Da governação de dados em Cidades Inteligentes

algumas questões relativas aos dados anónimos ou anonimizados

30 de junho de 2023

Manuel David Masseno

IPBeja Instituto Politécnico de Beja

UBINET

1 – da "livre circulação" à "governação" orgânica dos dados

- com a **Comunicação *Uma estratégia europeia para os dados*** (COM(2020) 66 final, de 19 de fevereiro) [apresentada em simultâneo com a Comunicação *Construir o futuro digital da Europa* (COM(2020) 67 final) e complementada pelas *Orientações para a Digitalização até 2030*: *a via europeia para a Década Digital* (COM(2021) 118 final, de 9 de março] a **Comissão infletiu o rumo anterior**, assente na **eliminação de obstáculos** técnicos e regulatórios à **circulação de dados**, sobretudo dos não pessoais, por acordos de natureza contratual, assentes em direitos sobre os dados, **e** na **reutilização dos dados do setor público** pelos privados, **propondo** a **criação** de "**espaços comuns de dados**", setoriais à escala da União e estruturados organicamente
  - aliás, esta inflexão começara a ser indiciada com a Comunicação *Rumo a um espaço comum europeu de dados* (COM(2018) 232 final, de 25 de abril), alterando as orientações presentes na Comunicação *Para uma economia dos dados próspera* (COM(2014) 0442 final, de 2 de julho) e nas seguintes, a *Estratégia para o Mercado Único Digital na Europa* (COM(2015) 192 final, de 6 de maio) e *Construir uma Economia Europeia dos Dados*, de 2017 (COM(2017) 9 final, de 10 de janeiro)

- no que se refere às **fontes legislativas**, coexistiam **instrumentos de disponibilização sistemática e obrigatória de dados não pessoais**, incluindo dados pessoais anonimizados:
  - **da Administração Pública para os particulares**, desde a **Diretiva 2003/98/CE** de 17 de Novembro de 2003, relativa à **reutilização de informações do sector público**, até à **Diretiva (UE) 2019/1024** de 20 de junho de 2019, relativa aos **dados abertos e à reutilização de informações do setor público e**
  - **dos particulares para a Administração Pública**, em **setores específicos**, como o da **mobilidade**, com a **Diretiva 2010/40/UE** de 7 de Julho de 2010, que estabelece um **quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário**, inclusive nas interfaces com outros modos de transporte **ou** o da **energia**, com **Diretiva (UE) 2019/944**, de 5 de junho de 2019, relativa a **regras comuns para o mercado interno da eletricidade**
- com a previsão de **circulações casuísticas**:
  - muito **limitadamente**, salvo com a anonimização, a anuência dos titulares ou previsões legais com especiais garantias, em **matéria de dados pessoais**, com o Regulamento (UE) 2016/679 de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (***Regulamento Geral sobre a Proteção de Dados***) – ***RGPD*** **e** com a Diretiva 2002/58/CE de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas – ***Diretiva ePrivacy***

- **em contraponto** com o Regulamento (UE) 2018/1807, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia – o ***RLFD***

- ora, este **ecossistema regulatório** tornava extremamente **difícil** o **acesso e** a **exploração das possibilidades** facultadas pela **agregação de dados** de diferentes origens e naturezas, **para benefício** dos **participantes** nos "**espaços comuns de dados**", inclusive secundarizando interesses comuns ou o interesse público
  - daí resultando as **Propostas de** Regulamento relativas à governação de dados (***Regulamento Governação de Dados***) (COM(2020) 767 final, de 25 de novembro) **e** a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (***Regulamento Dados***), este apenas pontualmente
  - **entretanto**, a primeira culminou no Regulamento (UE) 2022/868 de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (***Regulamento Governação de Dados***) – ***RGD*** [***DGA***]
- **se**, pelo menos em termos explícitos, **estes instrumentos não tiveram em consideração os territórios** / **cidades inteligentes**, **podem** / **devem** assumir uma **extrema relevância** para a sua **estruturação e consolidação**, ao deixar de exigir feixes de acordos parcelares e / ou assimétricos para o acesso e a partilha de dados

- assim, no referente ao ***RGD***, além de ampliar e estruturar a "Reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público" (Art.ºs 3.º a 9.º), disciplina **organizações mediadoras de dados**, como os "**serviços de intermediação de dados**", incluindo os "serviços de cooperativas de dados", de natureza profissional (Art.ºs 10.º a 15.º) **e** o "**altruísmo de dados**" (Art.ºs 16.º a 25.º)
- em atenção aos respetivos regimes, temos em crer que os **territórios** / **cidades inteligentes apenas** poderão seguir a **segunda via**, a do "**altruísmo de dados**", até pelos "**fins de interesse geral**" enumerados
  - o mesmo **é definido** 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 recebam uma gratificação que vá além de uma compensação 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." (Art.º 2.º 16)

2 – o tratamento por uma "organização de altruísmo de dados"

- além dos requisitos relativos à inscrição num registo público (Art.ºs 17.º a 19.º), a "**organização de altruísmo de dados**", no **cerne** de um **território** / **cidade inteligente**, estará obrigada a **deveres institucionais de transparência**, incluindo o reporte às respetivas autoridades responsáveis pelo registo público nacional, para **controlo do cumprimento** [*compliance*] (Art.ºs 20.º e 24.º)
- adicionalmente, o ***RGD*** prevê "**deveres específicos**" **para com** os "**titulares dos dados**" [pessoais] **e** os "**detentores dos dados**" [não pessoais], no que que se refere (Art.º 21.º):
  - à **informação** quanto aos "**objetivos de interesse geral e**, se for caso disso, a **finalidade específica**, explícita e legítima **para a qual os dados pessoais devem ser tratados**, e que permitem o tratamento dos seus dados por um utilizador de dados" (n.º 1 a)
  - quanto à **vinculação à finalidade de interesse geral** para a qual foi obtido o consentimento" (n.º 2) **e**
  - relativamente à **segurança do tratamento** dos **dados não pessoais** recolhidos, incluindo o reporte de incidentes (n.ºs 4 e 5)

- consequentemente e como também **resulta** do próprio ***RGD*** (Art.º 1.º n.º 3), cada "**organização de altruísmo de dados**" é **também** o "**responsável pelo tratamento**" de dados pessoais (Art.º 4.º 7) do *RGPD*), estando **adstrita**:
  - à **observância** dos "**Princípios relativos ao tratamento de dados pessoais**" (Art.º 5.º)
  - a **retirar** as devidas **consequências** de ter o "**consentimento**" como **único fundamento de licitude** para o **tratamento** de tais dados (Art.ºs 2.º, 5) e 16), 21.º, n.ºs 3 e 6, e 22.º n.º 1 a) e b), explicitado nos *Considerando*s (45), (46) e 50 do *RGD*, também remetendo para os Art.ºs 4.º 11), 7.º, 8.º e 9.º n.º 1 do *RGPD*), inclusive através da disponibilização de **instrumentos técnicos facilitadores** (Art.º 21.º n.º 3)
  - **respeitar** os **direitos dos titulares dos dados** (Art.ºs 22.º do *RGPD*), no que for compatível com um tratamento assento no "consentimento"
  - **aplicar** as "**medidas técnicas e organizativas que forem adequadas**", "**desde a conceção e por defeito**", **mantendo** um "**registo das atividades de tratamento**" (Art.ºs 24.º, 25.º e 30.º do *RGPD*)
  - também no que se refere à "**segurança do tratamento**", relativos a dados não pessoais, incluindo os reportes de incidentes (em termos análogos aos previstos nos Art.ºs 32.º a 34.º do *RGPD*), **além de**
  - **cumprir** os **requisitos** correspondentes à **seleção e controle** dos "**subcontratantes**", como os que facultarão o armazenamento dos dados na *nuvem* (em linha com o Art.º 28.º do *RGPD*), tendo por referência o [*EU Cloud CoC*] *Codigo de Conduta da UE para a Proteção de Dados pelos Fornecedores de Serviços de Nuvem*, formalmente aprovado em 20 de maio de 2021

- adicionalmente, pelo menos, será **prudente** proceder a uma **prévia** "**avaliação de impacto sobre a proteção de dados**", ainda que a mesma não seja legalmente obrigatória ou determinada por via regulamentar pela autoridade de controlo (Art.º 35.º do *RGPD*), não estando uma consulta prévia à autoridade de controlo (Art.º 36.º do *RGPD*)

- por outro lado, cada "«**Organismo do setor público**» [i.e.], 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» (Art.º 2.º 17) do *RGD*) está **legitimado a facultar** a "«**Reutilização**», [ou seja] **a utilização**, por **pessoas** singulares ou **coletivas**, de dados detidos por organismos do setor público, **realizada para fins** comerciais ou **não comerciais que não correspondem à finalidade** inicial **da missão de serviço público para a qual os dados foram produzidos**»" (Art.º 2.º 2) **a uma** "**organização de altruísmo de dados**", desde que cumpridos os devidos pressupostos (Art.ºs 3.º a 6.º e 9.º do *RGD*)
  - **sem esquecer** que, tratando-se de "**dados pessoais**" (Art.º 4.º 1) do *RGPD*, recebido pelo Art.º 2.º 3) do *RGD*), a "**reutilização**" **apenas é viável se** os mesmos **forem** "**anonimizados**" **ou**, se o respetivo **titular consentir**, não existindo uma outra base jurídica específica (Art.º 5.º n.ºs 3 e 6 do *RGD* e Art.ºs 6.º e 9.º do *RGPD*)

3 – a "anonimização" e os respetivos *riscos*

- como vimos de verificar, em princípio, a "**reutilização de dados**" **pessoais** detidos por um «**Organismo do setor público**» **pressupõe** uma prévia "**anonimização**", de modo a **afastar** a **aplicabilidade** do **regime relativo aos dados pessoais**
  - ao ser o **critério** a **associação**, originária ou provocada, **a identificadores**, pois "**é considerada identificável uma pessoa** singular **que possa ser identificada**, direta ou indiretamente, **em especial por referência a um identificador**, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (Art.º 4.º 1) do *RGPD*), o que inclui o quase-identificadores e os metadados
  - **consequentemente**, "[…] **Os princípios** [*rectius*, os regimes] **da proteção de dados não deverão**, pois, **aplicar-se** às **informações anónimas**, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem **a dados pessoais tornados** de tal modo **anónimos** que o **seu titular não seja ou já não possa ser identificado**. **O presente regulamento não diz**, por isso, **respeito ao tratamento dessas informações anónimas**, inclusive para fins estatísticos ou de investigação." (*Considerando* (26) *in fine*) do *RGPD*)

- porém, "**As pessoas** singulares **podem ser associadas a identificadores por via eletrónica** [**e**] **Estes identificadores podem deixar vestígios que**, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, **podem ser utilizados para a definição de perfis e** [consequentemente] **a identificação das pessoas singulares**." (*Considerando* (30) do *RGPD*), como ficou claro com o **Acórdão** de 19 de outubro de 2016, Processo C-582-14, ***Patrick Breyer***, do **TJUE – Tribunal de Justiça da União Europeia**
- por seu turno, o ***RLFD***, a propósito dos "**conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados** [**explicita que**] **Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais**, **e o** Regulamento (UE) 2016/679 [o *RGPD*] **deve ser aplicado em conformidade**." (*Considerando* (9)) **e**
- "**Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar** [direta ou indiretamente] **a pessoa singular** [quer pelo responsável pelo tratamento quer por outra pessoa]**, importa considerar todos os fatores objetivos**, como os custos e o tempo necessário para a identificação, **tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica**" (embora este excerto do *Considerado* (26) se refira à pseudonimização, a regra é também pertinente para a anonimização)
- **incluindo** os **meios** à disposição **de** «**terceiros**» (Art.º 4.º 10) do *RGPD*, nos termos do, muito recente, **Acórdão** no Processo T-557/20 - **CUR/AEPD** do TJUE, de 26 de abril de 2023)

- o que exige **usar** técnicas de ***anonimização* forte**, como explicitou o **Grupo de Trabalho do Artigo 29.º – GT 29** (Atual CEPD – Comité Europeu para a Proteção de Dados) no seu **Parecer n.º 5/2014**, de 10 de abril, sobre **as técnicas de anonimização**
  - aliás, **antecedido** pelos **Pareceres n.º 7/2003**, de 12 de dezembro, sobre a **reutilização de informações do setor público e a proteção dos dados pessoais e n.º 6/2013**, de 5 de junho, sobre **dados abertos e reutilização de informações do setor público (ISP)**
- ainda a este propósito, cabe **acrescentar** que, embora os atos legislativos anteriores se tenham abstido de o fazer, a **Diretiva (UE) 2019/1024 define-a** como "o **processo de transformar documentos em documentos anónimos** que não digam respeito a uma pessoa singular identificada ou identificável, **ou o processo de tornar anónimos os dados pessoais**, por forma a que a pessoa em causa não seja ou deixe de ser identificável." (Art.º 2.º 7)
- todos **estes riscos são enunciados** explícita e detalhadamente pelo ***RGD***, a propósito da "**reutilização de determinadas categorias de dados protegidos detidos por organismos do setor público**" (*Considerandos* (15) e (19), ao ponto de **determinar** que "**Os reutilizadores** [*in casu*, cada "organização de altruísmo de dados"] **ficam proibidos de reidentificar qualquer titular dos dados** a quem os dados digam respeito **e devem tomar medidas** técnicas e operacionais para **prevenir a reidentificação** e para notificar ao organismo do setor público qualquer violação de dados que resulte na reidentificação dos titulares dos dados em causa." (Art.º 5.º n.º 5), até em resposta ao **Parecer conjunto 3/2021** do **CEPD e** da **AEPD – Autoridade Europeia para a Proteção de Dados** sobre a **proposta de Regulamento**, de 10 de março / 9 de junho

- em síntese, o **limite entre** os **dados pessoais e** os **dados não pessoais** é **móvel**, dependendo da evolução das tecnologias, assim:
  - **sempre que passar a ser viável a (re)identificação**, ainda que *potencial*, já que o critério é de ser uma pessoa "identificável" (Art.º 4.º 1), **aplicar-se-ão os regimes** constantes do ***RGPD* e** o "**responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo** ([**Princípio da**] «**responsabilidade**) [*proactiva* ou *accountability*]»" (Art.º 5.º n.º 2, também enunciado no Art.º 24.º n.º 1), **cabendo-lhe os *riscos de desenvolvimento* que resultem de tais tratamentos** … **salvo** eventuais **disrupções**
  - **o mesmo valendo** sempre que **dados anónimos ou anonimizados** "**estejam indissociavelmente ligados**" a alguns **dados pessoas** (Art.º 2.º n.º 2 do *RLFD*)
  - o que **impõe reavaliações cíclicas dos riscos** inerentes, **por parte dos responsável pelo tratamento**, inclusive **com sucessivas avaliações de impacto**, sobretudo, quando estiverem em causa "**novas tecnologias**" (Art.ºs 24.º, 25.º e 35.º n.ºs 1 e 3 a) do *RGPD*) **e**
  - sendo certo que o acatamento de **esquemas autorregulatórios**, como os **códigos de conduta** (Art.ºs 40.º e 41.º) **ou** a **certificação** (Art.ºs 42.º e 43.º) [*v.g.*, a nova norma ISO/IEC 27559:2022 –Segurança da Informação, Cibersegurança e Proteção da Privacidade – Controlos de Segurança da Informação, de novembro], "**pode ser utilizado como elemento para demonstrar o cumprimento das obrigações**" (Art.º 32.º n.º 3), **não exime de eventuais responsabilidades** (Art.º 82.º a 84.º do *RGPD*)