Martha Leal: Dark patterns e leis de proteção de dados

Talvez muitos desconheçam a expressão "*dark patterns*" e o seu real significado. Mas, com certeza, todos nós convivemos com essa prática em nosso dia a dia. Literalmente, significa a utilização de padrões escuros através de técnicas maliciosas projetadas com a intenção de induzir os usuários de 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 não pretendidas. Trazendo para a nossa realidade, vivenciamos essa prática, a título ilustrativo, quando compramos algo ou nos inscrevemos em algum serviço sem a devida compreensão das consequências do nosso ato, além, é claro, das questões atinentes à privacidade, cujas consequências das escolhas impactam diretamente sobre os nossos direitos e liberdades individuais.

Em 2018, o Conselho de Consumidores Norueguês[1] publicou um relatório classificando os tipos de padrões obscuros nas seguintes categorias:

a) configurações padrão, onde as definições de opções de padrão de privacidade são intrusivas, obscurecendo os padrões pré-selecionados pelo usuário;

b) facilidade, onde se dificulta propositalmente a escolha da opção de privacidade, a exemplo do que ocorre com a necessidade de selecionar inúmeros botões de desativação de *cookies* levando à fadiga do titular;

c) enquadramento, onde o enfoque disponibilizado ao usuário evidencia propositalmente os aspectos positivos da escolha, encobrindo os aspectos negativos e potenciais riscos à privacidade;

d) esquema de recompensas e punições, o qual tem como objetivo forçar a escolha do usuário por meio de uma ameaça no caso de não opção de um serviço, a exemplo da possibilidade de exclusão da conta do titular em caso de não aceitação da funcionalidade proposta;

e) a ação forçada no tempo, onde os usuários são levados a tomar ações antes de acessar o serviço de forma condicionante e sem a possibilidade clara para adiar este processo que culmina num ato de decisão do titular.

Explora-se, portanto, através dessa prática, a vulnerabilidade dos indivíduos, dificultando a opção de preservação da privacidade em prol das facilidades oferecidas, resultando na exigência de que o usuário execute uma determinada ação para ter acesso a outra funcionalidade.

Em relação ao uso de *cookies* pelos *sites*, apesar da Lei Geral de Proteção de Dados não abordar especificamente o tema, não há qualquer dúvida de que, tratando-se de pequenos arquivos inseridos no navegador do usuário para fins de coleta de dados pessoais com diferentes finalidades, incidem sobre a maioria destes as leis protetivas de dados pessoais. E é exatamente nesse contexto que as práticas envolvendo a opacidade dos padrões para coleta de dados pessoais comprometem a autonomia da vontade do indivíduo e desafiam a conformidade às Leis de Proteção de Dados.

O Regulamento Europeu (GDPR[2]), complementado pela Diretiva *e-Privacy*, estrutura a proteção de dados na União Europeia e formula regras para o processamento de dados pessoais, garantindo direitos aos titulares. Cabem às autoridades supervisoras o papel de monitoramento e a responsabilidade por sanções administrativas, modelo este que predominantemente se reproduz no Brasil, por meio da LGPD, com a ressalva de que em nossa legislação a autoridade supervisora é apenas uma, a Autoridade Nacional de Proteção de Dados (ANPD).

Tanto o GDPR como a LGPD trazem princípios específicos relacionados ao tratamento de dados (art. 5º GDPR[3], art. 6º da LGPD), dentre os quais merecem especial atenção os princípios da transparência e da prestação de contas. Por princípio da transparência compreende-se a necessidade do usuário e titular de dados ser devidamente informado acerca do processo que envolve os seus dados pessoais e que impacta no resultado da sua decisão. Logo, um tratamento que não tenha as suas finalidades e eventuais consequências informadas e, sem as quais não seria possível presumirmos uma aceitação válida pelo titular, envolve-se pela ilicitude.

O consentimento no Regulamento Europeu apresenta requisitos legais para serem considerados válidos, sendo definido através do art. 4º (11) e complementado pelos arts. 6º e 7ºcomo consentimento válido aquele que se configura como livre, específico, informado e inequívoco. Por sua vez, a LGPD, em seu art. 8º, ao se referir ao consentimento previsto no art. 7º, I, da lei, estabelece a vedação do tratamento de dados mediante vício de consentimento, devendo referir-se às finalidades determinadas. As autorizações genéricas serão consideradas nulas, definindo ainda, em seu art. 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.

Assim, a partir das ponderações ora trazidas, parece natural a conclusão de que sendo o princípio da transparência um elemento de valor inestimável para conferir licitude ao tratamento de dados, a ausência do mesmo 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.

Dessa forma, nos casos exemplificados, onde se vislumbram a existência de práticas opacas que se utilizam propositalmente de mecanismos e ardis como meios de manipular a escolha do usuário sem que este tenha consciência do que de fato está em jogo, parece inverossímil admitirmos a caracterização de um consentimento livre, inequívoco e informado.

A constatação de que a falta do princípio da transparência no tratamento de dados pessoais ameaça a autonomia da vontade, comprometendo consequentemente o consentimento, impõe a necessidade de revisões urgentes sobre tais práticas.

Referências

[1] FORBRUKERRÅDET – Norwegian Consumer Council. *In:* Consumers International. Disponível em: https://www.consumersinternational.org/members/members/norwegian-consumer-council/. Acesso em: 02 nov. 2021

[2] GENERAL DATA PROTECTION REGULATION – GPDR. Disponível em: https://gdpr-info.eu/. Acesso em: 29 out. 2020.

[3] GENERAL DATA PROTECTION REGULATION – GPDR. Disponível em: https://gdpr-info.eu/. Acesso em: 29 set. 2020.

Date Created

16/11/2021