10.ª EDIÇÃO CAMINHO DOS HOSPITAIS
IPO COIMBRA
DESAFIOS DA CIBERSEGURANÇA

4 DE DEZEMBRO DE 2017

CARLA BARBOSA
CENTRO DE DIREITO BIOMÉDICO

Cibersegurança e dados pessoais? Qual a razão?

Informação de saúde em formato eletrónico (computadores)

Quem tem a obrigação de proteger – Lei 12/2005, de 26 de janeiro

Unidades de saúde depositárias da informação de saúde tem de garantir as medidas de segurança adequadas

- Mas:
- De quem é a informação?
- De que tipo de informação estamos a falar? Informação sensível ou pessoalissíma que requer uma proteção reforçada: legislação constituciinal, civil, penal…

- Esta informação de saúde é considerada como um dado pessoal.
- Há legislação própria relativa à proteção de dados pessoais.
  - **Diretiva n.º 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**
  - **Lei n.º 67/98, de 26 de Outubro - a designada Lei de Proteção de Dados Pessoais (LPDP)**
  - **Regulamento Geral Europeu sobre Proteção de Dados Pessoais**

- Europa com legislação fortemente protecionista;
- Nos termos da legislação da UE, os dados pessoais só podem ser recolhidos legalmente em condições estritas, com um objectivo legítimo.
- Além disso, as pessoas ou organizações que recolhem e gerem os dados pessoais devem protegê-los contra o uso indevido e devem respeitar determinados direitos dos titulares desses dados que são garantidos pela legislação da UE.
- Todos os dias, na UE, empresas, autoridades públicas e indivíduos transferem vastas quantidades de dados pessoais para além das fronteiras.
- Por conseguinte, foram estabelecidas regras comuns da UE para garantir que os dados pessoais gozam de um elevado nível de protecção em toda a UE.

O contexto que determinou a adoção da Diretiva 95/46/CE mudou.

O Mundo tornou-se uma Sociedade em Rede com os novos desafios carreados por:

-Universalização do acesso à Internet

-multiplicação dos operadores

-Globalização económica e cultura

-peso crescente das Redes Sociais

-Computação em nuvem

- A 4 de maio, foi publicado o REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE

- O Regulamento aplica-se em toda a UE a partir de 25 de maio de 2018. Contudo, após a publicação, as entidades devem começar o processo de adaptação às novas regras.

- A transição para o RGPD
- **um Regulamento**, já não uma Diretiva…
- possivelmente, **a principal mudança**; **deixando de existir 28 regimes harmonizados, para haver um único instrumento** (Art.º 288.º § § 2 e 3 do TFUE)
- **ainda que com margens para derrogação por parte dos Estados-membros**
- **exigiu um procedimento de cooperação e coerência**, entre as Autoridades nacionais (Art.ºs62 a 67.º)
- **resposta à Globalização**, sobretudo face aos EUA e suas empresas, **evitar** ao máximo **'forum shopping'**
- **resulta do reconhecimento da Proteção de Dados como uma matéria ao nível da União**

- Fim da regra de notificações prévias – Contudo exige a notificação obrigatória de violações de dados pessoais

- Aproxima a legislação existente aos rápidos desenvolvimentos tecnológicos do sector.

- Um único Regulador definido tendo em conta o local de estabelecimento principal da organização

- Saúde: os dados pessoais e os dados sensíveis (**a distinção é mantida e é aprofundada)**

"**«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada**, direta ou indiretamente, **em especial por referência a um identificador**, como por exemplo um nome, um número de identificação, dados de localização, **identificadores por via eletrónica** ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular**."** (Art.º 4.º 1)

- Dados sensíveis: **"É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa."** (Art.º 9.º n.º 1)

- Soluções diferenciadas quanto ao tratemnto de dados de saúde para fins assistenciais e para fins de investigação;
- O novo Regulamento mais permissivo quanto à investigação
- Deixa, no entanto, muito para regulamentação posterior por parte dos Estados

- Exemplos:
- Consentimento: continua a exigir um consentimento especifico e expresso no texto da lei no entanto, no preâmbulo do mesmo deixa a porta aberta para o *broad consent;*
- Afasta determinados direitos dos titulares dos dados pessoais em certas circunstâncias: p. ex. direito de acesso
- Fala expressamente em pseudoanonimização (o que não acontecia na Diretiva)
- Fala expressamente nos dados pessoais recolhidos em Biobancos (o que também não acontecia na Diretiva)

- Outras ideias gerais (novas) do novo Regulamento:
- Âmbito de aplicação territorial:
- âmbito do GDPR é alargado para que muitas empresas, com sede fora da UE, que estão a processar dados pessoais sobre os cidadãos da UE tenham de cumprir as regras do Regulamento e nomear um representante na UE
- O que abrange: p. ex. *cloud*

- As entidades que tratam os dados pessoais passam a ter deveres mais rígidos, de acordo com o Regulamento, em especial no que toca a:
  a. Segurança dos dados pessoais
  b. Manter documentação
  c. Cooperar com os Reguladores
  d. Nomeação de um *Data Protection Officer - Artigo 37.º*

- Todas as autoridades públicas e as empresas que desempenhem certas operações sensíveis de tratamento de dados terão igualmente de designar um **responsável pela proteção de dados**. As empresas cuja atividade principal não é o processamento de dados vão ser isentos desta obrigação, de modo a evitar a criação de burocracia.

- Tarefas do Data Protection Officer - *Artigo 39.º*
  1. Vigiar cumprimento
  2. Trabalhar com os representantes de trabalhadores
  3. Notificar violações de dados pessoais
  4. Realizar auditorias regulares
- Nomeado por **4 anos** (trabalhador) ou **2 anos** (prestador de serviços)

\

- Curso “O novo regulamento europeu de proteção de dados pessoais”
- Organização APAH – CDB - brevemente

- Obrigada!
- cbarbosa@fd.uc.pt