Ethics, Privacy, and Regulation in Informatics

Tópicos de Informática para Automação

Mário Antunes

22 de Dezembro de 2025

Universidade de Aveiro

Table of Contents i

Ética em Informática

RGPD (GDPR) e Garantia de Privacidade

AI Act Europeu

Como nos Protegermos e aos Nossos Utilizadores

Ética em Informática

O Impacto da Recolha e Partilha de Dados i

- **Data is Power**: Na era digital, “Dinheiro é uma coisa, mas dados são poder”.
- **Consequências no Mundo Real**:
  - **Manipulação Política**: Empresas de análise de dados (ex: Cambridge Analytica) usaram dados pessoais para fazer *micro-targeting* de eleitores, influenciando potencialmente resultados democráticos como o Brexit.
  - **Fraude Financeira**: Dados vazados ou mal geridos podem levar ao roubo de identidade e perda financeira, onde as instituições podem culpar os utilizadores por “phishing” apesar das vulnerabilidades sistémicas.

O Impacto da Recolha e Partilha de Dados ii

- **O Imperativo Ético**: Como *developers*, devemos reconhecer que por trás de cada *data point* existe um ser humano com direitos fundamentais.

Identificação Indireta i

- **O Mito dos Dados "Anónimos"**: Remover nomes é frequentemente insuficiente para proteger a identidade.
- **Definição**: Uma pessoa é "identificável" se puder ser distinguida não apenas diretamente (nome, ID), mas **indiretamente** combinando fatores como localização, idade, género ou características físicas.
- **Riscos de Reidentificação**:
  - Estudos mostram que 87% da população dos EUA poderia ser identificada de forma única usando apenas três *data points*: **Código Postal, Data de Nascimento e Sexo**.

Identificação Indireta ii

- **Exemplo**: O *dataset* do “Netflix Prize” foi anonimizado, mas os investigadores reidentificaram utilizadores através do cruzamento de dados (*cross-referencing*) das classificações de filmes com perfis públicos do IMDb.
- **Lição**: Assumam sempre que os dados podem ser reassociados.

RGPD (GDPR) e Garantia de Privacidade

O que é o RGPD? ℹ

- **Regulamento (UE) 2016/679**: O Regulamento Geral sobre a Proteção de Dados (RGPD/GDPR).
- **Filosofia Central**: A privacidade é um **direito humano fundamental**, não um luxo.
- **Âmbito**: Aplica-se a *qualquer* entidade que processe dados de residentes da UE, independentemente de onde o processamento ocorra.

O Nível de Privacidade que Devemos Fornecer i

Os *developers* devem garantir que os sistemas aderem a estes princípios chave:

1. **Liceidade, Lealdade e Transparência**: Sem processamento oculto; os utilizadores devem saber o que está a acontecer.
2. **Limitação da Finalidade**: Dados recolhidos para o "Projeto A" não podem ser usados para o "Projeto B" sem novo consentimento.
3. **Minimização dos Dados**: Recolher apenas o que é estritamente necessário.
4. **Exatidão**: Os dados devem estar corretos e atualizados.

O Nível de Privacidade que Devemos Fornecer ii

5. **Limitação da Conservação**: Apagar os dados quando estes já não forem necessários.
6. **Integridade e Confidencialidade**: Garantir segurança contra acesso não autorizado ou perda.

Privacy by Design & Default i

- **By Design**: As medidas de privacidade devem ser embutidas na arquitetura do *software* desde o início, não adicionadas como um *patch* posteriormente.
- **By Default**: As definições de privacidade mais rigorosas devem aplicar-se automaticamente sem intervenção do utilizador (ex: um perfil de rede social deve ser privado por defeito).
- **Accountability**: O *controller* (responsável pelo tratamento) deve ser capaz de *demonstrar* conformidade através de documentação e *logs*.

AI Act Europeu

Visão Geral do AI Act i

- **Abordagem Baseada no Risco**: O AI Act categoriza os sistemas de IA com base no risco potencial que representam para a segurança e direitos fundamentais dos utilizadores.
  - **Risco Inaceitável**: Banido (ex: *social scoring*, identificação biométrica remota em tempo real em espaços públicos pelas forças de segurança, com exceções).
  - **Risco Elevado**: Permitido mas estritamente regulado (ex: IA na educação, emprego, infraestruturas críticas).
  - **Risco Limitado**: Obrigações de transparência (ex: *chatbots* devem revelar que são IA).
  - **Risco Mínimo**: Não regulado (ex: filtros de *spam*).

Privacidade e Auditabilidade em IA i

- **Relação com a Privacidade**: Sistemas de IA de alto risco devem correr sobre dados de alta qualidade para evitar discriminação e devem aderir aos princípios do RGPD como a governança de dados.
- **Requisitos de Auditabilidade**:
  - **Logging**: Os sistemas devem registar eventos automaticamente (*logs*) para rastrear o funcionamento e identificar riscos.
  - **Documentação Técnica**: Os *developers* devem manter documentação detalhada para provar a conformidade às autoridades.

Privacidade e Auditabilidade em IA ii

- **Supervisão Humana**: Os sistemas devem ser desenhados de forma a que pessoas naturais possam supervisionar a sua operação e sobrepor-se às decisões.

Como nos Protegermos e aos Nossos Utilizadores

Garantir Proteção: Medidas Técnicas i

- **Pseudonimização**: Processamento de dados de forma a que estes já não possam ser atribuídos a um sujeito específico sem informação adicional (*key*), que deve ser mantida separada.
- **Anonimização**: Remoção irreversível de identificadores. *Nota: Dados verdadeiramente anonimizados caem fora do âmbito do RGPD, mas é difícil de alcançar*.
- **Encriptação**: Obrigatória para a transmissão e armazenamento de dados sensíveis para prevenir acesso não autorizado.

Garantir Proteção: Medidas de Processo i

- **Avaliação de Impacto sobre a Proteção de Dados (DPIA/AIPD)**:
  - Antes de iniciar um projeto com riscos elevados, devem avaliar o impacto na privacidade dos dados.
  - **Passos**:
    1. Descrever as operações de processamento.
    2. Avaliar a necessidade e proporcionalidade.
    3. Identificar riscos para os direitos e liberdades.
    4. Definir medidas para mitigar esses riscos.
- **Gestão de Consentimento**: O consentimento deve ser **livre, específico, informado e explícito**. Caixas pré-assinaladas são inválidas.

Proteermo-nos (Como Profissionais) i

- **Responsabilidade Clara**: Entendam quem é o "Controller" (determina a finalidade) vs. "Processor" (processador técnico). Como *developer*, atuas frequentemente em nome de um *controller*, mas deves garantir que as tuas ferramentas estão em conformidade.
- **Vigilância Contínua**:
  - Monitorizar riscos de reidentificação em *big data*.
  - Manter-se atualizado sobre decisões de adequação para transferências internacionais de dados (ex: dados armazenados em servidores nos EUA).

Recursos Adicionais

1. **Textos Legais Oficiais**:
   - RGPD (UE 2016/679) Texto Completo
   - Texto do AI Act Europeu
2. **Manuais**:
   - *Handbook on European Data Protection Law* (FRA/Conselho da Europa).
3. **Orientação Institucional**:
   - Contactos do *Data Protection Officer* (DPO) na tua instituição aqui
   - CNPD (Comissão Nacional de Proteção de Dados) diretrizes.