Da Cibersegurança nas *Cidades Inteligentes*

uma prospetiva cartográfica das novas fontes europeias

Manuel David Masseno

UBINET Segurança Informática e Cibercrime

IPBeja Instituto Politécnico de Beja

15 de julho de 2022

1 – as ***Cidades Inteligentes***, *préentendimentos*… repetidos

- antes de mais, as ***Cidades Inteligentes*** são uma ***species*** do *genus* ***Territórios Inteligentes***, a par das ***Áreas Protegidas Inteligentes***, dos ***Destinos Turísticos Inteligentes*** **ou** dos ***Espaços Rurais Int*****eligentes**, incluindo a *Agricultura Inteligente*
- por seu turno, os ***Territórios Inteligentes***, enquadram-se nos ***Ambientes Inteligentes***, **tal como** as **casas**, as **fábricas**, os **hotéis**, os **museus**, os **edifícios públicos**, os **aeroportos e portos**, assim como as **estradas e** as **ferrovias**… ***inteligentes***
- em todos os casos, objetivamente, temos **sensores e ativadores**, **ligados** entre si por **redes**, e assentes em **sistemas informáticos** dotados de ***Inteligência Artificial***, *i.e.*, capazes de aprenderem e reagirem por si sós, dentro dos fins para os quais foram criados, **e** quase sempre **dependentes** de fornecimentos externos de **energia elétrica**
- além das **questões** ligadas ao acesso e controle aos dados gerados, pessoais e não-pessoais, colocam-se as relativas à **segurança das** próprias **redes e sistemas**, assim como da **continuidade** do aprovisionamento da **energia elétrica**
- sendo as **Cidades Inteligentes** especialmente **vulneráveis a incidentes**, de todo tipo

- aliás, **esta** especial **vulnerabilidade** acaba de ser **assumida** pelas **Instituições** da União Europeia, até explicitamente:

  "Cities are increasingly connecting their utilities to their digital networks, to improve urban transport networks, upgrade their water supply and waste disposal facilities and make the heating of lights and buildings in the city more efficient. These digitalized utilities are vulnerable for cyber-attacks and run the risk to, in case of a successful attack, harm citizens at a large scale due to their interconnectness. Member States should develop a policy that addresses the development of these connected (or Smart) cities, and their potential effects on society, as part of their national strategy." ([Novo] *Considerando* 26e)

  (Texto, quase, final da *Diretiva NIS 2* / *SRI 2*, acordado entre o Parlamento Europeu e o Conselho no dia 13 de maio e publicado a 17 de junho, *infra*)

2 – sobre as ***gerações anteriores***… mesmo se ainda *in fieri*

3 – as razões e o sentido da ***mudança de rumo***

- com a ***Estratégia da UE para a União da Segurança*** (COM(2020) 605 final, de 27 de julho) a **Comissão Europeia** evidenciou como a Pandemia mostrara como a **vida em sociedade** estava **dependente** dos bom funcionamento dos **sistemas de informação e** das respetivas redes de comunicações
- mas **também vulnerável a ataques** da múltiplas origens, incluindo as **ameaças híbridas**, frequentemente patrocinados ou apoiados por Estados terceiros
- o que tornou **necessária** uma **mudança *geracional* das respostas**, também normativas, por parte da UE, dos Estados-Membros e da Sociedade no seu conjunto, articuladamente
- **especificadas** na ***Estratégia de Cibersegurança da UE para a Década Digital*** (JOIN(2020) 18 final, de 16 de dezembro) da **Comissão Europeia** e do **Alto Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança**
- estas **considerações** são **ainda mais relevantes para as *Cidades Inteligentes***, embora não sejam referidas em nenhuma das Comunicações da Comissão

4 – as **iniciativas legislativas**… agora, no término do seu curso

- um **novo regime transversal**: a **Proposta de Diretiva** relativa a ***medidas destinadas a garantir um elevado nível comum de cibersegurança na União*** e que revoga a Diretiva (UE) 2016/1148 [***Diretiva NIS 2 / SRI 2***] (COM(2020) 823 final, de 16 de dezembro), cujo acordo foi fechado a 13 de maio de 2022, tendo como **principais novidades**:
  - **âmbito de aplicação**: a administração pública, mas com opção dos Estados-Membros quanto ao nível local; a energia; os transportes, incluindo os "operadores de sistemas de transporte inteligentes"; as águas, potáveis e residuais; a saúde; e as infraestruturas digitais, incluindo as redes públicas de comunicações eletrónicas e respetivos os prestadores de serviços, dentro das que mais nos importam, que **sejam essenciais e importantes**
  - **regras mais exigentes** e precisas para a **gestão de risco e** para a **notificação de incidentes**, estas simplificadas, mas com prazos mais curtos, **e** ainda **responsabilizando os gestores de topo das organizações pelos incumprimentos**
  - **articulação com os regimes setoriais** referentes à resiliência das entidades críticas e à resiliência operacional digital do setor financeiro, *infra*
- a ser **transposta** até **21 meses após a respetiva publicação**

- a que **acresce** um **regime especial** com base na **Proposta de Diretiva** relativa à ***resiliência das entidades críticas*** (COM/2020/829 final, também de 16 de dezembro), neste caso, o acordo entre o Parlamento Europeu e o Conselho foi obtido a 28 de junho
  - vem **substituir** a **Diretiva 2008/114/CE**, de 8 de dezembro, relativa à **identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção**
  - para além da **energia e** dos **transportes**, passará a abranger os **mesmos setores** que a ***Diretiva NIS 2*** / **SRI 2**, a propósito da **segurança física** das "**entidades críticas**" e equivalentes
  - com o **objetivo** de **prevenir e**, sobretudo, **garantir a resiliência**, *i.e.*, a **continuidade das infraestruturas e dos serviços essenciais** necessários para efetivar as **funções sociais e** ao **funcionamento do mercado interno**, **perante quaisquer ameaças**, internas e externas, naturais ou de fonte humana
  - com **avaliações periódicas** exigentes para a **identificação dos riscos**, por parte dos Estados-Membros e das próprias entidades, a que acrescem **medidas**, técnicas e organizativas, adequadas **para assegurar a resiliência**, além da **notificação** obrigatória **dos incidentes**
  - o que **envolve** as redes e os **sistemas de informação**, impondo uma **articulação** entre as **autoridades competentes**, nacionais e europeias

- o um outro, o resultante da **Proposta de Regulamento** relativo à ***resiliência operacional digital do setor financeiro*** e que altera os regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014 [***Regulamento DORA***] (COM/2020/595 final, de 24 de setembro), com o acordo a datar de 11 de maio último
  - **assentará**, enquanto *lex specialis* explícita, **sobre** a ***Diretiva NIS 2*** / ***SRI 2***, mas com um **maior nível de exigência**, para **garantir a continuidade dos serviços financeiros**, perante quaisquer ameaças, o que também implicará uma articulação entre as autoridades
  - com **medidas organizacionais e tecnológicas**, incluindo sistemas de gestão de riscos, testes de resiliência, testes de penetração em regime de funcionamento, **e deveres de reporte de incidentes**
  - **importa-nos** pelos **serviços de pagamento e**, também, **de identificação** que neles assentam
- **e**, ainda, cumpre não esquecer a **derrogação** nos regimes relativos à **segurança no *Código Europeu das Comunicações Eletrónicas*** (Diretiva (UE) 2018/1972, de 11 de dezembro), resultante da ***Diretiva NIS 2*** / ***SRI 2***

5 – as **implicações para as fontes nacionais**, apenas telegraficamente…

- **quanto** à ***Diretiva NIS 2*** **/** ***SRI 2***, a **Lei n.º 46/2018**, de 13 de agosto, estabelece o ***Regime Jurídico da Segurança no Ciberespaço***, **e** o **Decreto-Lei n.º 65/2021**, de 30 de julho, que o regulamenta, **terão de ser reformulados**, embora até adiantem algumas questões e soluções, mormente o segundo
- **o mesmo** para a **Diretiva** relativa à ***resiliência das entidades críticas***, pois o **Decreto-Lei 20/2022**, de 28 de janeiro, aprova os ***procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias***, [substituindo o Decreto-Lei n.º 62/2011] **antecipou** boa parte do previsto na mesma
- com o **Regulamento DORA**, **cairá** o **Decreto-Lei n.º 91/2018**, de 12 de novembro, aprova o ***regime jurídico dos serviços de pagamento e da moeda eletrónica***, **nesta matéria**
- **e**, ainda, o **processo legislativo** da **Proposta de Lei 6/XV/1 - Aprova a Lei das Comunicações Eletrónicas e transpõe a Diretiva (UE) 2018/1972, que estabelece o Código Europeu das Comunicações Eletrónicas**, de 24 de abril de 2022, deverá **excluir os preceitos relativos à «Segurança das redes e serviços»…**