Black Friday 2021 e LGPD: Como preparar o comércio para evitar grandes problemas, multas e penalidades?

José Antonio Milagre *

Pela primeira vez o Brasil terá uma Black Friday já com o processo de fiscalização e administrativo sancionador da Autoridade Nacional de Proteção de Dados em vigor, onde autos de infração poderão ser lavrados e empresas autuadas. Saiba como preparar sua loja para evitar perdas financeiras, danos à imagem e grandes problemas.

A Black Friday já é tradição anual no Brasil e com ela, anualmente, muitos problemas consumeristas são submetidos às plataformas de arbitragem e Poder Judiciário. Propaganda enganosa, maquiagem de preços, atrasos e demais violações ao Código de Defesa do Consumidor movimentam a Justiça. Nesta edição, no entanto, outro assunto relevante ganha espaço e merece total atenção: A proteção de dados pessoais de consumidores e titulares de dados.

A Lei Geral de Proteção de Dados (Lei 13.709/2018) está em vigor desde setembro de 2020, sendo que desde agosto de 2021 as penalidades previstas no art. 52 da LGPD já podem ser aplicadas aos agentes que realizarem tratamentos irregulares de dados, com multas que podem chegar a R$ 50 milhões de reais.

No entanto, faltava ainda a regulamentação do processo de fiscalização e administrativo sancionador da ANPD, para que, eventualmente diante de um auto de infração e processo repressivo, garantindo-se a ampla defesa, lojas, e-commerces e agentes de tratamento pudessem ser responsabilizados, se

constatadas violações.

Este regulamento chega às vésperas da Blackfriday, em 29 de outubro de 2021. Com isso, a atenção máxima do lojista deve ser compreender como está sua conformidade com a LGPD, com o estabelecimento de uma governança de dados pessoais, envolvendo o uso de recursos e elementos para demonstrar que o agente de tratamento está em conformidade com a lei e melhores práticas de proteção de dados, respeitando os direitos dos titulares e princípios previstos no art. 6 da Lei Geral de Proteção de Dados.

Após um ano em vigor, a LGPD já embasava, em junho de 2021, mais de 1.000 sentenças na Justiça e mais de 600 decisões ligadas à temática, sendo São Paulo, Distrito Federal e o Paraná os Estados com maior concentração de processos. E este número só aumenta. Na mesma intensidade, os PROCONS dos Estados se estruturam para receber reclamações por violações de dados e fiscalizar empresas, que já começam a ser notificadas.

Em tempos de Blackfriday, ações de marketing que não considerem as melhores práticas de proteção de dados podem causar grandes transtornos para as empresas e lojistas, danos que podem ser irreparáveis para a marca da loja.

Os tratamentos de dados pessoais nas compras no e-commerce estão, via de regra (mas nem sempre), amparados pela premissa execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, porém, para outras ações e usos dos referidos dados pessoais, faz-se primordial a transparência ao titular de dados, ou, de acordo com o contexto, pode ser necessário o consentimento do mesmo, livre, expresso, informado, inequívoco.

Deve-se destacar, ainda, o dever de segurança da informação de responsabilidade dos controladores e operadores de dados

pessoais. Nos termos do art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Como medidas técnicas podemos citar testes de intrusão nos portais, criptografia, pseudonimização, controles de acesso, backups regulares, plano de recuperação de desastres, monitoramento de segurança e demais controles. Já como medidas organizativas é fundamental o treinamento e conscientização dos colaboradores e time de vendas para uso e manuseio adequado dos dados pessoais confiados, evitando-se incidentes com dados pessoais ligados à *insiders* ou pessoas com privilégios, confiança ou acesso a dados.

Em um cenário de aumento exponencial das compras online, sobretudo influenciadas pelo momento pandêmico atravessado e de vigência da LGPD e principalmente, em face da possibilidade de aplicações de sanções e autuações pela a ANPD e Procons, é importante que o comerciante esteja atento e preparado para gerir adequadamente questões ligadas à segurança da informação e proteção de dados, que poderão crescer especialmente nesta edição. As lojas físicas ou virtuais devem disponibilizar, de forma transparente, ponto de contato para que o titular possa requerer informações sobre o tratamento de seus dados bem como exercer os direitos previstos no art. 18 da norma. A ausência deste canal, por si só, é um indício de desconformidade e poderá gerar notificações e autuações.

Dentre as preocupações do e-commerce e comércio em geral, e que devem ser consideradas, sobretudo no período da BlackFriday, podemos citar:

1. *Uso indevido da identidade visual do e-commerce:* Engana-se a empresa ou lojista que não tem responsabilidade alguma diante do uso indevido de sua identidade visual,

como a criação de um “site falso”, por exemplo. Cabe a este desenvolver campanhas de conscientização, junto com o marketing, para evitar que criminosos usem sua identidade visual para fraudar, inclusive em redes sociais. A boa prática também recomendada monitorar o uso indevido da marca em redes sociais. Selos de certificação de autenticidade e conformidade do portal, como o Confiaweb, da CyberExperts, são ótimas alternativas.

2. *Uso indevido de dados pessoais para compras:* Criminosos cibernéticos negociam selfies, documentos e dados pessoais para criação de cadastros em marketplaces e lojas, para fraudes ligadas a compra e vendas de produtos. Tenha um anti-fraude ativo e atuante na revisão de integridade dos dados pessoais usados, como por exemplo, tentativa de cadastros duplicados, informando sempre o titulares de dados.
3. *Cancelamentos “chargebacks” fraudulentos:* A facilidade em obter cartões tem permitido que marginais compareçam, até mesmo fisicamente, em lojas, e passem o cartão, requerendo cancelamento tão logo a compra é entregue.
4. *Ataques ou códigos maliciosos:* Os criminosos podem conseguir acesso à base de dados de clientes, compras, cartões e com isso lesar clientes e titulares de dados. Tem crescido também a invasão aos meios de pagamentos utilizados pelos lojistas e com isso, ocorrendo os cancelamentos das compras feitas.
5. *Autenticação fraca ou insegurança nas comunicações:* Tem crescido no Judiciário processos favoráveis aos consumidores, quando é comprovado, por perícia técnica que o site não adotava autenticação forte com dois ou mais fatores, ou mesmo não aplicava criptografia ponta a ponta nas comunicações com o cliente, ou, ainda, ao ser informado de um incidente com dados pessoais, nada fez.

Neste sentido, são preocupações que exigem um reforço

analítico prévio e preparo dos recursos para a segurança da informação e dos dados pessoais tratados. Além do contexto de fraudes, é importante coordenar e revisar previamente as ações planejadas por marketing e outras ações pontuais para a temporada ou pré-temporada, que envolvam tratamento de dados pessoais.

É boa prática que um comitê interno esteja constituído e que os processos para validação das operações que envolvam novos tratamentos sejam considerados e executados. Caberá ao encarregado de proteção de dados (DPO) interagir com as áreas, buscando compreender atividades novas que precisam ter seus fluxos mapeados e com isso, adotadas medidas para reduzir, mitigar riscos, além da avaliação criteriosa da base legal adotada para os novos tratamentos de dados.

Landing pages ou hotsites, muito comuns neste período, e que busquem coletar dados além dos dados mínimos necessários para a compra, precisam contar com disposições transparentes sobre o uso dos dados, finalidade, compartilhamento, tempo de retenção e demais informações, sendo que, em determinadas situações, onde não for possível com clareza e segurança o enquadramento em outra base legal, o tratamento deverá, antes de iniciado, contar com mecanismo para registro do consentimento do titular, sendo que o ônus de provar o consentimento é do agente de tratamento de dados. Vale também o alerta para o não envio de mensagens ou abordagens para contatos que jamais tiveram qualquer relação com o negócio, conduta que poderá caracterizar spam, tratamento irregular ou indício de base de dados comprada.

É preciso cuidado especial com os avisos de privacidade, políticas e termos do site, que deverão estar atualizados e contemplar também as ações que envolvam tratamento de dados pessoais específicos para a Blackfriday, do mesmo modo, contemplando a política de cookies, sendo que o portal ou site da loja deverá dispor de forma transparente de recurso que permita ao usuário selecionar quais pacotes de dados poderão

ser registrados ou coletados, lembrando sempre que este só não terá opção diante dos cookies necessários, que são indispensáveis para o funcionamento seguro do site. Para os demais, devem estar desativados por padrão, em prestígio da privacidade *“by default”.*

Importante mencionar que, dentre todos os direitos do titular de dados, previstos no art. 18 da LGPD, está o direito de “se opor” a um tratamento que foi realizado sem o consentimento do mesmo. Esta oposição poderá se dar, por exemplo, caso as informações prestadas pelo e-commerce apresentem uma atividade de tratamento de dados cuja base legal adotada foi o legitimo “interesse” e o titular discorde.

Deste modo, é muito importante que, previamente, todos os novos processos e operações de tratamento de dados pessoais estejam devidamente mapeadas, analisadas e as medidas para proteção dos dados adotadas e ativas, sem descartar, ainda, a necessidade da manutenção atualizada de documentos e registros que são evidências de que a loja estabeleceu e mantém um sistema de gestão de proteção de dados, informações estas que poderão ser solicitadas a qualquer momento pela ANPD ou órgãos de defesa do consumidor.

É fundamental manter os processos e workflows ativados, com recursos humanos preparados para que, partir do recebimento de requerimentos de titulares ou notificações e até mesmo intimações e autuações, a empresa saiba claramente como agir e qual processo seguir.

Por fim, um dos pontos mais importantes: A gestão e resposta a incidentes. Por mais que o empreendedor invista em segurança da informação, enfrentar um incidente que possa envolver dados pessoais é questão de tempo. Neste sentido, processos de resposta a incidentes de segurança da informação e recursos necessários precisam ser aplicados e preparados para, diante do comprometimento de dados pessoais, sejam adotadas as medidas amparadas por melhores práticas para redução do

impacto e comunicação a titulares e ANPD. Antecipação é fundamental, com preparo de equipes internas e consultorias externas para dar suporte a todos os processos, especialmente nesta fase, onde os criminosos digitais também se preparam para lucrar com golpes, fraudes e crimes cibernéticos, lesando milhares de pessoas.

Deste modo, o que não se espera de um comércio ou loja virtual à esta altura é que tenha que fazer, em tempos de Black Friday, uma "adequação de última hora", mas na verdade, que considerando uma governança já em execução, atue para uma intensificação e revisão de todos os componentes do Sistema de Gestão de Proteção de Dados, com vistas a um período intenso de muitas compras, interações e compartilhamento de dados pessoais, o que somado ao crescimento do oportunismo, golpes e fraudes digitais, em alta no Brasil, pode gerar danos significativos a consumidores e ao varejo, com perdas financeiras e reputacionais irreparáveis. Se o seu negócio não iniciou um programa de governança para compliance com a LGPD, o risco é, evidentemente, ainda maior.

José Antonio Milagre, é Advogado especialista em Direito Digital e Proteção de Dados, Presidente de Instituto de Defesa do Cidadão na Internet – IDCIBrasil, Analista de Sistemas, Mestre e Doutor pela UNESP, DPO Exin, PECB Lead Implementer, e Diretor do PrivacyOffice, grupo de privacidade e proteção de dados da CyberExperts.

Advocacia José Milagre https://www.direitodigital.adv.br