EDPB atualiza orientações sobre padrões de design enganosos em interfaces de redes sociais

15.03.2023 2 minutos de leitura

Autores

Felipe Palhares

Fernanda Villela

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity Felipe Palhares

No dia 24 de fevereiro, o *European Data Protection Board* ("EDPB") publicou a versão atualizada das suas Orientações 03/2022 sobre padrões de *design* enganosos em interfaces de plataformas de redes sociais.

Preliminarmente, o EDPB destaca que o uso de padrões de *design* enganosos pode impactar o cumprimento do GDPR e resultar em violações às regras de proteção de dados pessoais, incluindo a obrigação de privacidade desde a concepção (*privacy-by-design*) e os princípios de transparência e prestação de contas.

O EDPB destaca seis diferentes padrões de *design* enganosos, fornecendo exemplos práticos de cada um:

1. *Overloading*

Sujeitar os usuários a uma enorme quantidade de solicitações, informações, ou opções, a fim de dissuadi-los e fazê-los manter ou aceitar determinadas práticas envolvendo o tratamento de dados pessoais. Por exemplo, fazer solicitações contínuas aos usuários, pressionando-os a fornecerem dados pessoais em excesso, ou a concordarem com outro uso de seus dados pessoais.

2. *Skipping*

Desenvolver a interface ou percurso do usuário de modo que esqueça ou ignore aspectos relacionados à proteção de dados pessoais. Por exemplo, disponibilizar uma informação sobre a proteção de dados pessoais em concorrência com outro elemento, o que pode levar o usuário a tomar decisões distraído.

3. *Stirring*

Afetar a escolha do usuário ao apelar para suas emoções ou utilizar estímulos visuais. Por exemplo, utilizar palavras ou elementos visuais (e.g., estilo, cor, imagem) para conferir uma perspectiva altamente positiva ou negativa a determinadas informações, influenciando o estado emocional do usuário na sua tomada de decisão.

4. *Obstructing*

Impedir ou bloquear usuários no processo de obtenção de informações ou gerenciamento dos seus dados pessoais. Por exemplo, impor etapas

demasiadas para que usuários ativem uma configuração de proteção de dados pessoais, em quantidade maior que o número de etapas necessárias para ativar configurações invasivas.

5. *Fickle*

A interface ter um *design* instável e inconsistente, tornando difícil que usuários identifiquem certas informações ou configurações. Por exemplo, fornecer informações sobre a proteção de dados pessoais de forma redundante ou fora de contexto.

6. *Left in the dark*

Desenvolver a interface para ocultar informações ou configurações de proteção de dados pessoais, ou deixar os usuários incertos. Por exemplo, fornecer informações conflituosas entre si, ou então de forma vaga e ambígua, o que torna os usuários incertos sobre a forma de agir.

>>> Este conteúdo faz parte do Informativo de Proteção de Dados e Cybersecurity. Clique aqui para ler mais
notícias. O artigo foi escrito por nossos profissionais Felipe Palhares, Fernanda Villela, Bárbara Iszlaji e Arthur Pichelli Ueda.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares

Fernanda Villela