



ISSN 0034-835X
e-ISSN 2596-0466

Revista de Informação Legislativa



volume 63

250

abril a junho de 2026

SENADO FEDERAL



A proteção de dados de saúde e a Administração Pública: uma análise das experiências portuguesa e brasileira

Health Data Protection and Public Administration: An Analysis of the Portuguese and Brazilian Experiences

Suzana Maria Fernandes Mendonça¹

Resumo

O estudo identifica tanto os caracteres comuns quanto os distintivos nas regulamentações sobre a proteção de dados de saúde em Portugal e no Brasil e analisa a forma como a Administração Pública de ambos os países incorporou à sua atuação. Examina também alguns dos seus principais desafios e riscos quanto ao tratamento de dados de saúde – tais como ataques cibernéticos e práticas discriminatórias. A análise dessas experiências pode contribuir para a compreensão da temática e para o alcance de soluções que promovam a adequada atenção à saúde, o desenvolvimento científico, tecnológico e social, bem como o amparo aos direitos dos titulares dos dados de saúde.

Palavras-chave: proteção de dados pessoais; uso de dados de saúde; dados pessoais sensíveis; Administração Pública; sistema público de saúde.

Abstract

This study identifies both the common and distinctive features of health data protection regulations in Portugal and Brazil and analyses how the Public Administration of both countries has incorporated them into its operations. It also examines some of its main challenges and risks regarding the processing of health data—such as cyberattacks and discriminatory practices. The analysis of these experiences can contribute to understanding the issue and to achieving solutions that promote adequate health care, scientific, technological and social development, as well as the protection of the rights of health data subjects.

¹ Suzana Maria Fernandes Mendonça é doutora e mestra em Ciências jurídico-políticas pela Universidade de Lisboa, Lisboa, Portugal; concluinte de estudos pós-doutorais em Bioética na Universidade de Lisboa, Lisboa, Portugal; advogada. E-mail: suzanamfm@gmail.com

Keywords: personal data protection; use of health data; sensitive personal data; Public Administration; public health system.

Recebido em 6/2/25

Aprovado em 17/7/25

DOI: https://doi.org/10.70015/ril_v63_n250_p107

Como citar este artigo: ABNT² e APA³

1 Introdução

Os dados relativos à saúde de alguém são uma mina de informações expressivamente valiosas, pois desvelam tendências relacionadas a hábitos, fatores de risco, preferências, condições hereditárias, histórico familiar, bem como a ações destinadas à manutenção do bem-estar físico e mental; por conseguinte, os dados pessoais de saúde registrados no presente alcançam o passado e o futuro. Por considerá-los relevantes, o *Regulamento geral sobre proteção de dados pessoais* (RGPD) da União Europeia e a Lei nº 13.709/2018 (*Lei geral de proteção de dados pessoais* (LGPD)) do Brasil conferem-lhes especial atenção ao definirem parâmetros que harmonizam o uso de dados pessoais (UDP) com os direitos dos seus titulares.

Este trabalho analisa os aspectos relacionados ao UDP de saúde, em particular o seu enquadramento normativo, os fundamentos de sua licitude, sua realização no âmbito da Administração Pública (AP) e os principais riscos e desafios inerentes a ele em Portugal e no Brasil. Com base em pesquisa exploratória de natureza bibliográfica e documental, o estudo tem natureza predominantemente descritiva; seu fim é analisar aspectos similares e distintos tanto nas normatizações portuguesa e brasileira quanto nas práticas da AP relacionadas a dados de saúde. Com isso, o trabalho propõe-se contribuir para a compreensão do panorama normativo dos dois países e do UDP pelas estruturas de saúde geridas pela AP.

² MENDONÇA, Suzana Maria Fernandes. A proteção de dados de saúde e a Administração Pública: uma análise das experiências portuguesa e brasileira. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 63, n. 250, p. 107-130, abr./jun. 2026. DOI: https://doi.org/10.70015/ril_v63_n250_p107. Disponível em: https://www12.senado.leg.br/ril/edicoes/63/250/ril_v63_n250_p107

³ Mendonça, S. M. F. (2026). A proteção de dados de saúde e a Administração Pública: uma análise das experiências portuguesa e brasileira. *Revista de Informação Legislativa*: RIL, 63(250), 107-130. https://doi.org/10.70015/ril_v63_n250_p107

2 Enquadramento normativo da proteção de dados de saúde

O impacto da tecnologia na rotina das sociedades, sobretudo com a digitalização dos meios, comprova a relevância atribuída aos dados pessoais. O *capitalismo digital* e o *capitalismo da informação* (Pollicino; De Gregorio, 2022), que fundam novos modelos de negócios, fazem girar uma nova economia que atribui valor especial aos dados pessoais.

Conforme são manejados, os dados mais simples podem converter-se em fonte de informações valiosas, mesmo para as estimativas orientadas para o futuro (Pollicino; De Gregorio, 2022). Em contrapartida, como desvelam informações sensíveis e bem singularizadas de uma pessoa, cuja vida privada e cuja saúde podem ser gravemente afetadas, os dados de saúde têm valor distinto e por isso ensejam proteção jurídica diferenciada.

Ao identificar a necessidade de proteger esse complexo de informações pessoais, o RGPD estabelece um tratamento normativo distinto para os dados dessas categorias, a fim de orientar a atuação pública e privada nessa questão. Com efeito, de acordo com o considerando 35 e o art. 4º, nº 15, do RGPD, denominam-se *dados de saúde* os que se relacionam ao estado de saúde de um titular de dados; eles contêm informações sobre sua saúde física ou mental no passado, no presente e no futuro (União Europeia, 2016). Na estrutura do RGPD, atribui-se aos dados de saúde a condição de integrantes das categorias especiais de dados pessoais, e em seu art. 9º define-se um regime diferenciado em comparação com dados de outra natureza.

A proteção de dados pessoais (PDP) conecta-se a um conjunto de direitos encartados na Constituição da República Portuguesa (CRP), como a privacidade, a intimidade, a identidade pessoal, o desenvolvimento da personalidade⁴ em geral, bem como a saúde⁵ e a identidade genética⁶, em particular. A PDP decorre do art. 35º da CRP, sobre a utilização da informática⁷. A Lei nº 58/2019, por sua vez, assegura a execução do RGPD na ordem jurídica portuguesa e estabelece os parâmetros nacionais nos temas relativos à PDP. Ela

4 CRP, art. 26º, nº 1: “A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação” (Portugal, [2005]).

5 CRP, art. 64º, nº 1: “Todos têm direito à proteção da saúde e o dever de a defender e promover” (Portugal, [2005]).

6 CRP, art. 26º, nº 3: “A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica” (Portugal, [2005]).

7 CRP, art. 35º: “1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei” (Portugal, [2005]).

define⁸ as bases do UDP genéticos e de saúde, especialmente o princípio da necessidade de conhecer a informação – em que se manifesta a compatibilidade da recolha de dados com a proporcionalidade relativa ao seu objetivo – e o dever de sigilo dos profissionais com acesso a esses dados. Quanto à atividade desenvolvida pela AP, o *Código de procedimento administrativo* – que orienta o exercício da função administrativa do Estado português –, afirma o princípio da PDP⁹, que consolida o direito do titular à segurança e à integridade relativa aos sistemas e aplicações pendentes do UDP; isso reforça não somente os direitos do titular, mas também o papel da AP na proteção desses dados.

Inspirada no RGPD europeu, a LGPD instituiu no Brasil um amparo específico e uma estrutura de PDP de saúde que evidencia a sensibilidade desse conjunto de dados. A LGPD dispõe sobre os dados de saúde especialmente nos arts. 7º, VIII, e 11, II, f. Assim como o RGPD, a LGPD estabelece a posição diferenciada dos dados de saúde, ao classificá-los como *dados pessoais sensíveis* (DPS). A PDP de saúde fundamenta-se também no direito fundamental à saúde definido na Constituição da República Federativa do Brasil de 1988 (CRFB)¹⁰, em cujo âmbito a Emenda Constitucional nº 115/2022 incorporou o direito fundamental à PDP¹¹ (Brasil, 2022). Nos arts. 23 e seguintes, a LGPD estabelece parâmetros de UDP pela AP; em particular, a lei considera o atendimento à finalidade pública e ao interesse público, bem como a consolidação de um formato *interoperável* (isto é, capaz de operar, funcionar

⁸ Lei nº 58/2019, art. 29º: “1 - Nos tratamentos de dados de saúde e de dados genéticos, o acesso a dados pessoais rege-se pelo princípio da necessidade de conhecer a informação. 2 - Nos casos previstos nas alíneas h) e i) do nº 2 do artigo 9º do RGPD, o tratamento dos dados previstos no nº 1 do mesmo artigo deve ser efetuado por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação. 3 - O acesso aos dados a que alude o número anterior é feito exclusivamente de forma eletrónica, salvo impossibilidade técnica ou expressa indicação em contrário do titular dos dados, sendo vedada a sua divulgação ou transmissão posterior. 4 - Os titulares de órgãos, trabalhadores e prestadores de serviços do responsável pelo tratamento de dados de saúde e de dados genéticos, o encarregado de proteção de dados, os estudantes e investigadores na área da saúde e da genética e todos os profissionais de saúde que tenham acesso a dados relativos à saúde estão obrigados a um dever de sigilo. 5 - O dever de sigilo referido no número anterior é também aplicável a todos os titulares de órgãos e trabalhadores que, no contexto do acompanhamento, financiamento ou fiscalização da atividade de prestação de cuidados de saúde, tenham acesso a dados relativos à saúde. 6 - O titular dos dados deve ser notificado de qualquer acesso realizado aos seus dados pessoais, cabendo ao responsável pelo tratamento assegurar a disponibilização desse mecanismo de rastreabilidade e notificação. 7 - As medidas e os requisitos técnicos mínimos de segurança inerentes ao tratamento de dados a que alude o nº 1 são aprovados por portaria dos membros do Governo responsáveis pelas áreas da saúde e da justiça, que deve regulamentar, nomeadamente, as seguintes matérias: a) Estabelecimento de permissões de acesso aos dados pessoais diferenciados, em razão da necessidade de conhecer e da segregação de funções; b) Requisitos de autenticação prévia de quem acede; c) Registo eletrónico dos acessos e dos dados acedidos” (Portugal, 2019).

⁹ *Código do procedimento administrativo*, art. 18º: “Os particulares têm direito à proteção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, nos termos da lei” (Portugal, [2023]).

¹⁰ CRFB, art. 196: “A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação” (Brasil, [2025]).

¹¹ CRFB, art. 5º, LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, [2025]).

ou atuar com outro) para o uso compartilhado de dados com o intuito de efetivar políticas públicas (PPs)¹².

Desse modo, o enquadramento normativo tanto da PDP em geral quanto da PDP de saúde em particular recebeu considerável reforço nos últimos anos, como o comprovam os acervos normativos portugueses e brasileiros. A necessidade de proteção diferenciada de informações pessoais, sobretudo dos DPS, contrasta com a importância dos dados pessoais para o funcionamento da economia e de diversas ferramentas tecnológicas.

3 Hipóteses de tratamento de dados de saúde

No domínio da União Europeia, o art. 9º do RGPD define as categorias especiais de dados pessoais em consonância com a sensibilidade que lhes é inerente. Nessas categorias há dados que revelam opiniões políticas, convicções religiosas e filosóficas, filiação sindical, origem étnica e racial, dados biométricos, genéticos e de saúde, bem como os relacionados à orientação sexual. Similarmente, o art. 5º, II, da LGPD denomina *dados pessoais sensíveis* os relativos à origem racial ou étnica, à filiação sindical, à opinião política, à convicção religiosa e à vida sexual, bem como os dados genéticos, biométricos e de saúde. Como eles se caracterizam pelo potencial lesivo e discriminatório (Mulholland, 2018), é crucial consolidar uma estrutura de proteção diferenciada. Assim, as matérias consideradas sensíveis pelas duas normas se correspondem, o que demonstra a relevância do conteúdo protegido e a busca de um uso de DPS uniforme em realidades distintas.

Todavia, quando se trata desses dados, a abordagem é um pouco diversa nessas normas. O art. 9º do RGPD veda o tratamento dos dados componentes das categorias especiais e fixa exceções a essa proibição, como no caso de consentimento do titular. Por sua vez, o art. 11 da LGPD indica que o uso de DPS somente se configura em determinadas hipóteses, com base no consentimento do titular ou na dispensa de consentimento para certas finalidades. Embora não o proíba, a LGPD impõe um óbice inicial ao determinar que apenas nas situações previstas se podem utilizar DPS: por um lado, com o consentimento do titular de dados e, por outro, sem esse consentimento, dispensado por contextos que justifiquem o UDP, como o do cumprimento de uma obrigação legal ou o da garantia da segurança pessoal.

Constata-se, pois, que o UDP de saúde não é regra de atuação, conforme firmam ambas as normas, mas uma exceção ou circunstância que demanda o preenchimento de parâmetros

¹² LGPD, art. 23: “O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 [*Lei de acesso à informação*], deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]. Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei” (Brasil, [2026]).

para torná-lo viável. Por outro lado, as duas leis apresentam aspectos em comum quanto à consolidação do consentimento como hipótese de licitude de uso de DPS; isto é, o consentimento livre e esclarecido possibilita o uso de quaisquer dados considerados sensíveis e pressupõe que o paciente compreenda de fato os termos nele envolvidos (Yuan; Li, 2019).

O interesse público também torna possível o uso de DPS de saúde ou de outra natureza. O art. 6º do RGPD fundamenta a licitude do UDP no interesse, ao passo que no art. 9º, nº 2, g, da LGPD se sustenta a possibilidade de uso de DPS; ele define que a finalidade e o UDP das categorias especiais devem ser proporcionais em razão de interesse público significativo. No art. 7º, § 3º, da LGPD, estabelece-se que o UDP deve ocorrer à luz do interesse público; e no art. 23 define-se esse interesse como um dos aspectos a que a AP deve ater-se no UDP. O interesse público não consta da seção da lei sobre o uso de DPS; porém, ele se depreende do enunciado do art. 11, II, b, concernente à hipótese desse uso para a execução de PPs.

3.1 Hipóteses de tratamento de dados de saúde em Portugal

Há circunstâncias específicas que demandam o UDP de saúde. O RGPD define três exceções à vedação de UDP: prestações e cuidados de saúde, saúde pública e investigação científica. Conforme a Lei nº 58/2019, que cuida de sua execução em Portugal, o RGPD orienta o procedimento de UDP de saúde dada sua sensibilidade e os riscos associados.

No RGPD, o UDP de saúde é definido¹³ relativamente: a) à medicina preventiva e do trabalho; b) ao diagnóstico médico; c) às prestações e aos cuidados de saúde; d) à gestão de sistemas de saúde; e e) à avaliação da capacidade de trabalho dos empregados. O uso de DPS de saúde funda-se também no Direito europeu e na relação jurídica com um profissional de saúde sujeito ao dever de sigilo profissional¹⁴.

A realização de consultas médicas e de tratamentos terapêuticos, o funcionamento de atividades em estabelecimentos médico-hospitalares, as avaliações efetivadas no âmbito do trabalho e a gestão de sistemas de saúde – estas são algumas das circunstâncias que compõem o panorama de UDP genéticos e de saúde definidos no art. 9º, nº 2, h, do RGPD. Consolidado como norma que tonifica direitos subjetivos (Cordeiro, 2019), o RGPD sustenta a ampliação da confiança dos pacientes na partilha de seus dados com entidades de saúde (Vukovic; Ivankovic; Hahl; Dimnjakovic, 2022).

¹³ Conforme o RGPD, art. 9º, nº 2, h, se “o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3” (União Europeia, 2016).

¹⁴ Conforme o RGPD, art. 9º, nº 3, os “dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, [nos termos do Direito da UE ou dos Estados-membros] ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo [do Direito da UE ou dos Estados-membros] ou de regulamentação estabelecida pelas autoridades nacionais competentes” (União Europeia, 2016).

Especialmente quanto à prestação de serviços públicos de saúde, os entes da AP devem exercer suas atividades conforme o RGPD; isso significa que relatórios, diagnósticos, prontuários, registros de exames e outros dados relativos a saúde devem ser salvaguardados por agentes e órgãos. No âmbito do ordenamento português, aprimorou-se a prestação de saúde como hipótese de uso de DPS definida no art. 29º da Lei nº 58/2019. Uma das principais medidas de segurança de dados no tratamento derivado das prestações e dos cuidados de saúde consiste no dever de confidencialidade que vincula a atuação dos profissionais responsáveis pelo manejo dos dados¹⁵.

O RGPD contém outro fundamento de licitude ao UDP de saúde: o interesse público¹⁶. Dentre as justificativas para esse uso está a salvaguarda contra graves ameaças transfronteiriças e a garantia de elevado nível de qualidade de segurança relacionada a prestações de saúde, medicamentos e dispositivos médicos. Nas situações em que se configura a necessidade, podem-se usar os dados de saúde, desde que se assegurem a proporcionalidade (Cordeiro, 2019), o sigilo profissional e a proteção de direitos e liberdades dos titulares de dados. O UDP para os fins da saúde pública deve decorrer do interesse público; essa ressalva não cabe, pois, quando se trata de mero interesse pessoal (Cordeiro, 2019).

A regulamentação do UDP no campo da saúde pública objetiva assegurar a PDP e seu aprimoramento, para reforçar tanto a fiabilidade dos dados quanto a confiança no seu compartilhamento (Taylor, 2015). Não obstante, o UDP para os fins de saúde pública enfrenta desafios próprios. No início da crise sanitária decorrente da Covid-19, houve preocupação relativa à necessidade de equilíbrio entre a PDP de saúde dos usuários e sua utilização para os fins da saúde pública (McLennan; Celi; Buyx, 2020). Com fundamento na ramificação da saúde pública correlata à grave ameaça transfronteiriça, o UDP de saúde tornou-se essencial para a compreensão do ciclo e das taxas de transmissão da doença. A coleta, a análise e a circulação de dados, como os números e as estatísticas referentes ao número de infectados e recuperados, foram decisivos para a elaboração de PPs de enfrentamento do vírus.

Entretanto, em Portugal houve algum nível de intercorrência na PDP de saúde durante a pandemia: com base em informações fornecidas por autarquias locais, meios tradicionais de comunicação divulgaram dados que podiam identificar pessoas infectadas (inclusive crianças), cuja vida privada foi afetada, o que produziu o registro de solicitações de análise da temática pela Comissão Nacional de Proteção de Dados (CNPd), entidade administrativa responsável pelo controle e pela fiscalização do cumprimento do RGPD. Com fundamento

¹⁵ Lei nº 58/2019, art. 29º, nºs 2 e 5: “Nos casos previstos nas alíneas h) e i) do nº 2 do artigo 9º do RGPD, o tratamento dos dados previstos no nº 1 do mesmo artigo deve ser efetuado por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação. [...] O dever de sigilo referido no número anterior é também aplicável a todos os titulares de órgãos e trabalhadores que, no contexto do acompanhamento, financiamento ou fiscalização da atividade de prestação de cuidados de saúde, tenham acesso a dados relativos à saúde” (Portugal, 2019).

¹⁶ Conforme o RGPD, art. 9º, nº 2, i: “Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional” (União Europeia, 2016).

no impacto negativo e desproporcional para a intimidade e a vida privada, uma orientação da CNPD assinalou a inviabilidade de se divulgarem dados pessoais com a identificação de indivíduos infectados. Essa orientação vedou a divulgação de dados de saúde relativos à contaminação no caso de número reduzido de infectados numa circunscrição territorial com baixos números populacionais, onde era maior a facilidade de identificação (Comissão Nacional de Proteção de Dados, 2020).

Esse caso demonstra que a efetivação da saúde pública num cenário de gravidade excepcional deve compreender as outras bases da PDP. O princípio da necessidade, por exemplo, norteia o UDP sobretudo quanto à efetivação da saúde pública, bem como os outros princípios gerais de PDP, como o da minimização dos dados (Monge, 2022), o qual prescreve a compatibilidade entre a coleta dos dados necessários e o alcance da finalidade pretendida. Porém, de acordo com o RGPD, a hipótese de UDP de saúde refletida pelas investigações de natureza científica, histórica ou estatística¹⁷ deve basear-se na necessidade de elaboração de arquivos de interesse público. Portanto, a norma explicita a imprescindibilidade do interesse público para o UDP nas situações relacionadas à saúde pública e à investigação científica.

O RGPD demonstra ser possível desenvolver investigações científicas sem violar dados sensíveis, com o fim de garantir resultados científicos seguros em termos não somente de pesquisa, mas também de PDP utilizados para isso. O texto do RGPD, assim, equilibra os direitos e interesses das partes envolvidas com as condutas associadas aos resultados que se podem alcançar por meio da pesquisa em saúde (Hallinan, 2021).

A pandemia de Covid-19 demonstrou a relevância dos dados de saúde para as demandas relacionadas à saúde pública e ao impacto das investigações científicas. Naquela conjuntura de crise, o UDP tornou-se essencial ao enfrentamento dos efeitos da disseminação do vírus (Monge, 2023). A utilização de todo o acervo de dados alicerçou-se nas hipóteses de UDP concernentes à saúde pública e à investigação científica, destinadas a consolidar o interesse público envolvido na questão; os dados de saúde foram decisivos para o monitoramento dos efeitos da doença e para a elaboração de PPs eficazes para aquele enfrentamento.

3.2 Hipóteses de tratamento de dados de saúde no Brasil

Assim como o faz o RGPD, a LGPD insere os dados de saúde numa categoria especial, com o fim de atribuir-lhes a condição de DPS. Ao dispor sobre eles no art. 11, a lei inclui os dados de saúde e consolida o consentimento livre e informado como hipótese geral para seu uso. Nos arts. 7º, VIII, 11, II, f, e 13, a LGPD considera a saúde pública, a tutela da saúde

¹⁷ Conforme o RGPD, art. 9º, nº 2, j: “Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados” (União Europeia, 2016).

e a pesquisa científica como circunstâncias que ensejam o UDP, independentemente do consentimento do seu titular.

Ao sustentar o UDP no caso em que alguém demanda serviços e procedimentos realizados por profissionais da área, a tutela da saúde tem viés pessoal, pois corresponde aos interesses de prevenção e recuperação de uma pessoa. Diferentemente, a saúde pública volta-se para os interesses coletivos; ela sustenta o UDP de saúde para os fins de execução de PPs que alcançam grupos e recortes sociais; assim, o fundamento do uso de DPS não é de natureza individual. Conforme o art. 13 da LGPD, os estudos e as pesquisas científicas justificam o UDP associado ao interesse público para objetivos que repercutem em toda a sociedade, como o registro de estatísticas sobre a transmissibilidade, incidência ou mortalidade de certa doença.

Os estudos fundados na saúde pública e no interesse público instruem os procedimentos de elaboração de PPs, com a finalidade de tornar precisas e eficazes as atuações administrativas de PDP. A hipótese de UDP de saúde para os fins de pesquisas científicas, entretanto, deve oferecer aos titulares dos dados garantias a seus direitos – tais como a *anonimização* ou a *pseudonimização* dos dados, sua manutenção em ambiente seguro e a atenção aos padrões éticos de pesquisa –, conforme o art. 13 da LGPD. Ademais, em definição ligeiramente distinta do conceito de *interesse público* no RGPD, no art. 11, II, *b*, da LGPD estabelece-se o UDP para os fins de execução de PPs para tornar viável o uso compartilhado de dados necessários ao interesse público.

Muito embora revelem aspectos privados, os dados de saúde integram um conjunto de informações essenciais ao bem comum e à compreensão de padrões coletivos numa sociedade (Aragão; Schiocchet, 2020). Nessa perspectiva, o UDP para os fins de tutela da saúde ou de saúde pública indica a valoração efetivada pelas disposições da LGPD para assegurar a proteção de interesses coletivos quando contrastados com interesse individual de privacidade dos dados. A LGPD indica essa direção ao arrolar no art. 11, II, *b*, o interesse público para a execução de PPs como hipótese de dispensa de consentimento do titular de dados, pois o interesse individual em saúde não se sobrepõe ao interesse coletivo (Botelho; Camargo, 2021). Contudo, a desnecessidade de consentimento do titular é seguida de garantias a seus direitos, como a da *anonimização* dos dados.

Nesse contexto, o Sistema Único de Saúde (SUS) – responsável pela rede de atenção à saúde no Brasil – recorre ao UDP com fundamento na tutela da saúde e na saúde pública, para preservar o interesse público e as necessidades coletivas mediante a atuação rotineira de órgãos e agentes. Além disso, as hipóteses específicas de UDP de saúde combinam-se nas medidas tomadas pela AP no período pandêmico. A divulgação dos números de óbitos, de contaminados e de recuperados segundo a localização demonstra a importância do UDP para a execução de PPs e a efetivação dos direitos fundamentais à saúde e ao acesso à informação. A propósito, o Ministério da Saúde desenvolveu um portal – o Coronavírus Brasil¹⁸ – com

¹⁸ Em Painel Coronavírus (2025), podem-se verificar as informações sobre o impacto da Covid-19 no Brasil.

informações diversas sobre o impacto do vírus. Trata-se de um painel com os números relativos aos casos e aos óbitos confirmados, com as taxas de incidência e letalidade do vírus e com gráficos e recortes regionais que permitem mapear a transmissão da doença.

Nesse cenário, as hipóteses gerais e específicas que justificam o UDP consolidam o consentimento livre e esclarecido como pilar desse uso e firmam a tutela da saúde ou serviços de saúde, a saúde pública e as pesquisas científicas como justificativas legais. O consentimento e a tutela da saúde como fundamentos de natureza individual, bem como a saúde pública e os estudos científicos como hipóteses de natureza coletiva, evidenciam o peso conferido aos dados pessoais de saúde em ambos os contextos normativos.

4 O tratamento de dados de saúde pela Administração Pública

Já se mencionou que os DPS podem ser usados para a consecução de interesse público relevante¹⁹. Contudo, a simples alegação desse interesse não é suficiente para possibilitar esse uso, caso seja necessária a demonstração da imprescindibilidade da sua realização com base em suas vantagens e nos efeitos negativos no caso de ausência de tratamento (Cordeiro, 2022). O RGPD confere ao interesse público a posição de duplo fundamento de licitude do UDP: por um lado, a necessária conexão do interesse público com as hipóteses de UDP em razão de saúde pública ou investigação científica; e, por outro, o interesse público significativo que torna viável a utilização de DPS, inclusive os de saúde. Como se afirmou, dado o objetivo de executar PPs definido no art. 11, II, *b*, da LGPD, o interesse público é essencial para se usarem DPS, e isso repercute no texto da LGPD, que a partir do art. 23 apresenta uma seção específica para orientar o UDP pela AP.

Em ambos os ordenamentos, o UDP pela AP recebe atenção especial e vincula ao interesse público e à finalidade pública a atuação administrativa no UDP. Isso significa que ela deve realizar-se com retidão e evitar o desvio de finalidade, especialmente no uso de DPS. Por conseguinte, a esse uso devem corresponder certas garantias aos titulares, tais como a harmonia entre a coleta de dados e a finalidade do tratamento, e conformar essa coleta aos princípios da adequação e da necessidade. Na prática administrativa portuguesa e brasileira, o UDP assenta-se no interesse público.

4.1 A experiência portuguesa

É rica a experiência portuguesa relacionada ao UDP. Destinado à consecução do interesse público relacionado à saúde pública e à investigação científica com finalidade estatística, o

¹⁹ Conforme o RGPD, art. 9º, g: “Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados” (União Europeia, 2016).

Sistema Nacional de Saúde (SNS) mantém em seu sítio eletrônico tabelas e relatórios com dados de saúde oriundos do monitoramento de enfermidades²⁰.

Satisfaz-se, assim, o princípio da publicidade e da transparência inerentes à atividade administrativa; e isso não é diferente em relação aos dados de saúde, tratados sob ressalvas à vedação ao uso definidas no RGPD. A transparência diz respeito aos DPS de saúde coletados para se produzirem estatísticas no âmbito da atuação do SNS; para isso, esses dados são *anonimizados*, tratados com fins estatísticos e então divulgados para o acesso de toda a população.

Essas estatísticas revelam, por localidade, o número de utentes acometidos por comorbidades e enfermidades, bem como a porcentagem em comparação com outras unidades de saúde dispersas no território português. As tabelas e os relatórios estatísticos podem ser verificados tanto nos programas de acompanhamento de diabetes, hipertensão ou síndrome gripal, quanto nos rastreios oncológicos, nas consultas médicas ou nas intervenções cirúrgicas.

A AP deve assegurar a harmonia do modelo virtual relativo a saúde por meio de sistemas que interconectem informações comumente separadas e dispersas (Cavet, 2023), com as finalidades de prestar atendimento adequado e reforçar o papel da saúde pública à luz do interesse público. Os Serviços Partilhados do Ministério da Saúde (SPMS) são a entidade responsável pela partilha de informações entre plataformas e aplicativos, como a Prescrição Eletrônica Médica ou o Sistema de Cuidados de Saúde Hospitalares.

Existe uma plataforma específica de integração local dos SPMS para a *interoperabilidade* dos sistemas – a Local Interoperability Gateway (Light)²¹. Além disso, um aplicativo de serviços digitais do SNS – o SNS24, destinado ao utente – permite aceder a vários serviços como boletim de vacinas, teleconsulta, solicitação de medicação habitual, consulta a exames e receitas médicas, cartão de doenças raras, histórico de profissionais que tiveram acesso às informações do usuário e uma calculadora que mede risco de diabetes²². Por sua vez, o Portal do Utente fornece acesso a serviços como agendamento de exames, registros de receitas médicas, consulta a lista de espera de cirurgia, autodeclaração de doença (que justifica ausências laborais de até três dias) e o registro dos profissionais que acederam ao prontuário do utente²³. Outro aspecto relacionado ao UDP de saúde é direito de acesso à

20 Podem-se verificar os DPS de saúde do SNS na aba Transparência (c2026).

21 Podem-se verificar as informações acerca das plataformas de tecnologia e comunicação vinculadas ao SPMS em Tecnologias [...] (c2025).

22 Podem-se verificar as informações relativas à aplicação no sítio eletrônico do SNS (Serviço [...], c2026).

23 Ver Portal do Utente (2025).

informação (como dados clínicos²⁴, resultados de exames e diagnósticos²⁵) com fundamento no art. 17º, nº 2, da Lei nº 58/2019, e no art. 3º, nº 1, da Lei nº 12/2005 (*Lei de informação genética e informação pessoal de saúde*).

Entretanto, há casos em que o acesso à informação é negado por órgãos da AP, como centros hospitalares e unidades locais de saúde. Por motivos diversos, órgãos administrativos obstam o acesso ao conjunto de dados de saúde relacionados aos usuários²⁶ ou aos seus familiares – falecidos ou não. Quem se sente lesado pela negativa da AP de acesso à informação encaminha a demanda à Comissão de Acesso aos Documentos Administrativos (Cada), que emite parecer acerca do caso. Dentre as principais demandas analisadas pela Cada constam os pedidos de acesso a dados de familiares – como filhos que solicitam prontuários de pais. Tais requerimentos de informações ocorrem: a) com o propósito de se conhecer o histórico familiar de saúde²⁷; b) com fins judiciais (Comissão de Acesso aos Documentos Administrativos, 2022a, 2022b, 2024f); ou c) devido a questões relacionadas a contratos de seguro (Comissão de Acesso aos Documentos Administrativos, 2023a, 2023b, 2024c). Em vários pareceres emitidos na última década, a Cada tem autorizado o acesso a dados de terceiros, com base na Lei nº 58/2019 e na legislação aplicável. Nesse cenário, é grande o UDP de saúde pela AP portuguesa, e ele se conforma aos fundamentos de licitude estabelecidos no RGPD.

4.2 A experiência brasileira

O Sistema Único de Saúde (SUS) atende a cerca de 190 milhões de pessoas; isso significa que em torno de 80% dos cidadãos dependem exclusivamente dele, que hoje ultrapassa dois bilhões de atendimentos por ano²⁸. Toda a população brasileira, porém, utiliza os serviços

²⁴ Lei nº 58/2019, art. 17º, nº 2: “Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros” (Portugal, 2019).

²⁵ Lei nº 12/2005 (*Lei de informação genética e informação pessoal de saúde*), art. 3º: “1 - A informação de saúde, incluindo os dados clínicos registados, resultados de análises e outros exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa, sendo as unidades do sistema de saúde os depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e a investigação em saúde e outros estabelecidos pela lei. 2 - O titular da informação de saúde tem o direito de, querendo, tomar conhecimento de todo o processo clínico que lhe diga respeito, salvo circunstâncias excepcionais devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial, ou de o fazer comunicar a quem seja por si indicado. 3 - O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento, é feito através de médico, com habilitação própria, escolhido pelo titular da informação” (Portugal, [2016]).

²⁶ Sobre as solicitações de informações acerca dos utentes, a Cada tem sido favorável ao acesso à informação genética e de saúde, conforme os pareceres nºs 58/2024, 177/2024 e 128/2024 (Comissão de Acesso aos Documentos Administrativos, 2024b, 2024d, 2024g).

²⁷ Sobre as solicitações de informações referentes ao histórico familiar por familiares ou herdeiros, a Cada tem sido favorável ao fornecimento de acesso à informação genética e de saúde, conforme o Parecer nº 45/2024 (Comissão de Acesso aos Documentos Administrativos, 2024a). No mesmo sentido são os pareceres nºs 407/2023, 196/2017, 61/2017 e 132/2024 (Comissão de Acesso aos Documentos Administrativos, 2017a, 2017b, 2023a, 2024e).

²⁸ De acordo com informações do Ministério da Saúde (Maior [...], [2022]).

do SUS, em especial a vacinação e o tratamento de enfermidades que demandam controle vinculado à saúde pública.

Nesse contexto, a Rede Nacional de Dados de Saúde (RNDS) é uma plataforma que sustenta a *interoperabilidade* dos sistemas de saúde, com modelos clínicos de natureza informacional e computacional para a utilização dos profissionais vinculados ao UDP genéticos e de saúde²⁹. A RNDS promove a conexão entre sistemas relacionados a saúde, com o fim de viabilizar: a) o controle de doenças transmissíveis; b) o adequado acompanhamento do paciente; c) a melhoria nos registros, nos atendimentos e nas ofertas de serviços; e d) a inovação, em especial pelo uso de *telessaúde* e de outras tecnologias emergentes³⁰. A *interoperabilidade* dos sistemas e das plataformas de fluxo permite acessar dados encaminhados de qualquer lugar do Brasil, o que facilita o atendimento. Além disso, há o DataSUS, uma plataforma desenvolvida pelo departamento de informática do SUS que amplia o acesso a informações de saúde conectadas com estatísticas demográficas³¹, resultantes do UDP *anonimizados*. Eles podem ser acessados por qualquer pessoa e são relevantes para a elaboração de PPs nos níveis federal, estadual ou municipal e para as investigações científicas relacionadas com a saúde.

Por sua vez, o aplicativo Meu SUS Digital³², destinado à experiência do paciente, consolida uma área exclusiva relacionada ao consentimento do UDP pelos serviços de saúde prestados pela AP, dividida em: a) não consentimento; b) consentimento geral; e c) consentimento específico. Com base na alternativa de consentimento específico, é possível registrar a opção pelo atendimento de certo médico mediante a adoção do número da sua identidade profissional para a autorização de acesso aos dados do usuário. O Meu SUS Digital registra um histórico de acesso aos dados do paciente, em que constam: a) as informações dos profissionais que incluíram e acessaram os dados; b) o propósito de garantir transparência ao fluxo de dados relativos à saúde do paciente; e c) informações relacionadas a vacinação, agendamento de exames, acesso a resultados, registro de medicamentos recebidos ou inscrição em programas como os de dignidade menstrual, que oferecem gratuitamente absorventes higiênicos.

5 Portugal e Brasil: desafios e riscos comuns

O UDP enfrenta múltiplos riscos e desafios, que se ampliam quando se trata de dados de saúde, em virtude da sensibilidade que lhes é inerente. Examinam-se aqui alguns desses desafios e riscos para a AP de Portugal e do Brasil.

²⁹ Conforme informações do *Guia RNDS* ([2026]).

³⁰ Podem-se verificar os pilares da atividade vinculada a RNDS em Rede [...] ([2026]).

³¹ Podem-se verificar informações e estatísticas de saúde em todo o País em DataSUS (Acesso [...], [2024]).

³² Conforme o sítio eletrônico do aplicativo Meu SUS Digital (Política [...], [2025]).

5.1 O uso secundário de dados de saúde

O princípio da finalidade vincula o UDP a objetivos específicos, com o intento de obstar o uso secundário de dados, nomeadamente os DPS. A problemática agrava-se quando o conjunto de dados de saúde é de difícil coleta ou de elevada relevância, já que esse princípio inviabilizaria o uso secundário desses dados. No entanto, os ordenamentos jurídicos português e brasileiro fornecem respostas para a questão dessa dissonância com a finalidade original.

Em Portugal, o UDP com fins diferentes dos estabelecidos no momento da coleta pode ser realizado por entidades públicas, desde que atenda ao interesse público, conforme o art. 23º da Lei nº 58/2019. O art. 6º, nº 4, do RGPD autoriza o uso secundário de dados pessoais nos casos de conexão entre a finalidade original e a finalidade secundária, e de consonância entre os contextos anterior e posterior em que os dados foram coletados; isso reforça a necessidade de se assegurar a proteção dos interesses do usuário.

Em contrapartida, a solução encontrada no Brasil para transpor a barreira que o princípio da finalidade pode impor ao uso secundário de DPS foi estabelecida pela LGPD. Seu art. 7º, § 3º, estabelece que o UDP de acesso público deve observar a finalidade, a boa-fé e o interesse público, ao passo que o art. 7º, § 7º, permite o uso secundário de dados pessoais coletados em razão de interesse público, desde que se salvaguardem os direitos do titular e se preservem os objetivos legítimos e específicos do UDP, de acordo com o princípio da adequação disposto no art. 6º, II. Ao considerar o UDP para os fins de execução de PPs definida no art. 26 da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) publicou um guia sobre o UDP destinado à AP; quanto ao tema do uso secundário, ele recomenda a avaliação do contexto da coleta, da compatibilidade entre a finalidade original e o tratamento posterior, da natureza dos dados, das expectativas dos seus titulares relativas à proteção de seus direitos e ao interesse público (Landerdahl; Maiolino; Barbosa; Carvalho, 2023).

Desse modo, ambas as regulamentações alcançaram respostas para a problemática do uso secundário de dados, em particular os relacionados a saúde. As soluções portuguesa e brasileira são similares, pois chamam atenção para a correspondência entre a finalidade original e a nova e para a harmonia entre os contextos que justificam o UDP e a proteção de direitos do titular. Elas atribuem peso diferenciado ao interesse público, o que torna viável o uso secundário de dados de saúde.

5.2 O desvio de finalidade

Quando se levam em conta as estruturas dos sistemas públicos de saúde, um desafio comum às experiências portuguesa e brasileira é conservar a retidão e a ética na atuação administrativa relativa ao UDP de saúde. Como qualquer ação da AP, o UDP é passível de desvio de finalidade, o qual ocorre quando um órgão ou agente público viola os DPS dos titulares. Esse é o caso, por exemplo, do agente público que detém credenciais de acesso a

dados e que as utiliza para obter informações relativas à saúde de alguém. Trata-se de uma conduta antiética com o fim de satisfazer a interesses privados ou a interesses públicos alheios ao objetivo de sua atuação (Sousa; Matos, 2008).

Como a coleta e o UDP devem relacionar-se com a finalidade pretendida, o desvio de finalidade funda-se em razão diversa para a recolha de dados para o UDP – ou seja, desconforme com seu objetivo e com a legislação. A atuação da AP relacionada aos dados de saúde deve assentar-se nos princípios da boa-fé e da tutela da confiança, pois os cidadãos esperam que seus dados sejam de fato usados para finalidades legítimas. Conforme o princípio da boa-fé, essa atuação deve basear-se na lealdade (Moncada, 2010), na retidão, na honestidade e na seriedade; por outro lado, os particulares devem agir conforme a boa-fé ao estabelecerem vínculos com a AP (Lopes, 2011).

No cenário caracterizado pela confiança há um comportamento anterior da AP que promove as expectativas do particular de que a atuação administrativa se conformará ao que previamente se determinou (Merusi, 2001), sem alterações drásticas ou repentinas. A tutela da confiança do indivíduo materializa-se no ato da AP que desencadeia a convicção de que a conduta administrativa seguirá um padrão estabelecido (González Pérez, 1999); a boa-fé e a tutela da confiança incidem no âmbito da AP ao comporem a estrutura de PDP, sobretudo os de saúde. A boa-fé sustenta a lealdade da atividade administrativa no UDP e reforça as bases de conformidade e integridade em todas as etapas de sua realização. E, como a boa-fé implica os particulares, os dados fornecidos por eles devem ser autênticos e verazes, para que se assegure o UDP fidedignos.

A boa-fé na atividade administrativa, associada aos dados de saúde, reforça as camadas de proteção contra eventuais desvios de finalidade ao vedar o indevido UDP. Como a tutela da confiança também envolve as expectativas do cidadão de que o UDP de saúde se converterá em benefício para si ou para a coletividade, a materialização do desvio de finalidade acarreta prejuízos à sua privacidade e aos cuidados voltados à sua saúde. O desvio de finalidade evidencia falhas de segurança da informação, aumenta o grau de vulnerabilidade dos mecanismos de PDP e amplia as chances de violação e vazamento de dados. Por isso, é necessário que o UDP de saúde se adéque à legislação, aos princípios que orientam a atividade administrativa e aos princípios que regem a PDP.

5.3 Práticas discriminatórias

No atual contexto de avanço exponencial da tecnologia, um enorme desafio tem desencadeado estudos em diversos campos do conhecimento: a reprodução de discriminações sociais por máquinas. Na esfera jurídica, a análise apoia-se nos vieses relacionados às percepções humanas que elas reproduzem, tais como: a) o reconhecimento facial e biométrico; b) as ofertas de produtos e serviços; ou c) as medidas de segurança pública que demandam atenção diferenciada. Os vieses que permeiam os dados utilizados para alimentar o funcionamento

das máquinas têm natureza histórica, social ou racial e apresentam tendências relativas a medidas, amostras, exclusões ou associações (Arowosegbe, 2023)³³.

As enfermidades correspondem fatores de discriminação, potencializados por ferramentas de alta tecnologia que permitem o conhecimento profundo de fatores de risco e de hábitos pessoais; dentre os problemas relacionados aos DPS estão os riscos inerentes a um quadro de saúde mental baseado em postagens nas redes sociais (Shaw; Sekalala, 2023). Além disso, há o risco de que a UDP realizada mediante essas ferramentas exclua grupos sociais já em seu desenho – o chamado *exclusionary design* (Shaw; Sekalala, 2023). Os vieses derivados dos dados de saúde revelam não só tendências reproduzidas por seres humanos (e não apenas por máquinas), mas também práticas discriminatórias em que se usa informação sobre a genética ou a saúde de alguém para promover exclusões fundadas em condições hereditárias ou de sanidade – como no caso de pessoas com certas deficiências ou das que superaram uma condição grave de saúde e encontram óbices para celebrar contratos de seguros, em vista dos obstáculos decorrentes do seu estado de saúde no passado.

Em virtude desses desafios, a Lei nº 75/2021 regula em Portugal o acesso ao crédito e aos seguros de saúde por quem tenha superado ou mitigado graves condições de saúde ou deficiência. Ela proíbe: a) a discriminação (e estabelece o direito ao esquecimento³⁴); b) a exclusão de garantias de contrato de seguro; e c) o aumento dos valores relativos ao seguro, de acordo com os prazos assinalados em suas disposições. Por outro lado, as informações de saúde em escalas mais amplas tornariam possível delinear o perfil populacional e promover práticas discriminatórias derivadas da saúde, da localidade, da etnia, da nacionalidade. O acesso a esses dados sem camadas de segurança pode acarretar enormes prejuízos, mas o desenho de perfis populacionais de saúde fundado na licitude da investigação científica pode produzir uma valiosa base de dados *anonimizados* acessível a qualquer interessado.

Em Portugal, o Plano Nacional de Saúde, desenvolvido no âmbito da Direção-Geral de Saúde, consolida dados relacionados à saúde da população, tais como: a) porcentagens de incidência de doenças a cada 100 mil habitantes; b) informações sobre natalidade e mortalidade; e c) a análise de fatores determinantes do estado de saúde atual da população (Plano [...], 2021). No Brasil, o Ministério da Saúde publica periodicamente relatórios sobre a incidência

³³ Entretanto, parcela considerável dos estudos diz respeito essencialmente aos vieses repercutidos pelas máquinas, sobretudo em relação à inteligência artificial, mediante o *machine learning* e o *deep learning*. Essa menção é oportuna, embora não se relacione diretamente com os temas abordados neste trabalho.

³⁴ Lei nº 75/2021, art. 3º: “1 - As pessoas que tenham superado ou mitigado situações de risco agravado de saúde ou de deficiência têm, na qualidade de consumidor, direito ao esquecimento na contratação de crédito à habitação e crédito aos consumidores, bem como na contratação de seguros obrigatórios ou facultativos associados aos referidos créditos, garantindo que: a) Não podem ser sujeitas a um aumento de prémio de seguro ou exclusão de garantias de contratos de seguro; b) Nenhuma informação de saúde relativa à situação médica que originou o risco agravado de saúde ou a deficiência pode ser recolhida ou objeto de tratamento pelas instituições de crédito ou seguradores em contexto pré-contratual. 2 - Nenhuma informação de saúde relativa à situação de risco agravado de saúde ou de deficiência pode ser recolhida pelas instituições de crédito ou seguradores em contexto pré-contratual desde que tenham decorrido, de forma ininterrupta: a) 10 anos desde o término do protocolo terapêutico, no caso de risco agravado de saúde ou deficiência superada; b) Cinco anos desde o término do protocolo terapêutico, no caso de a patologia superada ter ocorrido antes dos 21 anos de idade; c) Dois anos de protocolo terapêutico continuado e eficaz, no caso de risco agravado de saúde ou deficiência mitigada” (Portugal, 2021, p. 5).

de algumas enfermidades, com recortes associados a variáveis como região, faixa etária, etnia e sexo biológico. Os *Boletins epidemiológicos*³⁵ abordam infecções como Zika, malária e doença de Chagas, além de outras circunstâncias que afetam a saúde, como a obesidade, os acidentes com animais peçonhentos ou as lesões autoprovocadas.

Nesse cenário, os dados de saúde são decisivos: se, por um lado, podem promover condutas discriminatórias alicerçadas em condições hereditárias ou de saúde, por outro, sua adequada utilização oferece informações significativas para pesquisas, para a elaboração de PPs e para a definição de hábitos com potencial de mitigar fatores de riscos comportamentais e ambientais. Também é relevante uma governança de dados que se conforme às demandas específicas de certos segmentos sociais e que considere o valor da base de dados de saúde – em especial quanto aos danos que se podem produzir com o uso de DPS em desfavor de grupos historicamente vulneráveis (Shaw; Sekalala, 2023). Ambas as experiências procuram minimizar os riscos de discriminação em razão do estado de saúde, por meio da *anonimização* de dados para os fins de estudos científicos e do UDP de saúde para finalidades públicas.

5.4 Ataques cibernéticos e violação de dados

Os ataques cibernéticos violam dados pessoais e estão entre as principais ameaças num contexto de acelerado avanço da tecnologia. Dotado de uma pluralidade de usos e funções, o ciberespaço alcança o lazer, o conhecimento técnico e acadêmico, o mundo do trabalho e dos negócios (Elias, 2019) – e é terreno fértil para a captura de dados pessoais.

O impacto é ainda maior quando se trata de DPS, como os genéticos e os de saúde, pois sua inerente sensibilidade pode resultar em prejuízos incalculáveis aos titulares e aos seus direitos nos casos de violação e captura de dados. Os *cyberattacks* aos sistemas de saúde vinculados aos Estados ocorrem todos os dias; daí existirem sistemas de segurança da informação para neutralizá-los. Dentre as medidas que reforçam essa segurança está a promoção da *literacia* digital para se aperfeiçoar a compreensão dos aplicativos, dos sistemas informáticos de saúde, da sua utilização e dos direitos associados, como forma de garantir o pleno exercício do direito à saúde (Monge, 2021).

Quanto à ocorrência de ataques informáticos ao setor³⁶, o sítio eletrônico dos SPMS em Portugal divulga informações cruciais sobre o tema; são alertas, descrições de ferramentas

³⁵ Em Boletins [...] ([2026]), pode-se acessar o conteúdo dos boletins epidemiológicos produzidos pelo Ministério da Saúde do Brasil.

³⁶ A propósito, nos últimos anos em Portugal alguns hospitais, o Instituto Nacional de Emergência Médica (Inem), a Direção-Geral de Saúde e a Faculdade de Farmácia da Universidade de Lisboa foram alvos de ataques cibernéticos que pretendiam violar dados pessoais; entretanto, os revestimentos de segurança integrados aos sistemas de cada órgão foram suficientes para conter o risco de violação de dados genéticos e de saúde, embora em certos casos as consultas e os exames tenham sido paralisados até o restabelecimento dos sistemas de informação. E entidades de saúde brasileiras – como hospitais, o Instituto Nacional do Câncer e o Ministério da Saúde – também foram alvos de ataques cibernéticos que violaram dados de saúde de milhões de pacientes e provocaram a lentidão e a suspensão dos atendimentos (Comunicado [...], 2022; Bento, 2022; Caires, 2023; Instituto Nacional de Emergência Médica, 2022; Direção-Geral [...], 2023; Séneca; Franco; Dinis, 2023; Ataque [...], 2024; Abdala, 2024; Ataque [...], 2021).

maliciosas e de medidas de segurança para contê-las (Alertas [...], c2025). No Brasil, o Ministério da Saúde (Brasil, 2020) inclui a segurança dos dados entre os aspectos que podem ser aprimorados no âmbito da *Estratégia de saúde digital para o Brasil 2020-2028*. São iniciativas simples, que, conectadas à *literacia* digital, podem contribuir para o conhecimento das ameaças cibernéticas aos dados. Desse modo, a PDP de saúde depende de a AP desenvolver programas e mecanismos capazes de assegurar que os cidadãos compreendam os aplicativos e outras ferramentas de alta tecnologia relativas a dados pessoais. A medida pode reforçar consideravelmente a segurança ao propiciar a compreensão tanto do funcionamento de meios digitais quanto da forma como se deve proceder num contexto de saúde digitalizado.

Há riscos de eventuais vazamentos de dados decorrerem mais de falhas internas da entidade do que de ataques cibernéticos (Yuan; Li, 2019); por isso, é essencial realizar treinamentos regulares para aprimorar as habilidades de profissionais relativas à PDP de saúde. Também é indispensável contratar profissionais qualificados para as posições-chave na organização relacionadas essa proteção, em particular quanto à elaboração, ao aconselhamento e ao monitoramento de medidas associadas a isso (Yuan; Li, 2019) – o que significa agregar não apenas especialistas em PDP habituados a lidar com dados de saúde.

Para os ocupantes de posições-chave no âmbito da PDP manterem elevados níveis de conhecimento, a entidade deve promover cursos regulares de formação e de aprimoramento das capacidades associadas à PDP e ao adequado UDP de pacientes, em especial as tarefas de atendimento ao interesse público e de prestação adequada de serviços de saúde. Além disso, no âmbito das entidades da área, a obrigação de sigilo liga-se à atividade desenvolvida por todos os profissionais com acesso às informações genéticas ou de saúde, a fim de caracterizar segredo coletivo (Monge, 2023). Uma das principais medidas é a confidencialidade, cujos parâmetros devem ser periodicamente revisitados para ampliar as camadas de PDP.

Para conter ou mitigar as consequências de ataques cibernéticos, podem ser eficazes outras ações preventivas, tais como: a) a análise de riscos; b) a definição de protocolos de segurança em caso de tentativas de violação de dados; c) a criação de canais de queixa ou de denúncia para violações relacionadas ao conjunto de dados de saúde; d) a avaliação das medidas de segurança da informação; e e) a manutenção da atividade – seja do ente privado, seja da AP (Mantalero; Vaciago; Esposito; Monte, 2020). É crucial, pois, que sempre se atualizem as camadas de segurança e se mantenham íntegros tanto os sistemas de tratamento quanto o conjunto de dados.

O desafio para o qual Portugal e o Brasil não encontraram uma solução está na insegurança acarretada por ataques cibernéticos e pela violação de dados. Todavia, no âmbito dos dois sistemas públicos de saúde, o tema tem sido objeto de iniciativas que intentam minimizar esses riscos.

6 Conclusão

Com esteio nas experiências portuguesa e brasileira, este trabalho analisou a atuação da AP no UDP de saúde e examinou tanto os aspectos congruentes quanto os discrepantes. Dessa análise depreende-se que ambas as experiências apresentam mais pontos de similaridade que de distinção, dado que suas regulamentações mantêm relação de proximidade, devida à influência do RGPD sobre a LGPD.

O RGPD veda o UDP de saúde e estabelece exceções que viabilizam sua realização, ao passo que a legislação brasileira permite o UDP desde que satisfeitos alguns parâmetros. Embora o resultado seja o mesmo em termos de viabilidade de UDP de saúde, a técnica legislativa escolhida pelo RGPD transmite a mensagem de maior restrição para efetivar o UDP de saúde em comparação com a LGPD, a qual permite o uso condicionado de tais dados. No entanto, as hipóteses de UDP de saúde são idênticas nos dois atos normativos; há uma hipótese de natureza geral, que se reflete no consentimento livre e informado, e as hipóteses de natureza específica, como a atenção à saúde pública e as pesquisas científicas. As normas europeia, portuguesa e brasileira ressaltam o interesse público como fundamento de licitude de UDP de saúde independentemente do consentimento de seus titulares.

As dinâmicas estabelecidas no âmbito dos dois sistemas públicos denotam uma crescente digitalização dos meios que conectam o usuário ao atendimento à saúde pública e que lhe oferecem ferramentas destinadas a tornar mais prática, confortável e segura a sua experiência. Os desafios vividos por Portugal e Brasil são similares num ambiente digital globalizado, como a vulnerabilidade dos sistemas de segurança a ataques cibernéticos ou a possibilidade de práticas discriminatórias fundadas em informações sobre a saúde dos titulares de DPS. Há obstáculos ao adequado exercício da atividade administrativa, e eles não são exclusivos de um ordenamento jurídico: a ocorrência de desvio de finalidade no UDP afeta a AP de ambos os países. Para o desafio do uso secundário de dados de saúde, porém, as regulamentações portuguesa e brasileira encontram soluções que promovem a inovação tecnológica e o desenvolvimento científico, sem se desconectarem da PDP.

Constatam-se, pois, avanços na PDP de saúde manejados pela AP de Portugal e do Brasil. Ainda que seja necessário aprimorar essa proteção, o progresso das estruturas geridas por elas é considerável e virtualmente alcança todos os cidadãos desses países.

Referências

ABDALA, Vitor. Ataque hacker prejudica atendimento no Instituto Nacional de Câncer. *Agência Brasil*, Rio de Janeiro, 30 jan. 2024. Saúde. Disponível em: <https://agenciabrasil.ebc.com.br/saude/noticia/2024-01/ataque-hacker-prejudica-atendimento-no-instituto-nacional-de-cancer>. Acesso em: 6 mar. 2026.

ACESSO à informação. [Brasília, DF]: DATASUS, [2024]. Disponível em: <https://datasus.saude.gov.br/acesso-a-informacao/>. Acesso em: 6 mar. 2026.

ALERTAS e segurança. [Lisboa]: Ministério da Saúde, c2025. Disponível em: <https://www.spms.min-saude.pt/alertaseseguranca/>. Acesso em: 29 abr. 2025.

ARAGÃO, Suélyn Matos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *RECIIS – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde*, Rio de Janeiro, v. 14, n. 3, p. 692-708, jul./set. 2020. DOI: <https://doi.org/10.29397/reciis.v14i3.2012>. Disponível em: <https://www.reciis.iciet.fiocruz.br/index.php/reciis/article/view/2012>. Acesso em: 6 mar. 2026.

AROWOSEGBE, Jacob O. Data bias, intelligent systems and criminal justice outcomes. *International Journal of Law and Information Technology*, [s. l.], v. 31, n. 1, p. 22-45, 2023. DOI: <https://doi.org/10.1093/ijlit/eaad017>.

ATAQUE de hackers a sistema de hospital em Indaiatuba gera lentidão nos atendimentos. *GI*, [s. l.], 11 jul. 2024. Campinas e Região. Disponível em: <https://g1.globo.com/sp/campinas-regiao/noticia/2024/07/11/ataque-de-hackers-a-sistema-de-hospital-em-indaiatuba-gera-lentidao-nos-atendimentos.ghtml>. Acesso em: 6 mar. 2026.

ATAQUE hacker tira do ar site do Ministério da Saúde e o ConecteSUS. *GI*, [s. l.], 10 dez. 2021. Jornal Nacional. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml>. Acesso em: 6 mar. 2026.

BENTO, Helena. Hospital do Litoral Alentejo alvo de “tentativa” de ataque informático. *Expresso*, [s. l.], 26 abr. 2022. Sociedade. Disponível em: <https://expresso.pt/sociedade/2022-04-26-Hospital-do-Litoral-Alentejo-alvo-de-tentativa-de-ataque-informatico-7f0a24c7>. Acesso em: 6 mar. 2026.

BOLETINS epidemiológicos. Brasília, DF: Ministério da Saúde, [2026]. Disponível em: <https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/boletins/epidemiologicos>. Acesso em: 6 mar. 2026.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral. A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista de Direito Sanitário*, São Paulo, v. 21, p. 1-21, 2021. DOI: <https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023>. Disponível em: <https://www.revistas.usp.br/rdisan/article/view/168023>. Acesso em: 6 mar. 2026.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2025]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 6 mar. 2026.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 6 mar. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 mar. 2026.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. *Estratégia de saúde digital para o Brasil 2020-2028*. Brasília, DF: Ministério da Saúde, 2020. Disponível em: https://bvms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 6 mar. 2026.

CAIRES, Marta. Serviço de Saúde da Madeira: ataque informático deixa utentes sem consultas e sem exames. *Expresso*, [s. l.], 7 ago. 2023. Sociedade. Disponível em: <https://expresso.pt/sociedade/2023-08-07-Servico-de-Saude-da-Madeira-ataque-informatico-deixa-utentes-sem-consultas-e-sem-exames-e0cee143>. Acesso em: 6 mar. 2026.

CAVET, Caroline Amadori. Saúde digital: entre os dados e o consentimento. *Lex Medicinæ: revista portuguesa de direito da saúde*, Coimbra, ano 20, n. 40, p. 21-35, jul./dez. 2023. Disponível em: <https://www.centrodedireitobiomedico.org/publicacao/revista-portuguesa-de-direito-da-saude-ano-20n-40julho-dezembro-2023/1/>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 45/2024*. Entidade consulente: Unidade Local de Saúde de Matosinhos, E.P.E. Relator: Tiago Fidalgo de Freitas, 21 de fevereiro de 2024a. Disponível em: <https://www.cada.pt/files/pareceres/2024/045.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 56/2022*. Entidade consulente: Centro Hospitalar de Vila Nova de Gaia/Espinho, E.P.E. Relator: Renato Gonçalves, 17 de fevereiro de 2022a. Disponível em: <https://www.cada.pt/files/pareceres/2022/056.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 58/2024*. Entidade requerida: Centro Hospitalar de Vila Nova de Gaia/Espinho, E.P.E. Relator: João Miranda, 21 de fevereiro de 2024b. Disponível em: <https://www.cada.pt/files/pareceres/2024/058.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 61/2017*. Entidade consulente: Centro Hospitalar [...]. Relator: Renato Gonçalves, 14 de fevereiro de 2017a. Disponível em: <https://www.cada.pt/files/pareceres/2017/061.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 83/2022*. Queixosa: Santa Casa da Misericórdia de Lisboa. Entidade requerida: Agrupamento de Centros de Saúde da Amadora. Relator: João Miranda, 16 de março de 2022b. Disponível em: <https://www.cada.pt/files/pareceres/2022/083.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 84/2024*. Entidade requerida: Hospital de Braga, E.P.E. Relator: Renato Gonçalves, 21 de fevereiro de 2024c. Disponível em: <https://www.cada.pt/files/pareceres/2024/084.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 128/2024*. Entidade requerida: Centro Hospitalar Universitário de Lisboa Central. Relator: Francisco Lima, 20 de março de 2024d. Disponível em: <https://www.cada.pt/files/pareceres/2024/128.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 132/2024*. Entidade requerida: Serviço de Saúde da Região Autónoma da Madeira (SESARAM). Relator: João Perry da Câmara, 20 de março de 2024e. Disponível em: <https://www.cada.pt/files/pareceres/2024/132.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 139/2024*. Entidades requeridas: Centro Hospitalar do Tâmega e Sousa, E.P.E., e Serviços Partilhados do Ministério da Saúde, E.P.E. Relatora: Fernanda Maças, 17 de abril de 2024f. Disponível em: <https://www.cada.pt/files/pareceres/2024/139.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 177/2024*. Entidade requerida: Hospital de Braga, E.P.E. Relatora: Maria Cândida Oliveira, 17 de abril de 2024g. Disponível em: <https://www.cada.pt/files/pareceres/2024/177.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 196/2017*. Entidade consulente: Hospital [...]. Relatora: Fernanda Maças, 20 de junho de 2017b. Disponível em: <https://www.cada.pt/files/pareceres/2017/196.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 407/2023*. Queixosa: Santander Totta Seguros – Companhia de Seguros de Vida, S. A. Entidade requerida: Centro Hospitalar do Médio Tejo, E.P.E. Relatora: Maria Cândida Oliveira, 18 de outubro de 2023a. Disponível em: <https://www.cada.pt/files/pareceres/2023/407.pdf>. Acesso em: 9 mar. 2026.

COMISSÃO DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS (Portugal). *Parecer nº 424/2023*. Queixosa: Aegon Santander Portugal Vida – Companhia de Seguros de Vida, SA. Entidade requerida: Unidade de Saúde Familiar do Laranjeiro. Relator: Carlos Abreu Amorim, 22 de novembro de 2023b. Disponível em: <https://www.cada.pt/files/pareceres/2023/424.pdf>. Acesso em: 6 mar. 2026.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (Portugal). *Orientação sobre divulgação de informação relativa a infetados por Covid-19*. Lisboa: CNPD, 22 abr. 2020. Disponível em: https://www.cnpd.pt/media/4i4hmccv/orientacoes_divulgacao_informacao_infetados_covid-19.pdf. Acesso em: 6 mar. 2026.

COMUNICADO Ministério da Saúde, Hospital Garcia de Horta. *Ministério da Saúde*, Lisboa, 26 abr. 2022. Disponível em: <https://www.hgo.min-saude.pt/2022/04/26/comunicado-ataque-informatico-hgo/>. Acesso em: 29 abr. 2025.

CORDEIRO, A. Barreto Menezes. *Direito da proteção de dados: à luz do RGPD e da Lei nº 58/2019*. Coimbra: Almedina, 2022.

CORDEIRO, A. Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLÍVIA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 777-795.

DIREÇÃO-GERAL da Saúde foi alvo de ataque informático. *Diário de Notícias*, [s. l.], 28 jan. 2023. Disponível em: <https://www.dn.pt/sociedade/direcao-geral-da-saude-foi-alvo-de-ataque-informatico-15741626.html>. Acesso em: 6 mar. 2026.

ELIAS, Luís. Ciberameaças e (in)segurança. *Cyberlaw by CIJIC*, Lisboa, n. 7, maio 2019. Disponível em: https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_7.pdf. Acesso em: 6 mar. 2026.

GONZÁLEZ PÉREZ, Jesús. *El principio generale de la buena fe en el derecho administrativo*. 3. ed. Madrid: Civitas, 1999. (Monografías Civitas).

GUIA RNDS. [Brasília, DF]: Ministério da Saúde, [2026]. Disponível em: <https://rnds-guia.saude.gov.br/>. Acesso em: 6 mar. 2026.

HALLINAN, Dara. A normative framework for the reconciliation of UE data protection law and medical research ethics. *Medical Law Review*, [s. l.], v. 29, n. 3, p. 446-467, 2021. DOI: <https://doi.org/10.1093/medlaw/fwab019>.

INSTITUTO NACIONAL DE EMERGÊNCIA MÉDICA. *Comunicado*. Lisboa: INEM, 15 dez. 2022. Disponível em: <https://www.inem.pt/wp-content/uploads/2023/09/2022-12-15-ATAQUE-INFORMATICO.pdf>. Acesso em: 29 abr. 2025.

LANDERDAHL, Cristiane; MAIOLINO, Isabela; BARBOSA, Jeferson Dias; CARVALHO, Lucas Borges de. *Tratamento de dados pessoais pelo poder público: guia orientativo*. Versão 2.0. Brasília, DF: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 6 mar. 2026.

LOPES, Pedro Moniz. *Princípio da boa-fé e decisão administrativa: estrutura e operatividade na discricionariedade conferida por normas habilitantes*. Coimbra: Almedina, 2011. (Monografias).

MAIOR sistema público de saúde do mundo, SUS completa 31 anos. *Ministério da Saúde*, Brasília, DF, 1º nov. 2022. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2021/setembro/maior-sistema-publico-de-saude-do-mundo-sus-completa-31-anos>. Acesso em: 6 mar. 2026.

MANTELERO, Alessandro; VACIAGO, Giuseppe; ESPOSITO, Maria Samantha; MONTE, Nicole. The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, [s. l.], v. 28, n. 4, p. 297-328, 2020. DOI: <https://doi.org/10.1093/ijlit/eaad021>.

MCLENNAN, Stuart; CELI, Leo Anthony; BUYX, Alena. Covid-19: putting the general data protection regulation to the test. *JMIR Public Health and Surveillance*, [s. l.], v. 6, n. 2, p. 1-4, Apr./June 2020. DOI: <https://doi.org/10.2196/19279>.

MERUSI, Fabio. Buona fede e affidamento nel diritto pubblico: il caso della “alternanza”. *Rivista di Diritto Civile*, Padova, v. 47, n. 5, p. 561-571, sett./ott. 2001.

MONCADA, Luís Cabral de. Boa-fé e tutela da confiança no direito administrativo. In: MIRANDA, Jorge (coord.). *Estudos em homenagem ao Prof. Doutor Sérvulo Correia*. Coimbra: Coimbra Ed., 2010. v. 2, p. 573-612.

MONGE, Cláudia. Acesso à informação de saúde e à informação genética. In: FREITAS, Tiago Fidalgo de; ALVES, Pedro Delgado (coord.). *Acesso à informação administrativa*. Coimbra: Almedina, 2021. p. 549-649. (Coleção ICJP/CIDP).

MONGE, Cláudia. Direito internacional dos direitos humanos e derrogações por razões de proteção sanitária: fundamentos e limites. In: DUARTE, Maria Luísa; GIL, Ana Rita; FREITAS, Tiago Fidalgo de (org.). *Direitos humanos e Estado de direito: proteção no quadro europeu e internacional*. Lisboa: AAFDL, 2022. p. 135-198.

MONGE, Cláudia. Proteção de dados e tratamento de dados de saúde: algumas questões. In: FARINHO, Domingos Soares; MARQUES, Francisco Paes; FREITAS, Tiago Fidalgo de (coord.). *Direito da proteção de dados: perspectivas públicas e privadas*. Coimbra: Almedina, 2023. p. 349-402. (Coleção ICJP/CIDP).

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. DOI: <https://doi.org/10.18759/rdgf.v19i3.1603>. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603>. Acesso em: 6 mar. 2026.

PAINEL Coronavírus. [Brasília, DF]: Ministério da Saúde, 2025. Disponível em: <https://covid.saude.gov.br/>. Acesso em: 6 mar. 2026.

PLANO nacional de saúde 2021-2030: saúde da população em Portugal. Lisboa: República Portuguesa: SNS: DGS, 2021. Disponível em: https://pns.dgs.pt/files/2023/02/PNS2021-2030_Saude-da-Populacao-em-Portugal.pdf. Acesso em: 29 abr. 2025.

POLÍTICA de privacidade. In: MEU SUS Digital. [Brasília, DF]: Ministério da Saúde, [2025]. Disponível em: <https://meusdigital.saude.gov.br/perfil/politica-privacidade>. Acesso em: 6 mar. 2026.

POLLICINO, Oreste; DE GREGORIO, Giovanni. Constitutional law in the algorithmic society. In: MICKLITZ, Hans-W.; POLLICINO, Oreste; REICHMAN, Amnon; SIMONCINI, Andrea; SARTOR, Giovanni; DE GREGORIO, Giovanni (ed.). *Constitutional challenges in the algorithmic society*. Cambridge, UK: Cambridge University Press, 2022. p. 3-24.

PORTAL do Utente. Lisboa: Ministério da Saúde, 2025. Disponível em: <https://servicos.min-saude.pt/utente/>. Acesso em: 29 abr. 2025.

PORTUGAL. [Constituição (1976)]. *Constituição da República Portuguesa de 1976*. Lisboa: Assembleia da República, [2005]. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 6 mar. 2026.

PORTUGAL. *Decreto-lei nº 4/2015, de 7 de janeiro*. Código do Procedimento Administrativo. Lisboa: Procuradoria-Geral Regional de Lisboa, [2023]. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2248&tabela=leis. Acesso em: 6 mar. 2026.

PORTUGAL. *Lei nº 12/2005, de 26 de janeiro*. Informação genética pessoal e informação de saúde. Lisboa: Diário da República, [2016]. Disponível em: <https://diariodarepublica.pt/dr/detalhe/lei/12-2005-624463>. Acesso em: 6 mar. 2026.

PORTUGAL. *Lei nº 58/2019, de 8 de agosto*. Assegura a execução, na ordem jurídica nacional, do Regulamento (EU) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Lisboa: Diário da República, 2019. Disponível em: <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>. Acesso em: 6 mar. 2026.

PORTUGAL. *Lei nº 75/2021, 18 de novembro*. Reforça o acesso ao crédito e contratos de seguros por pessoas que tenham superado ou mitigado situações de risco agravado de saúde ou de deficiência, proibindo práticas discriminatórias e consagrando o direito ao esquecimento, alterando a Lei nº 46/2006, de 28 de agosto, e o regime jurídico do contrato de seguro. *Diário da República*: 1ª série, Lisboa, n. 224, p. 4-8, 18 nov. 2021. Disponível em: <https://files.dre.pt/1s/2021/11/22400/0000400008.pdf>. Acesso em: 6 mar. 2026.

REDE Nacional de Dados de Saúde. [Brasília, DF]: Ministério da Saúde, [2026]. Disponível em: <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds>. Acesso em: 6 mar. 2026.

SÉNECA, Hugo; FRANCO, Hugo; DINIS, David. Ciberativistas russos lançam ataque europeu. Sites da DGS e Faculdade de Farmácia atingidos. *Expresso*, [s. l.], 28 jan. 2023. Tecnologia. Disponível em: <https://expresso.pt/sociedade/tecnologia/2023-01-28-Ciberativistas-russos-lancam-ataque-europeu.-Sites-da-DGS-e-Faculdade-de-Farmacia-atingidos-86a5d2f0>. Acesso em: 6 mar. 2026.

SERVIÇO Nacional de Saúde. [Lisboa]: Ministério da Saúde, c2026. Disponível em: <https://www.sns24.gov.pt/>. Acesso em: 6 mar. 2026.

SHAW, James; SEKALALA, Sharifah. Health data justice: building new norms for health data governance. *NPJ Digital Medicine*, [s. l.], v. 6, n. 30, p. 1-4, 2023. DOI: <https://doi.org/10.1038/s41746-023-00780-4>.

SOUSA, Marcelo Rebelo de; MATOS, André Salgado de. *Direito administrativo geral: introdução e princípios fundamentais*. 3. ed. Lisboa: Dom Quixote, 2008. t. 1.

TAYLOR, Mark J. Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement. *Medical Law Review*, [s. l.], v. 23, n. 3, p. 348-374, 2015. DOI: <https://doi.org/10.1093/medlaw/fwv018>.

TECNOLOGIAS de Informação e Comunicação. [Lisboa]: Ministério da Saúde, c2025. Disponível em: <https://www.spms.min-saude.pt/tecnologias-de-informacao-e-comunicacao/>. Acesso em: 29 abr. 2025.

TRANSPARÊNCIA. In: SERVIÇO Nacional de Saúde. [Lisboa]: Ministério da Saúde, c2026. Disponível em: <https://transparencia.sns.gov.pt/explore/?sort=modified>. Acesso em: 6 mar. 2026.

UNIÃO EUROPEIA. *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). Bruxelas: EUR-Lex, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 6 mar. 2026.

VUKOVIC, Jakov; IVANKOVIC, Damir; HABL, Claudia; DIMNJAKOVIC, Jelena. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. *Archives of Public Health*, [s. l.], v. 80, n. 115, p. 1-9, 2022. DOI: <https://doi.org/10.1186/s13690-022-00866-7>.

YUAN, Bocong; LI, Jiannan. The policy effect of the General Data Protection Regulation (GDPR) on the digital public health sector in the European Union: an empirical investigation. *International Journal of Environmental Research and Public Health*, [s. l.], v. 16, n. 1.070, p. 1-15, 2019. DOI: <https://doi.org/10.3390/ijerph16061070>.

Responsabilidade e licenciamento

O conteúdo deste artigo é de responsabilidade exclusiva de seu(s) autor(es) e está publicado sob a licença Creative Commons na modalidade *atribuição, uso não comercial e compartilhamento pela mesma licença* (CC BY-NC-SA 4.0 DEED). Disponível em: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Acesse todas as edições da
Revista de Informação Legislativa

www.senado.leg.br/ril