

Os Desafios de Segurança Invisível

As novas tecnologias ao serviço da
segurança e
as questões de privacidade -

Conferência a Segurança e o desenvolvimento sustentável em Portugal 2006



O efeito “*bin laden*”

- A utilização de dados biométricos nos passaportes, bilhetes de identidade, documentos de viagem (a tecnologia RFID)
- Instalação de câmaras de videovigilância na via pública
- Novos prazos de conservação dos dados de tráfego e localização para fins de segurança (Directiva 2006/24/CE de 16 de Março)



Investigação, detecção e repressão de crimes graves

Algumas formas de segurança invisível:

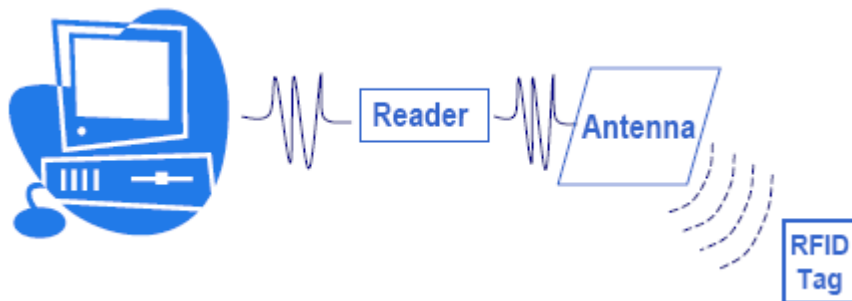
- A “vigilância” em espaços públicos (videovigilância em locais públicos e auto-estradas, a matrícula electrónica, etc.)
- A “vigilância nos nossos bolsos” nos espaços privados e nos espaços públicos (os telefones móveis, os cartões de fidelização, os cartões de crédito, o passaporte electrónico, etc.)



➤ Identificação por Rádio Frequência (RFID)

“Método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos chamados tags RFID”.

Uma tag RFID é um pequeno objecto, que pode ser colocado em uma pessoa, animal ou produto e contém chips de silício e antenas que lhe permitem responder aos sinais de rádio enviados por uma base transmissora” wikipedia



Existem diversos tipos de sistemas RFID (ativos ou passivos, em função das frequências utilizadas, capacidade de “leitura”/”escrita”, etc)

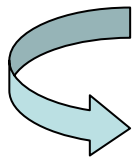


➤ Algumas potencialidade dos sistemas RFID





- Alguns dos desafios jurídicos da RFID
 - Gestão e utilização de frequências
 - Interoperabilidade dos sistemas
 - Propriedade intelectual
 - Segurança, privacidade e dados pessoais



Um dos principais desafios ao crescimento da tecnologia RFID



“ The overriding message that comes out of the consultation is that citizens have concerns over privacy issues”. I take this message from the consultation very seriously, because I want to see the benefits of RFID in terms of better services and productivity gains. But, there has to be a clear win-win, with the citizens on board.”

Viviane Reding

(Comissária Europeia da Sociedade da Informação e Media)



✓ Enquadramento Legal

- Lei n.º 67/98 (Lei de Protecção de Dados Pessoais – LPDP)
Directiva 95/4/CE
- Lei n.º 41/2004 (Sector das Comunicações Electrónicas)
Directiva 2002/58/CE
- Código do Trabalho



✓ Enquadramento Regulamentar

- Deliberações da Comissão Nacional de Protecção de Dados nº 9/2004 (CNPD) de 13 de Janeiro de 2004
- “*Working document on data protection issues related to RFID technologies*” do Grupo 29
- Política Europeia para o RFID



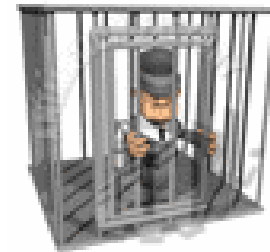
✓ Conhecer as regras para não ficar “preso”

➤ Pela falta de formalismos

➤ A uma tecnologia limitada

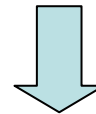
➤ ...

➤ “Atrás das grades”



O incumprimento do regime jurídico da privacidade pode dar origem a responsabilidade criminal

- Nem todos os sistemas RFID colocam questões de privacidade e **tratamento de dados pessoais**



Qualquer tipo de operação que incida sobre qualquer tipo de dados relativos a uma pessoa singular identificada ou

“Internet of things”



“Internet of People”

(um mundo onde bilhões de objectos reporta na sua localização, identidade e história através das comunicações wireless)

- Obter o **consentimento** do titular para o tratamento/informar o titular do tratamento



Colocar avisos nos produtos e nos locais

- Identificação do responsável pelo tratamento
- Identificação das finalidades do tratamento
- Identificação dos destinatários dos dados
- Tipo de dados recolhidos/tratados/interconexões
- Formas de acesso, rectificação, eliminação dos dados (dificuldades)
- Direito de oposição
- Como desactivar ou retirar a tags dos produtos
- Sempre que a leitura e a activação remotas das marcas RF sejam contempladas os titulares devem ser informados quando é que tal leitura/activação vai ocorrer

- Legalizar o tratamento dos dados junto da CNPD



- Recolher os dados para finalidades determinadas, explícitas e legítimas
- Assegurar que os dados recolhidos são adequados e pertinentes e não excessivos, atendendo às finalidades para que são recolhidos
- Eliminar os dados quando a sua manutenção deixar de ser pertinente para o objectivo definido



- Em alguns casos assegurar que o titular pode, a qualquer momento, interromper o tratamento dos dados - tecnologia que permita ao titular desactivar o “tag”.
- Assegurar o direito de acesso aos dados, por parte do titular.
- Obter autorização prévia da CNPD para realizar qualquer operação de interconexão de dados.
 - Adequação às finalidades legais ou estatutárias, aos interesses legítimos do responsável pelo tratamento
 - Não discriminação ou não diminuição dos direitos fundamentais do titular dos dados
 - Adequadas medidas de segurança

- Adotar medidas de segurança para proteger a confidencialidade dos dados (medidas de natureza técnica e organizativas)



- Standards (ISO, EPC* Global Inc) e Interoperabilidade (prós e contras)

- PETs (desactivadores temporários)

Os fabricantes, integradores e os Organismos de normalização têm um papel essencial



- Dotar os sistemas de protecções para evitar o acesso indevido aos dados – “PETs”* (encriptação dos dados e do processo de autenticação do leitor, medidas mais exigentes para o caso dos dados sensíveis).
- Adoptar soluções tecnológicas que possibilitem o direito de acesso, rectificação e eliminação dos dados (criação de sistemas de IT interactivos, de “*Killing Commands*”, o método “0”, escudos físicos, entre outros).
- Soluções inovadoras e competitivas.

* *Privacy Enhancing Technologies*



A violação das regras de tratamento de dados pessoais

- Responsabilidade civil pelos prejuízos causados.
- Responsabilidade criminal (pena de prisão até 2 anos ou pena de multa até 240 dias).
- Responsabilidade contra-ordenacional (coimas até € 30.000 e até € 5.000.000 nas comunicações electrónicas).
- Sanções acessórias (proibição temporária ou definitiva de tratamento, bloqueio, apagamento ou destruição dos dados; publicidade da sentença).

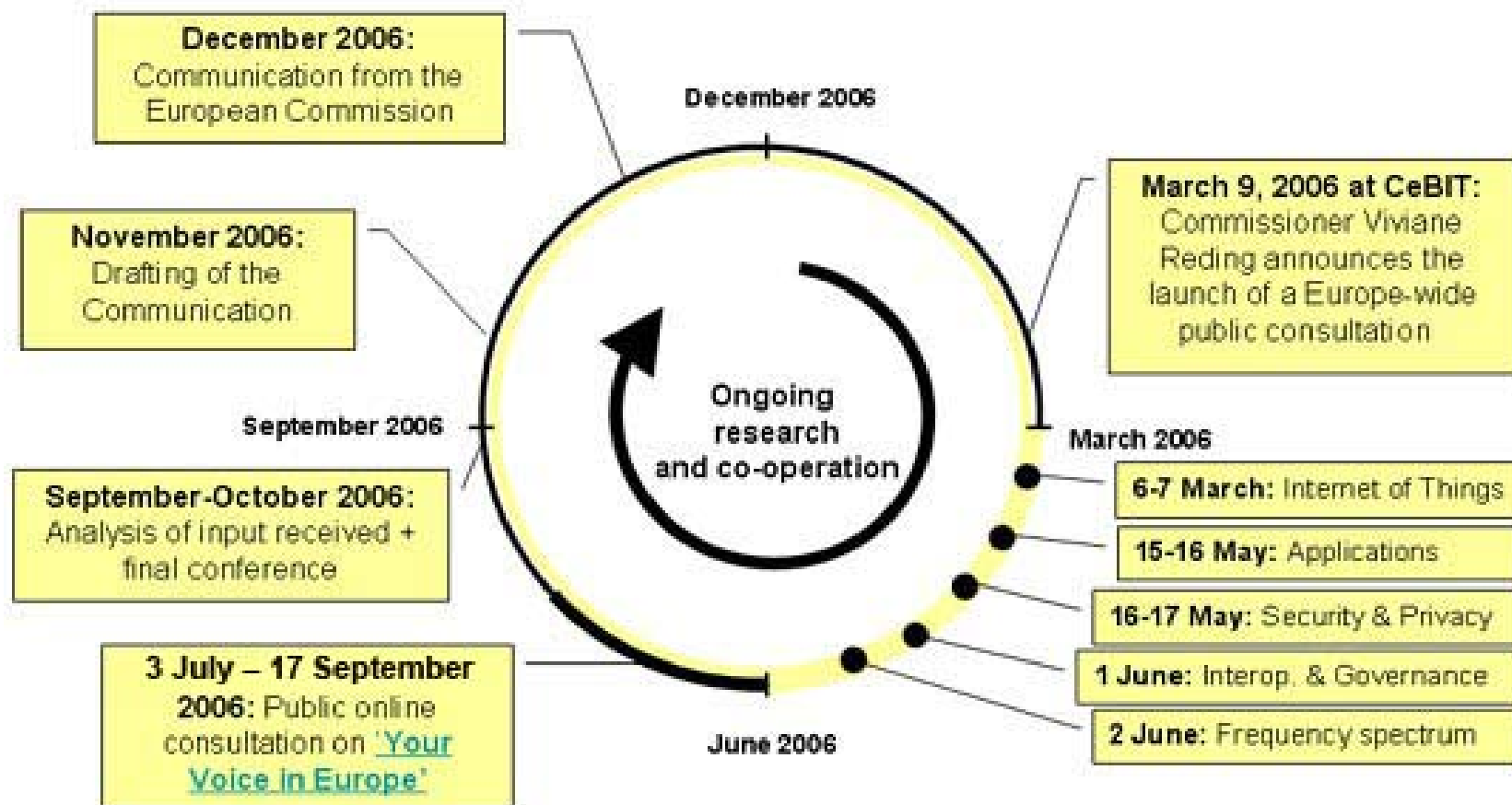


Pode ser crime...



- Omitir as notificações ou os pedidos de autorização à CNPD previstos na lei.
- Utilizar dados pessoais de forma incompatível com a finalidade da recolha ou com o instrumento de legalização.
- Aceder indevidamente ou facultar acesso indevido a dados pessoais.
- Promover ou efectuar interconexão ilegal de dados.
- ...

Roadmap: Towards an RFID Policy for Europe





- ✓ Resultados preliminares da consulta em matéria de segurança, privacidade e dados pessoais
- 66% dos participantes* consideraram que o actual enquadramento legal e regulamentar europeu é desadequado
 - Uma minoria de 14 % dos participantes manifestaram preferência pela “*self-regulation*” e pela introdução de regras de “*best practice*”.
 - Mas mais de metade consideraram que deveria ser aprovada legislação específica.

*Responderam à consulta aproximadamente 2,190 entidades



- 66% dos participantes consideraram que a melhor solução para ultrapassar as questões será através do desenvolvimento de soluções técnicas que permitam aos consumidores desactivar as *tags*, conjugadas com acções de sensibilização/educação dos consumidores
- Aproximadamente 50% dos participantes defendeu que as PETs devem ser obrigatórias nas aplicações RFID
- Em relação à utilização de *tags* em produtos de supermercado:
 - 61% manifestou-se no sentido de que estas devem ser automaticamente desactivadas na caixa de pagamento,
 - 46% defenderam que devem ser utilizadas “*tag autocolantes*” que possam ser facilmente removidas e
 - 40% consideraram que seria adequada a utilização de “*proximity tags*”

- 50% dos participantes consideraram que a limitação do alcance das “*proximity tags*” deve ser vista como um meio (completar) para assegurar o direito à privacidade, tendo uma forte maioria de participantes apontado para a distância de 10 cm.

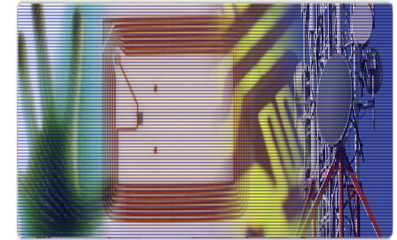
Em suma, as questões de privacidade devem ser resolvidas :

- Ao nível da política legislativa
- No domínio tecnológico (*privacy enhancing technologies*)



➤ Se é fabricante ou integrador

- Tenha em consideração as exigências de privacidade no desenvolvimento das soluções tecnológicas
- Observe de perto a “política da CE para os sistemas RFID”



➤ Se é utilizador da tecnologia/responsável pelo tratamento

- Adquira sistemas que ofereçam soluções técnicas que permitam dar resposta às questões de privacidade
- Tenha uma estratégia de privacidade para o ambiente RFID (obtenção da autorização dos clientes/legalização do sistema, etc.)

➤ Se é Cliente/Consumidor

- Mantenha-se atento e informado



MUITO OBRIGADA

Aviso:

Este documento destina-se única e exclusivamente a servir de suporte à apresentação no âmbito da Conferência “A Segurança numa perspectiva de criação de valor para as organizações e para a sociedade” organizado pela Premivalor, pelo que se encontra vedada a sua cópia ou circulação. As informações e opiniões expressas neste documento e na apresentação efectuada são de carácter geral, não substituindo o recurso a aconselhamento jurídico específico.