



A SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS NO SISTEMA JUDICIAL, EM PORTUGAL E NO BRASIL¹

SECURITY OF PERSONAL DATA PROCESSING BY THE JUSTICE SYSTEM, IN PORTUGAL AND IN BRAZIL

Manuel David Masseno²

Resumo. Este artigo expõe, comparativamente, os regimes jurídicos relativos às medidas de segurança no tratamento de dados pessoais em Portugal e no Brasil, depois do Regulamento Geral de Proteção de Dados da União Europeia e da Lei Geral de Proteção de Dados do Brasil. O que é feito tanto em termos gerais, quanto a propósito das especificidades legislativas aplicáveis à Justiça Criminal.

Palavras-chave: Proteção de Dados Pessoais, Portugal e Brasil comparados, Segurança,

Abstract. This paper addresses, from a comparative perspective, the legal regimes regarding security measures for the processing of personal data in Portugal and Brazil, after the General Data Protection Regulation of the European Union and the Brazilian General Data Protection Law. What is done in general, but also with a special attention to the specific rules applicable to Criminal Justice.

Keywords. Personal Data Protection, Portugal and Brazil compared, Security

Recebido: 18/05/2021.

Aprovado: 18/05/2021.

Artigo convidado por: Altieres de Oliveira Silva

¹ Comunicação ao VII Congresso Internacional Direito na Lusofonia “Dizer o Direito: o papel dos Tribunais no séc. XXI”. Escola de Direito da Universidade do Minho, 21 a 24 de junho de 2021.

² Professor Adjunto e Encarregado da Proteção de Dados do Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança de Segurança Informática. Além de pertencer ao Grupo de Trabalho de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo é Membro Consultor das Comissões de Direito Digital da Seção de Santa Catarina e da Subseção de Campinas, assim como das de Inovação, Gestão e Tecnologia e de Privacidade e Proteção de Dados das Subseções de Guarulhos e de Campinas, todas da Ordem dos Advogados do Brasil. Pertence ainda à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência da União Europeia para a Cooperação Policial.

1. Introdução.

Em matéria de tratamento de dados pessoais nos respetivos sistemas judiciais, os Ordenamentos português e brasileiro passam por vicissitudes semelhantes, ainda que em termos simétricos.

Assim, ambos assentam em regimes gerais, os dispostos pelo 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) – *RGPD*, e pela Lei n.º 13.709, de 14 agosto de 2018, Lei Geral de Proteção de Dados Pessoais – *LGPD*, de cujo âmbito objetivo excluem a justiça criminal (Art.ºs 2.º n.º 1, 9.º n.º 1 f), 37.º n.º 1 a) e 55.º n.º 3, bem como o *Considerando 20*, do *RGPD* e Arts. 1º e 4º III d), este *a contrario*, da *LGPD*).

Com efeito, para o tratamento de tais dados estão previstas disciplinas próprias. Em Portugal, pela 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 Conselho), no Brasil ainda estando por efetivar (Art. 4º III d) da *LGPD*).

De igual modo, ambos os Ordenamentos postulam a Segurança no tratamento dos dados como um dos seus “Princípios” (o da «integridade e confidencialidade» do Art.º 5.º n.º 1 f) do *RGPD*, subentendido no Art.º 4.º n.º 2 n.º 1 f) da Lei n.º 59/2019, assim como Art. 6º VII da *LGPD*).

2. Desenvolvimentos.

2.1. Os pontos de partida são muito distintos em cada um dos Ordenamentos. 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 Lei n.º 67/98, de 26 de outubro, a Lei da Proteção Dados Pessoais, a qual transpôs 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 no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados, embora esta não pretendesse ter um tal alcance (Art.º 3.º n.º 2). Por seu turno e na falta de uma Lei sobre proteção de dados pessoais, no Brasil estas questões foram reguladas pela Resolução n.º 215, de 16 de dezembro de 2015, do 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.

2.2. Entretanto, ambas as disciplinas passaram e passam por períodos de transição. Assim e para tanto, em Portugal e em julho de a última Legislatura, a Assembleia da República aprovou o Decreto n.º 333/XIII, alterando a Lei n.º 34/2009, o qual foi “devolvido sem promulgação” pelo Presidente da República, no final de julho, ainda que por razões não relacionadas com a segurança no tratamento de tais dados. Porém, não havendo sido reapreciado pelo Parlamento até ao final da Legislatura, a iniciativa caducou. No Brasil e porque a *LGPD* apenas entraria em vigor em agosto de 2020 (Art.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 Presidente deste), o Conselho Nacional de Justiça, 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.

2.3. No que tange à proteção de dados nos respectivos Sistemas Judiciais, em termos gerais, também verificamos existirem diferenças significativas. Assim, em Portugal e como referimos, continua vigente a Lei n.º 34/2009, na medida em que não contrarie o disposto no *RGPD*. Ao estar explícito que “os Estados-Membros deverão poder manter ou aprovar disposições mais específicas para adaptar a aplicação das regras previstas no presente regulamento” (*Considerando* (19)). O que coloca problemas especialmente complexos e controversos, sobretudo no respeitante à determinação do(s)

responsável(eis) pelo tratamento do dados, com a(s) correspondente(s) responsabilidade(s) proativa(s) (*accountability*, Art.º 5.º n.º 2, 24.º, 25.º e 32.º do *RGPD*) e a inerente imputabilidade das responsabilidades civil (Art.º 82.º do *RGPD* e Art.º 33.º da Lei n.º 58/2019, de 8 de agosto, a segura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679) e contraordenacional (Art.º 83.º do *RGPD*, Art.ºs 37.º a 45.º da Lei n.º 58/2019 e, ainda, a Lei n.º 67/2007, de 31 de dezembro, aprova o regime da responsabilidade civil extracontratual do estado e demais entidades públicas).

No entanto, se nos circunscrevermos ao nosso objeto, a questão resulta menos difícil, embora evidencie as consequências de uma decisão de base no que se refere ao funcionamento do Sistema Judicial português, a do controle dos meios materiais afetos ao Órgão de Soberania tribunais por parte do Governo, através do Ministério da Justiça.

Em qualquer caso e conforme ao disposto no *Código de Processo Civil* (Art.º 132.º n.º 4, na redação introduzida pelo Decreto-Lei n.º 97/2019, de 26 de julho, cujo regime é também aplicável nos Tribunais Administrativos e aos Tribunais Tributários, *ex vi*, Art.ºs 1.º e 2.º c) e e) dos respetivos *Códigos de Processo*), é necessário ter presente que:

“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”

Mas, começando pelo regime material, temos que o disposto no *RGPD* quanto à “Segurança do tratamento” (Art.º 32.º) é, perfeitamente, passível de ser compatibilizado o regime relativo às “Medidas de segurança” previstas na Lei n.º 34/2009 (Art.º 42.º), acrescentando a estas sobretudo no que se refere às análise de risco e ao nível exigível quanto às “medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco”.

Retomando a questão inicial e como foi repetidamente evidenciado aquando do processo legislativo conducente à aprovação parlamentar do Decreto n.º 333/XIII, designadamente pelo CSM – Conselho Superior da Magistratura, os meios informáticos afetos ao Sistema Judicial continuam sob a dependência do Ministério da Justiça, especificamente do Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., e não dos Tribunais ou do binómio CSM / CSTAF – Conselho Superior dos Tribunais Administrativos e Fiscais,

por força da respetiva Lei Orgânica (Decreto-Lei n.º 123/2011, de 29 de dezembro, Art.ºs 2.º n.º 1 i) e 14.º n.º 2 j) e l). O que é confirmado pela Lei n.º 34/2009, quanto às infraestruturas físicas, incluindo as linhas de transmissão e o arquivo eletrónico (Art.º 43.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”, 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”, em especial no atinente aos riscos de segurança (Art.ºs 4.º 7), 24.º n.º 1, 25.º e 32.º n.º 1), este apenas pode ser o Ministério da Justiça, com a inerente assunção de responsabilidades, com a intervenção específica da respetiva Encarregada da Proteção de Dados (Designada pelo Despacho n.º 5643/2018, de 6 de julho). O que ocorrerá em termos dissociados das demais funções dos responsáveis pelo tratamento, sejam estes os Tribunais, o CSM ou o CSTAF.

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

“A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrónico.

§ 1º Os autos dos processos eletrónicos 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 Princípio da “segurança” (Art. 6º VII) e a disciplina que o densifica (Arts. 46 a 49). Porém, os poderes aí conferidos à ANPD – Autoridade Nacional de Proteção de Dados, nomeadamente para a definição de “padrões técnicos mínimos” (Arts. 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 (Art. 103-B § 4º I). No mesmo sentido e em especial, a antes referida Lei n.º 11.419 determina que “Os órgãos do Poder Judiciário regulamentarão esta Lei, no que couber, no âmbito de suas respectivas competências” (Art. 18), também em função do previsto na Lei Complementar n.º 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” (Arts. 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 instituiu 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 (Arts. 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, a qual 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 (em especial, Art. 1º I d) e f) e III 8).

Neste sentido, a nova Resolução prevê a tomada de “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*”, pelos Tribunais (Art. 1º XI). Sendo estes a assumirem a qualidade de controladores, nos termos e para os efeitos previstos na *LGPD* (Arts. 5º VI e 37), com o apoio de um Comitê Gestor de Proteção de Dados Pessoais, com funções explícitas em matéria de segurança (Art. 1º I e XI b), cabendo-lhes ainda “designar o encarregado pelo tratamento de dados pessoais” (Art.º 1º II).

Cabe ainda acrescentar que o Supremo Tribunal Federal segue uma via paralela, com a aprovação da Resolução 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).

2.4. No tocante à Justiça Criminal, em Portugal, também por imposição do disposto no *Tratado sobre o Funcionamento da União Europeia* (Art.º 83.º n.º 1), as “regras mínima” relativas a “infrações penais” apenas podem ser “por meio 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 *RGPD* e a Lei n.º 58/2019.

Assim e embora, tal como no *RGPD* e por Princípio, os dados devem ser tratados “de uma forma que garanta a sua segurança adequada, 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” (Art.ºs 4.º n.º 1 f) da Diretiva e 4.º n.º 2 f) da Lei), verifica-se um maior rigor quanto à segurança nos “registos das atividades de tratamento” (Art.ºs 24.º da Diretiva e 26.º da Lei) e no “registo cronológico” (Art.ºs 25.º da Diretiva e 27.º da Lei). Por seu turno, no tocante à “segurança do tratamento”, em sentido próprio (Art.º 29.º da Diretiva e 31.º da Lei), o foco é posto no controle do acesso, detalhadamente.

A este propósito, há ainda a referir que a “omissão” pelo Legislador nacional quanto tratamento dever ocorrer “tendo em conta 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, apliquem medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco” (Art.º 29.º n.º 1 da Diretiva e 31.º n.º 1 da Lei), não poderá ter consequências atendendo ao “Princípio da interpretação conforme” (Enunciado no Acórdão do Tribunal de Justiça da União Europeia de 13 de Novembro de 1990, Processo C-106/89, *Marleasing*).

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” (Art.ºs 30.º e 31.º da Diretiva e 32.º e 33.º da Lei), com a Comissão Nacional de Proteção de Dados a assumir essa função. Para

tal, esta conta com a incorporação de um magistrado judicial designado pelo CSM e que se ocupará do controle do acesso aos dados e aos registos cronológicos das operações de tratamento (Art.º 43.º).

Por outro lado e a propósito da identificação do “responsável pelo tratamento”, ao ser este “a autoridade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais, ou, no caso em que estes são determinados por lei, a autoridade nela indicada” (Art.º 3.º n.º 1 j) da Lei), remetemos para as acima considerações aduzidas a propósito das funções do Ministério da Justiça.

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” (Art. 4º IV § 1º da *LGPD*), no mínimo, deverão ser aplicadas “medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais” previstas nas citadas Resoluções do CNJ, até porque essa legislação deverá observar “os princípios gerais de proteção e os direitos do titular previstos nesta lei”, como enuncia o mesmo preceito *in fine*, embora em articulação com os *Princípios do Processo Penal*. Embora e até esse momento, 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” (Art. 4º IV § 1º da *LGPD*), não deva considerar-se aplicável ao Poder Judiciário, atendendo ao seu estatuto constitucional, incluindo a respetiva autonomia administrativa (Art. 99).

4. Para terminar, deixo um par de **reflexões conclusivas**. Em Portugal e no Brasil, os tratamentos de dados pessoais nos respetivos Sistemas Judiciais estão passando por transformações profundas, também no que se refere às questões respeitantes à segurança. Para além de questões comuns, como a da previsão no *RGPD* e na *LGPD* de regimes jurídicos próprios para a Justiça Criminal, uma diferença marcante é evidenciada, a do controle dos meios operacionais afetos à Justiça por parte do Poder Executivo em Portugal. Ora, com especial uma especial incidência no que se refere à segurança no tratamento dos dados, a opção legislativa no sentido de não atribuir tais responsabilidades ao Órgãos do Poder Judiciário, incluindo o Conselho Superior da Magistratura e o Conselho Superior dos Tribunais Administrativos e Fiscais, afasta radicalmente as

soluções regulatórias e operacionais de ambos os países, por muito semelhantes que sejam o *RGPD* e o *LGPD*.

Referências bibliográficas:

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), pp. 11-15. ISBN 978-989-8908-17-9. Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Ciber_PDigital2018.pdf.

CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados*. Coimbra: Almedina, 2020. ISBN 978-972-40-8304-9.

CUEVA, Ricardo Villas Bôas. A incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário. DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Org.) *Lei Geral de Proteção de Dados (lei 13.709/18): a caminho da efetividade: contribuições para a implementação da LGPD*. São Paulo: Thomson Reuters Brasil / Revista dos Tribunais, 2020, pp. 199-209. ISBN 9786556140865.

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*. ISSN 2319-0884, vol. 8, n.º 1 (2020), pp. 1-28. Disponível em <https://revistadocejur.tjsc.jus.br/cejur/article/view/346>.

OLIVEIRA, Inês. Os regimes especiais de proteção de dados pessoais: exemplos de poluição legislativa da União Europeia? Lisboa. *Anuário da Proteção de Dados 2019*. ISSN 2184-5468, pp. 157-172. Disponível em https://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf.

SANTOS, Luciano Alves dos. A Lei Geral de Proteção de Dados Pessoais e os seus reflexos no Poder Judiciário brasileiro. Lisboa. *Privacy and Data Protection Magazine*. ISSN 2184-920X, n.º 1 (2021), pp. 92-107. Disponível em https://www.europeia.pt/content/files/pdpm_04_06_03.pdf.

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). *Ribeirão Preto. Migalhas*, 1983-392X, 16 de janeiro de 2006. Disponível em <https://www.migalhas.com.br/depeso/20381/os-limites-constitucionais-das-resolucoes-do-conselho-nacional-de-justica--cnj--e-conselho-nacional-do-ministerio-publico--cnmp>.

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://www.redecivil.csm.org.pt/wp-content/uploads/2020/01/PROTEC%C3%87%C3%83O-DE-DADOS-E-PROCESSO-CIVIL-Isabel-C-teixeira.pdf>.

Nota: todas as hiperligações foram verificadas no dia 12 de maio de 2021.