

Litígios, investigações e fontes de dados emergentes

29.06.2023 5 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e
Cybersecurity

Assuntos

Proteção de Dados e
Cybersecurity ANPD LGPD Felipe
Palhares

Por conta das regras estabelecidas na LGPD, quaisquer atividades de tratamento de dados pessoais precisam respeitar determinados princípios gerais e requisitos específicos

Atire a primeira pedra quem nunca começou uma conversa por WhatsApp, passou para o Instagram e continuou o papo por mensagem direta no LinkedIn. No âmbito corporativo, a mesma lógica é aplicável: uma troca por e-mail pode continuar no Teams, para depois o assunto ser discutido numa reunião via Zoom, e terminar em um plano de ação compilado no Trello.

Com a evolução da tecnologia e a crescente digitalização do ambiente de trabalho ocorrida em razão da pandemia, surgiram incontáveis fontes de dados emergentes, que antes não eram utilizadas para fins de troca de informações corporativas, mas que agora se tornaram ubíquas.

Uma fonte de dados emergente é qualquer banco de dados disponibilizado em nuvem, plataforma ou aplicativo de colaboração utilizado para fins comerciais. Os mais conhecidos são Microsoft 365, Google Workspace e ferramentas de chat como Slack e WhatsApp.

Por natureza, os aplicativos em nuvem estão em constante mudança, melhorando e ajustando-se às necessidades de negócios e produtividade. Embora o ritmo acelerado das mudanças possa ser benéfico na perspectiva do usuário final, da mesma forma é igualmente problemático no contexto de governança, conformidade, investigações e descobertas legais de dados. Quando uma nova funcionalidade ou ajuste são realizados, muitas vezes sem o devido controle de mudanças, surgem novas vulnerabilidades e as equipes especializadas de investigação trabalham para identificar, preservar, coletar, analisar e revisar os dados das plataformas.

As funções de e-Discovery e conformidade disponíveis em determinadas plataformas também mudam com frequência. Isso pode afetar os formatos de exportação dos dados, trazer mudanças nas opções de exportação, a inclusão de conteúdo vinculado e anexos, assim como metadados relevantes.

O uso de fontes de dados emergentes representa um desafio complexo para litígios e investigações que demandem a análise de conversas e informações trocadas por meios eletrônicos. Considerando a variedade de tecnologias utilizadas diariamente no ambiente corporativo, o mero conhecimento de todas as aplicações que são usadas por colaboradores de uma organização já se revela uma tarefa árdua, especialmente quando determinados softwares utilizados sequer foram catalogados pelo administrador dos recursos de tecnologia da informação (prática conhecida como Shadow IT).

Soma-se aos desafios a necessidade de coleta e organização dessa vastidão de informações, que para fins de uma investigação corporativa ou para servir

como evidência na resolução de litígios, precisa ser concatenada com todas as demais fontes de dados disponíveis, permitindo-se traçar uma linha do tempo dos acontecimentos e adequadamente aferir os fatos que ocorreram, com base em subsídios concretos e na preservação da cadeia de custódia.

No contexto de investigação de dados emergentes há quatro pilares que devem ser considerados como uma mudança de paradigma, são eles: (i) acesso compartilhado sem a identificação do usuário; (ii) mensagens de bate-papo com remoção rápida de conteúdo; (iii) compartilhamento de conteúdo e documentos com links e hiperlinks como anexo; e (iv) acesso a várias versões de arquivos, dificultando a visão histórica do conteúdo.

Do ponto de vista jurídico, a obtenção desses dados também encontra possíveis complicações e limitações. Por conta das regras estabelecidas na Lei Geral de Proteção de Dados Pessoais (LGPD), quaisquer atividades de tratamento de dados pessoais - que incluem a coleta e análise de informações - precisam respeitar determinados princípios gerais e requisitos específicos, a exemplo da existência de uma hipótese legal prevista na legislação.

Nesse aspecto, a expectativa de privacidade dos titulares de dados (nos quais se incluem os colaboradores de uma organização) é ponto relevante para avaliar a conformidade da coleta de dados de fontes emergentes com as disposições da LGPD. Embora existam argumentos razoáveis para defender que um empregado não deveria ter uma elevada expectativa de privacidade no uso de ferramentas disponibilizadas por seu empregador, a adoção frequente de políticas de bring your own device pelas organizações, que permitem que empregados utilizem seus dispositivos pessoais para a realização de suas tarefas corporativas, torna a situação nebulosa.

As mesmas dificuldades estão presentes sob o prisma de proteção de dados e segurança da informação. Quando mensagens são trocadas por aplicativos de mensageria instantânea instalados em telefones celulares de uso pessoal, como garantir que respectivo colaborador não apagará todo o histórico de mensagens, ou mesmo que utilizará uma aplicação segura para o intercâmbio de informações sensíveis?

Nesse cenário, é fundamental que as organizações adotem ao menos as seguintes medidas: (i) possuam um inventário das aplicações utilizadas por seus colaboradores para a troca de informações; (ii) investiguem a existência de ferramentas desconhecidas que estejam sendo utilizadas indevidamente; (iii) estabeleçam políticas internas sobre o uso de ferramentas, retenção dos dados e eventuais limites na adoção de dispositivos próprios; (iv) e estejam preparadas para analisar dados de fontes emergentes, com tecnologias que permitam uma avaliação sequencial de eventos, ainda que coletados de fontes distintas.

Sem elas, a adequada análise de dados provenientes de fontes emergentes durante futuros litígios ou investigações internas pode ficar comprometida, trazendo prejuízos potencialmente irreparáveis para respectivas organizações. A célebre frase de Isaac Newton também é aplicável em relação às fontes de dados emergentes: “O que sabemos é uma gota; o que ignoramos é um oceano”.

>>> Este artigo foi escrito por nosso sócio Felipe Palhares, da área de Proteção de Dados e Cybersecurity e por Antonio Gesteira, senior

managing director na FTI Consulting. O artigo foi publicado pelo Valor Econômico em 29/06/2023.

Clique aqui para acessar.

Profissionais que aliam visão jurídica e visão de mercado



Felipe Palhares