

Caso iFood mostra necessidade de proteção de dados, dizem advogados

03/11/2021

Alguns nomes de restaurantes cadastrados no iFood foram alterados na noite desta terça-feira (2/11) para mensagens de apoio ao presidente Jair Bolsonaro e contrárias à vacina. Segundo a empresa, as mudanças atingiram 6% dos estabelecimentos catalogados no aplicativo e foram feitas indevidamente por meio da conta de um funcionário de uma prestadora de serviço. Ainda de acordo com a plataforma, não houve vazamento de dados de clientes ou entregadores.

Reprodução



Reprodução

Advogados especializados em proteção de dados afirmam que o caso demonstra a vulnerabilidade dos sistemas de informação das empresas, além de reforçar a importância de práticas de segurança.

Sofia Rezende, do Núcleo de LGPD do **Nelson Wilians Advogados**, afirma que o incidente deixa visível a "imensa fragilidade dos processos de trabalho e medidas de segurança e privacidade envolvidas no tratamento de bases de dados pelas grandes companhias atuantes no mercado, suas parceiras de negócio e prestadoras de serviços".

"No caso do iFood, o uso indevido de credenciais por um usuário autorizado de uma empresa contratada, ou seja, de uma parceira, comprometeu os dados que lhe foram confiados. Sabemos que a gestão de empresas parceiras, que acessam e manuseiam as bases de dados, é um ponto crítico. O que se recomenda às empresas contratantes é que privilegiem a contratação de empresas adequadas à LGPD (Lei Geral de Proteção de Dados), que possuam programas robustos de Privacidade e Segurança da Informação", orienta.

A advogada também destaca a importância das empresas contratantes estabelecerem processos contínuos de auditoria e treinamentos junto às suas parceiras, restringindo o acesso às bases de dados ao estritamente necessário para a consecução do contrato.

"Quanto menos arquivos e sistemas um único usuário puder acessar, mais difícil será para ele abusar desse acesso. No entanto, essa medida também pode tornar o compartilhamento dos dados necessários mais difícil", complementa.

Rezende recomenda ainda que ambas as empresas atuem conjuntamente para garantir proteção e sigilo das bases de dados compartilhadas, em especial em relação aos dados pessoais, "pois a LGPD estabelece a responsabilização solidária em situações de exposição e vazamento". "Dessa forma, os contratos entre as empresas deverão ter cláusulas especificando as condições e obrigações de cada uma quanto aos dados compartilhados, delimitando, no que for possível, a responsabilidade de cada parte", conclui.

Iara Peixoto Melo, advogada, coordenadora da equipe de Direito Digital e Data Protection do **Chenut Oliveira Santiago Advogados**, segue a mesma linha. "O fato de o incidente ter sido ocasionado por meio de conta de usuário de



uma empresa prestadora de serviços demonstra a importância das empresas se preocuparem com seus fornecedores e com suas práticas de segurança da informação".

A advogada também lembra que a LGPD estabelece a possibilidade de responsabilização solidária entre controlador e operador dos dados. "Nesse caso, o iFood já se pronunciou informando que dados pessoais não foram afetados em razão do incidente. Porém, caso tivessem sido, essa empresa poderia vir a ser responsabilizada solidariamente, ainda que o incidente tenha acontecido em seu prestador de serviços", explica.

Ainda segundo Melo, a empresa terceirizada prestadora de serviços também poderá ser acionada civilmente para reparar eventuais danos que o iFood tenha sofrido. "Com relação às eventuais medidas penais cabíveis, a situação deverá ser analisada para verificar se houve a configuração de algum tipo penal, como por exemplo invasão de dispositivo informático", acrescenta.

Joaquim Pedro de Medeiros Rodrigues, advogado, mestre em Direito Constitucional pelo IDP e sócio-fundador do **Pisco & Rodrigues Advogados**, diz que cada vez mais os crimes cibernéticos estão se tornando uma realidade. Segundo ele, no caso do iFood, a adulteração dos dados existentes na plataforma pode levar os responsáveis a responder por crime cujas penas variam entre um e quatro anos de prisão. "Um aspecto que deve ser observado são as responsabilidades do iFood diante das empresas ali cadastradas. A política de manipulação dos dados deve ser constantemente atualizada para evitar esse tipo de prejuízo às lojas cadastradas no aplicativo, de modo que eventual quebra do protocolo pode gerar a responsabilização do próprio iFood frente aos restaurantes e lanchonetes", opina.

Fonte: <https://conjur.jumps.com.br/2021-nov-03/ifood-mostra-necessidade-protacao-dados-dizem-advogados/>