Por Carlos Rodrigues (*)

O LGPD deixa claro que a empresa só pode usar os dados do usuário enquanto forem necessários e, caso não atendam a esse requisito, não pode mantê-los

Uma das principais diferenças entre a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil em fevereiro, e a europeia General Data Protection Regulation (GDPR) é a ausência de artigos específicos que tratam do “direito ao esquecimento” na lei brasileira. Isso, no entanto, está longe de significar que as empresas não precisam se preocupar com a necessidade de abrir mão dos dados dos usuários quando necessário.

Mesmo que não conte com uma previsão específica relacionada ao direito ao esquecimento, o LGPD deixa claro que a empresa só pode usar os dados do usuário enquanto forem necessários e, caso não atendam a esse requisito, não pode mantê-los. Só isso pode significar um grande desafio técnico para as organizações, que vão ter de contar com controles que possibilitem uma configuração de regras mais completa para o tratamento de dados.

Como garantir que sua organização está capacitada para atender essa parte da LGPD? O primeiro passo é certificar-se de que você sabe onde estão os dados e como eles estão sendo usados. A próxima pergunta que você e sua organização precisam responder é sobre sua capacidade de rastrear essas informações e excluí-las (caso você de fato saiba onde estão). Se sua resposta for positiva para essa pergunta, você consegue garantir que esses dados de fato são excluídos e não foram apenas marcados como tal? O que acontece com os dados de histórico de transações? Como provar que as informações foram de fato excluídas?

Para atender às exigências do LGPD, as empresas, especialmente as que investiram pouco em gestão e segurança de dados nos últimos anos, vão enfrentar uma série de desafios para desenvolver uma estratégia com base nos dados coletados dos usuários e a necessidade de excluí-los quando for a hora.

O primeiro passo para atender essa exigência é ser capaz de identificar e classificar todas as informações de identificação pessoal na rede. Dados da Varonis coletados durante a condução de mais de mil risk assessments para clientes e potenciais clientes em 2017 mostraram que 47% das empresas têm, no mínimo, 1.000 arquivos sensíveis abertos a todos os funcionários, enquanto 22% das empresas têm mais de 12 mil arquivos nessa mesma situação.

Este cenário, principalmente quando falamos sobre a forma de coletar e gerenciar os dados da internet, estejam estes armazenados em ambientes físicos ou virtuais, deve sofrer mudanças drásticas em pouco tempo. Para isso, vai ser fundamental cuidar das informações de identificação pessoal que estejam armazenadas em ambiente corporativo, como números de CPF e cartão de crédito, entre outros documentos e dados.

O segundo passo para atender as exigências da LGPD é ter um processo específico para a necessidade de excluir os dados quando não estiverem mais em uso, como a definição de configurações de permissionamento que garantam o armazenamento da menor quantidade possível de informações de identificação pessoal – apenas as que forem realmente necessárias para a empresa – e, ainda assim, com acesso seguro e restrito às pessoas mais indicadas para fazer uso dos dados, eliminando o quanto antes as informações desnecessárias para a prestação de serviços.

A capacidade de configurar essas regras de forma flexível e ágil vai garantir às empresas a execução rápida e segura de exclusões de dados para implementar facilmente políticas de retenção ou exclusão de dados, evitando penalidades e violações de privacidade.

(*) **Carlos Rodrigues** é Vice-presidente da Varonis para a América Latina.

Fonte: Administradores, em 06.03.2019.