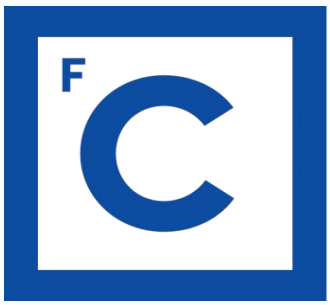

Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Faculdade de Ciências da Universidade de Lisboa

Departamento de Informática

Mestrado em Engenharia Informática

Relatório

Configuração e Gestão de Sistemas

Ethics – Facebook and Cambridge Analytica

Aluno: **Rodrigo Craveiro Rodrigues (fc64370)**

Professor: **Doutor Hugo Miranda**

2º Semestre Letivo 2024/2025

junho 2025

Índice

1. Contextualização do Problema

1.1 Perspetiva social

Em março de 2018 tornou-se público que a consultora *Cambridge Analytica* havia recolhido, sem consentimento, dados de **mais de 50 milhões** de utilizadores do *Facebook*, para micro-segmentação política na campanha presidencial dos EUA de 2016 [1]. A revelação suscitou indignação global, levando ao movimento *"#DeleteFacebook"* e obrigando a plataforma a enfrentar críticas acentuadas pela forma como monetiza dados pessoais e afeta o debate democrático [4]. Este escândalo expôs não apenas falhas técnicas, mas também a vulnerabilidade dos processos democráticos face à manipulação de dados em massa, questionando fundamentalmente a relação entre tecnologia e soberania popular.

1.2 Perspetiva do administrador de IT

Do ponto de vista técnico, o Facebook permitiu que a aplicação "*This Is Your Digital Life*", desenvolvida pelo académico Aleksandr Kogan, recolhesse não só os dados dos utilizadores que a instalaram (aprox. 270 000 pessoas), mas também dos seus amigos, totalizando dezenas de milhões de perfis sem consentimento explícito [3]. Esta falha sistémica resultou de políticas de API inadequadas que permitiam acesso transitivo a dados através de relações sociais. Em 16 de março de 2018, o Facebook suspendeu o acesso da *Strategic Communication Laboratories (SCL)* e da *Cambridge Analytica*, admitindo lacunas nas políticas de revisão e controlo de APIs de terceiros [2].

2. Análise Ética segundo o Código da ACM

O **Código de Ética da ACM** [5] define princípios fundamentais que foram violados neste caso, comprometendo não apenas regras técnicas, mas valores essenciais da dignidade humana:

2.1 Avoid Harm (1.2)

A utilização indevida dos dados permitiu manipulação psicológica dos eleitores e erosão da confiança pública, causando dano social e político. Esta violação é eticamente grave porque mina a autonomia individual - um princípio fundamental da ética deontológica - ao transformar cidadãos em objetos de manipulação sem o seu conhecimento. O dano transcende o individual, afetando a integridade do processo democrático e criando precedentes perigosos para futuras interferências eleitorais.

2.2 *Respect Privacy (1.6)*

Dados pessoais foram recolhidos e partilhados sem o devido consentimento, ferindo a

privacidade dos utilizadores. Esta violação representa mais do que uma quebra procedimental: constitui uma negação do direito fundamental à autodeterminação informacional. A privacidade não é meramente uma preferência pessoal, mas um pré-requisito para o exercício da liberdade individual e da participação democrática informada.

2.3 Give proper credit for intellectual property (2.5)

Kogan apresentou a recolha de dados como investigação académica, mas revendeu-nos para fins comerciais e políticos, ocultando a verdadeira finalidade. Esta deturpação viola não apenas normas académicas, mas compromete a confiança pública na investigação científica, essencial para o progresso social e a tomada de decisões baseada em evidência.

2.4 Guard against misuse (3.5)

O Facebook falhou em implementar salvaguardas eficazes contra abusos das suas APIs, permitindo que uma app académica atingisse fins partidários. Esta falha sistémica revela uma negligência ética grave, especialmente considerando o poder de mercado da plataforma e a sua responsabilidade social acrescida.

3. Juízo de Responsabilidade Ética

- **Aleksandr Kogan** (pesquisador): Violou fundamentalmente o princípio do consentimento informado (1.6) e da honestidade académica (2.5), ao comercializar dados académicos para *Cambridge Analytica*. A sua responsabilidade é agravada pela posição de confiança que ocupava como académico, traindo não apenas os participantes do estudo, mas toda a comunidade científica. Do ponto de vista ético, representa uma forma grave de instrumentalização de pessoas para fins ocultos.
- **Cambridge Analytica/SCL**: Utilizou indevidamente dados pessoais para influenciar eleições, violando os princípios de não causar danos (1.2) e de prevenir uso indevido (3.5). A empresa operou num modelo de negócio fundamentalmente antiético, transformando vulnerabilidades psicológicas individuais em vantagens políticas, comprometendo a integridade democrática.
- **Facebook**: Embora a opinião pública tenha apontado sobretudo o dedo à Cambridge Analytica, do ponto de vista da ética em TI, o Facebook incorre na responsabilidade mais grave. Como detentor de uma infraestrutura crítica para a comunicação social, tinha o dever ético acrescido de implementar salvaguardas robustas. A sua falha não foi meramente técnica, mas sistémica, revelando uma cultura organizacional que priorizou o crescimento sobre a proteção dos utilizadores (3.5) [2].
- **Utilizadores e Literacia Digital:** Embora sejam principalmente vítimas, existe uma dimensão de responsabilidade partilhada relacionada com a literacia digital. Contudo, é

crucial reconhecer a assimetria de poder e conhecimento técnico entre utilizadores comuns e plataformas tecnológicas.

- **Organismos Reguladores:** A ausência de supervisão eficaz e de quadros legais adequados também contribuiu para criar o ambiente propício a estes abusos, revelando lacunas na governança digital.

Embora a opinião pública tenha apontado sobretudo o dedo à *Cambridge Analytica*, do ponto de vista da ética em TI o Facebook também falhou gravemente na sua responsabilidade de guardião dos dados. O caso ilustra como o poder de mercado concentrado cria responsabilidades éticas acrescidas. O Facebook, como quasi-monopólio nas redes sociais, tinha obrigações éticas que transcendem as de empresas convencionais, aproximando-se das responsabilidades de um serviço público.

4. Medidas Preventivas e Impacto nos Utilizadores

Para evitar a ocorrência de novo de escândalos como o *Facebook–Cambridge Analytica*, é fundamental implementar um conjunto integrado de medidas técnicas, organizacionais e formativas, de modo a proteger os dados dos utilizadores e reforçar a confiança na plataforma.

4.1 Revisão rigorosa de aplicações de terceiros

Antes de qualquer aplicação aceder a dados sensíveis, deve passar por um processo de auditoria que combine análises automáticas que verificam padrões de requisição de API e conformidade com políticas de privacidade, e revisões humanas, capazes de avaliar riscos éticos e de segurança. Embora esta revisibilidade acrescente alguns dias ao ciclo de aprovação, garante que apenas apps confiáveis acedem a informações pessoais, reduzindo substancialmente o risco de recolhas indevidas.

4.2 Princípio do menor privilégio com consentimento

Cada aplicação só deve receber as permissões imprescindíveis para funcionar. Em vez de um consentimento genérico, o utilizador recebe pedidos granulares, separados por tipo de dado (por exemplo, lista de amigos, eventos, gostos). Esta abordagem dá às pessoas maior controlo sobre o que partilham e sobre com quem partilham, mesmo que implique uma interação ligeiramente mais demorada na configuração inicial.

4.3 Transparência em tempo real e auditabilidade

Disponibilizar um painel público onde os utilizadores possam ver, em qualquer momento, quais as aplicações que acederam aos seus dados, quantas vezes e com que finalidade. Esta visibilidade reforça a responsabilidade das empresas de software, estimula práticas mais éticas e permite ao cidadão detetar padrões de uso suspeito.

4.4 Formação ética contínua e cultura organizacional

Os engenheiros, gestores de produto e responsáveis de segurança devem participar regularmente em cursos e workshops sobre ética de dados, *privacy by design* e dilemas reais ocorridos noutras organizações. Através de estudos de caso, simulações de cenários e debates orientados, constrói-se uma cultura interna que valoriza a proteção da privacidade desde a conceção de cada funcionalidade.

4.5 Monitorização proativa e deteção de anomalias

Implementar sistemas de monitorização que analisem, em tempo real, os padrões de acesso às APIs, por exemplo, picos súbitos de leituras de perfis ou pedidos de dados fora do habitual. Sempre que for detetada uma anomalia, o sistema envia alertas automáticos à equipa de segurança, permitindo intervenções imediatas e a suspensão preventiva de chaves de acesso suspeitas.

4.6 "*Privacy by Design*" e conformidade regulamentar

Integrar mecanismos de proteção de dados desde a fase de conceção de cada nova funcionalidade: encriptação *end-to-end*, retenção mínima de informação, anonimação de registos e desenho de fluxos que limitem ao estritamente necessário a circulação de dados pessoais. Ao aplicar princípios e normas como o RGPD ou as ISO 27000 já na arquitetura inicial, evita-se a necessidade de adaptações posteriores, dispendiosas e potencialmente menos eficazes.

Em conjunto, estas medidas não só reduziriam drasticamente o alcance de recolhas indevidas de dados como também promoveriam uma relação de maior confiança entre plataforma e utilizadores, antecipando problemas antes de se tornarem crises.

5. Reflexão Crítica sobre Consequências e Perspetivas Futuras

O caso expõe tensões irreconciliáveis entre modelos de negócio baseados em dados pessoais e direitos fundamentais à privacidade. Uma resolução ética sustentável pode requerer transformações radicais nos modelos económicos das plataformas digitais.

As medidas preventivas devem considerar diferentes conceções culturais de privacidade e diferentes quadros regulamentares nacionais, evitando soluções universalistas que ignorem contextos locais.

Numa perspetiva consequencialista, as medidas justificam-se pelos resultados benéficos na proteção dos utilizadores. Numa abordagem deontológica, são imperativos éticos independentemente dos custos, por respeitarem a dignidade humana fundamental.

Conclusão

O escândalo *Facebook–Cambridge Analytica* constitui um marco na consciencialização sobre os riscos éticos das tecnologias digitais. Mais do que um caso isolado de má conduta, revela falhas sistémicas na governança de dados pessoais que requerem respostas coordenadas a múltiplos níveis.

A responsabilidade ética distribui-se de forma desigual, pois enquanto todos os atores falharam, o Facebook, pela sua posição dominante e capacidade técnica, carrega a responsabilidade mais pesada. As medidas preventivas propostas, embora necessárias, enfrentam desafios significativos de implementação e podem criar dilemas éticos.

O futuro da ética em tecnologias da informação depende da nossa capacidade coletiva de equilibrar inovação tecnológica com proteção dos direitos fundamentais, reconhecendo que a tecnologia nunca é neutra e que as escolhas de design incorporam sempre valores éticos implícitos.

A lição fundamental é que a privacidade não é uma preferência individual, mas um direito fundamental essencial para a preservação da dignidade humana e da democracia numa sociedade digital.

Referências

[1] *Carole Cadwalladr; Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian, 17 Mar 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election*

[2] *Facebook. "Suspending Strategic Communication Laboratories (SCL), including their political data analytics firm, Cambridge Analytica, from Facebook." Facebook Newsroom, 16 Mar 2018. Disponível em: https://about.fb.com/news/2018/03/suspending-cambridge-analytica/*

[3] *"Facebook–Cambridge Analytica data scandal." Wikipedia, atualizado Maio 2025. Disponível em: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal*

[4] *Kaveh Waddell. "A Hurricane Flattens Facebook." Wired, Mar 2018. Disponível em: https://www.wired.com/story/facebook-cambridge-analytica-response*

[5] ***ACM Code of Ethics and Professional Conduct.** Association for Computing Machinery, 2018. Disponível em:https://www.acm.org/code-of-ethics*