17 de março de 2023

6ª SESSÃO DO CICLO DE WEBINARS

SMART CITIES AND LAW,
E-GOVERNANCE AND RIGHTS

Da vigilância biométrica no Ordenamento da UE

para fins de segurança em espaços acessíveis ao público

Manuel David Masseno

1 – para **enquadramento**

- como explicitam as ***Diretrizes n.º 3/2019 relativas ao tratamento de dados pessoais através de sistemas de videovigilância – Versão 2.1***, de 26 de fevereiro de 2020, do **CEPD – Comité Europeu para a Proteção de Dados**, quando esta inclui o **tratamento de** "**dados biométricos**" emergem **riscos acrescidos** para os **direitos e liberdades dos titulares dos dados**, inclusive por se tratar sempre de procedimentos automatizados, frequentemente com recurso a sistemas de IA – Inteligência Artificial
  - por "«**Dados biométricos**», [têm-se os] **dados pessoais resultantes de um tratamento técnico** específico **relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam** ou confirmem **a identificação** única **dessa pessoa singular**, nomeadamente **imagens faciais** ou dados dactiloscópicos" (Art.º 4.º 14) do 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**) – o ***RGPD***

- o que implica **identificar**, por comparação com dados biométricos constantes duma base, através de **processamentos automatizados**, incluindo a IA
- o que diverge, radicalmente, da videovigilância, ao **permitir** a "**definição de perfis**", até com analíticas preditivas, **indo** até **além dos riscos** associados à **conservação e acesso ao metadados** resultantes das **comunicações eletrónicas**, com um **acrescido alarme social**, sobretudo **se** feita de um **modo indiscriminado e em espaços acessíveis ao público**, mais ainda **em territórios inteligentes**
  - muito além dos identificados nos Acórdãos *Digital Rights Ireland* (Processos apensos C-293/12 e C-594/12, de 8 de abril de 2014) e *Tele2 Sverige* (Processo C-203/15, 21 de dezembro de 2016) do TJUE – Tribunal de Justiça da União Europeia
  - pois, para além do "respeito pela vida privada e familiar" e da "proteção de dados", **estão em causa restrições a outras liberdades**, como a "**de pensamento, de consciência e de religião**" e a "**de reunião e de associação**" ou até a "**de circulação e de permanência**", sempre **sujeitas** ao "**princípio da proporcionalidade**" (Art.ºs 7.º, 8.º, 10.º, 12.º, 45.º e 52.º n.º 1 da *CDFUE* – *Carta dos Direitos Fundamentais da União Europeia*)

2 – o regime vigente

- se o ***RGPD*** disciplina a **vigilância biométrica**, enquanto tratamento duma "**categoria especial de dados**", sobretudo se "em grande escala" e com o recurso a "novas tecnologias" (Art.ºs 9.º e 35.º & *Considerando* 51), podendo **ainda** dar lugar à «definição de perfis» (*maxime*, Art.ºs 4.º 4) e 22.º & *Considerandos* 71 a 73)
- porém, o mesmo "**não se aplica ao tratamento de dados pessoais**: […] Efetuado pelas autoridades competentes **para efeitos de prevenção, investigação, deteção e repressão de infrações penais** ou da execução de sanções penais**, incluindo a salvaguarda e a prevenção de ameaças à segurança pública**." (Art.º 2.º n.º 2 d)
- mas sim, a **Diretiva (UE) 2016/680**, relativa à **proteção das pessoas singulares** no que diz respeito ao **tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais** ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho – a ***Diretiva LE***, adotada e publicada nas mesmas datas

- **transposta** pela **Lei n.º 59/2019**, de 8 de agosto, aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016
- **completada** pela **Lei n.º 95/2021**, de 29 de dezembro, regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som, revogando a Lei n.º 1/2005, de 10 de janeiro

- na ***Diretiva LE***, coincidindo a definição de «**Dados biométricos**» (Art.º 3.º 13) com a do *RGPD*, assim como a qualificação enquanto "categoria especial de dados" (Art.º 10.º), temos que o respetivo **tratamento**:
  - "**só é autorizado se for** estritamente **necessário** [indo além do "necessário" para a sua licitude em termos gerais, Art.º 8.º n.º 1], **se estiver sujeito a garantias** adequadas **dos direitos e liberdades do titular dos dados,** e se [adicionalmente]: a) **For autorizado pelo direito da União ou de um Estado-Membro**; b) **Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular**; ou c) **Estiver relacionado com dados** manifestamente **tornados públicos pelo titular dos dados**."

- impondo a **observância** estrita dos **Princípios** da «**licitude e lealdade**», da «**limitação das finalidades**», da «**exatidão**», da «**minimização dos dados**», da «**limitação da conservação**» **e**, ainda, da «**integridade e confidencialidade**» (Art.º 4.º n.º 1, para usar a terminologia do *RGPD*) **e** a
- garantia do **direito à informação** e de acesso, embora com limitações relativamente ao disposto no *RGPD* (Art.ºs 13.º, 14.º e 15.º & *Considerandos* 26 e 36 a 36)
- adicionalmente, a «**Definição de perfis**» (Art.º 3.º 4) a partir do tratamento de tais dados, ao ser inerente um acréscimo dos "riscos para os direitos e liberdades das pessoas" (*Considerandos* 38 e 51) está **vedada**, "**a não ser que sejam aplicadas medidas** [adicionais] **adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular**" **e**, em qualquer caso, sempre que "**conduzam à discriminação de pessoas singulares**" (Art.º 11.º n.ºs 2 e 3)
- além de pressupor a **realização** duma "**avaliação de impacto sobre proteção de dados**", ao ser, manifestamente, "suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares" (Art.º 27.º n.º 1) **e**

- **também** a "**consulta prévia da autoridade de controlo**", mesmo sem a avaliação de impacto, **quando** "**O tipo de tratamento envolva**, especialmente no caso de se utilizarem novas tecnologias, mecanismos ou procedimentos, **um** elevado **risco para os direitos e liberdades dos titulares dos dados**" (Art.º 28.º n.º 1 b)
- o que deverá conduzir ao **tratamento apenas** dos **dados** de titulares passíveis de integrar **uma das categoriais** previstas, no limite **só** de "**pessoas relativamente às quais existem motivos** fundados **para crer que cometeram ou estão prestes a cometer** [**ou** as já] **condenadas por uma infração penal**" (Art.º 6.º a) e b), **distinguindo-as dos *não suspeitos***, o que implica **interditar a utilização de** outras **bases de dados biométricos**, inclusive as criadas para finalidades distintas destas
  - a este propósito, cabe **ainda** sublinhar a **importância** dos **Pareceres** do **Grupo de Trabalho do Art.º 29.º** [atual CEPD], 01/2013, de 26 de fevereiro, 03/2015, de 1 de dezembro, **e**, ainda o **sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)**, de 29 de dezembro de 2017, **além das *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679***, de 3 de outubro de 2017 / 6 de fevereiro de 2018

3 – o que estará para vir

- na **Proposta de Regulamento que estabelece regras harmonizadas em matéria de Inteligência Artificial** (***Regulamento Inteligência Artificial***) (COM/2021/206 final, de 21 de abril de 2021), **Comissão Europeia**, avança com uma **disciplina centrada** nos próprios **sistemas de IA** e já não nos dados, com o **objetivo** de garantir "**respeito pela dignidade humana**" como referência mor (Art.ºs 2.º do *TUE* – *Tratado da união Europeia* e 1.º da *CDFUE*)
- em extrema síntese, a **Proposta distingue** entre as "**práticas de inteligência artificial proibidas**" (Art.º 5.º), os "**sistemas de inteligência artificial de risco elevado**" (Art.ºs 8.º a 51.º) **e** as "**obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial**", para os de **baixo risco** (Art.º 52.º), **e** ainda os de **risco mínimo**, que ficarão foram do âmbito de aplicação do futuro Regulamento (Art.º 1.º), atendendo também à **previsibilidade da respetiva utilização**

- assim, umas das "**práticas de inteligência artificial proibidas**" prende-se com:
  - "A **utilização de sistemas de identificação biométrica à distância em** «tempo real» **em espaços acessíveis ao público para efeitos de manutenção da ordem pública**, **salvo se** essa utilização for estritamente necessária para alcançar um dos seguintes objetivos: i) a **investigação** seletiva **de potenciais vítimas** específicas **de crimes**, nomeadamente crianças desaparecidas, ii) a **prevenção de uma ameaça** específica, substancial e iminente **à vida ou à segurança** física **de pessoas singulares ou de um ataque terrorista**, iii) a **deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal** referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho [relativa ao mandado de detenção europeu] e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro;" (Art.º 5.º n.º 1 d)
  - mas apenas **a título excecional e** com diversas **restrições ao exercício do poder legislativos pelos Estados-Membro e garantias**, incluindo a intervenção duma "autoridade judiciária ou por uma autoridade administrativa independente" (Art.º 5.º n.ºs 2, 3 e 4)

- aliás, a própria **Comissão** assume que "**A utilização de sistemas de IA para a identificação biométrica à distância** «em tempo real» **de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública é considerada** particularmente **intrusiva para os direitos e as liberdades das pessoas em causa**, visto que **pode afetar a vida privada de uma grande parte da população**, dar origem a uma **sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais**. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais" (*Considerando* 18, com desenvolvimentos detalhados nos *Considerandos* 19 a 23)

- no seu **Parecer conjunto 5/2021**, de 18 de junho, do **CEPD** e da **Autoridade Europeia para a Proteção de Dados** sobre a **Proposta**, em síntese, "**apelam à proibição** geral **de qualquer utilização de IA para o reconhecimento automatizado de características humanas em espaços acessíveis ao público** (tal como de rostos, mas também do andar, de impressões digitais, do ADN, da voz, da digitação e de outros sinais comportamentais ou biométricos) em qualquer contexto"
- logo depois, foi aprovada **Resolução** do **Parlamento Europeu**, de 6 de outubro de 2021, **sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais** (2020/2016(INI)), além de defender uma **maior rigor** no que se refere ao **reconhecimento facial**, incluindo uma moratória até à comprovação da robustez e precisão dos sistemas, salvo para a identificação de vítimas, **e** "apela, além disso, à **proibição** permanente **do recurso a análises automatizadas e/ou do reconhecimento em espaços acessíveis ao público de outras características humanas**, tais como o andar, as impressões digitais, o ADN, a voz e outros sinais biométricos e comportamentais."

- entretanto, a 6 de dezembro último, durante a Presidência checa, o **Conselho de Ministros** alcançou um **compromisso** sobre a ***Proposta*** no sentido de deixar **de fora todas as utilizações** de **IA** relacionadas com a **segurança nacional e** de **"clarificar"** os **limites da proibição** no que se refere à "**identificação biométrica**" para fins **de prevenção e combate ao crime** (nas novas redações do Art.º 5.º n.ºs 1 d), 2, 3 e 4, termos explicitados na nova redação dos *Considerandos* 19 a 24)
- enquanto o **Parlamento** ainda não tem um texto final, mas, de acordo com os esboços divulgados informalmente pelos Gabinetes dos Relatores, o último ainda esta semana, pretenderá **afastar** em absoluto **a possibilidade de serem criadas bases de dados biométricos de âmbito geral**

e, a modo de **apêndice**

- ainda que não prevaleça a posição do Conselho no trílogo, sobretudo depois da inevitável apreciação *a posteriori* pelo TJUE, é expectável que fique alguma **margem** para os **Legisladores nacionais**
- ora, **por cá** e de momento, a **Lei n.º 95/2021**, estabeleceu que **para** "os **fins** previstos do artigo 3.º [ou seja, os constantes na "Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, e em concreto para: [n.º 1] d) **proteção da segurança das pessoas**, animais e bens, **em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista** razoável **risco da sua ocorrência**], **o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados**, por aplicação de critérios técnicos [*i.e.*, através de IA], de acordo com os fins a que os sistemas se destinam [**mas**] **não é permitida a captação e tratamento de dados biométricos**." (Art.º 16.º, n.ºs 1 e 2)…