

PERIGOS DE FRAUDE NAS COMPRAS ONLINE

| MARIA CRISTINA DIEZ*

O e-commerce é, definitivamente, um mercado consolidado em todo o mundo. Os números que apontam para essa realidade chegam a impressionar. Só no Brasil, o faturamento no ano passado alcançou os R\$ 161 bilhões. A informação é da Neotrust, empresa que monitora o comércio digital no país. Ainda de acordo com o levantamento, o crescimento foi de 26,9% em relação a 2020. Isto levou a 353 milhões de entregas em 2021.

Esse aquecimento bem que poderia ser motivo apenas de comemoração do setor, não fosse por um detalhe: no universo digital, os casos de fraudes parecem superar de longe a esteira positiva da economia. Em toda a América Latina, as operações fraudulentas nos sites de compras foram 97% maiores do que as verificadas na América do Norte. Quando comparadas com a Ásia e com os países do Pacífico, os índices foram 222% mais altos. Os dados são da Stripe, no recorte 2019-2022.

Os perigos no e-commerce são vastos porque há muitos setores envolvidos. Além do cliente, que tem seus dados armazenados no site de compras, também estão envolvidos no negócio o vendedor, o fornecedor e o banco ou a operadora do cartão de crédito. Por isso, é necessário criar um protocolo de segurança bastante amplo, que resguarde de todas as formas possíveis os riscos de ataque.

De modo geral, o sistema de proteção mais usado na etapa de onboarding do site tem sido a autenticação em mais de um ou até de dois fatores, condicionando a efetivação do pagamento a outros meios externos ao site. Por exemplo, através do uso de confirmação de código via SMS ou e-mail, que chega unicamente ao dono dos dados.

Mas há outros percursos ainda mais usados para combater a fraude no e-commerce. O uso da biometria facial também oferece condições amplas de garantir que o acesso à conta do comprador, onde podem estar armazenados inclusive os dados do cartão de crédito e débito, seja feito



pelo próprio usuário. Uma das vantagens de se recorrer a soluções tecnológicas é que ele dispensa a aplicação de novos autenticadores, concentrando todas as conferências numa única etapa.

E esse, aliás, é um desafio extra para os sites de e-commerce dispostos a combater as fraudes. As tecnologias empregadas devem dar ampla proteção aos envolvidos nas operações, mas ao mesmo tempo não podem prejudicar a navegabilidade do site nem tam-

pouco promover dificuldades adicionais para que o usuário de fato execute a compra. Por isso, o tempo de resposta das ferramentas de segurança deve ser, de fato, bastante preciso.

Vale destacar também que o fraudador não necessariamente se resume ao falso comprador. O cliente está sujeito a deparar com sites construídos para enganar pessoas e obter dinheiro e dados indevidamente. A solução, nesse caso, passa pelo cuidado que os clientes de-

vem ter com os dados e a suspeição em caso de dados e links excessivos. É importante informar-se sobre a fonte e ter garantias de que a compra só será paga mediante a entrega do produto. Comparar no ambiente digital é excelente negócio para todo mundo, mas a (auto)proteção tem de ser altamente rigorosa.

*Diretora comercial e de marketing da Most Specialist Technologies