Vazamento de dados: quando a justa causa se sustenta?

19/07/2026

O debate sobre vazamento de dados sigilosos no ambiente corporativo deixou de ser periférico e passou a ocupar o núcleo do contencioso trabalhista empresarial por tocar, de forma cumulativa, dois pilares sensíveis: a fidúcia contratual que sustenta a continuidade do vínculo e a governança de dados, que já se apresenta como dever jurídico e não como mero padrão voluntário de boas práticas.

Freepik

Nesse cenário, a demissão por justa causa em razão de vazamento de dados não pode ser tratada como reflexo automático de qualquer falha, mas tampouco deve ser reduzida, em tese abstrata, à ideia de medida "excepcional" sempre residual. O que a experiência forense demonstra é que a validade da penalidade máxima depende de análise técnica, lastro probatório consistente e leitura contextual da gravidade, do risco e da finalidade do ato.

Sob o prisma estritamente trabalhista, o ponto de partida é o artigo 482 da CLT, com especial relevo para a alínea "g" (violação de segredo da empresa), sem prejuízo de enquadramentos concorrentes conforme a dinâmica do caso concreto, como mau procedimento (alínea "b"), indisciplina (alínea "h") e, em hipóteses mais agudas, improbidade (alínea "a"). Ainda assim, a experiência jurisprudencial contemporânea indica que a discussão raramente se resolve pela mera escolha da alínea.

O que sustenta ou derruba a justa causa é, sobretudo, a demonstração concreta de um núcleo de elementos: ciência prévia e inequívoca do dever de sigilo, materialidade e autoria do vazamento com rastreabilidade mínima, e gravidade suficiente para romper a confiança e tornar inexigível a continuidade do vínculo, observadas a imediatidade compatível com apuração interna e a proporcionalidade entre falta e sanção.

Nesse contexto, é particularmente relevante a racionalidade decisória que desloca o foco do "quantos receberam" para o "quem podia receber" e "para qual finalidade". Em precedente do TRT da 2ª Região no ROT 1000849-87.2024.5.02.0080, manteve-se a justa causa aplicada a empregado em cargo de gestão que divulgou documento sigiloso, de circulação restrita, a colega de trabalho sem autorização e sem finalidade profissional, em afronta a termo de confidencialidade firmado na contratação.

O aspecto determinante, ali, não foi a amplitude do compartilhamento, mas o desvio de finalidade e a transgressão objetiva da cadeia legítima de acesso, agravada pela posição ocupada, que eleva o *standard* de lealdade e reserva. Em matéria de sigilo empresarial (segredo

da empresa), a publicidade indevida pode se consumar mesmo com um único destinatário, desde que ele não integre o circuito autorizado e que a transferência represente quebra da lógica de proteção da informação.

Spacca

A gravidade tende a se acentuar quando a informação é deslocada do ambiente corporativo para canal pessoal, por razões que transcendem a mera formalidade do meio utilizado. Em julgado do TRT da 7ª Região no ROT 0000694-58.2024.5.07.0017, reconheceu-se que o compartilhamento de informações empresariais para e-mail pessoal configura quebra de confidencialidade e pode justificar a rescisão motivada. Há, nesse tipo de conduta, uma transformação qualitativa do risco: ao migrar dados para um ambiente fora da infraestrutura corporativa, criam-se zonas de exposição com perda de controle, fragilização de trilhas de auditoria, dificuldade de delimitar acessos subsequentes e incremento de potencial reiteração.

Por isso, é recorrente o enfrentamento, pelos tribunais, da tese de gradação de penas, com afirmação de que, diante de falta intrinsecamente grave e ruptura de confiança, a justa causa pode prescindir de advertências prévias, desde que o empregador demonstre, com segurança, o fato, a autoria e a incompatibilidade da manutenção do vínculo.

Divulgação nas redes

O risco também se maximiza quando o vazamento assume feição pública, especialmente em redes sociais, em razão do alcance, da velocidade de disseminação e da baixa reversibilidade do dano. No TRT da 17ª Região, no RO 0000544-92.2015.5.17.0121, a publicação de fotos do parque industrial em rede social foi considerada violação de segredo da empresa e quebra de fidúcia, apta a ensejar justa causa com fundamento no artigo 482, “g”, da CLT.

Em linha convergente, no TRT da 14ª Região, no ROT 0000500-89.2018.5.14.0141, reconheceu-se falta grave pela divulgação, em rede social, de vídeo gravado durante o labor, com ênfase no descumprimento de cláusula de confidencialidade e violação de normas internas. Esses casos são didáticos porque evidenciam que, frequentemente, a conduta não se resume a um único ilícito contratual: soma-se a quebra de sigilo à transgressão de regras de segurança, ética e proteção do ambiente industrial, reforçando a tipicidade e a proporcionalidade da sanção quando a prova é robusta.

Há, ainda, a categoria mais sensível em setores de serviços e varejo: o vazamento com vetor concorrencial, no qual a quebra de confidencialidade se associa à deslealdade e ao desvio de boa-fé objetiva. No TRT da 9ª Região, no RO 0000585-49.2017.5.09.0303, manteve-se a justa causa em cenário de repasse de lista de clientes e informações estratégicas a empresa

concorrente, em violação a cláusula de confidencialidade.

A relevância desse tipo de precedente está em neutralizar uma linha defensiva recorrente do trabalhador, fundada na ausência de prejuízo imediato: em matéria de segredo empresarial e dados estratégicos, a potencialidade de dano, aliada à ruptura do dever de lealdade, pode ser juridicamente suficiente, desde que o nexo probatório esteja solidamente delimitado, com indicação de origem da informação, meio de extração, destinatário e finalidade.

Disposições da lei

É nesse ponto que a LGPD e o debate sobre LGPD nas empresas deixa de ser pano de fundo e passa a atuar como elemento estruturante do risco jurídico do incidente. A Lei nº 13.709/2018 impõe deveres concretos de segurança e governança ao controlador e prevê, no artigo 48, a obrigação de comunicação de incidente de segurança à ANPD e ao titular, quando houver risco ou dano relevante. Além disso, em 24/04/2024, a ANPD aprovou a Resolução CD/ANPD nº 15/2024, que regulamenta a comunicação de incidentes de segurança, reforçando os eixos de responsabilização e prestação de contas, bem como a necessidade de registro e documentação dos incidentes por período mínimo determinado no próprio regulamento.

Na prática, quando o vazamento envolve dados pessoais de clientes, fornecedores ou empregados, o fato deixa de ser apenas desvio disciplinar interno: ele pode irradiar consequências regulatórias, reputacionais e de responsabilização, exigindo resposta rápida, estruturada, documentada e tecnicamente justificável. Isso não significa "punitivismo", mas evidencia que o ato do empregado, em determinadas circunstâncias, instaura risco juridicamente qualificado para a empresa, o que influencia a aferição da gravidade e a própria inexigibilidade de manutenção do vínculo.

Da perspectiva de gestão de risco e sustentação probatória no contencioso, as boas práticas deixam de ser ornamento de *compliance* e passam a funcionar como infraestrutura defensiva. A política de confidencialidade precisa existir, ser compreensível, ser efetivamente comunicada e aplicada de forma coerente, com controles de acesso compatíveis com a classificação da informação. Termos individuais de sigilo ajudam, mas não substituem treinamento, governança de acessos e mecanismos de auditoria.

No plano probatório, ganha especial relevância a capacidade de demonstrar, por registros minimamente auditáveis, como a informação foi acessada, por qual meio foi transferida, para quem foi enviada e qual o impacto ou risco potencial, preservando-se, sempre que possível, a cadeia de custódia digital. Do mesmo modo, a imediatidade deve ser lida com racionalidade: apurações internas são compatíveis com a exigência de pronta reação, desde que diligentes e delimitadas no tempo, justamente para afastar alegações de precipitação ou de punição baseada em percepções genéricas de "quebra de confiança", sem vínculo estrito com o fato e sua autoria.

Em síntese, a diretriz que se consolida é objetiva: quando ocorre justa causa por vazamento de informação sigilosa ou dado sensível compromete a confiança e expõe a empresa a risco relevante, especialmente em ambientes digitais e sob a moldura da LGPD, a justa causa tende a

ser juridicamente sustentável, desde que o empregador comprove a ciência prévia do dever de sigilo, a materialidade e autoria do ato com lastro técnico e a gravidade concreta apta a romper a fidúcia, com apuração diligente e proporcionalidade.

O poder disciplinar não é absoluto, mas, uma vez demonstrada a ruptura objetiva do dever de lealdade em contexto de risco qualificado, também não se pode exigir, como regra, a reconstrução artificial do vínculo por mera tolerância, sobretudo quando a conduta compromete a governança informacional e a responsabilidade externa da organização.

Fonte: https://conjur.jumps.com.br/2026-jul-19/vazamento-de-dados-quando-a-justa-causa-se-sustenta/