COMO EVITAR CONDENAÇÕES TRABALHISTAS POR VAZAMENTO DE DADOS SENSÍVEIS DE EMPREGADOS

Steffanie Silveira de Fraga[1]

Luiz Carlos Gomes Filho[2]

Com a consolidação da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) no ordenamento jurídico brasileiro, a responsabilidade das empresas quanto ao tratamento de dados de seus empregados passou a exigir atenção redobrada. Situações antes vistas como meramente administrativas ou descuidadas hoje configuram ilícitos civis e trabalhistas, ensejando condenações por danos morais.

Duas decisões recentes dos Tribunais Regionais do Trabalho ilustram como diferentes condutas empresariais – ainda que sem intenção dolosa – resultaram em penalizações à luz da proteção de dados. No Tribunal Regional do Trabalho da 3ª Região (TRT-MG)[3], no processo nº 0010034-38.2025.5.03.0167, ficou reconhecida a responsabilidade da empresa pelo vazamento de dados sensíveis de uma empregada, após um incidente cibernético. Embora a empresa tenha afirmado ter tomado providências após o fato, o Tribunal entendeu que não foram comprovadas medidas preventivas eficazes que garantissem a segurança dos dados, como exige a LGPD em seus artigos 46 e 47. O vazamento envolveu dados relativos a finanças pessoais e à saúde da empregada, o que, nos termos do artigo 5º, II, da LGPD, são considerados dados sensíveis, exigindo proteção reforçada. Portanto, a decisão adotou a tese do dano moral presumido (*in re ipsa*) e aplicou a responsabilidade objetiva do controlador de dados (artigo 42 da LGPD), fixando a indenização no valor de R$ 5.000,00.

Já, no TRT da 4ª Região (TRT-RS)[4], a condenação decorreu de uma falha aparentemente banal, mas igualmente imprudente: a empresa utilizou o Termo de Rescisão do Contrato de Trabalho (TRCT) de um ex-empregado como papel de rascunho. O documento, que continha dados pessoais do trabalhador, foi visto por colegas. Ainda que os dados expostos não fossem classificados como sensíveis, a conduta foi considerada negligente e atentatória à privacidade do trabalhador, direito fundamental previsto no artigo 5º, X, da Constituição Federal. Assim, a decisão foi fundamentada nos artigos 186 e 927 do Código Civil e entendeu estar configurado o dano moral, com fixação de indenização no valor de R$ 3.000,00.

---

[1] Advogada regularmente inscrita na OAB/RS 125.181. Sócia-Advogada no escritório Rossi Maffini Milman Advogados (RMM). Pós-graduanda em Direito e Processo do Trabalho pela Universidade Federal do Rio Grande do Sul (UFRGS). Bacharela com Láurea Acadêmica pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). E-mail: steffanie.fraga@rmm.com.br.

[2] Advogado regularmente inscrito na OAB/RS 109.588. Sócio no escritório Rossi Maffini Milman Advogados (RMM). Pós-graduado em Direito Digital pela UniRitter. E-mail: luiz.filho@rmm.com.br

[3] RORSum nº 0010034-38.2025.5.03.0167

[4] ROT nº 0020331-96.2023.5.04.0733

Essas decisões demonstram que o Judiciário trabalhista tem se mostrado cada vez mais atento à proteção de dados no contexto da relação de emprego. Além dos fundamentos clássicos da responsabilidade civil subjetiva (culpa, dano e nexo), a LGPD introduziu a possibilidade de responsabilização objetiva, especialmente quando estão envolvidos dados sensíveis, cuja violação acarreta presunção de dano moral.

Para evitar esse tipo de passivo, é essencial que a empresa adote uma postura preventiva e de aderência aos princípios da LGPD, principalmente, finalidade, adequação, necessidade e segurança. Esses vetores devem orientar as ações da empresa, desde a tomada de decisões sobre a forma e os motivos de coleta dos dados, até a elaboração de políticas de resposta a incidentes de segurança. Em outras palavras, é essencial a elaboração de um programa de governança em privacidade e proteção de dados, com políticas claras sobre coleta, tratamento, compartilhamento e descarte de informações dos empregados. Todos os setores que lidam com dados pessoais, especialmente os de recursos humanos, medicina do trabalho e tecnologia da informação, devem ser treinados para garantir o cumprimento das normas legais.

Vale lembrar ainda que, no ambiente laboral, o consentimento[5] deve ser aplicado em caráter excepcional, dada a assimetria da relação. Autorizações vagas e consentimentos amplos, especialmente em contextos de tratamento de dados pessoais de natureza sensível poderão fragilizar uma tese de defesa e, ainda, indicar tratamento irregular. Em razão disso, a regra é ancorar o tratamento em hipóteses legais compatíveis com o contexto laboral, que não apresentem risco de vícios formais no seu enquadramento, e assegurar que a utilização do consentimento, quando inevitável, seja, de fato, por manifestação livre, informada e inequívoca.

A prevenção exige governança viva. Nesse contexto, a nomeação de um Encarregado de Dados (DPO), embora obrigatória apenas para certas categorias de empresas, é altamente recomendada. Esse profissional será o elo de comunicação entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo a gestão adequada de incidentes, consentimentos e solicitações dos empregados. Trata-se de uma medida simples de governança, mas eficaz na sinalização de que a organização preza pela proteção de dados pessoais.

Também, é fundamental conhecer e registrar os fluxos internos de dados pessoais tratados pela empresa, identificando quais são sensíveis e exigem tratamento mais restrito e limitado a alguns setores ou funções específicas. Nesse cenário, não menos importante é mapear todos os parceiros e fornecedores com acesso a dados pessoais da organização, e garantir que os contratos firmados sejam completos, precisos e estejam em conformidade com as disposições da Lei Geral

[5] Hipótese (base legal) de tratamento prevista junto ao artigo 7, inciso I, quando aplicado a um contexto de tratamento de dados pessoais comuns, e junto ao artigo 11, inciso I, quando aplicado a um contexto de tratamento de dados pessoais de natureza sensível.

de Proteção de Dados. Além disso, as medidas técnicas de segurança da informação precisam estar na pauta de tomadores de decisão. O principal risco das organizações atualmente é cibernético: acessos não autorizados, vazamento de dados, invasões a sistemas e sequestro de arquivos (ransonware) são alguns dos maiores desafios enfrentados em uma economia fundamentalmente digital. Isso inclui a adoção de *firewalls*, padrões de criptografia em arquivos relevantes, políticas de controle de acesso a documentos e sistemas, além de práticas seguras de descarte de documentos físicos e digitais. Isso, porque situações como a reutilização de documentos com dados pessoais como papel de rascunho, como ocorreu no caso citado, devem ser eliminadas por completo por meio de políticas internas e fiscalização de rotina.

Incidentes de segurança certamente ocorrerão pelo caminho, por vezes mais ou menos graves. Por isso, a postura da empresa faz diferença no julgamento judicial e na apuração dos fatos pela ANPD, quando cabível. A LGPD, em seu artigo 48, exige que a empresa notifique a ANPD e os titulares afetados sobre qualquer vazamento relevante, demonstrando transparência e diligência, logo a falta de notificação ou a omissão de informações agrava a responsabilização civil.

A prevenção de condenações trabalhistas por vazamento de dados de empregados não é um ato isolado, mas o resultado de um programa contínuo de governança em privacidade. Empresas que negligenciam a proteção de dados de seus empregados, ainda que por descuido ou por falhas pontuais, se expõem a condenações judiciais, sanções administrativas e danos reputacionais. Por isso, mais do que uma exigência legal, a conformidade com a LGPD é uma prática estratégica de gestão de riscos no ambiente trabalhista e a prevenção, nesse caso, é o melhor e mais barato caminho.