UNIVERSIDADE CATÓLICA PORTUGUESA

O Regulamento Governação de Dados e a proteção de dados pessoais

Alguns desafios de interoperabilidade

Juliana Catarina Sousa Pinto

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

UNIVERSIDADE CATÓLICA PORTUGUESA

O Regulamento Governação de Dados e a proteção de dados pessoais

Alguns desafios de interoperabilidade

Juliana Catarina Sousa Pinto

Orientadora: Professora Doutora Maria Filipa Urbano Calvão

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

Agradecimentos

Aos meus pais por serem os pilares inabaláveis da minha vida. Obrigada por todo o esforço que fizeram pela minha formação.

Ao Paulo, pelo amor e apoio ao longo desta jornada. A tua presença foi o conforto que me impulsionou nos momentos de dúvida.

À Professora Doutora Filipa Calvão, cuja orientação e conhecimentos partilhados foram fundamentais para a conclusão desta investigação.

À FUTURA, por cultivar o meu interesse pela proteção de dados e por proporcionar a oportunidade de aprofundar, diariamente, os meus conhecimentos nesta tão especial área do Direito.

Resumo

A presente dissertação tem como objetivo analisar de forma abrangente a interação entre o Regulamento Governação de Dados (RGD) e o Regulamento Geral sobre a Proteção de Dados (RGPD), com um foco específico nas questões relacionadas com a reutilização de dados pessoais detidos por organismos do setor público e com o altruísmo de dados. Tem como desafio identificar obstáculos e incoerências que emergem da interoperabilidade entre os regulamentos, formulando perguntas e propondo soluções para os dilemas de proteção de dados pessoais que daí decorrem. Através desta abordagem, almeja-se contribuir para o melhor entendimento do quadro normativo da UE no que tange à proteção de dados pessoais no contexto da estratégia europeia para os dados.

Palavras-chave: Regulamento Governação de Dados; RGD; RGPD; reutilização de dados; altruísmo de dados; proteção de dados pessoais.

Abstract

This dissertation aims to comprehensively analyze the interaction between the Data Governance Act (DGA) and the General Data Protection Regulation (GDPR), with a specific focus on issues related to the re-use of personal data held by public sector bodies and data altruism. It seeks to identify inconsistencies and challenges arising from the interoperability between the regulations, formulating questions and proposing solutions to the dilemmas of personal data protection that arise from this interaction. Through this approach, it aims to contribute to a better understanding of the EU regulatory framework regarding the protection of personal data in the context of the european data strategy.

Keywords: Data Governance Act; DGA; GDPR; data re-use; data altruism; personal data protection.

Lista de siglas e abreviaturas

Ac.	Acórdão
Art(s).	Artigo(s)
CE	Comissão Europeia
cfr.	Confrontar
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
EEE	Espaço Económico Europeu
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EM(s)	Estado(s) Membro(s)
GT do artigo 29º	Grupo de Trabalho do Artigo 29.º
LADA	Lei de Acesso aos Documentos Administrativos
OADR	Organização de Altruísmo de Dados Reconhecida
OSP	Organismo do Setor Público
p.	Página(s)
PME	Pequena Média Empresa
RGD	Regulamento Governação de Dados
RGPD	Regulamento Geral sobre a Proteção de dados
TFUE	Tratado sobre o Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
v.	Ver
v.g.	Por exemplo, verbi gratia

Índice

1. Introdução 7

2. Enquadramento: o Regulamento Governação de Dados 8

2.1. Contexto: a estratégia europeia para os dados 8

2.2. Objeto e âmbito de aplicação do Regulamento Governação de Dados 9

2.3. O Regulamento Governação de Dados e o RGPD: convergência ou conflito? 10

3. A reutilização de dados pessoais detidos por organismos do setor público 12

3.1. Condições para a reutilização de dados pessoais 14

3.2. Desafios da anonimização: como distinguir dados não pessoais de dados pessoais 15

3.3. E quando a anonimização não é possível? 18

4. Altruísmo de Dados 20

4.1. O conceito de altruísmo de dados 21

4.2. As organizações de altruísmo de dados 23

4.2.1. Obrigações das organizações de altruísmo de dados 24

4.2.2. Atividades das organizações de altruísmo de dados 26

4.3. Fundamento de licitude para o altruísmo de dados 27

4.4. O tratamento posterior dos DP no âmbito do altruísmo de dados 30

4.5. Direitos 32

4.6. A ambiguidade do conceito "interesse geral" 34

5. O equilíbrio entre o direito fundamental à proteção de dados e o incentivo à partilha de dados pessoais 37

6. Conclusão 39

Bibliografia 40

1. Introdução

No epicentro da atual revolução tecnológica, os dados emergem como o principal catalisador do avanço económico e social[1]. Embora frequentemente comparados ao "petróleo"[2], os dados destacam-se por serem uma fonte inesgotável de valor, com a singular capacidade de serem utilizados, reutilizados, agregados e combinados de maneiras infinitas de forma a impulsionar a inovação[3]. Deste modo, se utilizados de forma eficiente, os dados têm o potencial de transformar todos os aspetos da sociedade, nomeadamente aprimorar a qualidade dos cuidados de saúde, otimizar a eficiência dos sistemas de transporte e reduzir os custos associados aos serviços públicos.

Reconhecendo os desafios e o valor intrínseco dos dados, a UE lançou, em 2020, a estratégia europeia para os dados[4], que visa criar um mercado único para os dados, facilitando a sua livre circulação entre os EM. Esta estratégia representa um marco crucial na jornada da UE que tem como objetivo "tornar-se um modelo de liderança para uma sociedade que, graças aos dados, estará habilitada a tomar melhores decisões – nas empresas e no setor público"[5].

O RGD[6] foi o primeiro regulamento a ser publicado no âmbito da estratégia para os dados e vem reconhecer não só a importância estratégica dos DP, mas também a imperativa necessidade de orientar os rumos tecnológicos futuros, onde os dados assumirão um protagonismo ainda mais significativo.

Neste âmbito, surge a importante questão da interoperabilidade entre o RGD e o RGPD[7], dado que, o RGD também regula o tratamento de DP. Na presente dissertação visamos explorar a interação entre os dois diplomas, bem como as eventuais inconsistências, concentrando-nos, sobretudo, nas questões relacionados com a

[1] CE, 2020b, p. 1.
[2] Carrière-Swallow, 2019, p. 1.
[3] V. Vestager, 2021: "Data is not oil - it is a renewable resource that can be pooled, shared, reused ...".
[4] Este esforço da CE para democratizar o acesso aos dados, abre o caminho para um futuro onde a tecnologia serve a humanidade e não o contrário (CE, 2020a, p. 17).
[5] A estratégia europeia para os dados assenta em quatro pilares fundamentais: (i) promover um quadro de governação transetorial para o acesso e a utilização dos dados; (ii) investir em dados e no reforço das capacidades e infraestruturas da Europa para alojamento, tratamento e utilização de dados e interoperabilidade; (iii) capacitar as pessoas, investir em competências e nas PME; e, (iv) estabelecer espaços comuns europeus de dados em setores estratégicos e domínios de interesse público (v. CE, 2020b, p. 12-22).
[6] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados).
[7] Regulamento (EU) 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.

reutilização de DP detidos por OSP e com o altruísmo de dados[8]. Deixaremos para futuras investigações, dada a sua própria complexidade, os problemas e desafios relacionados com os serviços de intermediação dos dados, as transferências internacionais de dados e a criação do comité europeu da inovação de dados[9].

2. Enquadramento: o Regulamento Governação de Dados

2.1. Contexto: a estratégia europeia para os dados

O RGD, proposto pela CE em 2020 e aprovado pelo PE em 2022, é aplicável desde setembro de 2023. O RGD tem como base jurídica os art. 4.º/2/3 e 114.º do TFUE. Ao ser concebido como um regulamento, tem aplicabilidade direta nos EM, mitigando a morosidade inerente ao processo de implementação, evitando, em princípio, discrepâncias entre os EM e facilitando a criação de espaços comuns europeus de dados[10]. O RGD enquadra-se na estratégia europeia para os dados e a sua adoção surge como resposta à constatação de que, na UE, existem algumas barreiras à partilha e ao acesso a dados, que a CE pretende ultrapassar.

Efetivamente, tem-se assistido a uma concentração do poder e da capacidade tecnológica para o tratamento de dados nas mãos de um restrito número de entidades dominantes, as *Big Tech*[11], o que suscita obstáculos significativos, especialmente no que concerne ao desenvolvimento tecnológico para fins de interesse público[12]. Por outro lado, no relatório da avaliação de impacto da proposta do RGD, apontou-se o "problema" de os titulares dos dados não confiarem na partilha dos seus DP[13]. De facto, a falta de

[8] Deste modo, o âmbito deste trabalho limita-se à análise dos aspetos do RGD relacionados com a proteção de DP, os quais, representam um aspeto chave do regulamento.
[9] O caminho que conduziu ao atual RGD é fruto da reforma legislativa já iniciada em 2009 pela CE, que culminou, na adoção do RGPD em 2016, que representa expoente máximo desse processo (Moniz, 2023, p. 7 e 8).
[10] Para aproveitar o potencial dos dados em prol da economia e da sociedade europeias, a estratégia europeia para os dados, propôs a criação de espaços europeus comuns de dados em diversos domínios estratégicos, incluindo saúde, agricultura, indústria transformadora, energia, mobilidade, finanças, administração pública, competências e a nuvem europeia para a ciência aberta. Além disso, surgiram espaços de dados em áreas adicionais, como os meios de comunicação social e o património cultural. Estes espaços de dados serão progressivamente interligados para formar um mercado único de dados, potenciando ainda mais a cooperação e a partilha de informação entre os diferentes setores e partes interessadas (CE, 2020b).
[11] De facto, apesar da crescente produção diária de dados, a verdade é que o controlo sobre esses dados está maioritariamente concentrado nas designadas *Big Tech* (Birch, 2022, p. 8).
[12] Esta realidade reforça o desequilíbrio de poder nas sociedades modernas e prejudica a inovação, uma vez que está centrada nos lucros económicos e tem uma relevância limitada para o bem comum (Micheli, 2023, p. 3).
[13] CE, 2020a, p. 3-4.

confiança dos titulares dos dados e a complexidade dos regimes jurídicos e técnicos que regem a partilha dos dados têm limitado o potencial da sua utilização na economia europeia. Adicionalmente, a crescente abundância de dados tem sido acompanhada por desafios em termos de garantir o acesso aos mesmos, bem como a sua qualidade e fiabilidade[14]. Neste sentido, a criação de um mercado europeu para os dados[15], marca um ponto de viragem fundamental no panorama económico e social da UE. A estratégia europeia tem como principal objetivo facilitar a livre circulação e sem entraves de dados dentro do EEE, criando um ambiente propício para o desenvolvimento de negócios transfronteiriços e a oferta de serviços mais adaptados às necessidades individuais dos titulares dos dados[16].

Posto isto, as metas do RGD são ambiciosas[17]. Com o RGD, a UE reconheceu a necessidade urgente de criar um quadro regulamentar claro que aumente a confiança dos titulares dos dados, e, consequentemente, promova a partilha de dados de forma segura e transparente, enquanto respeita os direitos fundamentais dos cidadãos europeus, especialmente o direito fundamental à proteção de DP[18].

2.2. Objeto e âmbito de aplicação do Regulamento Governação de Dados

Nos termos do art. 1.º do RGD, que define o objeto e âmbito de aplicação do regulamento, o RGD regula quatro áreas: (1) a disponibilização de dados do setor público para reutilização; (2) a regulamentação da prestação de serviços de intermediação de dados[19]; (3) um regime para as organizações altruístas de dados; e (4) a criação de um comité europeu da inovação de dados[20]. Assim, num único regulamento, regula-se três

[14] Streinz, 2021, p. 43.
[15] "Os recentes avanços legislativos (...) em particular, o Regulamento de Governação de Dados, evidenciam a adoção de um modelo de mercado minimamente estruturado – aquele a que chamamos mercado 1.0" (Carneiro, 2023, p. 156).
[16] Hoerning, 2023, p. 5-9.
[17] Fischer, 2021, pp. 6-9.
[18] CE, 2020b, p. 1-2.
[19] O RGD define os prestadores de serviços de intermediação de dados como aqueles que fornecem "um serviço que visa estabelecer relações comerciais para efeitos de partilha de dados entre um número indeterminado de titulares dos dados e detentores dos dados, por um lado, e utilizadores de dados (...)" (art. 2.º/11) do RGD). De acordo com a CE, estas entidades são cruciais para garantir a concorrência justa e a disponibilidade de dados entre países e setores, especialmente para *start-ups* e PME. O RGD implementou um mecanismo de controlo para estes intermediários, baseado no registo obrigatório e na supervisão *ex-post* pelas autoridades competentes, incluindo sanções por infrações, aplicáveis a estas entidades (v. capítulo III – arts. 10.º a 15.º do RGD).
[20] O comité europeu da inovação de dados (EDIB) é um órgão técnico composto por especialistas representando as autoridades competentes, juntamente com outras instituições europeias e órgãos

áreas diferentes - os dados abertos, a economia dos dados e o altruísmo dos dados – que, aparentemente, não têm conexão entre si, mas, estão ligadas pelo objetivo comum de promover a partilha de dados existentes e a subsequente reutilização desses dados.

O RGD define dados[21] como "qualquer representação digital de atos, factos ou informações e qualquer compilação desses atos, factos ou informações, nomeadamente sob a forma de gravação sonora, visual ou audiovisual"[22]. Deste modo, a definição de "dados" do RGD abrange o conceito de "DP" conforme estipulado pelo RGPD, segundo o qual os DP são informações relativas a uma pessoa singular identificada ou identificável. Aliás, o art. 2.º/3 do RGD remete explicitamente para a definição de DP prevista no RGPD[23].

Assim, para se concretizar a visão da CE que "assenta nos valores e direitos fundamentais europeus, bem como na convicção de que o ser humano é e deve permanecer no centro"[24], as disposições previstas no RGD devem estar em conformidade com o disposto no RGPD, sempre que esteja em causa a regulação do tratamento de DP.

2.3. O Regulamento Governação de Dados e o RGPD: convergência ou conflito?

O conceito "GDPR mimesis"[25] tem sido objeto de discussão no contexto da regulamentação de dados na UE, referindo-se à tendência do quadro normativo pós-RGPD "imitar" este regulamento. O RGD é um exemplo claro do fenómeno em análise, demonstrando paralelismos significativos com o RGPD, que atualmente é a pedra angular do regime geral de proteção de DP[26]. Na verdade, o RGD remete várias vezes para o disposto no RGPD, especialmente nos casos que envolvem conceitos chave como "dados pessoais", "consentimento", "titular dos dados" e "tratamento", assim como no que diz respeito aos princípios fundamentais de proteção de dados[27].

especializados. As principais tarefas do EDIB serão aconselhar e auxiliar a CE, bem como propor orientações para os espaços de dados europeus comuns (v. capítulo VI – arts. 29.º a 30.º do RGD).

[21] Na verdade, a legislação da UE carece de uma definição uniforme de "dados". O RGD vem acrescentar mais uma camada de inconsistências entre várias leis secundárias ao estabelecer uma definição adicional (v. Streinz, 2021, p. 22-23).

[22] Art. 2.º/1) RGD.

[23] Art. 4.º/1 do RGPD.

[24] CE, 2020b, p. 4.

[25] Papakonstantinou, 2021, p. 1 e Miadzvetskaya, 2023, p. 14-19.

[26] Moniz, 2023, p. 7 e 8.

[27] Referências no RGD ao RGPD: considerando 4, 7, 8, 15, 30, 31, 35, 44, 46, 50, 51 e arts. 1.º/3. 2.º, 5.º/6, 9.º/2, 10.º/b) e 25.º/3. Por outro lado, o art. 2.º do RGD introduz um novo conjunto de conceitos: "detentores de dados", "utilizadores de dados", "dados" ou "organizações de altruísmo de dados" etc.

Por um lado, o paralelismo entre o RGD e o RGPD traz vantagens consideráveis. Ao adotar uma abordagem consistente com o RGPD, o RGD promove a harmonização e a coerência das normas de proteção de dados em toda a UE, o que proporciona segurança jurídica e facilita a conformidade e a compreensão das obrigações regulatórias. Além disso, o paralelismo, à partida, fortalece a proteção dos direitos dos titulares de dados, assegurando que os princípios fundamentais do RGPD são aplicados de forma abrangente em todas as áreas abordadas pelo RGD. Por outro lado, o paralelismo entre os dois regulamentos também apresenta desvantagens. Efetivamente, ao seguir os moldes do RGPD, o RGD pode falhar em abordar questões específicas e emergentes relacionadas com o incentivo à partilha e à disponibilização de dados[28]. Adicionalmente, embora o RGD remeta várias vezes para as disposições do RGPD, é fundamental compreender que cada regulamento possui contextos e objetivos próprios, os quais, como veremos, podem divergir em determinados pontos e, até, ser conflituantes.

Neste contexto, tal como referido na exposição de motivos que acompanha o texto da proposta do RGD, "a interação com a legislação em matéria de dados pessoais reveste-se de especial importância"[29]. Neste sentido, o art. 1.º/3 do RGD dispõe que "o direito da União e nacional em matéria de proteção de dados pessoais são aplicáveis a todos os dados pessoais tratados no âmbito do presente regulamento. Em especial, o presente regulamento aplica-se sem prejuízo dos Regulamentos (UE) 2016/679 (...). Em caso de conflito entre o presente regulamento e o direito da União em matéria de proteção de dados pessoais (...), prevalece o direito da União ou o direito nacional aplicável em matéria de proteção de dados pessoais"[30]. Ora, o próprio RGD reconhece a proteção de DP como um elemento fundamental para promover a confiança dos indivíduos e das organizações com vista a facilitar a partilha e a disponibilidade de dados para beneficiar a economia digital.

Deste modo, na medida em que o RGPD deve ser aplicado sempre que houver tratamento de DP, nas próximas secções exploraremos a interação entre o RGD e o RGPD, especialmente no contexto da reutilização de DP detidos por OSP[31] e no contexto da

[28] Papakonstantinou, defende que a "mimese" do RGPD é, em última análise, prejudicial – "o RGPD é um instrumento jurídico extremamente bem-sucedido que tem uma vida e uma história próprias. A proteção de DP da UE está atualmente ocupada a inclinar o planeta para uma proteção mais forte da privacidade dos indivíduos ao abrigo do dilúvio tecnológico. Este lugar está, portanto, ocupado. Qualquer nova iniciativa regulatória da UE terá de criar a sua própria história" (Papakonstantinou, 2021, p. 8).
[29] CE, 2020b, p. 1.
[30] Art. 1.º/3 do RGD.
[31] V. ponto 3 da presente dissertação.

partilha altruísta de dados[32], com o objetivo de avaliar a compatibilidade da aplicação dos regulamentos.

3. A reutilização de dados pessoais detidos por organismos do setor público

O capítulo II do RGD tem como principal objetivo desbloquear o potencial associado à reutilização de determinadas categorias de dados protegidos detidos por OSP[33]. Os OSP, definidos no RGD como "o Estado, as autoridades regionais ou locais, os organismos de direito público ou as associações formadas por uma ou mais dessas autoridades ou por um ou mais desses organismos de direito público"[34], desempenham um papel crucial na produção e recolha de grandes volumes de dados, representando, assim, uma aposta estratégica para promover a reutilização. O art. 2.º/ 2) do RGD, define reutilização como "a utilização, por pessoas singulares ou coletivas de dados detidos por organismos do setor público, para fins comerciais ou não comerciais diferentes da missão de serviço público para a qual foram recolhidos".

A questão da reutilização de dados detidos por OSP não é nova. Aliás, a Diretiva Dados Abertos[35] versa exatamente sobre essa questão. Em Portugal, a transposição desta Diretiva deu-se através da alteração à LADA[36], reforçando assim os princípios dos dados abertos e da transparência administrativa. Perante este cenário, torna-se relevante questionar os limites da aplicação da Diretiva Dados Abertos e do RGD no que diz respeito à reutilização de DP detidos por OSP. O RGD esclarece que o seu Capítulo II sobre a "reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público (...) aplica-se aos dados (...) protegidos por motivos de: (...) proteção dos dados pessoais, na medida em que os dados em causa não sejam abrangidos

[32] V. ponto 4 da presente dissertação.
[33] Capítulo II (arts. 3.º a 9.º) do RGD.
[34] Art. 2.º/17) do RGD.
[35] Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público.
[36] A Lei n.º 68/2021, de 26 de Agosto aprovou os princípios gerais em matéria de dados abertos e transpôs para a ordem jurídica interna a Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informação do setor público, alterando a Lei n.º 26/2016, de 22 de agosto. V. art. 2.º da LADA: "as entidades sujeitas às regras e princípios da administração aberta devem assegurar que os documentos e dados que produzam ou disponibilizem sejam, sempre que possível, abertos desde a sua conceção, tendo em vista a sua disponibilização futura aos cidadãos e organizações sociais".

pelo âmbito de aplicação da Diretiva (UE) 2019/1024"[37]. Por sua vez, a referida Diretiva "(...) não é aplicável a (...) documentos cujo acesso é excluído ou restrito por força dos regimes de acesso por motivos de proteção de dados pessoais, e partes de documentos acessíveis por força desses regimes que contêm dados pessoais cuja reutilização foi definida por lei como incompatível com a legislação relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, ou como comprometedora da proteção da privacidade e integridade da pessoa em causa, nomeadamente em conformidade com o direito nacional ou da União relativo à proteção dos dados pessoais"[38]. Ora, embora à primeira vista possa parecer que existe uma sobreposição entre o RGD e a Diretiva Dados Abertos, o legislador esclarece que o RGD abrange as categorias de dados detidos por OSP que são expressamente excluídas pela Diretiva. Concretamente, aplica-se a dados que não são acessíveis por motivos de confidencialidade comercial ou estatística e os que estão protegidos pela legislação de proteção de dados pessoais[39]. Deste modo, o RGD amplia significativamente o escopo da reutilização de DP, aplicando-se nos casos em que tal reutilização não seria possível ao abrigo da Diretiva[40]. Adicionalmente, o RGD procura reduzir a disparidade entre os EM no que concerne à regulação da reutilização de dados detidos por OSP[41].

O RGD introduz também um novo ator no âmbito da reutilização de dados, os organismos competentes. O art. 7.º especifica que os EM são obrigados a designar organismos competentes específicos[42], que têm como objetivo ajudar os OSP nas novas

[37] V. art. 3.º/1/d) do RGD. Especificamente, o RGD incide sobre os dados detidos por OSP protegidos por motivos de confidencialidade comercial (incluindo segredos comerciais, profissionais e empresariais), confidencialidade estatística, proteção da propriedade intelectual e proteção dos DP. O EDPB-EDPS criticam a redação do art. 3.º/1 do RGD, uma vez que agrupa sob a mesma categoria de "direitos protegidos" a proteção de dados pessoais, os direitos de propriedade intelectual e a confidencialidade comercial. No parecer conjunto, argumentaram que esta formulação sugere a ideia de que a regulação da proteção de dados impede a livre circulação dos mesmos, em vez de estabelecer as regras para o livre fluxo de DP, protegendo simultaneamente os direitos e interesses das pessoas envolvidas (v. EDPB-EDPS, 2021, p. 19).

[38] Art. 1.º da Diretiva Dados Abertos.

[39] Concretizando, apesar da Diretiva Dados Abertos não excluir automaticamente a reutilização de DP detidos por OSP, o RGD vem complementar a Diretiva Dados Abertos. Neste sentido, o considerando 9 do RGD dispõe que "os Estados-Membros deverão incentivar os organismos do setor público a criarem e disponibilizarem os dados em conformidade com o princípio "abertos desde a conceção e por defeito" referido no art. 5.º, n.º 2, da Diretiva (UE) 2019/1024 (...)". Deste modo, o RGD pretende encontrar um equilíbrio entre o incentivo à disponibilização de DP detidos por OSP para reutilização e os interesses dos titulares dos dados. Cfr. considerando 6 RGD.

[40] Cfr. considerando 9 e 10 do RGD e considerando 52 da Diretiva Dados Abertos.

[41] Note-se que o RGD não abrange os dados detidos por empresas públicas, organismos de radiodifusão de serviço público e suas filiais, instituições culturais e estabelecimentos de ensino, dados protegidos por razões de segurança pública e defesa nacional, bem como os dados que não se enquadrem no âmbito das missões de serviço público dos OSP em questão.

[42] Nos termos do art. 7.º/5 do RGD, o EM deve notificar a CE da identidade dos organismos competentes designados até 24 de setembro de 2023. Até ao dia de hoje, não temos conhecimento de que Portugal tenha

incumbências, decorrentes do capítulo II do RGD, nomeadamente, prestar orientações técnicas para o armazenamento e tratamento de dados, ajudar com a anonimização, supressão, aleatorização de dados e outras técnicas que garantam a privacidade, confidencialidade, integridade e acessibilidade dos DP[43]. Além disso, o art. 6.º abre a porta à cobrança de taxas pelos OSP que autorizem a reutilização de dados e, o art. 9.º estabelece como regra um prazo de decisão de dois meses a contar da data do pedido de reutilização.

Dito isto, os DP detidos por OSP estão abrangidos pelo capítulo II do RGD e, consequentemente, a reutilização de tais DP deve estar sujeita às disposições do RGPD. No entanto, como veremos, o alcance das obrigações impostas aos OSP no que diz respeito à disponibilização para reutilização de DP não é claro. Assim, cabe-nos agora analisar quais as condições de reutilização de DP detidos por OSP nos termos do RGD.

3.1. Condições para a reutilização de dados pessoais

A reutilização deve ser realizada em conformidade com uma série de condições estabelecidas no art. 5.º do RGD. Desde logo, as condições para a reutilização devem cumprir os princípios de não discriminação, transparência e proporcionalidade, além de serem justificadas no que respeita às categorias de dados, às finalidades da reutilização e à natureza dos dados cuja reutilização é permitida[44]. Adicionalmente, devem ser publicadas as condições exigidas para autorizar a reutilização, bem como o procedimento para solicitar a mesma[45].

Ao analisar o n.º 3 do art. 5.º do RGD, surgem algumas questões de interpretação acerca da obrigação de os OSP cumprirem os requisitos delineados nessa norma, relativamente à anonimização dos dados. Concretamente, o referido preceito dispõe que "os organismos do setor público asseguram (...) que a natureza protegida dos dados seja preservada. Podem estabelecer os seguintes requisitos: o acesso para fins de reutilização de dados só deve ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, tiver assegurado que os dados foram anonimizados, no caso dos dados pessoais" (sublinhado nosso). Ora, é complexo

nomeado a autoridade competente, existindo apenas uma Portaria n.º 10/2024, que dispõe que a Agência para a Modernização Administrativa, I. P. (AMA, I. P.) garante a implementação do Regulamento (UE) 2022/868, do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo à governação europeia de dados.

[43] Art. 7.º/4/c) do RGD.

[44] Art. 5.º/2 do RGD.

[45] Art. 5.º/1 do RGD.

compreender como é que as expressões sublinhadas, aparentemente contraditórias ("podem"/"devem"), são implementadas na prática[46]. Na nossa perspetiva, a palavra "podem" (opção facultativa) deveria ser substituída por "devem" (obrigação legal), de forma a dissipar quaisquer incertezas quanto à obrigação dos OSP de anonimizarem os DP antes de os disponibilizarem para reutilização. De facto, consideramos que a anonimização dos DP detidos por OSP, tal como definidos no art. 3.º/1/d) do RGD, é uma medida crucial para assegurar a adequada e efetiva proteção dos DP[47].

Todavia, questão diferente será saber se as técnicas de anonimização empregadas pelos OSP são eficazes de forma a tornarem os DP em "dados anonimizados" e, por isso, não sujeitos ao RGPD. De facto, a discussão relativamente à fronteira entre DP e dados anónimos não é nova. O próprio RGPD, além do disposto no considerando 26 e no art. 4.º/1, não fornece orientações sobre as condições necessárias para determinar a anonimização dos dados. Ora, o RGD ao adotar uma definição de dados bastante ampla[48] não resolveu o debate já existente na doutrina[49] quanto à dificuldade de distinguir claramente os conceitos de "dados não pessoais" e "DP", sendo que esta distinção se afigura de especial relevância no que diz respeito à reutilização de dados detidos por OSP.[50]

Deste modo, na medida em que, o RGD estabelece, ao longo do seu texto, regras diferentes consoante os tratamentos envolvam DP ou dados não pessoais[51], consideramos importante tecer algumas considerações sobre o conceito de anonimização.

3.2. Desafios da anonimização: como distinguir dados não pessoais de dados pessoais?

Para que se aplique o regime excecional do RGPD para os dados anonimizados, nos termos do qual, esses dados são excluídos da proteção do RGPD, é necessário que seja objetivamente demonstrado que não existe capacidade material para associar os dados anonimizados a uma pessoa singular determinada, direta ou indiretamente, mesmo que através da utilização de outros conjuntos de dados, informações ou medidas técnicas que

[46] Carovano, 2023, p. 9.
[47] Dito isto, o art. 5.º/3/b) e c) do RGD também prevê que os OSP podem/devem assegurar um ambiente de tratamento seguro, seja remoto ou físico.
[48] V. art. 2.º/1 do RGD e cfr. Purtova, 2018.
[49] Finck, 2020.
[50] Neste sentido, o EDPB-EDPS consideram que a confusão entre os dois conceitos é um dos principais motivos que está na origem das inconsistências entre o RGD e o RGPD (v. EDPB-EDPS, 2021, p. 16).
[51] Baloup, 2021, p. 9.

possam estar disponíveis para terceiros[52]. O principal ponto de debate[53] resulta do crescimento do potencial de re-identificação dos titulares dos dados na sequência do avanço das tecnologias e da inteligência artificial, que permitem, em muitas situações, que exista uma probabilidade razoável de re-identificação dos titulares[54]. Efetivamente, quanto maior for a quantidade de informações disponíveis e mais frequente for a partilha e reutilização de dados, mais complexo se torna garantir a preservação da anonimização[55].

Dessa forma, no contexto da reutilização de DP detidos por OSP, consideramos que a pseudonimização, por si só, não é suficiente[56]. A pseudonimização, ao reduzir a possibilidade de associação entre um conjunto de dados e a identidade original de um titular representa uma medida de segurança útil, porém, não consubstancia um método de anonimização de DP, pois, ainda existe a possibilidade de re-identificação dos indivíduos com o uso de informações adicionais[57]. Por conseguinte, os "dados pseudonimizados" são, ainda, DP.

Todavia, de forma contraditória a este entendimento, o RGD abrange a possibilidade de a reutilização versar sobre dados não anonimizados, nos casos em que a anonimização comprometer a utilidade dos dados para o reutilizador. Concretamente, o considerando 15 afirma que "antes de serem transmitidos, os dados pessoais deverão ser anonimizados, de modo a impedir a identificação dos titulares dos dados (...). Nos casos em que o fornecimento de dados anonimizados (...) não responda às necessidades do reutilizador, sob reserva de terem sido cumpridos todos os requisitos para a realização de uma avaliação de impacto em matéria de proteção de dados e a consulta da autoridade de

[52] De facto, os dados apenas são anonimizados e, por isso, não sujeitos às disposições do RGPD, quando a anonimização é irreversível. No entanto, quanto mais dados forem combinados com outras informações disponíveis, mais difícil será garantir a anonimização devido ao aumento do risco de re-identificação para os titulares dos dados (Henriksen-Bulmer, 2016, p. 1184-1192).

[53] De facto, muitas das soluções para esta, e outras, discussões serão determinadas pela jurisprudência, particularmente pelo TJUE. Por exemplo, numa decisão proferida em abril de 2023 (SRB v. EDPS, 2023), o tribunal estabeleceu que a transmissão de dados pseudonimizados a um destinatário que não possui meios adicionais para reidentificar a pessoa singular referida não qualifica esses dados como dados pessoais, contribuindo para a melhor compreensão da aplicação prática do disposto no RGPD.

[54] V. considerando 26 do RGD.

[55] Atualmente, a crescente interconexão e digitalização dos dados, conduz a que informações anteriormente consideradas não identificáveis podem, de facto, revelar a identidade de um indivíduo quando combinadas ou analisadas em conjunto (v. GT do art. 29º, 2014).

[56] Neste sentido, o próprio n.º 5 do art. 5.º do RGD dispõe que "os reutilizadores ficam proibidos de reidentificar qualquer titular dos dados a quem os dados digam respeito", o que implica que o reutilizador dos dados receba os dados do OSP já anonimizados.

[57] O art. 4.º/5 do RGPD define "pseudonimização" como "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável".

controlo, nos termos dos arts. 35.º e 36.º do Regulamento (UE) 2016/679, e os riscos para os direitos e interesses dos titulares dos dados tenham sido considerados mínimos, poderá ser permitida a reutilização dos dados nas instalações ou de forma remota num ambiente de tratamento seguro. Tal poderá consistir num mecanismo adequado para a reutilização de dados pseudonimizados"[58]. Na nossa perspetiva, a utilização dos conceitos de pseudonimização e anonimização de forma indiscriminada, sem considerar as diferenças nos efeitos na esfera jurídica dos titulares consoante a utilização de um ou outro mecanismo e sem fornecer orientações claras sobre quando e como cada um deve ser utilizado, pode acarretar incertezas jurídicas e comprometer a aplicação consistente do RGD[59].

Deste modo, a não ser que exista um fundamento de licitude válido que legitime o tratamento de DP, consideramos que a reutilização de dados, tal como regulada pelo capítulo II do RGD, deveria versar apenas sobre dados anonimizados. Neste sentido, a doutrina nacional defende que há casos em que a figura do segredo administrativo é necessária, sendo que o segredo constitui um "instrumento de desenvolvimento da função administrativa e de defesa dos espaços de autonomia e de privacidade"[60]. Alexandre Sousa Pinheiro sustenta a importância de estabelecer uma relação entre os arts. 268.º[61] e 35.º da CRP sempre que esteja em causa o tratamento de DP[62]. Por outras palavras, deve existir um equilíbrio entre o princípio da transparência e a proteção de DP, sendo que a proteção dos DP deve ser encarada como um limite ao direito de acesso à informação administrativa[63].

Perante estas inconsistências, torna-se evidente a necessidade de esclarecer e harmonizar as disposições do RGD quanto à distinção entre DP e dados não pessoais, bem como entre pseudonimização e anonimização. Além disso, é crucial garantir que os

[58] Em virtude da consciência dos riscos associados, o regime jurídico dos dados pseudonimizados não os exclui completamente da proteção do RGPD. Por outras palavras, os dados pseudonimizados continuam a ser considerados dados pessoais e, por isso, estão abrangidos pela legislação de proteção de dados (Torbay, 2020, p. 57).
[59] É frequente que ocorra confusão entre os termos "pseudonimização" e "anonimização". Efetivamente, não são raros os casos em que um conjunto de dados é descrito como "anonimizado" quando, na verdade, ainda contém DP que apenas estão pseudonimizados (v. ICO, 2022, p. 3).
[60] Antunes, 1993, p. 16.
[61] O art. 268.º/2 da CRP estabelece um direito abrangente, assegurando a todos os cidadãos a possibilidade de acesso a arquivos e registos administrativos, independentemente da existência de um procedimento administrativo em curso, v. Amaral, 2017, p. 599.
[62] Pinheiro, 2016, p. 35.
[63] O acesso a documentos nominativos (art. 3.º/1/b) da LADA), ou seja, que incluam DP, não deve ser diretamente permitido. Requer-se uma análise cuidadosa, utilizando critérios definidos para tal efeito. Cfr. Coutinho, 2017, p. 152.

OSP têm os recursos necessários para anonimizar efetivamente os DP que disponibilizam para reutilização[64].

3.3. E quando a anonimização não é possível?

Nos termos do considerando 15 do RGD, existem situações em que a reutilização pode versar sobre dados pseudonimizados. Nestes casos, como vimos, consideramos que o tratamento de DP deve estar obrigatoriamente sujeito às disposições do RGPD, nomeadamente ao princípio da licitude[65]. Neste sentido, o art. 5.º/6 do RGD estipula que "sempre que a reutilização de dados não possa ser autorizada em conformidade com as obrigações estabelecidas nos n.ºs 3 e 4 do presente art. e não exista base jurídica para a transmissão de dados ao abrigo do Regulamento (UE) 2016/679, o organismo do setor público envida todos os esforços, nos termos do direito da União e nacional, para ajudar os potenciais reutilizadores a obter o consentimento dos titulares dos dados (...)" (sublinhado nosso).

Ora, a norma em análise não deixa claro qual é o papel do OSP no apoio aos reutilizadores para a obtenção do consentimento para a finalidade de reutilização, no caso em que não exista outro fundamento de licitude que legitime a reutilização dos DP. No texto da proposta do RGD, o art. 5.º/6 dispunha que, nos casos em que a reutilização não possa ser concedida "o organismo do setor público deve ajudar os reutilizadores a obter o consentimento dos titulares dos dados" (sublinhado nosso). Neste sentido, as autoridades de controlo e de supervisão consideraram que a disposição estabelecia uma obrigação vinculativa para os OSP em apoiar na obtenção do consentimento[66]. No entanto, na versão final do RGD, o legislador substituiu a expressão "o organismo do setor público deve ajudar" por "o organismo do setor público envida os esforços necessários" (sublinhado nosso). Esta alteração contribui para aumentar a ambiguidade em torno do conteúdo do art. 5.º/6 do RGD[67].

Ainda no que diz respeito à posterior obtenção do consentimento para a reutilização, levanta-se a questão de saber qual é o fundamento de licitude, ao abrigo do RGPD, para entrar em contacto com os titulares dos dados para obter o seu consentimento, questão que não é esclarecida no RGD. Adicionalmente, o texto do RGD não esclarece claramente

[64] Cfr. Buttow, 2023, p. 12-15.
[65] Art. 5.º/1/a) do RGPD.
[66] EDPB-EDPS, 2021, p. 39-35.
[67] Esteves, 2023, p. 223.

quem é responsável por obter um consentimento válido nos termos do art. 7.º do RGPD. Essa falta de clareza pode levar a ambiguidades e incertezas quanto às responsabilidades das partes envolvidas. Se a responsabilidade recair sobre os OSP, é importante considerar o desequilíbrio de poder que muitas vezes existe na relação entre o titular dos dados e as autoridades públicas. Esse desequilíbrio pode dificultar a obtenção de um consentimento genuíno e livremente dado pelos titulares dos dados, comprometendo, assim, a conformidade com os princípios de proteção de dados e os direitos dos indivíduos[68].

Neste contexto, é ainda crucial salientar que os requisitos delineados nos nºs 3 e 4 do art. 5.º do RGD, que abrangem o acesso e reutilização de dados num ambiente de tratamento seguro, não devem ser interpretados como substitutos de um fundamento de licitude válido para o tratamento. Pelo contrário, devem ser vistos como condições cumulativas que devem ser atendidas juntamente com a necessidade de existir, pelo menos, um dos fundamentos de licitude previstos no art. 6.º do RGPD[69].

Portanto, torna-se crucial esclarecer o teor do n.º 6 do art. 5.º do RGD, estabelecendo de forma clara qual seria o fundamento jurídico para o tratamento de DP necessário para estabelecer contacto com os titulares dos dados para a finalidade de obter o consentimento[70]. Além disso, é imperativo estabelecer os perfis de responsabilidade decorrentes desta nova regulação tanto para os OSP quanto para os organismos competentes e reutilizadores de dados, especialmente em situações em que a anonimização não foi adequadamente realizada ou verificada, o ambiente de tratamento seguro não foi configurado, ou os requisitos necessários para um consentimento válido não foram atendidos.

[68] No mesmo sentido, veja-se o considerando 43 do RGPD: "A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir um fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa (...)". Neste exemplo, as autoridades públicas devem recorrer a outros fundamentos, nomeadamente, às alíneas c) e e) do n.º 1 do art. 6.º do RGPD (v., Moniz, 2023, p. 73 e 74 e GT29, 2018, p. 7 e 8.
[69] Gerritsen, 2023, p. 4.
[70] Cordeiro, 2023, p. 117 e ss.

4. Altruísmo de Dados

O RGD veio, pela primeira vez, regulamentar a possibilidade de os titulares disponibilizarem voluntariamente os seus DP para fins altruístas[71]. Esta possibilidade é especificamente regulada pelo capítulo IV do RGD[72] que estabelece as diretrizes para o registo das organizações de altruísmo de dados. Este capítulo abrange também a criação do manual de regras, os requisitos de conformidade exigidos para estas organizações, a designação das autoridades competentes neste âmbito e a implementação do formulário europeu de consentimento para o altruísmo de dados[73].

O art. 2.º/16) do RGD define o altruísmo de dados como "(...) a partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais ou na autorização, por parte de outros detentores dos dados, da utilização dos seus dados não pessoais, sem que esses titulares ou detentores procurem ou recebem uma gratificação que vá além de uma compensação geral pelos custos em que incorrem ao disponibilizarem os seus dados, para fins de interesse geral, previstos no direito nacional, se aplicável, tais como os cuidados de saúde, a luta contra as alterações climáticas, a melhoria da mobilidade, a facilitação do desenvolvimento, produção e divulgação de estatísticas oficiais, a melhoria da prestação dos serviços públicos, a elaboração de políticas públicas ou a investigação científica de interesse geral"[74].

Para compreender o objeto e âmbito do altruísmo de dados, é necessário, desde logo, esclarecer o que se entende por "autorização do detentor dos dados". O RGD define "detentor dos dados" no seu art. 2.º/8) como "uma pessoa coletiva, incluindo organismos do setor público e organizações internacionais, ou uma pessoa singular que não seja o titular dos dados no que diz respeito aos dados específicos em causa, que, em conformidade com o direito da União ou o direito nacional aplicáveis, tem o direito de conceder acesso a determinados dados pessoais ou dados não pessoais ou de os partilhar". Esta definição levanta algumas dúvidas[75], sobretudo no que concerne à abrangência e legitimidade da autorização do detentor de dados. Ao longo do texto do RGD, não fica

[71] Na verdade, à luz do RGPD, já era possível que os titulares dos dados consentissem o tratamento dos seus DP por exemplo, para fins de investigação científica. Neste sentido, o RGD vem apenas formalizar e regulamentar a partilha voluntária de dados (v. Halvorson, 2014, p. 1-2 e EDPB-EDPS, 2021, p. 39).
[72] Cfr. arts. 16.º a 25.º do RGD.
[73] Bulla, 2022, p. 20 a 38.
[74] Art. 2.º, 16) do RGD.
[75] Vardanyan defende que interpretação sistemática das normas citadas pode conduzir a uma situação em que a "autorização" do RGD e o "consentimento" do RGPD se tornam conceitos concorrentes. (Vardanyan 2022, p. 101).

claro, em muitos casos[76], se a autorização dos detentores dos dados abrange o tratamento de DP, dados não pessoais, ou ambos. No entanto, o caso do altruísmo de dados é uma exceção positiva, na medida em que, o RGD esclarece que os detentores dos dados só podem autorizar a partilha dos seus dados não pessoais para fins altruístas, excluindo explicitamente dessa autorização os DP.

Posto isto, sucintamente, o altruísmo de dados fundamenta-se na autorização concedida pelos detentores para a partilha dos seus dados não pessoais ou no consentimento dos titulares para a partilha dos seus DP, para fins de interesse geral e sem fins lucrativos[77].

Considerando que a partilha voluntária de DP com as organizações de altruísmo de dados consubstancia um tratamento de DP, o RGD dispõe que o direito da União em matéria de proteção de DP é aplicável a esses tratamentos[78]. Portanto, é fundamental analisar as questões de proteção de DP que emergem da partilha voluntária de dados com base no consentimento dos titulares para fins de interesse geral. Nas páginas seguintes, exploraremos a relação entre o Capítulo IV do RGD e o RGPD, analisando como a aplicação simultânea das normas estabelecidas pelos regulamentos se materializa na prática.

4.1. O conceito de altruísmo de dados

Dado o caráter inovador do termo "altruísmo" no contexto da legislação sobre proteção de DP, é prudente, desde logo, fazer uma distinção clara entre este conceito e outras expressões semelhantes que possam causar confusão.

Em primeiro lugar, o conceito "altruísmo de dados", previsto no RGD, não se confunde com a noção conexa "doação de dados". Com efeito, a palavra "doação" foi deliberadamente evitada pelo legislador no RGD, uma vez que a doação implica a transferência de propriedade e o direito fundamental à proteção de DP é inalienável[79]. Adicionalmente, no contexto do regime da doação, uma vez efetuada a doação, o doador perde o controlo sobre o bem doado. Em contrapartida, no domínio do altruísmo de dados, o titular que partilha os seus DP tem o direito de ser informado sobre os termos e

[76] Por exemplo, em situações em que os dados são utilizados para fins comerciais, no âmbito dos serviços de intermediação dos dados (capítulo III do RGD). Nestes casos, a ambiguidade do que se entende por "autorização dos detentores dos dados" pode levar a interpretações variadas e a potenciais violações dos direitos dos titulares dos dados.
[77] Veil, 2021, p. 2.
[78] Art. 1.º/3 do RGD e EDPB-EDPS, 2021, p. 40.
[79] Hansen, 2021, p. 17.

condições em que os seus DP serão tratados. Além disso, o titular dos dados mantém a prerrogativa de revogar o seu consentimento a qualquer momento, conferindo-lhe, assim, um controlo permanente e efetivo sobre a utilização dos seus DP[80].

Por outro lado, o altruísmo de dados também não deve ser confundido com o conceito "solidariedade de dados". Efetivamente, enquanto que o altruísmo de dados parte do pressuposto que, ao agir de forma altruísta, as pessoas estão a ajudar os outros em detrimento dos seus próprios interesses individuais, a solidariedade em matéria de dados baseia-se na convicção de que fazer algo pelos outros não necessariamente tira algo da pessoa que o faz[81]. Em poucas palavras, a solidariedade tem como foco a distribuição equitativa dos riscos e benefícios das práticas digitais, facilitando apenas os tratamentos de dados que têm potencial para criar valor público[82]. Por outro lado, como veremos, o altruísmo de dados baseia-se no conceito de interesse geral.

De uma perspetiva técnica, o altruísmo dos dados pode ser descrito como a partilha voluntária de DP para o benefício da sociedade. Ilustrando, vários exemplos de altruísmo surgiram durante a pandemia de Covid-19, onde foram desenvolvidas várias aplicações[83] para diminuir o risco de contaminação, contribuindo para proteger a saúde pública[84]. Em Portugal, a aplicação STAYAWAY, que visava contribuir para a interrupção das cadeias de infeção, tinha uma vertente voluntária, dando a possibilidade de o utilizador controlar os DP tratados pela aplicação em várias etapas[85]. Neste sentido, a pandemia de Covid-19 serviu como exemplo paradigmático que evidenciou a necessidade de regulamentar o tratamento de DP sob a ótica do altruísmo de dados[86]. O RGD emerge como resposta a esta necessidade premente, visando estabelecer uma cultura de partilha de dados para fins altruístas. De forma a atingir esse objetivo e a promover a confiança dos titulares, o RGD

[80] Adicionalmente, ao contrário do que acontece com as doações, a partilha altruísta de dados permite que os dados possam ser utilizados por várias partes ao mesmo tempo, sem perda de utilidade para nenhum dos intervenientes. V. Paal, 2023, p.1323.
[81] Um dos principais objetivos da solidariedade dos dados é garantir que uma parte justa dos lucros resultantes da utilização comercial de dados seja devolvida às pessoas que tornaram possível o uso dos dados em primeiro lugar (Prainsack, 2023, p. 1 e 2).
[82] Para mais desenvolvimentos sobre a teoria da solidariedade dos dados, v. Prainsack, 2022.
[83] Outros exemplos (não exaustivos) de aplicações através das quais os titulares fornecem os seus dados pessoais de forma voluntária para fins de interesse geral: Open SCHUFA; SmartCitzen e Europe Plan Against Cancer.
[84] CE, 2019, p. 17.
[85] CNPD, 2020, pp. 1 e 8.
[86] Kamocki, 2023, p. 2.

introduziu um novo interveniente na cadeia de valor associada aos dados – as organizações de altruísmo de dados[87].

4.2. As organizações de altruísmo de dados

No contexto do altruísmo de dados, diversos intervenientes desempenham papéis significativos, cada um contribuindo para a dinâmica da partilha de dados. Em concreto, o altruísmo de dados pode implicar a intervenção dos seguintes atores: (i) o titular dos DP; (ii) o detentor dos dados não pessoais; (iii) as organizações de altruísmo de dados; (iv) os utilizadores de dados; e (v) a autoridade competente para o registo[88]. Neste âmbito, as organizações de altruísmo de dados ocupam uma posição central, desempenhando um papel fundamental na facilitação e promoção de práticas transparentes e éticas de partilha de dados.

O capítulo IV do RGD estabelece um sistema de registo voluntário[89], no qual as entidades que realizem atividades de altruísmo de dados se podem inscrever para se registarem como "organização de altruísmo de dados reconhecida na União" (OADR). O principal objetivo destas normas é permitir que os titulares dos dados (e os detentores, no caso dos dados não pessoais) partilhem os seus dados para fins de interesse geral com maior transparência e confiança.

Para que o altruísmo de dados se concretize, é necessário que cada EM designe uma ou mais autoridades competentes para o registo das OADR. Para esse efeito, os EM podem criar uma ou mais entidades ou recorrer a entidades já existentes. Todavia, estas entidades devem ser distintas e não relacionadas com qualquer OADR e funcionar de forma independente das mesmas[90]. As autoridades competentes devem exercer as suas tarefas de forma imparcial e transparente, devendo ter à sua disposição os recursos financeiros e humanos necessários para levar a cabo essas tarefas[91].

[87] De acordo com a CE, prevê-se que até ao ano de 2028 existam cerca de 1250 organizações a facilitar o altruísmo de dados, com a participação de cerca de 5 milhões de cidadãos e 500 empresas. Cfr. CE, 2020b, pp. 32 e ss.
[88] Paseri, 2024, p. 136.
[89] V. art. 18.º do RGD.
[90] Art. 23.º do RGD.
[91] Bencze, 2023 p. 23.

4.2.1. Obrigações das organizações de altruísmo de dados

Para assegurar a integridade e a confiança no seu funcionamento, as OADR devem cumprir um conjunto de obrigações, conforme delineado pelo RGD.

Em primeiro lugar, as OADR devem operar sem fins lucrativos, garantindo assim que as suas atividades são conduzidas exclusivamente em prol do bem comum, sem qualquer motivação financeira. Além disso, devem ser juridicamente independentes de qualquer entidade que opere com fins lucrativos e realizar as suas atividades de altruísmo de dados através de uma estrutura separada das suas outras atividades, de forma a assegurar a imparcialidade e a independência das suas operações[92]. Dito isto, as OADR distinguem-se dos prestadores de serviços de intermediação de dados previstos no capítulo III do RGD, na medida em que estes últimos visam "estabelecer relações comerciais para efeitos de partilha de dados entre um número indeterminado de titulares dos dados e detentores dos dados, por um lado, e utilizadores de dados, por outro, através de meios técnicos, jurídicos ou outros (...)". Pelo contrário, o altruísmo de dados consiste na partilha de dados sem a intenção de obter recompensas financeiras, ou seja, não são estabelecidas relações comerciais entre os intervenientes[93].

Em segundo lugar, para serem reconhecidas, as OADR devem atender a um conjunto de requisitos de transparência, nomeadamente, manter registos completos e atualizados sobre os tratamentos de dados e, apresentar um relatório anual de atividades à autoridade competente[94]. Adicionalmente, devem oferecer garantias específicas para proteger os direitos e interesses dos titulares dos dados, nomeadamente prestar informações relevantes sobre o tratamento de DP aos titulares dos dados, não utilizar os DP para outros objetivos que não os de interesse geral com os quais o titular dos dados consentiu, implementar os instrumentos necessários para obter e retirar o consentimento, e implementar as medidas de segurança necessárias e adequadas[95]. Por último, deverão, ainda, cumprir o conjunto de regras previstos no art. 22.º[96].

---

[92] Note-se que ao longo de todo o diploma nunca é definido, de forma clara, o conceito de "organização de altruísmo de dados", nem das atividades por elas levadas a cabo. Considerando, por exemplo, a exigência de as organizações de altruísmo de dados realizarem as suas atividades de altruísmo de dados através de uma estrutura separada das suas outras atividades, é imperativo saber qual é o âmbito exato das "atividades de altruísmo de dados" (Baloup, 2021, p. 44).

[93] V. art. 2.º/11)/16) do RGD.

[94] Art. 20.º do RGD.

[95] Art. 21.º do RGD.

[96] O art. 22.º do RGD estipula um "conjunto de regras" que deverá ser adotado pela CE, através de atos delegados, em cooperação com as OADR e com as partes interessadas. O futuro manual de regras deverá estabelecer os requisitos de informação adequados para garantir que o consentimento dos titulares dos dados é informado (n.º 1, alínea a)), as medidas técnicas e de segurança a adotar pelas OADR (n. º1, alínea b)),

Após cumprir todos os requisitos necessários, as organizações que pretendam realizar atividades altruístas de dados podem registar-se como OADR, o que lhes confere o direito de utilizar um logótipo comum, sendo incluídas no registo público da CE e no registo nacional do EM correspondente[97].

No entanto, é importante salientar que as OADR que efetuem tratamentos de DP devem, para além das obrigações adicionais decorrentes do RGD, cumprir também as obrigações estabelecidas pelo RGPD[98]. Esta sobreposição de obrigações levanta a questão de saber se alguma entidade se irá sujeitar ao cumprimento adicional dos requisitos do RGD, quando, em muitas situações, poderiam realizar os mesmos tratamentos ao abrigo do RGPD. De acordo com a doutrina, como apenas as entidades que cumprem as obrigações previstas no RGD se podem registar enquanto OADR, os custos decorrentes dessas obrigações adicionais são compensados com a reputação e confiança comprovadas que as organizações alcançam quando recebem a certificação formal e o logótipo comum[99]. No entanto, consideramos que este "rótulo" pode ter um efeito contraproducente ao objetivo de fomentar a partilha de dados. De facto, como consequência das regras do RGD, as organizações de altruísmo de dados não registadas podem ser percebidas como menos confiáveis em comparação às OADR, mesmo estando em conformidade com as disposições do RGD. Isso parece injusto, especialmente considerando que o registo em análise é voluntário[100].

Assim, o capítulo IV do RGD impõe uma série de obrigações às OADR sem proporcionar benefícios visíveis ou tangíveis para essas entidades[101]. Esta abordagem levanta questões importantes sobre a eficácia do regulamento em incentivar a partilha de dados altruístas. Além disso, como veremos, a falta de uma definição clara das atividades

os roteiros de comunicação (n.º 1, alínea c)) e as recomendações sobre as regras de interoperabilidade (n.º 1, alínea d)). O art. 18.º/e) do RGD dispõe que as OADR devem cumprir com o "conjunto de regras" até 18 meses após a entrada em vigor dos atos delegados.

[97] O logótipo comum e os registos auxiliam os titulares dos dados a identificar as organizações confiáveis para a partilha altruísta de dados. V. art. 17.º do RGD.

[98] De acordo com Veil, só no RGPD existem 68 obrigações aplicáveis às OADR nos casos em que estas efetuem tratamentos de DP (v. Veil, 2021, p. 6).

[99] Cfr. Paal, 2023, p. 1326. Como vimos, as obrigações adicionais são, essencialmente, manter e atualizar os registos das atividades, o relatório anual, as obrigações adicionais de informar os titulares e estar em conformidade com as regras a definir nos termos do art. 22.º/1 do RGD.

[100] Na verdade, organizações não governamentais (ONGs), fundações, iniciativas ad hoc e outros responsáveis pelo tratamento com fins altruístas podem até ficar em desvantagem em comparação com responsáveis pelo tratamento registados, uma vez que podem sentir a pressão de se registar como OADR para evitar serem considerados "menos confiáveis" (v, Veil, 2021, p. 8).

[101] Paal, 2023, p. 1325.

das OADR no RGD amplia essas preocupações, abrindo espaço para interpretações diversas e potencialmente conflituantes das obrigações impostas às organizações.

4.2.2. Atividades das organizações de altruísmo de dados

No que diz respeito às atividades de tratamento de dados realizadas pelas OADR, o considerando 50 do RGD estipula que "as organizações de altruísmo de dados reconhecidas deverão poder recolher dados relevantes diretamente de pessoas singulares e coletivas ou tratar dados recolhidos por terceiros" [102]. Além disso, nos termos do art. 20.º/2/c) do RGD, como vimos, as OADR devem elaborar um relatório anual de atividades, sendo que esse relatório deve conter "uma lista de todas as pessoas singulares e coletivas às quais foi permitido tratar os dados detidos pela entidade"[103]. Com base nos preceitos citados, é possível depreender que as OADR podem levar a cabo as seguintes atividades de tratamento de dados: (i) recolher e armazenar os dados para fins de interesse geral; (ii) tratar os dados recolhidos para fins de interesse geral; e, (iii) permitir a terceiros tratar os dados recolhidos para fins de interesse geral[104].

Neste sentido, apenas a última das atividades acima elencadas implica a intermediação[105]. Surge, portanto, a indagação sobre como os titulares dos dados podem depositar confiança na capacidade das OADR de garantir que os terceiros com quem partilham os dados cumpram integralmente as normas de proteção de DP. Efetivamente, uma das principais questões que daqui pode emergir é se os titulares podem confiar que os terceiros tratarão os seus DP apenas nas condições e para as finalidades para as quais deram o seu consentimento[106].

O texto da proposta do RGD tentou acautelar esta questão no seu então art. 19.º, estabelecendo uma espécie de "obrigação de fiscalização" para as organizações de altruísmo de dados, nomeadamente para garantir que os dados partilhados altruisticamente "(..) não são utilizados para outros fins que não os objetivos de interesse geral para que o tratamento foi autorizado"[107]. Ora, da interpretação do art. 19.º da proposta do RGD depreende-se que as OADR foram inicialmente concebidas como

[102] Considerando 50 do RGD
[103] Obrigação semelhante à prevista no art. 30.º do RGPD, nos termos do qual "cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade".
[104] Micheli, 2023, p. 21-22.
[105] Cfr. Ditfurth, 2022, p. 290-291.
[106] CE, 2020a, pp. 71-81.
[107] V. art.19.º/ (2) da Proposta do RGD.

"supervisoras e aplicadoras", incumbindo-lhes verificar e fiscalizar o cumprimento das disposições previstas no RGD, nomeadamente verificar se os terceiros cumprem os princípios fundamentais relativos ao tratamento de DP previstos no art. 5.º do RGPD[108]. No entanto, a verdade é que, esta "obrigação de fiscalização" não foi transposta para a versão final do RGD. Por sua vez, de acordo com o atual art. 21.º/2 do RGD, as OADR têm apenas a obrigação de não utilizar "(...) os dados com outros objetivos que não os de interesse geral com os quais o titular dos dados (...) autoriza o tratamento"[109]. Assim, ao não existir qualquer referência à obrigação de fiscalização, presume-se que as OADR apesar de terem a obrigação de não utilizarem os DP disponibilizados pelos titulares dos dados para outras finalidades que não as de interesse geral com que o titular consentiu, estão isentas de controlar se os terceiros a quem disponibilizam os DP tratam os DP de acordo com as leis de proteção de dados aplicáveis[110]. Esta análise levanta preocupações quanto ao princípio da responsabilidade previsto no art. 5.º/2 do RGPD, especialmente porque, como veremos, o fundamento de licitude para a partilha de DP para fins altruístas é, em princípio, o consentimento dos titulares dos dados.

4.3. Fundamento de licitude para o altruísmo de dados

No que diz respeito ao fundamento de licitude para o tratamento de DP para fins altruístas, o considerando 50 do RGD dispõe que "(...) regra geral, o altruísmo de dados deverá basear-se no consentimento dos titulares dos dados (...)"[111]. Embora alguns autores considerem que o consentimento para o altruísmo de dados configura um "novo modelo de consentimento"[112], a verdade é que o RGD dispõe que o consentimento no âmbito do

[108] Os princípios relativos ao tratamento de dados pessoais ((i.) licitude, lealdade e transparência; (ii.) limitação das finalidades; (iii) minimização dos dados; (iv) exatidão; (v.) limitação da conservação; (vi.) integridade e confidencialidade; e, (vii.) responsabilidade previstos no art. 5.º e no considerando 39 do RGPD são o "coração" do regime geral de proteção de DP. Cfr. Moniz, 2023, p. 65.
[109] Ver art. 21.º/2 do RGD.
[110] É crucial destacar que as responsabilidades adicionais impostas pelo RGD às OADR não se estendem aos utilizadores dos dados. Por exemplo, embora as OADR sejam obrigadas a operar sem fins lucrativos, isso não implica que os utilizadores também devam fazê-lo. Reconhecemos que uma restrição tão rígida poderia limitar excessivamente as atividades das entidades. No entanto, também é importante considerar que os titulares dos dados podem não estar plenamente conscientes dos riscos envolvidos na partilha dos seus DP com os subsequentes intervenientes da cadeia de dados. Uma possível solução poderia ser a implementação de obrigações de transparência específicas para com os titulares dos dados. Além de serem informados sobre os destinatários dos dados e as categorias de DP por estes tratados, os titulares dos dados poderiam também ser informadas sobre a natureza empresarial do utilizador dos dados (ou seja, se tem fins lucrativos ou não), bem como das suas atividades. Cfr. Baloup, 2021, pp. 44-46.
[111] Consideramos que a expressão "regra geral" merecia, neste âmbito, uma interpretação textual. Cfr. considerando 45; 46 e 52 e arts. 2.º, 16); 21.º/5 e 25.º do RGD.
[112] Lalova-Spinks, 2023, p. 5.

altruísmo dos dados deve estar em conformidade com os requisitos para um consentimento válido na aceção do RGPD[113]. Além da questão supra, o art. 2.º, 5) do RGD remete para o RGPD quanto à definição aplicável de consentimento[114]. Assim, coloca-se a questão de como são cumpridos os requisitos para um consentimento válido ao abrigo do RGPD no contexto da partilha altruísta de dados, especialmente no que concerne à informação que deve ser prestada ao titular dos dados e às finalidades específicas para as quais os dados são recolhidos.

Efetivamente, o RGD vem ressuscitar a discussão em torno do consentimento enquanto base de licitude[115]. A utilização do consentimento como fundamento de licitude para alguns tratamentos de DP tem sido desde há muito criticada[116]. A doutrina[117] critica a atribuição de um lugar de destaque ao consentimento no âmbito dos fundamentos de licitude do RGPD por diversas razões, nomeadamente, por se traduzir, muitas das vezes, numa falsa ideia de controlo sobre os DP que o titular dos dados disponibiliza e porque a maioria das pessoas se limita a consentir sem o fazer conscientemente, sendo que os titulares não compreendem realmente o que estão a consentir[118]. De acordo com os pontos de vista mais céticos[119], há poucas razões para acreditar que, no âmbito da partilha de dados para fins altruístas, o consentimento cumpra integralmente os requisitos previstos no art. 4.º/11) do RGPD, isto é, seja "uma manifestação de vontade, livre, específica, informada e explícita[120], pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[121].

De acordo com o art. 25.º e considerando 52 do RGD, para facilitar a recolha de dados com base no altruísmo, as organizações de altruísmo de dados devem utilizar um

[113] Cfr. arts. 7.º e 9.º do RGPD.
[114] Cfr. art. 2.º/5) do RGD e art. 4.º/11) do RGPD.
[115] Uma das alterações mais significativas introduzidas pelo RGPD, em contraste com a Diretiva 95/46/CE, foi a mudança de paradigma que reduziu a ênfase no consentimento como base legal predominante, substituindo a abordagem baseada no consentimento que se revelou ineficaz. Para mais detalhes, consultar Solove, 2012, pp. 180 ss.
[116] Cfr. Cordeiro, 2021, p. 111 e Custers, 2013, p. 437.
[117] V. Cordeiro, 2020, p. 169.
[118] No entanto, embora estas críticas sejam válidas, a solução oposta, isto é, a de caber ao legislador determinar que dados pessoais podem ser partilhados e em que termos é suscetível de críticas ainda mais onerosas. Cfr. Cordeiro, 2020, p. 170.
[119] Ruohonen, 2021, 441 e ss.
[120] A expressão "explícita" encontra-se apenas na versão portuguesa do RGPD, resultando de um erro de tradução, pelo que onde consta explícita deve ler-se inequívoca (v. Moniz, 2023, p. 172).
[121] Para o consentimento ser válido, deve cumprir uma série de requisitos, nomeadamente: (i.) ser livre, específico e informado; (ii.) o titular deve poder revogar o seu consentimento a qualquer momento. De facto, a necessidade de obter o consentimento agrava, só por si, os deveres dos responsáveis pelo tratamento, devendo garantir uma proteção mais efetiva dos titulares dos dados.

formulário europeu de consentimento para o altruísmo de dados que visa permitir a obtenção do consentimento para o tratamento de DP num formato uniforme, promovendo a confiança dos titulares[122]. No entanto, é crucial ressaltar que o formulário não cumpre automaticamente os requisitos do consentimento previstos pelo RGPD. De acordo com o GT do art. 29.º para o consentimento ser informado é necessário, pelo menos, que o titular dos dados tenha acesso às seguintes informações: "(i) identidade do responsável pelo tratamento; (ii) finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento; (iii) que tipo de dados serão recolhidos e utilizados; (iv) a existência do direito de retirar o consentimento; (v) quando pertinente, informações acerca da utilização dos dados para decisões automatizadas, e; (iv.) sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no art. 46.º".[123]

O requisito "específico" do consentimento decorre do art. 6.º/1/a) do RGPD e pode ser dividido em três dimensões: (i) especificação em função da finalidade como salvaguarda contra o desvirtuamento da função; (ii.) granularidade nos pedidos de consentimento; e (iii.) separação clara entre as informações relacionadas com a obtenção do consentimento para a atividade de tratamento de dados e as informações sobre outras questões[124]. No que diz respeito à primeira dimensão, afigura-se de especial relevância no contexto do altruísmo dos dados, analisarmos as questões jurídicas que emergem dos casos em que não é possível, no momento da recolha do consentimento, definir as finalidades do tratamento[125].

De acordo com a interpretação do EDPB[126], em determinadas situações excecionais relacionadas com a investigação científica, onde não é possível identificar todas as finalidades do tratamento no momento da recolha dos DP, o considerando 33 do

[122] O formulário europeu de consentimento para o altruísmo de dados é apenas uma ferramenta que visa facilitar a partilha de DP, não sendo o fundamento de licitude para esse tratamento. Além disso, o formulário não coloca as OADR numa posição privilegiada comparativamente com outros responsáveis pelo tratamento de dados, apenas as confronta com termos gerais do consentimento. Cfr. Micheli, 2023, p. 46-49 e Paal, 2023, p. 1324-1325.
[123] GT do art. 29.º, 2020, pp. 14 e 15.
[124] Reforçando este entendimento, o art. 5.º/1/b) do RGD, dispõe que os DP devem ser recolhidos para finalidades determinadas, apenas podendo ser tratados à luz desses fins. V. GT do art. 29.º, 2020, p. 13.
[125] Agravando esta questão, o RGD vem ainda complicar a compreensão das noções de "finalidade" e "operação de tratamento". Nos termos do RGPD, o consentimento está associado a uma ou mais *finalidades* específicas (art. 6.º/1/a) do RGD). No entanto, o n.º 3 do art. 25.º do RGD, dispõe que "(...) os titulares dos dados possam dar e retirar o seu consentimento relativamente a uma *operação* especifica de tratamento de dados, em conformidade com os requisitos do Regulamento (UE) 2016/679" (itálico nosso). Ora, somos da opinião que os dois conceitos – operação e finalidade - não são equivalentes uma vez que, podem ser efetuadas várias operações de tratamento para uma única finalidade.
[126] EDPB-EDPS, 2021, p. 7 e ss.

RGPD permite uma descrição mais geral da finalidade[127]. Portanto, quando as finalidades de um determinado projeto de investigação científica não podem ser totalmente especificadas à partida, o responsável pelo tratamento deve procurar outras formas de garantir que os requisitos essenciais do consentimento sejam cumpridos, por exemplo, permitindo que os titulares consintam apenas com determinada área específica da investigação cujos contornos já estão bem definidos no momento da recolha dos DP[128]. No mesmo sentido, o considerando 50 do RGD vem complementar o disposto pelo RGPD, afirmando que "as finalidades de investigação científica podem basear-se no consentimento para determinados domínios da investigação científica, desde que sejam respeitados padrões éticos reconhecidos para a investigação científica, ou apenas para certos domínios ou partes de projetos de investigação"[129]. No entanto, o RGD não fornece qualquer clarificação adicional sobre a possibilidade da utilização do consentimento mais geral[130].Deste modo, consideramos que os titulares dos dados devem saber para que fins os seus DP serão utilizados e não devem ser influenciados a partilhar mais dados do que os necessários para a finalidade pretendida, meramente por estar em causa uma partilha altruísta de dados[131].

Deste modo, a conformidade com todas as obrigações relativas ao consentimento, conforme delineado no art. 7º do RGPD, revela-se uma tarefa ainda mais desafiadora no contexto do altruísmo de dados. Este cenário suscita diversas questões complexas que não encontram respostas explícitas no texto do RGD.

4.4. O tratamento posterior dos DP no âmbito do altruísmo de dados

A utilização, no considerando 50 do RGD, da expressão "regra geral" parece significar que, embora o consentimento seja o fundamento de licitude preferencial para o

[127] Note-se, todavia, que esta exceção não pode aplicar-se a projetos futuros que ainda nem sequer estão definidos. Cfr. EDPB-EDPS, 2021, p. 9.
[128] É importante ressaltar que esta exceção delineada no c onsiderando 33 não deve ser interpretada como uma brecha que permite ao responsável pelo tratamento desviar-se do princípio fundamental da limitação das finalidades e da obrigação de especificidade que deve cumprir ao recolher o consentimento dos titulares dos dados (GT do art. 29.º, 2020, p. 35 e 36).
[129] V. considerando 50 do RGD.
[130] Conforme destacado pelo EDPB-EDPS no documento "Joint Opinion 03/2021", as considerações referentes ao então considerando 38 da proposta do RGD (agora considerando 50) deveriam ser incorporadas na parte substantiva do regulamento, especialmente no que diz respeito à definição de consentimento amplo. Além disso, essa definição deveria incluir uma distinção clara entre (i.) consentimento para áreas específicas da investigação científica; (ii.) tratamento adicional para fins científicos, históricos ou estatísticos; e, (iii.) tratamentos para fins de interesse geral. No entanto, a versão final do RGD não incorporou as considerações do EDPB-EDPS, não refletindo o conteúdo do considerando 50 na parte substantiva do Regulamento (v. EDPB-EDPS, 2021, pp. 41 e 42).
[131] CE, 2020b, pp. 27 e ss.

tratamento de DP para fins altruístas, não é o único fundamento de licitude possível. Esta interpretação levanta alguma confusão uma vez que, parece contraproducente existir uma partilha altruísta de dados sem que o titular dos DP tenha partilhado, voluntariamente, os seus DP com a organização de altruísmo de dados. No entanto, se olharmos da perspetiva do tratamento posterior dos DP[132], pode existir uma justificação plausível para a expressão "regra geral".

Relativamente ao tratamento posterior de DP, o considerando 50 do RGD remete para o art. 5.º/1/b) e 89.º/1 do RGPD, reforçando a presunção de compatibilidade de certas finalidades prevista no RGPD. Neste sentido. de acordo com o RGD, "(...) o tratamento posterior para fins de investigação científica ou histórica ou para fins estatísticos não deverá (...) ser considerado incompatível com as finalidades iniciais"[133]. No entanto, o capítulo IV do RGD não fornece qualquer orientação adicional sobre o tratamento posterior de DP no âmbito do altruísmo de dados.

Uma interpretação restrita do RGPD significaria que a recolha de DP por organizações de altruísmo de dados poderia ser considerada como finalidade inicial, enquanto qualquer outra operação de tratamento posterior efetuada com esses DP constituiria um tratamento posterior ou utilização secundária[134]. Neste sentido, ao disponibilizar a terceiros os DP partilhados pelos titulares dos dados numa base altruística, a organização de altruísmo de dados estaria a levar a cabo um tratamento posterior. Isto significaria que, antes de partilharem os dados com terceiros, as organizações de altruísmo de dados teriam de efetuar o teste da compatibilidade previsto no art. 6.º/4 do RGPD[135].

No entanto, o consentimento para altruísmo de dados, conforme delineado no considerando 50 e no art. 25.º do RGD, parece abranger os tratamentos de DP realizados por terceiros[136]. Nesta ótica, as atividades de tratamento levadas a cabo pelos utilizadores de dados, que receberam DP das organizações de altruísmo de dados, parecem estar incorporadas na finalidade inicial, uma vez que a intenção de disponibilizar esses DP para

[132] Embora existam várias designações (tratamento subsequente, finalidade secundária...), a expressão "tratamento posterior" foi a usada pelo TJUE no Ac. Digi, C-77/21.
[133] Cfr. considerando 50 do RGPD e Cordeiro, 2020, p. 158.
[134] V. Shabani, 2020, p. 128-134.
[135] O teste da compatibilidade exige uma avaliação minuciosa de vários fatores, nomeadamente: o contexto da recolha dos DP, as expectativas razoáveis das pessoas em causa relativamente à reutilização dos dados, o impacto do tratamento posterior dos dados nos titulares e as garantias adotadas pelo responsável pelo tratamento para assegurar a licitude do tratamento (v. Cordeiro, 2021, p. 167 e ss.).
[136] Reforçando esta posição está o facto de os titulares dos dados poderem revogar o seu consentimento de operações de tratamento específicas. Deste modo, o consentimento fornecido pelo titular dos dados parece abranger os tratamentos realizados pelos utilizadores de dados. Cfr. art. 25.º do RGD.

fins altruístas constituiu a razão principal para a obtenção do consentimento[137]. Adotando-se esta interpretação, as normas do RGPD relativas ao tratamento posterior de dados não se aplicariam[138]. Neste sentido, sustentamos a visão de que o objetivo subjacente à estratégia europeia para os dados, que visa facilitar o acesso aos dados, só será verdadeiramente concretizado se prevalecer esta interpretação, desde que se assegure, simultaneamente, o respeito pelos princípios fundamentais de proteção de dados. No entanto, é crucial considerar que tudo depende da informação que é prestada ao titular dos dados no momento em que este dá o seu consentimento.

Chegados a este ponto, consideramos que é essencial encontrar uma resposta para a questão de como distinguir a finalidade inicial dos tratamentos posteriores no contexto do altruísmo de dados, sob pena de colocarmos em causa a segurança jurídica. Como vimos, as duas interpretações possíveis das regras do RGD conduzem a dois entendimentos opostos da forma como o RGPD deve ser aplicado pelas organizações de altruísmo de dados, ou seja, ou as disposições sobre o tratamento subsequente dos dados teriam de ser cumpridas por estas organizações, ou não.

4.5. Direitos

Ao explorarmos a interoperabilidade entre o RGD e o RGPD, é fundamental analisar como é que o capítulo IV do RGD se articula com o capítulo III do RGPD, que se dedica aos "direitos do titular dos dados"[139].

O considerando 52 do RGD dispõe que "a fim de promover a confiança e de proporcionar segurança jurídica adicional e facilidade de utilização no que toca ao processo de concessão e de retirada do consentimento deverá ser elaborado e utilizado, no contexto da partilha altruísta de dados, um formulário europeu de consentimento para o altruísmo de dados". Além disso, o art. 22.º do RGD determina que a CE deve adotar atos delegados para completar o regulamento, incluindo a definição de requisitos técnicos e de segurança adequados, bem como os instrumentos para dar e retirar o consentimento.

Ora, das cláusulas acima citadas, é óbvio que o RGD enfatiza o direito de o titular de dados retirar o seu consentimento no âmbito do altruísmo de dados. Todavia, o RGD

[137] Becker, 2022, pp. 135 e ss.
[138] Veja-se o art. 6.º/4 do RGPD que densifica o princípio da limitação das finalidades, na sua dimensão relativa aos tratamentos subsequentes. O art. estabelece uma série de requisitos exemplificativos que o responsável pelo tratamento deve cumprir para aferir se determinada finalidade subsequente é compatível com a finalidade inicial. Cfr, Cordeiro, 2020, pp. 119 e 120.
[139] Art. 12.º a 23.º do RGPD.

não tece quaisquer considerações quanto à forma como os titulares poderão exercer os restantes direitos previstos no referido capítulo III do RGPD, nomeadamente, o direito de acesso, retificação, apagamento e portabilidade. Esta opção do legislador pode sugerir que as disposições do RGPD relativamente ao exercício de direitos devem ser aplicadas na íntegra, sem qualquer recomendação ou obrigação adicional decorrente do altruísmo de dados.

No entanto, considerando as especificidades das relações jurídicas em análise, defendemos que o RGD deveria detalhar de forma mais explícita a obrigação das OADR cumprirem as regras para o exercício dos direitos dos titulares dos dados decorrentes do RGPD. Nesse sentido, seria adequado que o art. 22.º acima citado estipulasse que a CE, além de adotar um conjunto de regras para a obtenção e revogação do consentimento, também esclarecesse os mecanismos através dos quais os direitos dos titulares dos dados podem ser exercidos no contexto do altruísmo de dados.

No que diz respeito ao direito de retirar o consentimento[140], embora não esteja explicitamente incluído no capítulo dedicado aos direitos dos titulares dos dados, o art. 7.º/3 do RGPD estabelece que o titular tem o direito de revogar o consentimento previamente concedido para o tratamento dos seus DP. Consequentemente, o responsável pelo tratamento não deve, em qualquer circunstância, criar entraves ao exercício deste direito. Aliás, o consentimento deve ser tão fácil de retirar como foi de dar[141], devendo o titular dos dados ser informado, previamente à recolha do consentimento, da possibilidade de o retirar, sem que, todavia, seja comprometida a licitude das operações já realizadas ao abrigo do consentimento inicial[142]. Importa também mencionar que o titular tem o direito de solicitar o apagamento dos seus dados ao abrigo do art. 17.º do RGPD, que confere ao titular a faculdade de "obter do responsável pelo tratamento dos seus dados pessoais"[143]. No entanto, a aplicação destes direitos pode suscitar questões complexas no contexto do altruísmo de dados, especialmente quando os dados são usados para fins de investigação científica. Na verdade, o apagamento de dados já utilizados em pesquisas em andamento pode, em certas circunstâncias, ser praticamente inviável[144].

[140] V., v.g., o considerando 46, 52, o art. 21.º/3 e o art. 22.º/1/a) /b) do RGD.
[141] V. art. 7.º/3 do RGPD.
[142] Alves, 2023, pp. 65 e 66.
[143] O direito ao apagamento é o reflexo da jurisprudência do TJUE na decisão *Google Spain, C-131/12* que reconheceu ao titular dos dados o direito "a ser esquecido" ou à supressão.
[144] Lalova-Spinks expressa reservas sobre a eficácia do mecanismo de altruísmo de dados em simplificar o quadro normativo para a partilha de DP no âmbito da investigação científica. Há uma preocupação generalizada entre os investigadores de que tal mecanismo possa, paradoxalmente, complicar os

Adicionalmente, dada a complexidade das relações jurídicas que emergem da prática de altruísmo de dados, é fundamental estabelecer mecanismos que garantam que todos os intervenientes sejam notificados sobre o exercício dos direitos pelo titular dos dados. Caso contrário, tal exercício pode não ter um impacto prático, uma vez que os intervenientes não notificados da revogação ou apagamento podem, inadvertidamente, continuar o tratamento de DP sem um fundamento legal válido[145]. Por exemplo, o n.º 2 do art. 17.º do RGPD estipula que, quando o titular dos dados solicita o apagamento de dados pessoais que foram tornados públicos pelo responsável pelo tratamento, este deve tomar todas as medidas razoáveis para informar os responsáveis que estão efetivamente a tratar esses DP, para que removam quaisquer ligações a esses dados, bem como quaisquer cópias ou reproduções dos mesmos[146]. Além disso, o art. 19.º do RGPD obriga o responsável pelo tratamento a notificar os destinatários aos quais os DP foram divulgados de qualquer eliminação realizada em resposta a um pedido do titular, a menos que tal notificação seja impossível ou implique um esforço desproporcionado. Neste contexto, defendemos que estas obrigações sejam igualmente impostas ao responsável pelo tratamento envolvido na partilha altruísta de dados, seja este um terceiro ou a OADR, garantindo assim que os direitos dos titulares dos dados sejam rigorosamente protegidos.

Em suma, a interação entre o RGD e o RGPD requer clarificação, particularmente em relação à gestão eficaz do consentimento e à implementação do direito ao apagamento. Contudo, ainda é prematuro avaliar a eficácia dos mecanismos para a revogação do consentimento, dado que os atos delegados previstos no art. 22.º do RGD ainda não foram adotados[147].

4.6. A ambiguidade do conceito "interesse geral"

No contexto do RGD, a partilha altruísta de dados deve contribuir para objetivos de "interesse geral". No entanto, o texto do RGD apenas fornece alguns exemplos não

procedimentos de consentimento e intensificar a carga burocrática (para mais desenvolvimentos, v. Lalova-Spinks, 2023, p. 4; Castela, 2023 e Gefenas, 2022).

[145] Baloup, 2021, p. 38 e ss.

[146] Cordeiro, 2020, p. 274 e 275.

[147] De qualquer das maneiras, o responsável pelo tratamento, seja ele a OADR ou um terceiro, deverá sempre tomar as precauções devidas para permitir o exercício de direitos adequado por partes dos titulares dos dados. Cfr. Moniz, 2023, p. 169 e ss.

exaustivos[148] de possíveis objetivos de interesse geral, sendo que a definição do conceito permanece uma questão em aberto que suscita dúvidas[149].

Uma das principais questões que surge diz respeito à possível relação entre o conceito de "interesse geral" estabelecido pelo RGD e o fundamento de licitude "interesse público" previsto no art. 6.º/1/e) do RGPD. Efetivamente, a escolha do termo "geral" em vez de "público" no RGD carece de justificação nos documentos que acompanharam a proposta do regulamento[150]. Aliás, a avaliação de impacto e a exposição de motivos contribuíram para a ambiguidade e incerteza do conceito "interesse geral", uma vez que utilizam um terceiro termo quando se referem ao altruísmo de dados - "bem comum"[151]. Consideramos que a intenção do legislador foi desassociar o altruísmo de dados do fundamento de licitude "interesse público" previsto no RGPD, uma vez que a utilização desse conceito poderia levar a potenciais equívocos quanto ao fundamento de licitude a ser utilizado para a partilha altruísta de dados - se o consentimento (art. 6.º/1/a) do RGPD) ou o interesse público (art. 6.º/1/e) do RGPD).

Por outro lado, embora o RGD disponha que "os Estados-Membros podem definir políticas nacionais para o altruísmo de dados", não fica claro se é imperativo implementar e esclarecer a noção de "fins de interesse geral" e, em caso afirmativo, quem seria responsável por essa definição e de que maneira seria feita. Embora seja compreensível que os EM reivindiquem competências neste aspeto, a falta de clareza e a possibilidade de divergências nas implementações nacionais podem comprometer o principal objetivo das disposições de altruísmo de dados - construir confiança para que os titulares dos dados se sintam seguros ao partilhar os seus DP de forma altruísta para o bem comum.

---

[148] Por exemplo, o considerando 45 do RGD dispõe que "esses objetivos deverão incluir os cuidados de saúde, a luta contra as alterações climáticas, a melhoria da mobilidade, a facilitação do desenvolvimento, produção e divulgação de estatísticas oficiais, a melhoria da prestação de serviços públicos ou a preparação de políticas públicas O apoio à investigação científica também deverá ser considerado um objetivo de interesse geral".

[149] Na opinião conjunta, o EDPB e o EDPS consideraram que a CE deveria definir melhor o conceito de interesse geral no âmbito do altruísmo de dados, uma vez que "a falta de definição pode conduzir a incertezas jurídicas, bem como a um menor nível de proteção de DP na UE". (ver EDPB-EDPS, 2021, p. 41). Neste sentido, a versão final do RGD oferece mais especificações em comparação com a versão anterior, mas, ainda assim, continuam a existir muitas dúvidas sobre a definição do conceito "interesse geral".

[150] É importante observar que o termo "interesse geral" é utilizado ao longo do texto do RGD, abrangendo outros temas, além do altruísmo de dados. No entanto, em nenhum momento é oferecida uma definição precisa desse conceito. Por exemplo, o considerando 13 do refere que "os organismos do setor publico deverão respeitar o direito da concorrência ao estabelecerem os princípios de reutilização dos dados que detêm, evitando celebrar acordos que possam ter por objetivo ou efeito a criação de direitos exclusivos de reutilização de certos dados. Tais acordos só deverão ser possíveis quando tal se justifique e seja necessário para a prestação de um serviço ou o fornecimento de um produto no interesse geral" (sublinhado nosso).

[151] Cfr. CE, 2019, pp. 27 e ss e CE, 2020c.

Investigações recentes têm-se empenhado em elucidar o conceito de altruísmo de dados e, consequentemente, a definir o que se entende por interesse geral, explorando várias perspetivas sobre como o enquadramento normativo poderia efetivamente incentivar a partilha de dados[152]. Neste contexto, destaca-se a teoria da solidariedade dos dados[153], que propõe que o estímulo à partilha de dados se baseie no princípio da solidariedade, em vez do altruísmo. Segundo esta perspetiva, o critério principal para promover a partilha de dados em prol do bem comum é discernir entre tratamentos de dados que geram valor público significativo sem representar riscos inaceitáveis para os indivíduos, dos tratamentos de dados que não geram tal valor. Assim, esta teoria centra-se na criação de valor público através da utilização de dados, em vez de apenas visar a contribuição para o interesse geral (conceito subjetivo), como propõe o altruísmo de dados no RGD. Ao adotar o valor público como critério central para a governação de dados, estabelece-se um critério objetivo, impulsionando o progresso social e aproveitando o potencial dos dados para melhorar a vida das pessoas e das comunidades[154].

Em suma, a definição do conceito de "interesse geral" desempenha um papel crucial na operacionalização do altruísmo de dados. Ao adotar-se uma definição ampla e sem identificar limites claros, há o risco de muitos casos serem englobados no conceito de "interesse geral", resultando no que se denomina “Mathew Effect”[155]. Este fenómeno implica que as grandes empresas já estabelecidas, com amplos recursos à disposição, possam facilmente argumentar que os seus tratamentos de DP visam fins de interesse geral, quando, na verdade, estão associados a objetivos comerciais. Neste contexto, defendemos que a utilização de dados para fins altruístas deveria ser orientada pelo princípio de que apenas as partilhas que efetivamente geram valor público significativo (e não causem danos injustificados) devem ser incentivadas. Em vez de utilizar o critério de "interesse geral", que, tal como existe no RGD, é vago e demasiado abrangente, é

[152] Cfr. Prainsack, 2022, p. 11.
[153] V. ponto 4.1. da presente dissertação que desenvolve o conceito de altruísmo de dados e a teoria da solidariedade em comparação com o altruísmo.
[154] Para ajudar a avaliar o valor público dos tratamentos de DP, um grupo de investigadores da universidade de Viena lançou uma ferramenta para avaliar os riscos e os benefícios de casos específicos de utilização dos dados - o PLUTO. A ponderação dos riscos e benefícios realizada pela ferramenta resulta numa pontuação que indica o valor público da utilização de dados. O PLUTO teve a sua estreia durante o evento de lançamento do Laboratório de Digital Transformations for Health Lab (DTH-Lab) organizado no World Health Summit 2023 (15-17 de outubro, Berlim).
[155] O “Mathew Effect” consiste no fenómeno segundo o qual “os ricos ficam mais ricos e os pobres ficam mais pobres”. Para mais desenvolvimentos, v. Perc, 2014, pp. 1-2.

crucial adotar uma abordagem mais precisa e criteriosa na definição dos objetivos do altruísmo de dados, avaliando cuidadosamente os riscos e benefícios envolvidos.

5. O equilíbrio entre o direito fundamental à proteção de dados e o incentivo à partilha de dados pessoais

O RGD constitui uma mudança no paradigma regulatório da UE, ao promover ativamente a partilha de DP como forma de impulsionar a economia digital[156].

De facto, uma das principais questões que se levanta é o facto do RGD ver os dados como um objeto, o que contrasta com a abordagem do RGPD. Enquanto o foco principal do RGPD é garantir o cumprimento do direito à proteção dos DP, estabelecendo, para isso, requisitos rigorosos para o tratamento desses dados, o RGD parece apoiar a ideia de que os dados podem ser tratados como uma mercadoria negociável[157]. Por um lado, ao incentivar a partilha e a utilização de dados, a UE abre novos horizontes para a inovação, para o desenvolvimento de novos serviços e produtos e para a melhoria da tomada de decisão baseada em dados. Por outro lado, esta mudança exige uma gestão cuidadosa para assegurar que a partilha de dados não compromete a proteção dos titulares dos dados.

No que diz respeito a este último desafio, embora o RGD reconheça a prevalência do RGPD em caso de conflito, o equilíbrio entre os objetivos de fomentar a partilha de dados do RGD e a necessidade de garantir a conformidade com os princípios fundamentais de proteção de dados estabelecidos no RGPD, é crucial para evitar conflitos e garantir a segurança e a privacidade dos cidadãos europeus. Neste sentido, a declaração europeia sobre os direitos e princípios digitais reforça que a transformação digital deve ter o ser humano como centro das prioridades e preconiza a necessidade de uma conformidade das estratégias de transformação digital com os direitos fundamentais dos cidadãos[158]. Deste modo, consideramos que, tanto a reutilização de DP detidos por OSP, como a patilha altruísta de dados, devem sempre ter por base os princípios fundamentais da proteção de dados previstos no art. 5.º do RGPD[159].

---

[156] Costa, 2023, p. 622.

[157] Este entendimento é reforçado pelas definições "detentores dos dados" e "utilizadores dos dados" previstas no art. 2.º/8) e 9) do RGD, respetivamente.

[158] No Capítulo V, dedicado à segurança, proteção e capacitação, em particular no que se refere à privacidade e ao controlo individual dos dados, é reconhecido que o direito à proteção de dados pessoais engloba o controlo sobre a forma como os dados são utilizados e partilhados (cfr. CE, 2022).

[159] EDPB-EDPS, 2021, p. 9-19.

Outra questão que suscita preocupações e que evidencia a possibilidade de colocar a proteção de DP em segundo plano diz respeito aos desafios práticos da implementação do RGD, especialmente no que diz respeito às autoridades nacionais de proteção de dados. De facto, os deveres das autoridades nacionais de proteção de dados aumentam com o RGD. Por exemplo, de acordo com o considerando 15 do RGD, antes de fornecerem acesso a DP para posterior reutilização por terceiros, os OSP devem realizar avaliações de impacto e consultar as autoridades de controlo, em conformidade com os arts. 35.º e 36.º. O RGD refere também, no considerando 26, que os organismos competentes que prestam apoio aos OSP, não devem ter uma função de controlo, sendo que essa função está reservada às autoridades de controlo nos termos do RGPD. Ora, tendo em conta os problemas de recursos, coordenação e outras dificuldades já enfrentadas pelas autoridades de controlo na UE e, em particular, em Portugal, surge uma preocupação pertinente sobre como as disposições estipuladas no RGD serão, de facto, implementadas e executadas na prática[160].

Em suma, é de especial importância garantir que seja alcançado um equilíbrio entre o objetivo do RGD de promover a economia e o mercado de dados e o cumprimento das disposições estabelecidas pelo RGPD. Como as autoridades de controlo e de supervisão[161] têm vindo a salientar, a necessidade de aumentar os níveis de disponibilidade de DP em prol do mercado único digital, não pode traduzir-se na subversão da tutela do direito à proteção de DP. De facto, a proteção de DP deve constituir a base fundamental do RGD, assegurando que os direitos fundamentais dos cidadãos não sejam subordinados aos interesses económicos do mercado nem à procura pela prosperidade económica da União.

Na conceptualização da estratégia europeia para os dados, a CE compreendeu a necessidade de salvaguardar que os titulares estejam munidos dos mecanismos adequados para controlar os seus DP, de forma a aumentar a sua confiança no comércio jurídico, e, assim, contribuir com a partilha dos seus DP[162]. Contudo, como observamos, a ambiguidade e incoerência de algumas das disposições do RGD no que diz respeito ao tratamento de DP dificultam a prossecução desse equilíbrio, levantando preocupações

[160] Além disso, nos casos em que os EM nomeiem, quando possível, autoridades ou organismos competentes diferentes das autoridades de proteção de dados pode criar uma complexidade significativa para os intervenientes digitais e para os titulares dos dados, além de comprometer a consistência na aplicação das disposições do RGPD. Por outro lado, ao deixar à descrição dos EM a referida designação dos organismos competentes, também existe o risco de inconsistências e divergências nas abordagens regulatórias em toda a União. Cfr. Ruohonen, 2022, p. 106.
[161] EDPB-EDPS, 2021, p 42-44.
[162] CE, 2020b e considerando 16 do RGD.

quanto a um possível retrocesso na confiança dos titulares de dados, conquistada gradualmente ao longo dos últimos anos pelo RGPD[163].

6. Conclusão

No cenário atual, onde a digitalização permeia todos os aspetos da sociedade, a disponibilização e partilha de DP desempenham um papel vital no desenvolvimento económico e social. Neste contexto, o RGD emerge como uma peça fundamental da estratégia europeia para os dados, visando criar as condições necessárias ao desenvolvimento de um sistema confiável de partilha de DP.

No entanto, é crucial reconhecer os desafios e ambiguidades legais que surgem da interoperabilidade entre o RGD e o RGPD. Questões como a delimitação de DP e dados não pessoais, a falta de orientações claras para a reutilização de DP detidos por OSP e a incerteza em torno de conceitos jurídicos como "altruísmo de dados" e "interesse geral" levantam preocupações significativas quanto à possível erosão das garantias que o RGPD oferece.

Portanto, torna-se evidente que o RGD apresenta desafios consideráveis na sua articulação com o RGPD, suscitando interpretações diversas e prejudiciais do ponto de vista da proteção de DP. Para mitigar essas preocupações, é fundamental consolidar e esclarecer as questões levantadas ao longo da presente dissertação, garantindo a conformidade e complementaridade entre o RGD e o RGPD. De facto, consideramos que o sucesso do RGD dependerá da robustez do quadro legal, que deve fomentar não apenas inovação e o desenvolvimento económico, mas também a proteção do direito fundamental à proteção de DP.

Concluindo, é de extrema importância que a UE reafirme o seu compromisso com a proteção de dados[164], assegurando que o avanço em direção a uma economia digital próspera não seja feito à custa dos direitos individuais e da privacidade dos cidadãos. Assim, o grande desafio reside em garantir que a inovação tecnológica e a proteção de dados caminhem lado a lado, em benefício de toda a sociedade.

[163] A falta de clareza e de harmonização entre os diplomas legais são motivo suficiente para a perda da confiança dos cidadãos no mercado e nas políticas da União (v. Carneiro, 2023, p. 177).
[164] O RGPD permitiu "colocar os DP e o seu tratamento no centro das preocupações jurídicas", sendo que a UE assume um papel de liderança no domínio da proteção de dados (v. Cordeiro, 2020, p. 9).

Bibliografia

AMARAL, D. F. (2017). Curso de Direito Administrativo, Vol. II. Almedina.

ANTUNES, C. J. (1993). Mito e realidade da Transparência Administrativa. *Estudos em homenagem ao Prof. Doutor Afonso Rodrigues Queiró*. Universidade de Coimbra.

BALOUP, J., et. al. (2021). White Paper on the Data Governance Act. *CiTiP Working Paper 2021*. Disponível aqui.

BECKER, R., et. al. (2022). Secondary use of personal health data: when is it "further processing" under the GDPR, and what are the implications for data controllers? *Eur J Health Law*. (2022) 1:1–29. Disponível aqui.

BENCZE, L. (2023). Report on lessons learned to be applied and recommendations for data altruism practices in the implementation of construction of national and European health data spaces (including broad consent). Disponível aqui.

BIRCH, K., & Bronson, K. (2022). Big Tech. in. *Science as Culture*, 31(1), 1-14. Disponível aqui.

BULLA, Z., et. Al. (2022). Primary recommendations to foster GDPR-compliant data altruism mechanisms for the EHDS. Disponível aqui.

BUTTOW, C., & Weerts, S. (2023). Managing public sector data: National challenges in the context of European Union's new data governance models. *Information Polity*, 1-16. Disponível aqui.

CARRIÈR-SWALLOW, Y., & HAKSAR, V. (2019). The economics and implications of data - An integrated perspective. *International Monetary Fund, Strategy Policy and Review Department, n.º. 16*. Disponível aqui.

CARNEIRO, P. (2023). Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal? *Anuário de proteção de dados, 2023*, 145-178. Disponível aqui.

CAROVANO, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review, 50*. Disponível aqui.

CASTELA, E., & Branco da Costa, T. (2023). A investigação clínica na era do altruísmo dos dados: algumas considerações em torno da proteção de dados pessoais. *Anuário de proteção de dados, 2023(2)*, 249-282. Disponível aqui.

CORDEIRO, A. B. M. (2020). Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019. Almedina.

CORDEIRO, A. B. M. (2023). Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Almedina

COSTA, T. (2023). O altruísmo (económico?) de dados: Breves considerações sobre o Espaço Europeu de Dados de Saúde e a proteção de dados pessoais. *A. S. P. Oliveira & P. Jerónimo (Eds.), Liber Amicorum Benedita Mac Crorie volume II (pp. 613–643)*. UMinho Editora. Disponível aqui.

COUTINHO, J. (2017). A transparência administrativa e o acesso à informação pessoal. *IX Encontro de Professores de Direito Público*. Universidade Católica Portuguesa Editora.

DITFURTH, L. & Lienemann, G. (2022). The Data Governance Act: – Promoting or Restricting Data Intermediaries? Competition and Regulation in Network Industries, 23(4), 271-295. Disponível aqui.

ESTEVES, B., et. al. (2023). Semantics for Implementing Data Reuse and Altruism Under EU's Data Governance Act. *M. Acosta et al. (Eds.), Knowledge Graphs: Semantics, Machine Learning, and Languages*. Disponível aqui.

FINCK, M., & Pallas, F. (2020). They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data under the GDPR. *Internacional Data Privacy Law, 10*, 11-36. Disponível aqui.

FISCHER, B., & Piskorz-Ryń, A. (2021). Artificial intelligence in the context of data governance. *International Review of Law, Computers and Technology, 35(3)*, 419-428. Disponível aqui.

GEFENAS, E., et. al. (2022). Controversies between regulations of research ethics and protection of personal data: informed consent at a cross-road. *Medicine, Health Care and Philosophy, 25*, 23–30. Disponível aqui.

GERRITSEN, J.B.A. (2023). The Data Governance Act (DGA): Modern, Yet Irrelevant? *Legal Beetle*. Disponível aqui.

HALVORSON, G. C., & Novelli, W. D. (2014). Data Altruism: Honoring Patients' Expectations for Continuous Learning. Georgetown University. Disponível aqui.

HANSEN, J., et. al. (2021). Assessment of the EU Member States' Rules on Health Data in the Light of GDPR. Disponível aqui.

HENRIKSEN-BULMER, J., & Jeary, S. (2016). Re-identification attacks—A systematic literature review. *International Journal of Information Management, 36(6),* 1184-1192. Disponível aqui.

HOERNING, S., & Ilharco, A. (2023). European Data Strategy: Regulatory & Policy Aspects. *Institute of Public Policy*. Disponível aqui.

ICO. (2022). Chapter 3: Pseudonymisation. *Draft anonymization, pseudonymization and privacy enhancing technologies guidance*. Disponível aqui.

KAMOCKI, P., et. al. (2023). EU Data Governance Act: Outlining a Potential Role for CLARIN. *CLARIN Annual Conference 2022*. Disponível aqui.

LALOVA-SPINKS, T., Meszaros, J., & Huys, I. (2023). The application of data altruism in clinical research through empirical and legal analysis lenses. *Frontiers in Medicine*. Disponível aqui.

MIADZVETSKAYA, Y. (2023). Data Governance Act: On International Transfers of Non-Personal Data and GDPR Mimesis. *European Data Protection Law Review. 9(1),* 13-26. Disponível aqui.

MICHELI, M., et. al. (2023). Mapping the landscape of data intermediaries — Emerging models for more inclusive data governance. *Publications Office of the European Union*. Disponível aqui.

MONIZ, G. C. (2023). Manual de Introdução à Proteção de Dados Pessoais. Almedina.

PAAL, B. P., & Cantürk, B. C. (2023). The concept of data altruism in comparison of the Data Governance Act and the General Data Protection Regulation. *GSÜHFD, 2*, 1317-1330. Disponível aqui.

PAPAKONSTANTINOU, V., & De Hert, P. (2021). Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI. Disponível aqui.

PASERI, L. (2024). The ethical and legal challenges of data altruism for the scientific research sector. Smart Ethics in the Digital World Proceedings of the Ethicomp 2024, 137-141. Disponível aqui.

PERC, M. (2014). The Matthew effect in empirical data. *J. R. Soc. Interface 11: 20140378*. Disponível aqui.

PINHEIRO, A. (2018). Privacy e Proteção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional. AAFDL.

PURTOVA, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. Disponível aqui.

PRAINSACK, B. (2022). White Paper Data Solidarity. Disponível aqui.

PRAINSACK, B. & El-Sayed, S. (2023). Beyond Individual Rights: How Data Solidarity Gives People Meaningful Control over Data. *American Journal of Bioethics*. Disponível aqui.

RUOHONEN, J., & Hjerppe, K. (2022). The GDPR Enforcement Fines at Glance. *Information Systems*. Disponível aqui.

SHABANI, M., & Yilmaz, S. (2022). Lawfulness in secondary use of health data: interplay between three regulatory frameworks of GDPR, DGA & EHDS. Disponível aqui.

SOLOVE, D. J. (2012) Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review 126*, 1880-1903. Disponível aqui.

STREINZ, T. (2021). The Evolution of European Data Law. P. Craig & G. de Búrca (Eds.), The Evolution of EU Law 3rd ed, 902–936. Disponível aqui.

TORBAY, A. (2020) "A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia", *Anuário de Proteção de Dados 2020.* Disponível aqui.

VARDANYAN, L. (2022). The GDPR and the DGA Proposal: Are They in Controversial Relationship? *European Studies*. Disponível aqui.

VEIL, W. (2021). Data Altruism: How the EU Is Screwing Up a Good Idea. *AlgorithmWatch*. Disponível aqui.

VESTAGER, M. (2021). Data is not oil - it is a renewable resource that can be pooled, shared, reused .... Twitter. Disponível aqui.

Jurisprudência e outros documentos oficiais

Acórdão Conselho Único de Resolução contra Autoridade Europeia para a Protecção de Dados (AEPD). T-557/20. (Tribunal Geral (oitava secção alargada), 26 de abril de 2023). Disponível aqui.

Acórdão Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság. C-77/21 (TJUE, 20 de outubro de 2022). Disponível aqui.

Acórdão Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. C-131/12 (TJUE, 13 de maio de 2014). Disponível aqui.

CNPD. (2020). Deliberação/2020/277. Disponível aqui.

COMISSÃO EUROPEIA. (2019). Impact Assessment on enhancing the use of data in Europe: Report on Task 1 – Data governance SMART 2019/0024. Disponível aqui.

COMISSÃO EUROPEIA. (2020a). Commission Staff Working Document: Executive summary of the impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). Disponível aqui.

COMISSÃO EUROPEIA. (2020b). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Económico e Social Europeu e ao Comitê das Regiões: Uma estratégia europeia para os dados. Disponível aqui.

COMISSÃO EUROPEIA. (2020c). Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados). Disponível aqui.

COMISSÃO EUROPEIA. (2022). Declaração Europeia sobre os direitos e princípios digitais para a década digital. Disponível aqui.

EDPB-EDPS. (2021). Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). Disponível aqui.

EDPS. Summary of the Opinion of the European Data Protection Supervisor on EDPS Opinion on the European strategy for data, 2020/C 322/04, *Official Journal of the European Union*. Disponível aqui.

GT do artigo 29º. (2014). Opinion 05/2014 on Anonymisation Techniques. Disponível aqui.

GT do artigo 29.º (2020). Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Disponível aqui.