Compartilhamento de dados do open banking exige cuidado

Nesta sexta-feira (13/8), começa a funcionar o sistema de compartilhamento de dados do *open banking*, no qual os clientes poderão autorizar a troca de informações pessoais entre instituições bancárias. A ideia é facilitar o acesso a produtos, serviços e ofertas.

Marcello Casal Jr./Agência Brasil

Marcello Casal Jr./Agência Brasil

A implementação do *open banking* vem de uma resolução conjunta do Banco Central e do Conselho Monetário Nacional (CMN), publicada no último ano. O ato prevê a necessidade de consentimento do cliente para que haja o compartilhamento. A solicitação deve ser feita por meio eletrônico e esclarecer quais dados estarão envolvidos.

Luiza Sato, sócia da área de Proteção de Dados, Direito Digital e Propriedade Intelectual do escritório ASBZ Advogados, lembra que a resolução traz diversos outros requisitos, como a estipulação das finalidades determinadas, o uso de linguagem clara e objetiva, o prazo máximo de um ano etc. Ela ressalta que os clientes devem se atentar a esses requisitos, "não apenas pelo cuidado com a proteção de seus dados, mas também para evitar golpes".

Isso porque criminosos podem criar sites falsos ou serviços fraudulentos para ter acesso aos dados das pessoas. "A nova fase do *open banking* é um prato cheio para a prática do *phishing* (e-mail), do *vishing* (telefone) e do *smishing* (SMS) e exigirá que a população como um todo já esteja preparada para identificar não apenas os golpes mais simples e genéricos, mas também aqueles elaborados e direcionados, feitos inclusive com dados pessoais vazados em incidentes recentes", aponta **Márcio Chaves**, sócio e responsável da área de Direito Digital do Almeida Advogados.

Sato recomenda que os clientes verifiquem a instituição que pedir o consentimento; não cliquem em links suspeitos; e concedam as autorizações apenas dentro dos canais seguros e oficiais da instituição — nunca fora do meio digital.

Chaves também sugere que os usuários exijam meios de comprovação da autenticidade dos contratos. Mas ele enfatiza que as instituições financeiras e empresas ligadas ao sistema financeiro devem reforçar a divulgação por meio de seus canais oficiais. "Para haver segurança, são imprescindíveis bons meios de autenticação de ambos os lados, mas sem prejudicar a usabilidade, pois as pessoas têm preguiça e

2023 - www.conjur.com.br - Todos os direitos reservados.

preferem o caminho mais fácil, ainda que menos seguro, por descuido ou por desconhecimento mesmo", diz.

"A implementação do *open banking* é uma estratégia muito positiva para o Brasil, por diversos motivos, como o aumento da competitividade e da transparência dentro do mercado financeiro, e deve ser fomentada. Para que tenha sucesso, é imprescindível que seja estabelecida uma relação de confiança entre as instituições financeiras e seus clientes, que estarão cada vez mais conscientizados quanto ao devido tratamento de seus dados", conclui Sato.

Anna Luiza Berredo, sócia da área de TMT, Privacidade e Proteção de Dados do Maneira Advogados, concorda que é necessário muita atenção e rigidez de controles pelas instituições e clientes. Mas a advogada confia nos normativos sobre compartilhamento de dados. "Vale considerar também que o Banco Central estará supervisionando todo o processo, e as medidas de segurança a serem adotadas pelas instituições autorizadas serão munidas de diversas etapas de autenticação, confirmação dos clientes e demais regras rígidas para garantia da segurança cibernética exigida", reforça.

Opt–in* e *opt-out
Conforme explica **Marcelo Cárgano**, advogado da área de regulação e proteção de dados pessoais do escritório Abe Giovanini Advogados, o modelo adotado no Brasil com o *open banking* é chamado de *opt-in*, já que o cliente opta pelo compartilhamento dos dados.

Já em 2019, a nova Lei do Cadastro Positivo havia instituído um modelo de *opt-out*, no qual o usuário expressa seu desejo de sair e ter seus dados removidos do cadastro.

Para Cárgano, o *opt-out* facilita o compartilhamento de dados, enquanto o *opt-in* privilegia a vontade do cliente e o que a Lei Geral de Proteção de Dados Pessoais (LGPD) chama de "autodeterminação informativa" — o direito de as pessoas exercerem controle sobre seus dados pessoais, incluindo quem pode ter acesso a eles e para qual finalidade.

"Dado o impacto que eventual mau uso de tais dados poderia causar aos clientes e o recente megavazamento de informações de 223 milhões de brasileiros, parece-me que a escolha pelo *opt-in* foi correta", opina o advogado.

Date Created
12/08/2021

2023 - www.conjur.com.br - Todos os direitos reservados.