União pressupõe a existência de regras que permitam afastar qualquer dúvida legítima, no espírito dos litigantes, quanto à impermeabilidade da instância em causa em relação a elementos externos e à sua neutralidade relativamente aos interesses em confronto [v., neste sentido, designadamente, Acórdãos de 27 de fevereiro de 2018, *Associação Sindical dos Juízes Portugueses*, C-64/16, EU:C:2018:117, n.º 44; de 25 de julho de 2018, *Minister for Justice and Equality* (Falhas do sistema judiciário), C-216/18 PPU, EU:C:2018:586, n.º 63; de 24 de junho de 2019, *Comissão contra a Polónia* (Independência do Supremo Tribunal), C-619/18, EU:C:2019:531, n.º 72; e de 21 de dezembro de 2021, *Euro Box Promotion* e o., C-357/19, C-379/19, C-547/19, C-811/19, C-840/19, EU:C:2021:1034, n.º 225]. (34) Como tal, a referência às operações de tratamento efetuadas pelos órgãos jurisdicionais «no exercício da sua função jurisdicional» […] deve ser entendida, no contexto deste regulamento, 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. [Consequentemente,] (35) A este respeito, embora a natureza e a finalidade do tratamento efetuado por um órgão jurisdicional estejam principalmente ligadas ao exame da legalidade deste último, podem constituir indícios que podem revelar que esse tratamento decorre do exercício, por esse órgão jurisdicional, da sua «função jurisdicional».". Sobre este aresto, contamos com o comentário concordante de Wengorovius (2023, 466-471).

Conselho)[9]-[10]; ao passo que, no Brasil, esse desiderato ainda está por concretizar, decorridos quase seis anos desde a publicação da *LGPD*[11].

Da mesma maneira, os dois Ordenamentos postulam a garantia da segurança no tratamento dos dados, como um dos seus "Princípios" (o da «integridade e confidencialidade» do Artigo 5.º n.º 1 f) do *RGPD*, cujo conteúdo é replicado no Artigo 4.º n.º 2 n.º 1 f) da Lei n.º 59/2019, transpondo o Artigo 4.º n.º 1 f) da Diretiva, o qual corresponde ao da "segurança" do Artigo 6º VII da *LGPD*). Aliás, as redações e os conteúdos de ambos enunciados são muito semelhantes:

> Os dados pessoais são: […] 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 ", no *RGPD*; ou com a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, na *LGPD*.

[9] Como ocorre com o *RGPD*, o *Considerando* (80) da Diretiva *de qua* esclarece que, "Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta.". A este propósito, são de atender as considerações de de Martins (2022, 117-118) e de Wengorovius (2023, 465-466).

[10] A propósito da distinção e da articulação entre ambos regimes, sobretudo quanto à diferença entre os Direitos Fundamentais protegidos e aos interesses sociais em causa, CASTRO (2020, 15-16) e MASSENO (2022, 2-8), enquanto Oliveira (2019, 160-163) entende não se justificar a duplicação de regimes.

[11] Sobre a comummente chamada *LGPD Penal*, apenas deixo notícia de que, em 2020, uma Comissão de Juristas sobre Segurança Pública, nomeada pelo Presidente da Câmara dos Deputados, Rodrigo Maia, presidida pelo Ministro do Superior Tribunal de Justiça Nefi Cordeiro e tendo como Relatora Laura Schertel Mendes, elaborou um "Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal". Depois, sem se basear no "Anteprojeto", a 7 de junho de 2022, o deputado Coronel Armando (PL-SC) apresentou o Projeto de Lei nº 1.515/22, ementado como "Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais", com o então Presidente da Câmara, Arthur Lira, a determinar a criação de Comissão Especial para analisar a matéria, a 20 do mesmo mês. Não tendo ocorrido mais desenvolvimentos, desde essa data. A este propósito, Azevedo *et al*. (2022) e Fernandes & Resende (2023, 485-489).

No entanto, os pontos de partida são muito distintos. Assim, em Portugal vigorava, e vigora ainda, a Lei n.º 34/2009, de 14 de julho, que *estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial*, especificando a, ao tempo vigente, Lei n.º 67/98, de 26 de outubro, a *Lei da Proteção Dados Pessoais*, a qual transpusera para a Ordem Jurídica portuguesa a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, *relativa à proteção das pessoas singulares* [naturais] *no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados*, embora esta não pretendesse ter um alcance tão amplo, deixando os tratamentos feitos pelos Poderes Públicos de fora do seu âmbito[12].

Por seu turno e na falta de uma Lei sobre proteção de dados pessoais, no Brasil estas questões tinham sido reguladas pela Resolução n.º 215, de 16 de dezembro de 2015, do CNJ – Conselho Nacional de Justiça, a qual *dispõe, no âmbito do Poder Judiciário, sobre o acesso à informação e a aplicação da Lei 12.527, de 18 de novembro de 2011*, explicitamente apenas para as atividades de natureza administrativa do mesmo[13].

[12] Ao delimitar negativamente o seu âmbito de aplicação, o Artigo 3.º n.º 2 dispunha que "A presente directiva não se aplica ao tratamento de dados pessoais: - efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal.". Até porque o objetivo estava focado nos tratamentos de dados para fins empresariais, enquanto pressuposto para o funcionamento do Mercado Interno da União Europeia, como mostram os seus *Considerandos* iniciais: "(3) Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado *[que institui a Comunidade Europeia*, o *Tratado de Roma*, de 25 de março de 1957, na redação resultante do *Tratado de Maastricht*, de 7 de fevereiro de 1992], é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas; [e] (4) Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados;", o que era também confirmado pela indicação do Artigo 100.º-A como base, o qual aplicava-se à "[…] aproximação das disposições legislativas, regulamentares e administrativas dos Estados-membros, que têm por objectivo o estabelecimento e o funcionamento do mercado interno." (n.º 1 *in fine*).

[13] O que suscita a questão relativa ao alcance do Poder Regulamentar do CNJ, como nos dão conta os estudos de Pizzol (2019, 312-323) e de Miranda (2020, 76949-76958), sem esquecer os apontamentos críticos de Streck, Sarlet & Clève (2006).

Entretanto, ambas as disciplinas passaram, e ainda passam, por processos de transição. Em Portugal e em 2019, a Assembleia da República aprovou o Decreto n.º 333/XIII, alterando a Lei n.º 34/2009, de modo a adequá-la ao *RGPD*[14]. Porém, o mesmo foi "devolvido sem promulgação", ou seja, foi vetado politicamente, pelo Presidente da República, no final de julho, ainda que por razões não relacionadas com a segurança no tratamento de tais dados[15]. Contudo, não havendo o mesmo sido reapreciado pelo Parlamento até ao final da Legislatura, a iniciativa caducou. Desde esse momento, não foi retomado o processo legislativo, nem há notícias de qualquer movimentação dos Governos os dos Deputados com esse objetivo[16].

No Brasil, porque a *LGPD* apenas entraria em vigor em agosto de 2020[17], o CNJ, pela Portaria n.º 63, de 26 de abril de 2019, começou por criar um Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais.

2 A SEGURANÇA NA PROTEÇÃO DE DADOS NOS SISTEMAS JUDICIAIS

Em termos gerais, como referimos, em Portugal continua vigente a Lei n.º 34/2009, sempre e quando não contrarie o disposto no *RGPD*. Ao estar explicito, neste diploma legislativo, como já verificámos, que,

[14] A múltipla documentação correspondente a este processo legislativo está disponível, em acesso aberto, https://bit.ly/3USuPs2.

[15] Sobre a atual situação das Fontes em Portugal, são de atender as considerações sintéticas de CASTRO (2020, 13-15), de Martins (2022, 117-118) e de Wengorovius (2023, 448-451 e 471-474).

[16] Sendo certo que o CSM, na Sessão Plenária de 4 de outubro de 2022, criou um "grupo de trabalho para elaboração de projeto de alteração do regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial", o qual ainda não foi divulgado e apenas poderá ser tido como um contributo suscetível de espoletar o debate a este respeito; tal como ocorreu com a "Agenda da Reforma da Justiça - Uma reflexão aberta e alargada do judiciário", de março de elaborada por um "Think Tank" constituído pela Associação Sindical dos Juízes Portugueses, com a coordenação do Juiz Conselheiro Nuno Coelho, com recurso a especialistas externos, e em cujo subgrupo de trabalho "Justiça Digital e Inteligência Artificial nos Tribunais", coordenado pelo Juiz de Direito José Joaquim de Oliveira Martins, tivemos o gosto e a honra participar.

[17] Por força do seu Artigo.º 65.º II. Embora, essa vigência haja ocorrido no dia 18 de setembro desse ano, após a devido à aprovação pelo Senado da MP 959/2020 (PLV 34/2020) e ao declarado regimentalmente pelo seu Presidente.

> 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 [constituído ou a constituir] quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. (*Considerando* (20)).

O que coloca problemas muito complexos e controversos, em especial quanto à garantia da segurança no tratamento dos dados, sobretudo no respeitante à determinação do(s) responsável(eis) pelo tratamento dos dados [controlador(es)], isto é,

> […] a pessoa singular ou coletiva [natural ou jurídica], a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro [como é o caso], o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro. (Art.º 4.º 7) do *RGPD*)[18]

De uma tal determinação decorrem a(s) correspondente(s) responsabilidade(s) proativa (*accountability*), civil e contraordenacional [administrativa], designadamente no que importa à segurança dos dados[19].

Ora, ainda vigorando a Lei n.º 34/2009, essa responsabilidade cabe ao CSM – Conselho Superior da Magistratura, para todos os tribunais comuns, assim como ao CSTAF – Conselho Superior dos Tribunais Administrativos e Fiscais e à Procuradoria-Geral da República para todo o Ministério Público, sendo cada uma a "entidade responsável pela gestão dos dados" (Artigo 24.º n.ºs 1, 2 e 3, especificamente). Cabendo-lhes, quanto ao nosso objeto, "b) Garantir o cumprimento de medidas necessárias à segurança da informação e dos tratamentos de dados; [e] c) Assegurar o cumprimento das regras de acesso e de segurança referentes ao arquivo electrónico." (Artigo 24.º n.º 2).

[18] No mesmo sentido, com considerações adicionais, argumenta Wengorovius (2023, 458-459).

[19] Respectivamente, Artigos 5.º n.º 2, 24.º, 25.º, 32.º a 34.º, 82.º e 83.º do *RGPD*, bem como Artigos 47.º a 56.º da Lei n.º 34/2009, incluindo a responsabilidade penal, como é facultado pelo Artigo 84.º *RGPD*, a mesma não abrange a matéria da segurança dos dados. Para um enquadramento articulado da *accountability* com as demais responsabilidades, são sobretudo de atender as considerações de Barbosa (2018), além das de Masseno, Martins & Faleiros Jr. (2020).

O que deverá ser articulado com o *Código de Processo Civil* (Artigo 132.º n.º 4, na redação introduzida pelo Decreto-Lei n.º 97/2019, de 26 de julho, o qual é também aplicável nos Tribunais Administrativos e aos Tribunais Tributários, *ex vi*, Artigos 1.º e 2.º c) e e) dos respetivos *Códigos de Processo*)[20], em cujos termos,

> A tramitação eletrónica dos processos [a regra, sendo excecional e transitória a práticas de atos em papel] deve garantir a respetiva integralidade, autenticidade e inviolabilidade, bem como o respeito pelo segredo de justiça e pelos regimes de proteção e tratamento de dados pessoais e, em especial, o relativo ao tratamento de dados referentes ao sistema judicial.

Do mesmo modo, no respeitante ao regime material, temos que o disposto no *RGPD* quanto à "Segurança do tratamento" (Artigo 32.º)[21] deve ser integrado com as "Medidas de segurança" previstas na Lei n.º 34/2009 (Artigo 42.º)[22], as quais são

[20] Aprovados pela Lei n.º 15/2002, de 22 de fevereiro, e pelo Decreto-Lei n.º 433/99, de 26 de outubro, A propósito destas questões, são muito pertinentes as reflexões breves, assim como as referências bibliográficas, de Teixeira (2019, 4-8) e de Martins (2022, 117-118).

[21] "1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. 2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.". Sobre a disciplina da segurança no tratamento de dados pessoais no Sector Público, remeto para o meu estudo técnico detalhado (Masseno 2024), tendo também interesse a perspectiva, aliás não coincidente, de Alves (2021).

[22] Assim, "1 - Tendo em vista a segurança dos dados, são objecto de controlo: a) A entrada nas instalações utilizadas para o armazenamento de dados, a fim de impedir o acesso às mesmas por pessoa não autorizada; b) Os suportes utilizados, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada; c) A consulta dos dados, a fim de assegurar que é efectuada apenas por pessoas autorizadas e que se processa nos termos da presente lei; d) A inserção, a alteração, a eliminação e a realização de qualquer outra operação sobre os dados, de forma a verificar-se que operações foram realizadas, quando e por quem, e para impedir a introdução, assim como qualquer tomada de conhecimento, alteração ou eliminação não autorizadas dos mesmos; e) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de tratamento de dados; f) A transmissão de dados, para garantir que o envio destes, através de instalações de transmissão de dados, se limite às entidades autorizadas; g) A transmissão de dados e o transporte de suportes de dados, para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada; h) O acesso aos dados a partir de fora das instalações físicas onde

plenamente compatíveis e até o adaptam às finalidades próprias da função jurisdicional, embora devam ser lidas na pespectiva da neutralidade tecnológica intertemporal, em atenção ao período já transcorrido[23].

Neste âmbito, uma questão crucial prende-se com a obrigatoriedade de realização de uma AIPD – avaliação [relatório] de impacto sobre a proteção de dados,

> Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (Artigo 35.º n.º 1 do *RGPD*)

Uma exigência que resulta de uma mudança muito significativa relativamente ao modelo anterior de proteção de dados pessoais, na União Europeia e em Portugal, tendo também importantes projeções quanto à segurança dos dados pessoais tratados na atividade jurisdicional. Especificamente e pelo menos, uma AIPD deverá ser feita sempre que estiverem em causa de categorias especiais de dados [dados sensíveis][24] ou for intentada a introdução de tecnologias novas, como ocorre com os sistemas dotados de Inteligência Artificial no apoio à judicatura[25].

---

se encontram armazenados, de modo a garantir a sua segurança. 2 - O controlo da consulta dos dados e das operações realizadas sobre os dados, previsto nas alíneas c) e d) do número anterior, é feito através do registo electrónico referido no n.º 3 do artigo 29.º, devendo esse registo ser periodicamente comunicado aos responsáveis pela gestão dos dados, para fins de auditoria aos acessos. 3 - Para as finalidades referidas no número anterior é também mantido um registo das permissões de acesso atribuídas a cada utilizador, devendo os dados constantes de tal registo ser eliminados 10 anos após a data do seu registo. 4 - Tendo em vista a segurança e a preservação da informação, são feitas, periodicamente, cópias de segurança da mesma."

[23] Aliás, a este propósito, importa atender também à "Atualização dos Critérios de seleção e pseudonimização das decisões Judiciais", relativamente aos aprovados a 23 de março de 2021, aprovada por deliberação do Plenário do CSM, de 11 de abril de 2023; estando disponível o Parecer cujo conteúdo foi adotado, https://bit.ly/3V9KvIG.

[24] Ou seja, de "dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como […] de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." (Artigo 9.º n.º 1 do *RGPD*).

[25] Para uma exposição dos pressupostos, conteúdo e procedimentos relativos à realização de uma AIPD, assim como do correspondente enquadramento regulatório, em termos gerais, basta indicar o texto de Lopes (2022, 114-136).

Em qualquer caso, atendendo à exclusão das "operações de tratamento efectuadas por tribunais que atuem no exercício da sua função jurisdicional" do âmbito das atribuições das autoridades de controlo, *in casu* a Comissão Nacional de Proteção de Dados (Artigo 55.º do *RGPD*), estará fora de causa a realização de uma consulta prévia[26], pelo menos até existir uma base legal própria que o determine, como já ocorre na Justiça Penal.

No entanto, se aprofundarmos a análise, tornam-se evidentes as consequências de uma decisão de base no que se refere ao funcionamento do Sistema Judicial / Judiciário português, a do controle dos meios materiais afetos ao Órgão de Soberania tribunais por parte do Governo, através do Ministério da Justiça. O que coloca em risco o próprio *Princípio da Separação de Poderes* e a inerente "Independência" da Justiça (Artigos 2.º, 111.º n.º 1, 288.º j) e 203.º da *Constituição da República Portuguesa*). Sem esquecer que a "defesa da independência judiciária e dos processos judiciais" é até suscetível de legitimar a limitação, pelo "direito da União ou dos Estados-Membros", de direitos dos titulares dos dados e dos responsáveis pelo tratamento ou dos subcontratantes [controladores ou processadores], "[…] desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática […]" (Artigo 23.º n.º 1 f)[27].

Retomando a questão inicial, como foi repetidamente evidenciado aquando do processo legislativo conducente à aprovação parlamentar do Decreto n.º 333/XIII, designadamente pelo CSM, os meios informáticos afetos ao Sistema Judicial / Judiciário continuam sob a dependência do Ministério da Justiça, especificamente do IGFEJ – Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., e não dos Tribunais ou do binómio CSM / CSTAF, por força da respetiva *Lei Orgânica* (Decreto-Lei n.º 123/2011, de 29 de dezembro, Artigos 2.º n.º 1 i) e 14.º n.º 2 j) e l)).

[26] "[…] antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco" (Artigo 36.º n.º 1 do *RGPD*).

[27] A propósito do sentido e do alcance destas limitações, Martins (2022, 120-121) e Wengorovius (2023, 454-56).

O que é confirmado pela própria Lei n.º 34/2009, quanto às infraestruturas físicas, incluindo as linhas de transmissão e o arquivo eletrónico, ao estar explicito que o IGFEJ

> […] assegura, através do departamento com competência para a matéria em causa, sem prejuízo dos regimes do segredo de justiça e do segredo de Estado, o desenvolvimento das aplicações informáticas necessárias à tramitação dos processos e à gestão do sistema jurisdicional, incluindo a necessária análise, implementação e suporte (Artigos 43.º n.º 1 e 26.º n.º 1).

Por isso mesmo e em atenção ao critério presente no *RGPD* para identificar o «Responsável pelo tratamento», *i.e.*, além das "finalidades", é quem determina "os meios" e aplica as "medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento" (Artigos 4.º 7), 24.º n.º 1, 25.º e 32.º n.º 1), temos que, no respeitante à segurança dos dados, este apenas poderá ser o Ministério da Justiça, com a inerente assunção de responsabilidades, incluindo a intervenção específica do respectivo EPD – Encarregado da Proteção de Dados. O que ocorrerá em termos dissociados das demais funções dos responsáveis pelo tratamento, sejam estes o CSM ou o CSTAF[28].

Entretanto, face ao impasse legislativo, foi intentada uma "via criativa", sobretudo destinada a legitimar a anterior situação *de facto*. Sendo certo que a via mais consentânea com a *Constituição* e o *RGPD* teria sido a da transferência das competências e dos meio materiais relativos aos sistemas e às redes informáticas da Justiça para o CSM e para o CSTAF.

Assim, no dia 5 de dezembro de 2023, foi assinado um "Acordo de Tratamento de Dados Pessoais", tendo por objeto tanto a Justiça Cível quanto a Criminal, pelos Presidentes do CSM e do IGFEJ, aliás coadjuvados pelas correspondentes EPDs. De fora ficou a Justiça Administrativa e Fiscal, continuando nesta a desagregação entre a determinação das finalidades e dos meios de cada tratamento dos dados, com a inerente diferenciação das responsabilidades em matéria de segurança.

[28] Quanto a esta dissociação funcional, é de atender a posição crítica de Martins (2022, 120-121), aliás, em expressa consonância com a versão inicial deste estudo.

Conforme ao Acordo[29], o IGFEJ passou a assumir formalmente a posição de "subcontratante" [processador], tratando os dados por conta do CSM, enquanto "responsável pelo tratamento" [controlador] (Artigo 4.º 7) e 8) e 28.º n.ºs 1 e 3 do *RGPD*). Em especial, o primeiro assumiu obrigações quanto à aplicação de medidas técnicas e organizativas destinadas a efetivar a segurança dos dados objeto de tratamento, assim como no respeitante à notificação das violações de dados pessoais ao CSM, assistindo ainda este na comunicação de tais violações aos titulares dos dados (Cláusulas Sexta, Décima Primeira e Décima Segunda e Décima Terceira).

Por sua vez, no Brasil, a Lei nº 11.419, de 19 de dezembro de 2006, que *dispõe sobre a informatização do processo judicial*, explicita que (Artigo 12, *caput* e § 1º):

> A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.
> § 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares.

O que pode facilmente ser enquadrado na *LGPD*, em articulação com o, referido, Princípio da "segurança" (Artigo 6º VII) e a disciplina que o densifica (Artigos 46 a 49)[30]. Porém, os poderes aí conferidos à ANPD – Autoridade Nacional de Proteção de Dados, nomeadamente para a definição de "padrões técnicos mínimos" (Artigos 55-J XIII e 46 § 1º), terão de considerar-se como prejudicados pelas competências regulamentares do CNJ, devido ao disposto na *Constituição Federal* com o objetivo de garantir a autonomia do Poder Judiciário (Artigos 99 e 103-B § 4º I).

No mesmo sentido, a Lei nº 11.419 determina que "Os órgãos do Poder Judiciário regulamentarão esta Lei, no que couber, no âmbito de suas respectivas competências"

[29] Embora não tenha sido publicado, o Acordo *de quo* pode ser lido no seguinte endereço, https://bit.ly/3KgdnsC.

[30] Quanto à disciplina disposta pela *LGPD* para a segurança no tratamento dos dados pessoais, são de atender as considerações comparatísticas de Masseno, Martins & Faleiros Jr. (2020) e também o estudo de ROSAS (2022), além do artigo sobre a matéria *de qua* do Ministro Ricardo Cueva (2021), referido *supra*.

(Art. 18), também em função do previsto na Lei Complementar nº 35, de 14 de março de 1979, a *Lei Orgânica da Magistratura Nacional*.

Embora, um tal entendimento não afaste uma articulação entre a ANPD e o CNJ, até por maioria de razão relativamente ao disposto na *LGPD* a propósito das "autoridades reguladoras públicas" ou dos "outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais" (Artigos 55-J XXIII e 55-K parágrafo único, embora não podendo ser neste domínio a ANPD "o órgão central de interpretação desta lei e do estabelecimento de normas e diretrizes para a sua implementação.").

Aliás, o CNJ, através da sua Resolução nº 185, de 18 de dezembro de 2013, que *Institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento*, já estabelecera regras sobre a autenticação segura no acesso aos sistemas e a segurança destes (Artigos 4º, 6º, 27 e 28, nomeadamente).

Sempre por iniciativa do CNJ, está em andamento a aplicação da Resolução nº 363, de 12 de janeiro de 2021, que *Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais*[31].

Efetivamente, esta Resolução vai além do previsto na Recomendação nº 73, de 20 de agosto de 2020, que *Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD*, a qual indicara aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados, em especial[32],

> I - elaborar plano de ação que contemple, no mínimo, os seguintes tópicos: [d)] retenção de dados e cópia de segurança" [e, f) [um] plano de respostas a incidentes de segurança com dados pessoais" [assim como] "III - elaborar ou adequar, bem com publicar nos respectivos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários […] b) os registros de tratamentos de

[31] A propósito da qual são de atender as considerações breves de Scodro (2021, 88-90) e de Maiolino (2023, 453-454).

[32] Sobre o seu conteúdo e contexto da sua adoção pelo CNJ, contamos com os apontamentos de Santos (2021, 102-106) e de Scodro (2021, 87-88).

> dados pessoais contendo, entre outras, informações sobre: [as] 8) medidas de segurança adotadas; [e] 9) a política de segurança da informação. (Artigo 1º)

Neste sentido e especificamente, a Resolução prevê que os Tribunais venham a,

> XI – implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, nos termos do art. 46 e seguintes da LGPD, por meio: a) da elaboração de política de segurança da informação que contenha plano de resposta a incidentes (art. 48 da LGPD), bem como a previsão de adoção de mecanismos de segurança desde a concepção de novos produtos ou serviços (art. 46, § 1º); b) da avaliação dos sistemas e dos bancos de dados, em que houver tratamento de dados pessoais, submetendo tais resultados à apreciação do CGPD para as devidas deliberações; c) da avaliação da segurança de integrações de sistemas; d) da análise da segurança das hipóteses de compartilhamento de dados pessoais com terceiros;", assim como a "XII – elaborar e manter os registros de tratamentos de dados pessoais contendo informações sobre: [o] g) prazo de conservação e medidas de segurança adotadas, nos termos do art. 37 da LGPD; (Artigo 1º)

Além de serem os Tribunais, e não o CNJ, a assumirem a qualidade de controladores, isto é, "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Artigos 5º VI da LGPD)[33], com o apoio de um Comitê Gestor de Proteção de Dados Pessoais, ao qual são assignadas funções explícitas em matéria de segurança (Artigo 1º I e XI b)), cabendo-lhes ainda "designar o encarregado pelo tratamento de dados pessoais" (Artigo 1º II)[34].

Cabe acrescentar que o Supremo Tribunal Federal seguiu uma via paralela, com a aprovação da Resolução STF nº 724, de 2 de março de 2021, que *Institui o Comitê Executivo de Proteção de Dados para identificar e implementar as medidas necessárias à adequação do Supremo Tribunal Federal às exigências da Lei n. 13.709, de 14 de agosto de 2019 (LGPD)*. A mesma foi logo seguida da Resolução STF nº 759, de 17 de

[33] Com as inerentes responsabilidades proativa e civil, ao ser problemática a aplicação de sanções administrativas pela ANPD aos tribunais (Artigos 37, 42 a 44, 50 e 52 a 54 da *LGPD*). A este propósito, além das considerações comparatísticas de Masseno, Martins & Faleiros Jr. (2020), são de atender os estudos de Capanema (2020) e de Gondim (2021), além das reflexões breves de Moraes (2019) e de Rosas (2022).

[34] A propósito da implementação da Resolução *de qua*, são interessantes os estudos, também empíricos, de Rocha (2021), de Scodro (2021, 90-99) e de Maiolino (2023, 457-460), além do metodológico de Keppen (2024).

dezembro de 2021, a qual *Institui a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do Supremo Tribunal Federal*, em cujos termos,

> O STF dispõe de Política de Segurança da Informação, além de CCSI [Comitê Corporativo de Segurança da Informação], que especifica e determina a adoção de medidas técnicas e administrativas de segurança para a proteção de dados pessoais contra acessos não autorizados, situações acidentais ou incidentes culposos ou dolosos de destruição, perda, adulteração, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito." (Artigo 19), "[…] adotará boas práticas e governança em segurança da informação visando orientar comportamentos adequados e mitigar os riscos de comprometimento dos dados pessoais tratados em suas atividades jurisdicional e administrativa." (Artigo 20) e "O Encarregado e o CEPD [Comitê Executivo de Proteção de Dados] deverão manter a Alta Administração do STF informada a respeito de aspectos e de fatos significativos para a integridade dos sistemas do Tribunal. Parágrafo único. Os membros do CEPD e o Encarregado deverão informar e ser informados pelo CCSI sobre os incidentes envolvendo dados pessoais." (Artigo 21); sendo que "Encarregado contará com apoio efetivo do […] (CEPD) com a finalidade de estabelecer regras de segurança, de boas práticas, de governança, e de procedimentos envolvendo a proteção de dados pessoais para o adequado desempenho de suas funções. (Artigo 16), *i.e.*, são-lhe atribuídas funções significativamente mais amplas que as previstas na *LGPD* (Artigo 5º VIII e 41 § 2º).

Ainda a este propósito, cumpre dar conta que, mesmo perante a falta de referências explícitas nas Resoluções do CNJ e do STF, o Poder Judiciário brasileiro não ficou isento do dever de realizar um "relatório de impacto à proteção de dados pessoais: [*i.e.*, a] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco." (Artigo 5º XVII da *LGPD*), embora esteja fora de causa que tal ocorra por determinação da ANPD (Artigo 38 da mesma lei), em razão do estatuto constitucional do Poder Judiciário[35].

[35] Quanto à disciplina predisposta em geral pela *LGPD*, tendo por referência a do *RGPD*, é de referir o texto de Gomes (2019), assim como os apontamentos sobre a sua aplicabilidade aos tribunais de Cardoso (2022, 576-579), antecedidos de uma explanação do regime geral.

3 A SEGURANÇA NA PROTEÇÃO DE DADOS NA JUSTIÇA CRIMINAL

No respeitante a Portugal, também por imposição do disposto no *Tratado sobre o Funcionamento da União Europeia* (Artigo 83.º n.º 1), decorre que as "regras mínimas" relativas a "infrações penais" apenas podem resultar de "diretivas adotadas de acordo com o processo legislativo ordinário", excluindo os regulamentos.

O que também facilitou técnica, e até politicamente, uma compressão dos direitos dos titulares dos dados na Diretiva (UE) 2016/680 e na Lei n.º 59/2019, em contraste com o previsto no *RGPD* e, consequentemente, na Lei n.º 58/2019[36].

Por essa razão, embora, tal como no *RGPD* e por Princípio, os dados devem ser tratados "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 acidentais, recorrendo a medidas técnicas ou organizativas adequadas." (Artigos 4.º n.º 2 f) da Lei), é patente um maior rigor quanto aos "regist[r]os das atividades de tratamento", pois este, também,

> Deve conter: […] i) Uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 31.º (Artigo 26.º) e também quanto ao registo cronológico das atividades de tratamento, o qual deve […] permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais, servindo […] exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo, exercício do poder disciplinar e garantia da integridade e segurança dos dados pessoais, bem como no âmbito e para efeitos de processo penal. (Artigo 27.º n.ºs 2 e 3).

Por seu turno, no tocante à "segurança do tratamento", em sentido próprio, enuncia que,

> O responsável pelo tratamento e o subcontratante [o controlador e o processador] adotam as medidas técnicas e organizativas apropriadas a fim de assegurarem um nível de segurança adequado ao risco[37], em particular no que

[36] Sobre estas questões, permito remeter para o meu estudo recente (Masseno, 2022, 5-8), além de para os apontamentos de Castro (2020, 15).

[37] Como explicitam o *Considerandos* (60) e (61) da Diretiva, "A fim de preservar a segurança e evitar o tratamento em violação da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e deverá aplicar medidas que os atenuem, como, por exemplo, a cifragem. Estas medidas deverão assegurar um nível de segurança adequado, nomeadamente no que

> diz respeito ao tratamento das categorias especiais de dados pessoais referidos no artigo 6.º[38]

Em especial, o foco é posto no controle do acesso aos sistemas informáticos em casos de tratamento automatizado de dados, inclusive com um alto grau de detalhe[39] (Artigo 31.º n.ºs 1 e 2, respetivamente)[40]. A este propósito, há ainda a referir que a "omissão" pelo Legislador português quanto ao tratamento dever ocorrer "tendo em conta

respeita à confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função do risco e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados, de dados pessoais transmitidos, conservados ou tratados de outro modo, riscos esses que podem conduzir, em particular, a danos físicos, materiais ou morais. O responsável pelo tratamento e o subcontratante deverão assegurar que o tratamento de dados pessoais não seja efetuado por pessoas não autorizadas.", pois "Se não forem tomadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, tais como a perda de controlo dos dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social importante para as pessoas singulares em causa".

[38] Em termos análogos aos do Artigo 9.º n.º 1 do *RGPD*, o preceito refere-se a "dados sensíveis" como os "[…] dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como dos dados genéticos, dos dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dos dados relativos à saúde ou dos dados relativos à vida sexual ou à orientação sexual." (Artigo 6.º n.º 1).

[39] Assim, "[…], o responsável pelo tratamento ou o subcontratante [o controlador ou o processador], tendo em conta a avaliação dos riscos, devem aplicar medidas que: a) Impeçam o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento (controlo de acesso ao equipamento); b) Impeçam que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização (controlo dos suportes de dados); c) Impeçam a introdução não autorizada de dados pessoais, bem como qualquer operação não autorizada relativamente a dados pessoais conservados (controlo da conservação); d) Impeçam que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados (controlo dos utilizadores); e) Assegurem que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso (controlo do acesso aos dados); f) Assegurem que possa ser verificado e determinado a que organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados (controlo da comunicação); g) Assegurem que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem foram introduzidos (controlo da introdução); h) Impeçam que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização (controlo do transporte); i) Assegurem que os sistemas utilizados possam ser restaurados em caso de interrupção (recuperação); j) Assegurem que as funções do sistema funcionam, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por funcionamento defeituoso do sistema (integridade)."

[40] Com especial ênfase nos riscos acrescidos destes tratamentos e nos meios predispostos para os mitigar, remeto para o meu estudo (Masseno 2022, 5-8).

as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos de probabilidade e gravidade variáveis que este tratamento representa para os direitos e liberdades das pessoas singulares [naturais], apliquem medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco" (Artigo 31.º da Lei, em contrate com o 29.º n.º 1 da Diretiva), não poderá ter consequências atendendo ao "Princípio da interpretação conforme", enunciado pelo TJUE desde há quatro décadas[41].

Mais próximos do previsto no *RGPD* estão os enunciados a propósito da "notificação de uma violação de dados pessoais à autoridade de controlo" e da "comunicação de uma violação de dados pessoais ao titular dos dados" (Artigos 30.º e 31.º da Diretiva e 32.º e 33.º da Lei)[42], com a CNPD a assumir as correspondentes funções, em termos análogos ao previsto no *RGPD*. Para o efeito, a mesma conta com a incorporação de um magistrado judicial designado pelo CSM, o qual se ocupará do controle do acesso aos dados e aos registos cronológicos das operações de tratamento (Artigo 43.º).

---

[41] Desde os Acórdãos de 10 de abril de 1984, Processo 14/83, Sabine von *Colson e* Elisabeth *Kamann* contra Land Nordrhein-Westfalende, e, mais ainda, 13 de novembro de 1990, Processo C-106/89, *Marleasing* SA contra La Comercial Internacional de Alimentacion SA.

[42] Como sublinham o *Considerando* (60) *in fine* e (61) da Diretiva, "[…] logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá comunicá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar a comunicação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem mais demora injustificada. [e] Caso a violação de dados pessoais seja suscetível de criar um elevado risco para os direitos e liberdades das pessoas singulares, estas deverão ser informadas sem demora injustificada, a fim de permitir que tomem as precauções necessárias. Da comunicação deverá constar a natureza da violação de dados pessoais e recomendações destinadas à pessoa singular em causa para atenuar potenciais efeitos adversos. A comunicação aos titulares dos dados deverá ser feita o mais rapidamente possível, em estreita cooperação com a autoridade de controlo, e de acordo com as orientações fornecidas por esta ou por outras autoridades competentes. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá que se envie uma comunicação rápida aos titulares dos dados, enquanto a necessidade de aplicar medidas adequadas contra violações de dados recorrentes ou similares poderá justificar um prazo maior para a comunicação. Se não for possível, através do atraso ou da restrição da comunicação à pessoa singular em causa de uma violação de dados pessoais, evitar criar entraves a inquéritos, investigações ou procedimentos oficiais ou legais, evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública, preservar a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros, essa comunicação poderá, em circunstâncias excecionais, ser omitida.".

Neste âmbito, cabe recordar que a aplicação das correspondentes medidas técnicas e organizacionais e a efetivação das obrigações de notificação e de comunicação é feita pelo CSM, enquanto responsável pelo tratamento[43], assistido para tanto pelo IGFEJ, por força do Acordo antes referido.

Adicionalmente, cumpre ainda dar conta da obrigatoriedade de realizar uma "avaliação de impacto", "No caso de um certo tipo de tratamento ser suscetível de representar um elevado risco para os direitos, liberdades e garantias das pessoas" (Artigo 29.º n.º 1 da Lei), nomeadamente por razões de segurança, a qual pode também conduzir a uma consulta prévia da CNPD,

> […] antes de proceder ao tratamento de dados pessoais a integrar em ficheiro a criar nos casos em que: a) A avaliação de impacto prevista no artigo anterior indique que o tratamento resultaria num elevado risco, na ausência de medidas adequadas para atenuar esse risco; ou b) O tipo de tratamento envolva um elevado risco para os direitos, liberdades e garantias dos titulares dos dados, designadamente se utilizar novas tecnologias. (Art.º 30.º).

Quanto ao Brasil e enquanto não estiver em vigor "a legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal" (Artigo 4º IV § 1º da *LGPD*), no mínimo, deverão ser aplicadas as "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" constantes das citadas Resoluções do CNJ, no quadro da *LGPD*, até porque essa futura legislação deverá observar "os princípios gerais de proteção e os direitos do titular previstos nesta lei". Embora em articulação com os *Princípios do*

[43] Nos termos do disposto no Artigo 3.º n.º 1 j) da Lei n.º 59/2019, «Responsável pelo tratamento» é a "entidade competente que […] no caso em que estes ["as finalidades e os meios de tratamento dos dados pessoais"] são determinados por lei, a autoridade nela indicada", o que nos leva de volta ao previsto no Artigo 24.º n.º 1 da Lei n.º 34/2009, também no respeitante à responsabilização civil, contraordenacional [Administrativa] e inclusive penal, Artigos 52.º a 66.º da Lei 59/2019, sendo a previsão da última facultada pelo Artigo 57.º da Diretiva (UE) 2016/680, embora nenhuma das previsões típicas consista no incumprimento de medidas de segurança por parte do responsável, ou responsáveis, pelos tratamentos de dados ou pelos subcontratantes [controladores ou processadores].

Processo Penal, o que exige um esforço suplementar por parte do Poder Judiciário em cada tratamento dos dados pessoais[44].

Adicionalmente, deve ser explicitado que a previsão segundo a qual a ANPD "[…] emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais" (Artigo 4º IV § 3º da *LGPD*), não deve considerar-se aplicável ao Poder Judiciário, atendendo ao seu estatuto constitucional. Mas, em todo caso, o dever de realizar relatórios de impacto também é aplicável nestes tratamentos de dados, até por maioria de razão, atendendo à sua particular incidência em outros Direitos Fundamentais, incluindo o direito à liberdade.

REFERÊNCIAS

ALVES, Diogo Lopes. "O papel fundamental da Cibersegurança na Proteção de Dados Pessoais". *Anuário da Proteção de Dados – 2020* (2021), p.121-154. Disponível em: https://bit.ly/4bnOIhH. Acesso: 10 maio. 2024.

AZEVEDO, Cynthia Picolo Gonzaga de *et al*. *Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022*. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), (2022). Disponível em: https://bit.ly/3U0OuU0. Acesso: 10 maio. 2024.

BAIÃO, Renata Barros Souto Maior & TEIVE, Marcelo Muller. "O artigo 23 da LGPD como base legal autônoma para o tratamento de dados pessoais pelo poder judiciário". PALHARES, Felipe (coord.). *Temas Atuais de Proteção de Dados*. 2.ª ed. rev. e atual. São Paulo: Thomson Reuters / Revista dos Tribunais (2022), p. 287-302. Disponível em: https://bit.ly/4bhtm5m. Acesso: 10 maio. 2024.

BARBOSA, Mafalda Miranda. "*Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil". Revista de Direito Comercial, n. 2, p. 423-493 (2018). Disponível em: https://acesse.dev/stf4n. Acesso: 10 maio. 2024.

[44] Ainda que em termos necessariamente prospectivos, sobretudo atendendo aos riscos decorrentes de tratamentos automatizados de dados para estes fins, são muito pertinentes as considerações de FERNANDES & RESENDE (2023, 485-495).

CAPANEMA, Walter Aranha. "A responsabilidade civil na Lei Geral de Proteção de Dados". *Cadernos Jurídicos* – Escola Paulista da Magistratura, (2020), a. 21 n. 53, p. 63-170. Disponível em: https://l1nq.com/OuD4C. Acesso: 10 maio. 2024.

CARDOSO, Oscar Valente. "Relatório de Impacto à Proteção de Dados Pessoais nos Tribunais". LIMA, Ana Paula Canto de & ROSAS, Eduarda Chacon (coord.). *LGPD 2022. Debates e temas relevantes*. Recife: Editora Império (2022), p. 579-598. Disponível em: https://l1nq.com/wqIJd. Acesso: 10 maio. 2024.

CASTRO, Raquel A. Brízida. "Proteção de Dados e a Diretiva EU 2016/680: o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais". *Cibercriminalidade e Prova Digital*. Lisboa: Centro de Estudos Judiciários (2018, atualizado em 2020), p. 9-15. Disponível em: https://acesse.dev/Uv77X. Acesso: 10 maio. 2024.

DONEDA, Danilo. *Diretrizes para Atores Judiciais sobre Privacidade e Proteção de Dados*. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura (2022). Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381298_por. Acesso: 10 maio. 2024.

FERNANDES, Fernando Andrade & RESENDE, Ana Paula Bougleux Andrade. "Regulamentação do tratamento automatizado de dados pessoais em matéria penal". *Suprema - Revista de Estudos Constitucionais*, v. 3 n. 1 (2023), p. 471–500. Disponível em: https://acesse.dev/UWO5V. Acesso: 10 maio. 2024.

GOMES, Maria Cecília Oliveira. "Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD". *Revista do Advogado* - AASP, a. 39 n.144 (2019), p.174-183. Disponível em: https://bit.ly/4bQrL6p. Acesso: 10 maio. 2024.

GODIM, Glenda Gonçalves. "A responsabilidade civil no uso indevido dos dados pessoais". *Revista IBERC*, v. 4 n. 1 (2021), p. 19–34. Disponível em: https://l1nq.com/z5Q3N. Acesso: 10 maio. 2024.

KEPPEN, Mariana. "Dados em pauta: a adequação dos Tribunais de Justiça à LGPD". *Revista da ACONJUR – Associação dos Consultores Jurídicos do Poder Judiciário do Paraná* (2024), p. 34-49. Disponível em: https://acesse.dev/GhIQr. Acesso: 10 maio. 2024.

LOPES, Eliseu F. Pinto. "Avaliação de impacto sobre a proteção de dados". *Privacy and Data Protection Magazine*, n. 5 (2022), p. 101-142. Disponível em: https://encr.pw/j1WUj. Acesso: 10 maio. 2024.

MAIOLINO, Eurico Zecchin. "A LGPD e o Poder Judiciário: desafios de adequação e perspectivas". *Revista Jurídica Brasileira*, v. 3 (2023), p. 449-468. Disponível em: https://acesse.dev/9SZxF. Acesso: 10 maio. 2024.

MARTINS, José Joaquim. "Proteção de Dados e o Sistema Judicial Português – Uma síntese". BARZOTTO, Luciane Cardoso & COSTA, Ricardo Hofmeister de Almeida Martins (Eds.) *Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018: doutrina e aplicabilidade no âmbito laboral*. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região / Diadorim Editora (2022), p. 112-128. Disponível em: https://acesse.dev/1ECgI. Acesso: 10 maio. 2024.

MASSENO, Manuel David: "Inteligencia Artificial y Protección de Datos: la "elaboración de perfiles" para la prevención de delitos graves y del terrorismo en las fuentes de la Unión Europea". *Revista Eletrônica do Curso de Direito da UFSM*, v. 17 n. 2 (2022), e83679. Disponível em: https://encr.pw/wGIEY. Acesso: 10 maio. 2024.

MASSENO, Manuel David. "Da Disciplina da Segurança na Proteção de Dados, Aplicada ao Poder Local". *CYBERLAW by CIJIC - Revista Científica sobre Cyberlaw do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa*, Edição XII (2024), p. 116-143. Disponível em: https://encr.pw/hS3KH. Acesso: 10 maio. 2024.

MASSENO, Manuel David; MARTINS, Guilherme Magalhães & FALEIROS Jr., José Luiz de Moura. "A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira". Florianópolis. *Revista do CEJUR/TJSC: Prestação Jurisdicional*, v. 8 n. 1 (2020), pp. 1-28. Disponível em: https://acesse.dev/Z7rJR. Acesso: 10 maio. 2024.

MIRANDA, Gladson Rogério de Oliveira. "Ativismo judicial e poder normativo do CNJ". *Brazilian Journal of Development*, v. 6 n. 10 (2020), p. 76947–76959. Disponível em: https://l1nq.com/HrvOQ. Acesso: 10 maio. 2024.

MORAES, Maria Celina Bodin de. "LGPD: um novo regime de responsabilização civil dito 'proativo'". *Civilistica.com*, a. 8 n. 3 (2019), p. 1-6. Disponível em: https://encr.pw/w1cb5. Acesso: 10 maio. 2024.

OLIVEIRA, Inês. "Os regimes especiais de proteção de dados pessoais: exemplos de poluição legislativa da União Europeia?". Lisboa. *Anuário da Proteção de Dados - 2019*, (2019), p. 157-172. Disponível em: https://bit.ly/3K9gfHu. Acesso: 10 maio. 2024.

PIZZOL, Ricardo Dal. "Limites do poder regulamentar do Conselho Nacional de Justiça. Estudo de um caso: Resolução CNJ nº 236/16". PRETTO, Renato Siqueira de; KIM, Richard Pae & TERAOKA, Thiago Massao Cortizo (coord.). *Federalismo e*

Poder Judiciário. São Paulo: Escola Paulista da Magistratura (2019), p. 311-330. Disponível em: https://encr.pw/X0OWi. Acesso: 10 maio. 2024.

ROCHA, Willian Alessandro. "LGPD e os dados das secretarias das varas do trabalho". *Revista Síntese trabalhista e previdenciária*, v. 32, n. 386 (2021), p. 188–218. Disponível em: https://encr.pw/07uIG. Acesso: 10 maio. 2024.

ROSAS, Eduarda Chacon & HAMAOKA, Sayuri Pacheco. "As medidas de segurança e a accountability do agente de tratamento de dados pessoais no âmbito extrajudicial". LIMA, Ana Paula Canto de & ROSAS, Eduarda Chacon (coord.). *LGPD 2022*, *cit*. (2022), p. 229-247. Disponível em: https://l1nq.com/wqIJd. Acesso: 10 maio. 2024.

SANTOS, Luciano Alves dos. "A Lei Geral de Proteção de Dados Pessoais e os seus reflexos no Poder Judiciário brasileiro". *Privacy and Data Protection Magazin*e, n. 1 (2021), p. 92-107. Disponível em: https://l1nq.com/Z2z5n. Acesso: 10 maio. 2024.

SCODRO, Carolina Lopes. "Proteção dos Dados Pessoais nos Tribunais Brasileiros: Análise da influência da Resolução nº 363/2021 do CNJ no TJPR, TJSC, TJGO e TJDFT". *Revista de Política Judiciária, Gestão e Administração da Justiça*, v. 7 n. 1 (2021), p. 82-101. Disponível em: https://acesse.dev/Yk18q. Acesso: 10 maio. 2024.

STRECK, Lênio L.; SARLET, Ingo W.; CLÈVE, Clèmerson M. "Os limites Constitucionais das resoluções do Conselho Nacional de Justiça (CNJ) e Conselho Nacional do Ministério Público (CNMP)". *Migalhas* (2006). Disponível em: https://bit.ly/3wLhklF. Acesso: 10 maio. 2024.

TEIXEIRA, Isabel M.ª Curto. *Proteção de Dados e Processo Civil – Recentes Alterações Legislativas e Novas Problemáticas*. Lisboa. Conselho Superior da Magistratura - Rede Nacional de Juízes para apoiar a actividade da RJE Civil (2019). Disponível em: https://bit.ly/3wtOyGn.

WENGOROVIUS, Sofia. "Tribunais e Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a proteção de dados (RGPD)". *O Direito*, A. 155, III (2023), pp. 447-481. Disponível em: https://encr.pw/ygGyd. Acesso: 10 maio. 2024.