Por André Cilurzo (*)

Com a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2019, as pessoas passaram a ter direito sobre dados que as identificam, e, as empresas, obrigações de proteger, armazenar e realizar atividades com tais dados apenas se tivessem respaldo nas exceções trazidas pelas bases legais estabelecidas pela Lei.

Entretanto, antes e vigorar a LGPD, as empresas já armazenavam dados de todos os tipos, inclusive pessoais, muitas vezes de maneira massiva, desordenada e desestruturada, atividade que foi intensificada com a crescente necessidade de abastecer modelos que utilizam *machine learning*.

Isto tem gerado um volume crescente de dados que, em sua maior parte, não tem finalidade, ou caso tenha, é para uso com um objetivo específico e em um único momento apenas. Temos visto situações que profissionais utilizam tais dados para uma atividade específica e, uma vez concluída e seu objetivo atingido, as informações são armazenadas indefinidamente nas organizações.

Essa prática empresarial, além de aumentar os custos de armazenamento nas organizações, pode potencializar os impactos em uma eventual situação de vazamento de dados. É uma situação análoga a uma usina nuclear, que armazena mais urânio (combustível que alimenta usinas nucleares) que o necessário para uma geração de energia prevista. Em caso de um acidente, os impactos são muito maiores, diferente se tal usina armazenasse apenas o necessário.

Além dos possíveis impactos de um vazamento, empresas armazenam dados pessoais sem um objetivo específico, aumentando a probabilidade de uso sem uma finalidade específica e sua exposição a órgãos reguladores.

Para reduzir tais problemas, as empresas têm adotado programas de conscientização sobre o uso

adequado, não apenas de dados pessoais, mas também de outros tipos de dados que podem expor a organização a riscos desnecessários. Tais programas passam pelo mapeamento de quais são os dados essenciais para a realização de suas atividades, seu período de retenção e se tem respaldo regulatório.

Além disso, muitas empresas têm adotado ferramentas de descoberta de dados (*Data Discovery*) para ajudá-las na jornada de identificação, localização e direcionamento de ações para manutenção ou eliminação de dados de seus servidores. Tais ferramentas, além de identificar os dados, podem ajudar na classificação e endereçamento de ações para anonimização ou eliminação, tornando a gestão e a governança de dados mais leve e facilitada.

Ainda podemos observar a ausência de processos adequados, atividades formalizadas e políticas internas para ajudar profissionais no direcionamento do tratamento de dados nas organizações. Esse problema permite que dados sem utilidade sejam internalizados, modificados e fiquem disponíveis para o uso indiscriminado dentro das organizações.

Portanto, as empresas devem implementar, de maneira gradativa, as ações sobre a redução do excesso de dados que armazenam em seus servidores e sistemas a fim de buscar uma melhor governança, proteção de suas informações e assegurar os direitos de seus clientes, colaboradores, investidores e fornecedores.

O tratamento apenas de dados essenciais permitirá às organizações mais tranquilidade para focar em suas atividades que geram valor, além de trazer mais eficiência a suas operações.

(*) **André Cilurzo** é diretor de Data Privacy e especialista em LGPD e Proteção de Dados da Protiviti, empresa global que provê soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.