Que implicações da Proposta de Regulamento Inteligência Artificial para a Proteção de Dados nas Cidades Inteligentes na UE?

Manuel David Masseno

UBINET
Segurança Informática e Cibercrime

IPBeja
Instituto Politécnico de Beja

11 de março de 2022

1 – as **Cidades** [*rectius* os **Territórios**] ***Inteligentes*** (**TI**)

- antes de tudo, os **TI** constituem a **confluência** do **Urbanismo**, do **Ordenamento e Governança Territoriais**, bem como do **Património Natural e Cultural com** a **Sociedade da Informação**, em termos Regulatórios e de Políticas Públicas
  - além das **Cidades**, temos **Áreas Protegidas**, **Destinos Turísticos ou** até **áreas rurais**, **e**
  - **integram** os **Ambientes Inteligentes**, as **casas**, **fábricas**, **hotéis**, **museus**, **edifícios públicos**, **aeroportos e portos**, assim como as **estradas e** os **caminhos de ferro**…
- todos com um **ponto comum**, a **otimização dos meios**, incluindo a energia, **e dos resultados**, também reduzindo a *pegada ecológica* das atividades
- mas, **com riscos para** a **Privacidade e** os **outros Direitos Fundamentais**, não apenas por parte **Poderes Públicos** mas também dos **Privados**, enquanto parte do *Capitalismo de Vigilância*, orientado à *monetarização* (Shoshana Zuboff), **incluindo a partilha ou a interconexão** de dados entre uns e outros, definindo **perfis**, designadamente no que se refere à videovigilância algorítmica

2 – as **bases tecnológicas** dos **TI**:

- resultaram do **desenvolvimento da *Inteligência Artificial***, sobretudo com a *Big Data* (Megadados), incluindo a *Nuvem*, as ligações de banda muito larga e a *Internet das Coisas*, e sempre
- assentes em **redes de sensores e atuadores**, assim como em **sistemas de Inteligência Artificial** (**IA**)
- **porém**, sobretudo por força da evolução do aprendizagem de máquina, o modo de **processamento** interno da informação foi-se tornando **cada vez mais ininteligível** (*black boxes*), **dependendo os resultados da quantidade e qualidade das informações inseridas**, cujos enviesamentos aliás reproduzem e potenciam, **colocando em risco as Liberdades dos cidadãos**
- mais ainda, **possibilita** a **deteção de micropadrões e** com **respostas em tempo real**, assim como a **predição de comportamento futuros**, possibilitando o seu condicionamento preventivo

- **concretizando**, "**Os sistemas de inteligência artificial são sistemas de *software*** (e eventualmente também de *hardware*) **concebidos por seres humanos, que,** tendo recebido um objetivo complexo, **atuam na dimensão física ou digital percecionando o seu ambiente mediante a aquisição de dados, interpretando os dados** estruturados ou não estruturados **recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido**. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores." (***Orientações Éticas para uma IA de Confiança***, **do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial**, recebidas na *Comunicação* da **Comissão** [**Europeia**] *Aumentar a confiança numa inteligência artificial centrada no ser humano* (COM/2019/168 final, de 8 de abril)

- entretanto, a **Comissão Europeia avançou com uma definição**, efetivamente, **operativa de** "**«sistema de inteligência artificial»** (Sistema de IA) um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage [Art. 3.º 1), **o que inclui**, "(**a**) **Abordagens de aprendizagem automática**, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda bordagens de aprendizado de máquina; (**b**) **Abordagens baseadas na lógica e no conhecimento**, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais; [**e ainda**] (**c**) **Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização**", Anexo I]" (**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)

2 – o ***atual enquadramento regulatório***

- 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***, a **União Europeia** pretendeu efetivar uma ***funcionalização*** **da Tecnologia ao Homem**
- o que **decorre** da ***constitucionalização*** da **proteção de dados pessoais**, enquanto **Direito Fundamental à Autodeterminação Informacional** (Art.º 16.º do ***TFUE*** – ***Tratado sobre o Funcionamento da União Europeia***, do Art.ºs 7.º e 8.º da ***CDFUE*** – ***Carta dos Direitos Fundamentais da União Europeia*** e dos Art.º 2.º e 6.º do *TUE* – *Tratado da União Europeia*, com abertura também para a *CHDE* – *Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais*, do Conselho da Europa, e para a Jurisprudência do Tribunal Europeu dos Direitos do Homem)

- porém, **antes**, a **Diretiva 95/46/CE** de 24 de Outubro de 1995, relativa à **proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**, já **dava resposta** às principais **questões** que se colocam com a **IA – Inteligência Artificial**, mesmo num contexto tecnológico muito diferente do atual

- **em especial**, do ***RGPD*** consta uma disciplina que **restringe o acesso dos sistema de IA às massas de dados** [*Big Data* / Megadados] destinadas a identificar padrões e prever a evolução dos acontecimentos, antes de mais, pela **ação** dos "**Princípios relativos ao tratamento de dados pessoais**" **e**, bem assim, dos **direitos dos titulares e** dos **deveres dos responsáveis pelo tratamento**:
  - com **especial relevância** para os da «**limitação da finalidade**» **e** na «**minimização dos dados**» (Art.º 5.º n.º 1 alíneas b) e c), **com expressão** em termos de "**licitude do tratamento**" (Art.º 6.º n.ºs 3 e 4), no "**direito à limitação do tratamento**" (Art.º 18.º), na "**responsabilidade do responsável pelo tratamento**" (Art.º 24.º) **e** na "**proteção desde a conceção e por defeito**" (Art.º 25.º), **além de**

- **na** «**limitação** [**no tempo**] **da conservação**» (Art.º 5.º n.º 1 e), **no** "**direito ao apagamento dos dados** («**direito a ser esquecido**»)" (Art.º 17.º) **e no** "**direito à portabilidade dos dados**" (Art.º 20.º)

- **por outro lado**, do ***RGPD*** resulta que a **IA está subjacente**:
  - à **previsão** relativa às **situações nas quais** "**um certo tipo de tratamento, em particular que utilize novas tecnologias e** tendo em conta a sua natureza, âmbito, contexto e finalidades, **for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares**" **exige a realização prévia de uma** "**avaliação de impacto em proteção de dados**" [*DPIA*] (Art.º 35.º n.º 1), o que é corroborado pelas referências à "avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares" e, mais ainda, ao "controlo sistemático de zonas acessíveis ao público em grande escala" (Art.º 35.º n.º 3 a) e c), assim como
  - ao "**controlo do** seu [*i.e.*, de titulares de dados pessoais que se encontrem no território da União Europeia] **comportamento efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União**, desde que esse comportamento tenha lugar na União." (Art.º 3.º n.º 2 b), implicando o emprego de sistemas de IA

- quanto aos **perfis e** às **decisões automatizadas**, também neste âmbito:
  - entendendo-se por "**«Definição de perfis»**, **qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular**, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (Art.º 4.º 4)
  - além da **obrigatoriedade das avaliações de impacto**… (Art.º 35.º n.º 3 a)
  - estão previstos **direitos reforçados de acesso à informação** quanto à "**existência de decisões automatizadas, incluindo a definição de perfis**" **e** também "**informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados**" (Art.ºs 13.º n.º 2 f), 14.º n.º 2 g) e 15.º n.º 1 h) **e**, ainda

- "**O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada** exclusivamente **com base no tratamento automatizado**, incluindo a definição de perfis, **que produza efeitos na sua esfera jurídica ou que o afete significativamente** de forma similar", embora com **ressalvas**, mas sempre **com garantias** (Art.º 22.º n.ºs 1 e 2)
- domínio, são de **especial interesse** as ***Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679***, do **Grupo de Trabalho do Artigo 29.º** [antecessor do **CEPD** – **Comité Europeu para a Proteção de Dados**], de 3 de outubro de 2017, atualizadas a 6 de fevereiro de 2018

- em particular, no que se refere ao **controle por reconhecimento facial**:
  - estamos perante um **tratamento de** "**dados biométricos**", os quais estão entre as "**categorias especiais de dados**" (Art.º 9.º n.º 1), *i.e., 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)

- indo **além da videovigilância**, pois "O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que **são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular** [através sistemas de IA e, consequentemente] **Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos** definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas a fim de adaptar a aplicação das regras do presente regulamento **para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento.**" (*Considerando* 51)
- nesta matéria e especialmente, **relevam** 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**

- **e**, ainda, há a referir a **questão** relativa à (**re**)**personalização dos dados anónimos**
  - o ***RGPD*** apenas **se aplica aos tratamentos de dados pessoais**, (Art.º 1.º n.º 1) **ou** quando **não for viável separar** tecnicamente **dados pessoais de dados não pessoais** (Art.º 1.º n.º 1 e Art.º 2.º n.ºs 1 e 2 do 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 - *RLFD*)
  - **mas**, "**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 deve ser aplicado em conformidade**." (*Considerando* 9 do *RLFD* e Art.º 4.º 1) do *RGPD*), o **mesmo** valendo para os **dados anónimos**
  - o que é **viável** através de **Sistemas de IA**, através da «**definição de perfis**», inclusive desde o tratamento de metadados (*Considerando* 30 do *RGPD*) e Acórdão Breyer (Processo C-582/14), do Tribunal de Justiça da União Europeia, de 19 de outubro de 2016, **e** ficara explícito no **Parecer n.º 5/2014**, de 10 de abril, sobre **técnicas de anonimização**, do **Grupo de Trabalho do Artigo 29**

3 – a, possível, ***disciplina futura***

- culminando um **caminho** encetado, pela **Comissão Europeia**, com a Comunicação *Inteligência artificial para a Europa* (COM/2018/237 final, de 25 de abril), a **Proposta de Regulamento Inteligência Artificial** avança com uma **disciplina** própria e **adicional** ao ***RGPD***, também **assente em análises dos riscos para os Direitos Fundamentais**, sempre com o "**respeito pela dignidade humana**" como referência mor (Art.ºs 2.º do *TUE* e 1.º da *CDFUE*), **mas** agora **centrada** nos próprios **sistemas de IA** e já não nos dados
- 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**

- **concretizando**, na perspetiva das **cidades** / **territórios inteligentes**, em **primeiro** lugar, quanto "**práticas de inteligência artificial proibidas**", temos

  1) "A colocação no mercado, **a colocação em serviço ou a utilização de sistemas de IA por autoridades públicas** ou em seu nome **para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais**, conhecidas ou previsíveis, **em que a classificação social conduz a uma das seguintes situações** ou a ambas: i) **tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas** em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos, ii) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é **injustificado e desproporcionado** face ao seu comportamento social ou à gravidade do mesmo;" (Art.º 5.º n.º 1 c)

2) "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 [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), **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)

- no que se refere aos "**sistemas de inteligência artificial de risco elevado**", por as **regras** serem **também aplicáveis aos utilizadores**, interessam-nos (Anexo III):

  1) a "1. **Identificação biométrica e categorização de pessoas singulares**: a) Sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância «em tempo real» e «em diferido» de pessoas singulares;

  2) a "2. **Gestão e funcionamento de infraestruturas críticas**: a) Sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo do trânsito rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade.;"

  3) o "5. **Acesso a serviços privados e a serviços e prestações públicas essenciais**, bem como o usufruto dos mesmos: a) Sistemas de IA concebidos para serem utilizados por autoridades públicas ou em nome de autoridades públicas para avaliar a elegibilidade de pessoas singulares quanto a prestações e serviços públicos de assistência, bem como para conceder, reduzir, revogar ou recuperar tais prestações e serviços; […] c) Sistemas de IA concebidos para serem utilizados no envio ou no estabelecimento de prioridades no envio de serviços de resposta a emergências, incluindo bombeiros e assistência médica."

4) a "6. **Manutenção da ordem pública**: a) Sistemas de IA concebidos para serem utilizados por autoridades policiais em avaliações individuais de riscos relativamente a pessoas singulares, a fim de determinar o risco de uma pessoa singular cometer infrações ou voltar a cometer infrações ou o risco para potenciais vítimas de infrações penais; […]"

- daí resultando a **aplicação do correspondente regime**, aliás denso, incluindo:
  - **sistemas de gestão de riscos**, durante todo o ciclo de vida de cada sistema de IA (Art.º 9.º), especialmente quando implicarem técnicas envolvendo o treino de modelos, para **prevenir e corrigir enviesamentos** (Art.º 10.º)
  - **documentação técnica** sobre os sistemas de IA, detalhada e atualizada (Art.º 11.º)
  - manutenção de **registos automáticos de eventos** (Art.º 12.º)
  - **transparência** quanto à sua **conceção e funcionamento**, para possibilitar uma atuação adequada dos utilizadores (Art.º 13.º)
  - nível apropriado de **exatidão, solidez e cibersegurança** (Art.º 15.º), até para permitir a
  - **supervisão** efetiva **do seu funcionamento por seres humanos** (Art.º 14.º).
- além de estabelecer **obrigações** também **para** os **utilizadores** (Art.º 29.º), **prevendo** ainda **avaliações de conformidade**, (Art.ºs 40.º a 51.º) **e sanções administrativas**, ainda mais pesadas que as do *RGPD*… (Art.º 71.º)

- já para os **sistemas** de **baixo risco**, temos **apenas** que a **utilização** de "um **sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas**. [Mas] Esta obrigação não se aplica a sistemas de IA usados para categorização biométrica que sejam legalmente autorizados para detetar, prevenir e investigar infrações penais.", mas **aplicando-se** os **regimes** relativos aos **de risco elevado aos** respetivos **fornecedores** (Art.º 52.º n.ºs 2 e 4)
- finalmente, os **sistemas de risco mínimo**, como os que implicarem exclusivamente o tratamento de dados não pessoais, estarão fora deste âmbito, como já estavam do do *RGPD*, mas poderão vir a estar abrangidos pelo futuro *Regulamento Dados*, proposto pela Comissão Europeia no dia 23 de fevereiro (COM/2022/68 final)