



UNIVERSIDADE  
**FUMEC**  
Universidade de Idéias

# Vigilância e Privacidade na Sociedade em Rede

Belo Horizonte, 24/11/2011

***Manuel David Masseno***



**IPBeja**

INSTITUTO POLITÉCNICO  
DE BEJA



UBINET



Instituto Jurídico Interdisciplinar  
da Faculdade de Direito da Universidade do Porto

- **“A Sociedade em Rede é uma sociedade cuja estrutura social é composta por redes assentes nas tecnologias da informação e da comunicação” (Manuel Castells)**
  - perspectiva **diferente da Sociedade da Informação / Sociedade do Conhecimento**
  - os **aspectos cruciais** já não correspondem ao controle (“proprietário”) da informação, mas ao **acesso de cada nó aos outros nós da rede e ao controle do que circula na própria Rede**
  - inclusive, **noção de Governo eletrónico precisa de ser reformulada**

## Um *Pré-entendimento* constitucional:

- na Sociedade da Informação, o equilíbrio conflitual entre os Poderes e as Liberdades passa pela consideração da **Autodeterminação Informacional**
  - Hoje, quase, 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 Gfoverno de Portugal**

### 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.”**

## Vigilância e Privacidade na Sociedade em Rede

- “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 Diretiva 95/46/CE, nomeadamente sobre os objectivos do processamento.”, Art.º 5.º n.º 3

## Nos recentrando

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

- **“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 **proteção 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 Diretiva)

### 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 **cauteladas 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, devido a um reenvio prejudicial irlandês

### 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 Telekommunikationsüberwachung*), 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

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:

- “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)

**Obrigado**