

seminário | seminar

PROTEUS



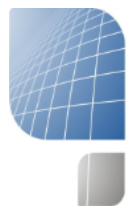
Co-financiado pela Comissão Europeia -
DG Assuntos Internos: Programa Prevenir
e Combater a Criminalidade

furto de identidade online prevenção, combate & apoio à vítima
online identity theft preventing, fighting & supporting victims

Polícia Judiciária, Lisboa, 29/30.10.2015

Do furto de identidade digital **nas Fontes Internacionais e Europeias**

Manuel David Masseno



UBINET



IPBeja

I – Alguns *Pré-entendimentos*

a) o objeto

- o **furto de identidade**, em sentido amplo: a **obtenção**, **detenção**, **transferência de dados pessoais** de uma pessoa, de forma ilícita, com o objetivo de praticar, ou em conexão com a prática, de crimes ou de outras **atividades ilícitas** (a partir do *Documento de Orientação sobre o Furto de Identidade Em-Linha*, de 2008, da OCDE)
- em causa está a **identidade digital** de alguém, os dados que permitem caraterizar uma **persona electronica, no contexto da Sociedade em Rede**
- inclui tanto a **obtenção** (*Identity theft* em sentido restrito), como a **transferência** e a **utilização** (*Identity abuse*), ilícitas, **dos dados**

- **sempre dados pessoais:**
 - “[...] qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação (‘titular dos dados’).” (Art.º 2.º, alínea a) da **Convenção do Conselho da Europa para a Proteção dos Indivíduos face ao Tratamento Automático de Dados Pessoais** - Convenção 108, de 28 de janeiro de **1981**) ou
 - “[...] qualquer informação relativa a uma pessoa singular identificada ou identificável (‘pessoa em causa’); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.” (Art.º 2.º alínea a) da **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**)

b) uma prioridade, o Sistema Financeiro

Se nos colocarmos na perspetiva da **União Europeia**, o foco foi o do **combate às fraudes e ao Terrorismo**

- a **Comunicação da Comissão [...] “Um Quadro para as Ações de Combate à Fraude e à Falsificação de dos Meios de Pagamento que Não em Numerário”** (COM(1998), 395 final, de 1 de julho de 1998)
- a **Decisão-quadro do Conselho**, de 28 de maio de 2001, relativa ao **combate à fraude e à falsificação de meios de pagamento que não em numerário e**
- a **Diretiva 2005/60/CE** do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativa à **prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo**

c) e aproximações diversas

Da mesma forma, a **OCDE** partiu de considerações fragmentárias, a propósito da segurança das transações eletrónicas em geral:

- as Linhas Diretrizes que Regem a Proteção dos Consumidores no Contexto do Comércio Eletrónico, de 1999
- as Linhas Diretrizes que regem a Proteção dos Consumidores contra as Práticas Comerciais Transfronteiriças Fraudulentas e Enganosas, de 2003 até
- ao Documento de Orientação (*Scoping Paper*) sobre o Furto de Identidade Em-Linha, de 2008
- e às Orientações de Políticas (*Policy Guidance*) sobre o Furto de Identidade Em-Linha, também de 2008

d) as Fontes essenciais

- no que se refere à **proteção de dados pessoais**:

- a *Convenção do Conselho da Europa para a Proteção dos Indivíduos face ao Tratamento Automático de Dados Pessoais*, de 1981
- **Diretiva 95/46/CE**, do Parlamento Europeu e do Conselho, de 1995

- em **matéria penal**:

- a *Convenção* do Conselho da Europa **sobre o Cibercrime**, adotada em **Budapeste**, a 23 de novembro de 2001
- a **Diretiva 2013/40/UE** do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, **relativa aos ataques contra os sistemas de informação**, e que revoga a Decisão-Quadro 2005/222/JAI

II – A Obtenção dos Dados

a) os dados em aberto (OSINT)

Em causa está o **tratamento de dados pessoais livremente disponíveis na Rede**, facultados pelos respetivos titulares ou deixados por terceiros

- **será aplicável *in casu* a “exceção doméstica”** (Art.º 3.º n.º 2 da Diretiva 95/46/CE)?
 - **não com finalidades políticas ou sociais**
 - **não a grande número de dados**, incluindo de pessoas potencialmente desconhecidas
 - **Acórdãos Lindqvist** (C-101/01), de 6 de novembro de 2003, e, sobretudo, **Satamedia** (C-73/07), de 12 de setembro de 2008, **do Tribunal de Justiça da UE**

- e quanto aos dados provenientes de registos públicos?
 - não é compatível com o **princípio da vinculação finalística** e sobretudo com o **princípio do tratamento leal e lícito** (Art.º 6.º n.º 1, alíneas b) e a) da Diretiva 95/46/CE)
 - nem com o **respeito pela vida privada** (Art.º 1.º n.º 1 da Diretiva 95/46/CE), garantido pela **Carta dos Direitos Fundamentais da União Europeia** (Art.ºs 7.º e 8.º), enquanto corolário do à Dignidade do ser humano (Art.º 1.º)
- a criminalização dos tratamentos de dados não autorizados dependerá das Leis nacionais de transposição (Art.º 24.º da Diretiva 95/46/CE)

b) pelo acesso ilícito

- criminalizado pela **Convenção de Budapeste** (Art.º 2.º) e pela **Diretiva 2013/40/UE** (Art.º 3.º)
- obtenção de dados sem autorização do titular de direitos sobre o sistema, ou parte dele (Art.º 2.º alínea d) da **Diretiva 2013/40/UE**)
- porém, enquanto a **Convenção de Budapeste** prevê a **penalização da tentativa** (Art.º 8.º n.º 2), a **Diretiva 2013/40/UE** vai em sentido contrário (Art.º 8.º n.º 2 *a contrario*), com consequências em termos de *Web Harvesting* de nomes e de senhas

c) pela intercepção ilícita

- criminalizada pela **Convenção de Budapeste** (Art.º 3.º) e pela **Diretiva 2013/40/UE** (Art.º 6.º)

III – A Transmissão a Terceiros

Objeto de uma criminalização *per se*, e não enquanto trabalhos preparatórios, **tanto** na ***Convenção de Budapeste*** (Art.º 6.º n.º 1 alínea a) ii) **quanto** na ***Diretiva 2013/40/UE*** (Art.º 7.º)

- designadamente “uma palavra passe, um código de acesso ou dados similares que permitem aceder, no todo ou em parte, a um sistema informático, com a intenção de os utilizar para cometer qualquer uma das infrações [...]” (***Convenção***)

IV – Utilização Indevida

a) no acesso ilícito

- *vide supra*
- incluindo **a entrada**, não autorizada, **em Perfis de terceiros em Redes Sociais...**

a) na falsificação informática

- **criminalizada** apenas **pela *Convenção de Budapeste*** (Art.º 7.º), como “[...] a introdução, a alteração [...] de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis.”

c) na burla informática

- também só **criminalizada pela *Convenção de Budapeste*** (Art.º 8.º), e caracterizada por corresponder a um “[...] prejuízo patrimonial causado a outra pessoa por meio de: a) Qualquer introdução, alteração [...] de dados informáticos; [...] com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo.”

d) e ainda enquanto elemento qualificante

- tal como previsto na **Diretiva 2013/40/UE** (Art.º 9.º n.º 5), quando se dê uma “[...] utilização abusiva de dados pessoais de outra pessoa com o objetivo de conquistar a confiança de terceiros, causando assim danos ao legítimo titular da identidade, tal possa, de acordo com o direito nacional, ser considerado uma circunstância agravante, salvo se tal circunstância já estiver abrangida por outra infração punível pelo direito nacional.”
- **apenas** para os tipos **interferência ilegal no sistema** (Art.º 4.º / Sabotagem informática) **ou interferência ilegal nos dados** (Art.º 5.º / Dano nos dados), remetendo outra abordagem da “usurpação de identidade” para o futuro (Considerando 14)