

**X Curso Intensivo de Verão de
Direito de Autor e da Sociedade da Informação**



**Vigilância e Proteção de Dados
nas comunicações eletrónicas
em especial os ‘dados de tráfego’**

Manuel David Masseno



Um *Pré-entendimento* constitucional:

- na **Sociedade da Informação**, o equilíbrio conflitual entre os Poderes e as Liberdades passa pela consideração da **Autodeterminação Informacional**
 - hoje já não faz sentido pensar em termos de privacidade
- daí a **constitucionalização** da proteção de dados:
 - Portugal (Art.º 35.º da **Constituição da República Portuguesa**)
 - União Europeia (Art.º 16.º do **Tratado da União Europeia** e Art.º 8.º da **Carta dos Direitos Fundamentais da União Europeia**)

- **Micro-sistema centrado na Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, 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**
 - atualmente em revisão...
- **Em Portugal, a transposição foi realizada pela Lei n.º 67/98, de 26 de Outubro, a *Lei da Proteção de Dados Pessoais***

Colocação do problema:

- o **acesso, pelos Poderes Públicos e Privados, aos dados** como uma das questões mais controversas na regulação europeia da Sociedade da Informação
- em especial aos **“dados de tráfego”**
- é este um **ponto nevrálgico na ponderação entre a eficácia da investigação criminal e a salvaguarda das Liberdades Fundamentais**, bem como na efectivação de outros interesses, como os dos titulares de direitos intelectuais
 - **monitorização, v.g., HADOPI ou Novo Governo e a IGAC**

Colocação do problema:

- Também para os Prestadores de Serviços da Sociedade da Informação, a abstenção de acesso aos dados é especialmente relevante
- Aliás as **isenções de responsabilidade** dos Art.ºs 12.º a 14.º da **Diretiva 2000/31/CE**, do Parlamento Europeu e do Conselho, de 18 de Junho de 2000 (**'Diretiva sobre comércio eletrónico'**) dependem disso mesmo, como demonstram
 - o **Acórdão** de 23 de Março de 2010, Caso **Google France** (C-236/08 a C-238/08) e
 - o **Acórdão** de 12 de Julho de 2011, Caso **L'Oréal** (C-324/09)

Também releva a recente Reforma da Regulação das Comunicações Eletrónicas:

- **Diretiva 2009/136/CE** do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que altera [...], a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrónicas [...] (**'Diretiva Cidadãos'**)
- **“As medidas nacionais relativas ao acesso ou à utilização de serviços e aplicações através de redes de comunicações electrónicas pelos utilizadores finais devem respeitar os direitos fundamentais dos cidadãos, nomeadamente em relação à privacidade e ao direito a um processo equitativo previsto no artigo 6.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais.”**

- “No caso de violação de dados pessoais, o prestador dos serviços de comunicações electrónicas acessíveis ao público comunica, sem atraso injustificado, a violação à autoridade nacional competente. **Caso a violação de dados pessoais possa afectar negativamente os dados pessoais e a privacidade do assinante ou de um indivíduo, o prestador notifica essa violação ao assinante ou ao indivíduo sem atraso injustificado.**”, **Art.º 4.º n.º 3**
- “Os Estados Membros asseguram que **o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas**, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento.”, **Art.º 5.º n.º 3**

Recentrando-nos

Qual o nosso **objeto** em questão, isto é, de que dados estamos a falar?

- **“Dados’**: os **dados de tráfego e os dados de localização**, bem como os dados conexos necessários para identificar o assinante ou o utilizador” (Art.º 2.º n.º 2 alínea a) da **Diretiva 2006/24/CE**, do Parlamento Europeu e do Conselho, de 15 de Março de 2006, **relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações**)

Especificando:

- “**Dados de tráfego**’ são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas [...]”
- “**Dados de localização**’ são quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível.” (**Art.º 2.º** alíneas **b) e c)** da **Diretiva 2002/58/CE**, do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao **tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas**)

Antecedentes, normativos:

Numa primeira fase, o **objectivo** foi o da protecção contra o processamento privado destes dados:

- “1. [...] os **dados de tráfego** relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações electrónicas publicamente disponíveis **devem ser eliminados ou tornados anónimos quando deixem de ser necessários** para efeitos da transmissão da comunicação.
- 2. Podem ser tratados dados de tráfego necessários para efeitos de facturação dos assinantes e de pagamento de interligações. O referido tratamento **é lícito apenas até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado.**” (Art.º 6.º da mesma Directiva)

Antecedentes, normativos:

No mesmo instrumento, era já prevista a possibilidade de retenção de dados:

- “Os Estados-Membros podem adoptar **medidas legislativas para restringir o âmbito dos direitos e obrigações** previstos [...] que essas restrições constituam uma **medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional** (ou seja, a segurança do Estado), **a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas.** [...] Para o efeito, os Estados-Membros podem designadamente **adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado**, pelas razões enunciadas no presente número.”, **Art.º 15.º n.º 1**

Com **cautelas reforçadas**, ligadas ao respeito pelos **Direitos dos Homem**:

- “[...] Todas as **medidas** referidas no presente número deverão ser **conformes com os princípios gerais do direito comunitário**, incluindo os mencionados nos n.ºs 1 e 2 do **artigo 6.º** do Tratado da União Europeia).” (**Art.º 15.º n.º 1 da Diretiva relativa à privacidade e às comunicações electrónicas**)
- Porém, esta *abertura* **não foi utilizada**, nem seria necessária em face do ***Princípio da Especialidade*** (**Art.ºs 4.º n.º 1 e 5.º do TUE**).

Antecedentes, materiais (a *occasio legis*):

- os **atentados terroristas** de Madrid de 11 de Março de 2004 e de Londres de 7 de Julho de 2005, e as
- **Dificuldades na investigação policial**, apenas superadas pelo acesso aos dados de conexão telefónica
- **pressão das opiniões públicas e dos Governos sobre o Parlamento Europeu** no sentido de ser relaxada a, habitual, atitude “garantista” dos Direitos Fundamentais no Processo de Co-decisão
- O que permite qualificar a Directiva de 2006 como uma peça de “**Legislação de Emergência**”, com as inerentes restrições hermenêuticas

Conteúdo essencial da Diretiva relativa à conservação de dados:

- Trata-se de disciplinar “[...] as obrigações dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista **garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves**, tal como definidos no direito nacional de cada Estado-Membro.”, **Art.º 1. n.º 1**
- E “Os Estados-Membros devem assegurar que as categorias de dados [...] sejam conservadas por **períodos não inferiores a seis meses e não superiores a dois anos**, no máximo, a contar da data da comunicação.”, **Art.º 6.º**

Este regime tem estado sob, intenso, escrutínio da **Jurisprudência, Europeia e sobretudo Nacional:**

- em face do **Princípio do Primado** do Direito da U.E. sobre os Direitos nacionais, os **Tribunais Nacionais** apenas têm podido avaliar as Leis de transposição e considerado **inconstitucionais** vários preceitos das mesmas, como ocorreu já na Alemanha, na Roménia e na Bulgária, e
- mas o Tribunal de Justiça da União Europeia está em vias de o fazer relativamente à própria Directiva, como veremos

A Sentença do Tribunal Constitucional da Alemanha (Sentença n.º 10/2010, de 2 de Março)

Considerou **inconstitucional** a Lei de Emenda da Vigilância das Telecomunicações (*Gesetz zur Neuregelung der Telekommunikationsüberwachun*), de 21 de Dezembro de 2007

A **fundamentação** da Sentença centrou-se no seguinte:

- provocou um legítimo **alarme social**
- **restringe** acentuadamente **Direitos Fundamentais** garantidos pela *Grundgesetz* (Art.º 10 sobre a Confidencialidade das Telecomunicações e o Direito à Auto-determinação Informacional)
- **não** se adequa aos **Princípios da Proporcionalidade** e da **Certeza**, ao não especificar claramente os crimes a que se aplicaria e a possibilitar o acesso à um número excessivo de autoridades

Também o Tribunal Constitucional da Roménia (Decisão n.º 1258, de 8 de Outubro de 2009)

Considerou **inconstitucional** a Lei 298/2008, que transpôs a Directiva.

A fundamentação da Sentença sublinha que:

- em si mesma, a medida pode **colocar em questão os próprios direitos fundamentais** ao segredo da correspondência, à privacidade e à liberdade de expressão, protegidos pela Constituição Romena (Art. 26.º, 28º e 30.º), a DUDH (Art. 12.º e 19.º) e a CEDH (Art. 8º e 10.º)
- cita a **Jurisprudência do Tribunal Europeu dos Direitos do Homem** (Casos *Klass et al. c. Alemanha*, 1978 e *Dumitru Popescu c. Roménia*, 2009)
- de onde resulta um **dever**, para o Legislador nacional, de **ser o mais restritivo possível** na transposição

Ainda o Supremo Tribunal Administrativo da Bulgária (Sentença de 18 de Dezembro de 2008)

Anulou o Art.º 5.º do Regulamento n.º 40 da Agência Estatal para as Tecnologias da Informação e da Comunicação e do Ministério do Interior, que **permitia o “acesso passivo através de um terminal de computador” pelo Ministério do Interior**, bem como o **acesso aos dados** retidos pelos ISPs e os operadores de comunicações móveis, **sem autorização judicial**, por parte dos serviços de segurança e de investigação criminal

- **assim, o preceito violaria o Art.º 32 da Constituição Búlgara e o Art.º 8.º da CEDH/LF (Protecção da Privacidade)**

Finalmente, o Tribunal Superior da Irlanda suscitou junto do TJUE a questão da validade da Directiva em face dos Tratados, em 5 de Maio de 2010

- trata-se de determinar **se uma vigilância em massa é compatível com a salvaguarda dos Direitos Fundamentais**
- em suma, volta a consideração da ***Proporcionalidade***, mesmo não indicada expressamente no texto da Decisão
- cabe recordar que a **U.E. está vinculada pela CEDH e pela sua Carta dos Direitos Fundamentais e pelas tradições constitucionais comuns aos Estados membros, Art.º 6.º do Tratado U.E.**

Recordar ainda o **Acórdão** de 29 de Janeiro de 2008, Processo C-275/06, Productores de Música de España (*Promusicae*) / Telefónica de España SAL

O qual teve por **objecto** o **acesso a dados de tráfego** “[...] o direito comunitário exige que os referidos Estados, na transposição dessas directivas, zelem por que seja seguida uma interpretação das mesmas que permita **assegurar o justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária**. Seguidamente, na execução das medidas de transposição dessas directivas, compete às autoridades e aos órgãos jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com essas mesmas directivas mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o **princípio da proporcionalidade**.”

Em Portugal, uma transposição *razoável*

Lei n.º 32/2008, de 17 de Julho, relativa conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações

- “**Crime grave**’, crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.”, **Art.º 2.º n.º 2 alínea g)**
- “As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo **período de um ano** a contar da data da conclusão da comunicação ”, **Art.º 6.º**

“1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por **despacho fundamentado do juiz** de instrução, **se houver razões para crer que a diligência é indispensável** para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 - Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido

4 - A decisão judicial de transmitir os dados deve **respeitar os princípios da adequação, necessidade e proporcionalidade**, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.”, **Art.º 9.º**

Em suma, com respeito pelos limites constitucionais:

- do **Art.º 18.º n.º 2**, em cujos termos “A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.”
- bem com e em especial, dos **Art.º 34.º n.º 4**. “É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal” e **35.º n.º 2** “A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.”

Orientação mantida na nova *Lei do Cibercrime* (Lei n.º 109/2009, de 15 de Setembro)

Implementou

- a **Decisão-Quadro** 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a **ataques contra os sistemas de informação**

e, sobretudo

- a Convenção do Conselho da Europa, de 23 de Novembro de 2001, sobre o Cibercrime, **“Convenção de Budapeste”**

- Assim, “As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.”, **Art.º 11.º n.º 2)**
- Embora seja viável ordenar a preservação expedita (Art.º 12.º), bem como a apreensão de dados (Art.º 16.º) e de registos de comunicações (Art.º 17.º), a interceção de comunicações (Art.º 18.º) e até desenvolver ações encobertas (Art.º 19.º), para um elenco de tipos mais amplo que o dos “crimes graves”
- **Evitámos** a evolução para um **Direito Penal do Risco** (*Risikostrafrecht*), com uma compressão das Liberdades Fundamentais, a partir de considerações securitárias

Mas, voltando à *Proporcionalidade*, fará mesmo sentido impor aos ISPs a conservação destes dados?

Segundo Heinz Kiefer, Presidente da Eurocop (Confederação Europeia Polícia), “[...] continua a ser fácil para os criminosos evitar a detecção através de meios bastante simples, por exemplo os cartões telefónicos podem ser comprados a fornecedores estrangeiros e frequentemente trocados. Daí resulta que é feito um vasto esforço com poucos mais efeitos nos criminosos e nos terroristas que o de os irritar. Acções como estas não são susceptíveis de reforçar a confiança dos cidadãos na capacidade da UE em dar solução às suas exigências de protecção contra os crimes graves e o terrorismo.” (2005)

Possível, **ponto de viragem** é o **Relatório da Comissão** ao Conselho e ao Parlamento Europeu - **Avaliação da Diretiva relativa à Retenção de Dados** (COM(2011) 225final) de 18 de Abril de 2011:

- avaliação **obrigatória** em face do Art.º 14.º da própria Diretiva, até 15 de Setembro de 2010...
- assumiu como um dado a necessidade da Diretiva, e **pediu aos Estados-membros elementos e dados de suporte**
- Carta enviada a 15 de Julho, **só 10 responderam**, sendo que Portugal não o fez...

“The moment of truth for the Data Retention Directive’ [...] It goes without saying that such a massive invasion of privacy needs profound justification. This justification is not established if the retention of all such information is only considered ‘a useful tool’ for law enforcement authorities or if it just ‘helps’ solving serious crimes.” (**Peter Hustinx** - Autoridade Europeia para a Protecção de Dados, Conferência sobre a Diretiva, Bruxelas, 3 Dezembro de 2010).

Sendo de atender também ao **“Shadow evaluation report”**, divulgado pela *European Digital Rights*, publicado em simultâneo.

Questões essenciais:

- **Base Jurídica**, articulada com os objetivos da Diretiva, **Art.º 1.º**
 - relação com a construção do mercado interno, **Art.º 114.º** do TFUE
 - **não com cooperação policial**, ou com acesso aos dados retidos
- **Acesso aos dados**: Por que Autoridades? Com que métodos e em que condições, **Art.º 4.º**?
 - por outras palavras, **quem pode ter acesso aos dados e em que circunstâncias?**

- **Âmbito da retenção e categorias de dados cobertas, Art.º 1.º**
 - como lidar com os “anonimizadores”, por exemplo;
- **Períodos de retenção, Art.ºs 6.º e 12.º**
- **Proteção de dados e a ação das Autoridades de Supervisão, Art.ºs 7.º e 9.º**
- **Estatísticas, Art.º 10.º**
- **Balanço da Jurisprudência**
 - **Nacional, mas também do TEDH e do TJUE**

Em conclusão, a **Comissão Europeia** assume uma **abertura a alterações à Diretiva:**

- Depois de uma avaliação do impacto, sobretudo em termos de eficácia diante de políticas alternativas:
 - aprofundar a harmonização
 - compensação dos custos dos operadores de comunicações eletrónicas

E, sobretudo

- assegurar uma melhor observância do ***Princípio da proporcionalidade***:
 - limitação dos objetivos e dos tipos de dados a serem retidos
 - eventual redução dos prazos de retenção,
 - controle independente dos acessos
 - limitação das autoridades com acesso
 - reforço das medidas técnicas de segurança
 - e prevenção da *data mining*

No que se refere à **Jurisprudência relevante**:

- O **Tribunal Superior da Irlanda** suscitou junto do TJUE a questão da **validade da Directiva** em face dos Tratados, em 5 de Maio de 2010
 - trata-se de determinar **se uma vigilância em massa é compatível com a salvaguarda dos Direitos Fundamentais**
 - em suma, volta a consideração da ***Proporcionalidade***, mesmo não indicada expressamente no texto da Decisão

- Cabe, sempre, recordar que a U.E. está vinculada pela **Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais**, pela sua *Carta dos Direitos Fundamentais* e ainda pelas *tradições constitucionais comuns aos Estados membros*, Art.º 6.º do Tratado da U.E.

- **Tribunal Europeu dos Direitos do Homem**
 - Acórdão de 4 de Dezembro de 2008
 - “In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State **[So] the retention at issue constitutes a disproportionate interference with the applicants' right** to respect for private life and cannot be regarded as necessary in a democratic society.”

- **Tribunal de Justiça da União Europeia**
 - **Acórdão** de 9 de Novembro de 2010, Casos **Schecke** (C-92/09) e **Eifert** (C-93/09)
 - dados de todos os beneficiários de ajudas no âmbito da PAC
 - sempre, o ***Princípio da proporcionalidade***
 - **Acórdão** de 10 de Fevereiro de 2009, Caso **Irlanda c. o Parlamento e o Conselho** (C-301/06)
 - **base jurídica da Diretiva**

Obrigado