

Martha Leal: Dark Patterns e as orientações do EDPB

02/04/2022

Talvez muitos desconheçam a expressão *Dark Patterns* e o seu real significado, mas certamente todos nós convivemos com essa prática no nosso dia a dia e somos vítimas de suas técnicas, tenhamos ou não consciência do fato.



Literalmente, significa a utilização de padrões escuros

através de técnicas maliciosas projetadas com a intenção de induzir intencionalmente os usuários de serviços na web a optarem por determinadas escolhas, manipulando as suas decisões. Poderíamos conceituar como sendo um tipo de técnica enganosa, comumente usada em sites e aplicativos com a finalidade de fazer com que o indivíduo tome decisões as quais não pretendia.

Tendo em vista que essas práticas estão cada vez mais presentes em nosso cotidiano, de formas muito obscuras e que por vezes podem comprometer a autonomia dos indivíduos com reflexos em suas tomadas de decisões, a *European Data Protection Board* (EDPB) emitiu recentemente, no último dia 14 de março, as Diretrizes de nº 3/2022 focadas em *Dark Patterns* no ambiente das plataformas de mídias sociais.

Em suas diretrizes, a EDPB oferece recomendações práticas tanto para usuários como para designers de plataformas de mídias sociais com o objetivo de facilitar a identificação dos chamados padrões escuros, possibilitando assim que sejam evitados. É ratificada a responsabilidade dos provedores de mídias sociais em garantir a conformidade com o Regulamento Geral de Proteção de Dados (GDPR).

E, nesta linha, é condicionante para que um tratamento seja considerado lícito, a observância aos princípios normativos, com destaque à transparência. Evidentemente que não seria crível considerarmos válida uma decisão baseada em cenários que são construídos propositalmente para ocultarem aspectos sobre os quais, se os indivíduos tivessem conhecimento, provavelmente, levariam ao questionamento por parte do usuário, afetando o processo de



tomada de decisão.

No contexto das Diretrizes n.º 03/2022 foram consideradas "dark patterns" interfaces assim entendidas como os meios pelos quais o usuário interage com as plataformas de mídias sociais e a sua experiência neste ambiente que os levam, muitas vezes, a tomar decisões não intencionais, involuntárias e potencialmente prejudiciais com relação aos seus dados pessoais. E, partindo do princípio de que as autoridades de proteção de dados possuem a responsabilidade de sancionar o uso desses padrões quando eles violarem o Regulamento Europeu de Proteção de Dados, o *European Data Protection Board* (EDPB) apresenta diferentes categorias destas técnicas de forma a facilitar a identificação por parte dos usuários quando estiverem diante das mesmas.

São essas categorias assim diferenciadas: 1) sobrecarga, quando são impostas ao titular uma imensidão de informações e solicitações de forma a induzir no fornecimento e/ou compartilhamento de informações desnecessárias à finalidade; 2) ignorância, quando a experiência do usuário é projetada de forma que ele não foque sua atenção nos aspectos da privacidade e proteção dos seus dados; 3) agitação, quando são utilizados recursos com o objetivo de induzir emocionalmente a escolha do usuário; 4) impedimento, através de obstrução ou bloqueio de informações aos usuários, dificultando ao máximo e até mesmo tornando inviável o gerenciamento dos seus dados; 5) inconstância, quando o design da interface é confuso e descontextualizado, confundindo o usuário e prejudicando o controle da proteção dos seus dados; e, 6) obscuridade, quando uma interface é projetada de forma a ocultar informações e/ou ferramentas de controle do usuário com relação a proteção dos seus dados.

As orientações deixam claro que o GDPR se aplica a todo e qualquer tratamento de dados pessoais decorrentes da operação das plataformas de mídia social, em todo o ciclo de vida de uma conta do usuário. E disponibilizam as melhores práticas a serem adotadas por parte dos usuários e recomendações específicas para projetar interfaces que facilitem a aderência às regras protetivas de dados pessoais.

O texto é altamente didático uma vez que apresenta exemplos práticos, de forma que o leitor, o usuário, consiga se projetar para as situações trazidas e que compreendem todo o ciclo de vida de uma conta de rede social.

Situações como o provedor que solicita reiteradamente aos seus usuários, ao fazerem um *login*, para que forneçam um dado pessoal o qual já foi recusado anteriormente, com o objetivo de convencê-lo a consentir; a plataforma de mídia social que solicita aos seus usuários que compartilhem sua geolocalização mediante a utilização de conteúdo de cunho emocional persuasivo para o convencimento do indivíduo; o processo de inscrição em que os usuários após evitarem a inserção de determinados dados pessoais são questionados reiteradamente sobre suas decisões com o objetivo de fazê-los duvidar das mesmas; e em situações que os recursos e opções mais invasivos de dados são ativados por padrão, levando o usuário manter a seleção previamente optada e que não representa a alternativa mais protetiva, entre inúmeras outras situações práticas vivenciadas em nossa rotina desenvolvida no ambiente virtual.



A cada exemplo fático apresentado, o EDPB expõe orientações de boas práticas a serem seguidas pelos agentes de tratamento. Traçando uma comparação com a legislação nacional e europeia, tanto o GDPR como a LGPD trazem princípios específicos relacionados ao tratamento de dados — artigo 5 GDPR — artigo 6 LGPD —, dentre os quais, especial atenção aos princípios da transparência e prestação de contas.

Por princípio da transparência, compreende-se a necessidade do usuário e titular de dados estar sendo devidamente informado acerca do processo que envolve os seus dados pessoais e que impacta no resultado da sua decisão. Consequência lógica será a ilicitude de um tratamento que não tiver as suas finalidades e eventuais consequências devidamente informadas e sem as quais não seria possível presumirmos uma aceitação válida pelo titular.

O consentimento no Regulamento Europeu apresenta requisitos legais para serem considerados válidos, sendo definido através do artigo 4 (11) e complementado pelos artigos 6º e 7º como consentimento válido aquele que se configurar como livre, específico, informado e inequívoco.

Por sua vez, a LGPD em seu artigo 8º, ao se referir ao consentimento previsto no artigo 7º, I da lei, estabelece a vedação do tratamento de dados mediante vício de consentimento, devendo referir-se a finalidades determinadas. As autorizações genéricas serão consideradas nulas, definindo ainda, em seu artigo 5º, XII, que o consentimento válido se trata de uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Desta feita, a partir das ponderações ora trazidas parece natural a conclusão de que em sendo o princípio da transparência um elemento de valor inestimável para conferir licitude ao tratamento de dados, a sua ausência tem potencial de macular toda a sequência de atos posteriores podendo caracterizar vício de consentimento, na medida em que os padrões obscuros utilizados, a exemplo dos *cookies*, não permitem ao titular que compreenda as consequências de sua escolha.

Assim, nos casos exemplificados, onde se vislumbram a existência de práticas opacas as quais se utilizam propositalmente de mecanismos e ardis como meio de manipular a escolha do usuário, afetando a consciência no processo decisório, parece inverossímil admitirmos a caracterização de um consentimento livre, inequívoco e informado.

Sem sombra de dúvida, as orientações trazidas através das Diretrizes nº 3/2022, do European Data Protection Board (EDPB) representam um avanço inestimável sobre tema trazendo ainda mais nitidez aos usuários das plataformas e a responsabilização aos agentes de tratamento.

Fonte: <https://conjur.jumps.com.br/2022-abr-02/martha-leal-dark-patterns-orientacoes-edpb/>