Impactos da LGPD no teletrabalho

04.11.2021 4 minutos de leitura

Autores

Felipe Palhares

Assuntos

Trabalhista | Proteção de Dados e Cybersecurity | ANPD | LGPD | Home Office

A transição do trabalho presencial para o teletrabalho, especialmente quando realizada de forma abrupta, como foi o caso para muitas organizações em razão da pandemia do Covid-19, também traz complicações do ponto de vista de proteção de dados pessoais.

A partir de 18 de setembro de 2021, com a entrada em vigor da **Lei Geral de Proteção de Dados Pessoais (LGPD)**, todas as atividades de tratamento de dados pessoais passaram a ter que se adequar aos requisitos previstos em respectiva legislação. Se no trabalho presencial as preocupações com o tema já são relevantes, no teletrabalho elas passam a ganhar um patamar ainda mais elevado.

Para que não restem dúvidas, se a sua organização implementou o teletrabalho, ela realiza atividades de tratamento de dados pessoais a todos os instantes. O envio e recebimento de e-mails, troca de mensagens em aplicativos corporativos de comunicação, realização de vídeo chamadas ou conferências telefônicas, entre tantas outras atividades diárias, envolvem a coleta, compartilhamento, processamento e armazenamento de dados.

Nesse cenário, há dois aspectos centrais que merecem atenção por parte das organizações. O primeiro deles diz respeito à verificação da observância das hipóteses legais para o tratamento de dados, as chamadas bases legais. Nos termos da LGPD, para que o tratamento de dados seja admitido, é necessário que o controlador (organização que define as finalidades e meios do tratamento) identifique qual das hipóteses previstas no art. 7º ou no art. 11 da legislação são aplicáveis e permitem que respectiva atividade de tratamento seja realizada.

Importante frisar que o consentimento do titular de dados não é a única base legal prevista na LGPD e que, quando se trata de relações entre empregador e empregado, dificilmente será a base legal mais apropriada para amparar o tratamento de dados pessoais. Devido ao desbalanceamento de posições entre as partes, pode-se argumentar que eventual consentimento concedido pelo empregado não seria livre, um dos requisitos estipulados pela legislação para a qualificação de consentimento válido.

O segundo ponto de atenção está relacionado à segurança da informação, um dos pilares disciplinados pela LGPD para garantir a proteção dos dados pessoais contra acessos indevidos ou tratamentos inadequados ou ilícitos. Implementar medidas efetivas de segurança da informação no ambiente presencial já é um grande desafio, que se acentua ainda mais no contexto do teletrabalho.

Nesse aspecto, é fundamental que a organização avalie quais medidas administrativas e técnicas podem ser adotadas para diminuir a exposição aos riscos inerentes do trabalho remoto. É sempre preferível, quando possível, que a organização ofereça aos seus empregados dispositivos corporativos para o exercício do trabalho, que sejam adequadamente configurados pela

área de tecnologia da informação, de modo a garantir melhor proteção aos equipamentos que serão utilizados pelo empregado.

O uso de equipamentos pessoais aumenta consideravelmente o risco de que dados pessoais mantidos pela organização sejam acessados por terceiros indevidamente, uma vez que a organização não tem condições de avaliar se aquele equipamento já não está infectado, se conta com antivírus e aplicativos atualizados e se é utilizado somente pelo próprio empregado.

Outra preocupação afeta à segurança da informação é a proteção da confidencialidade dos dados pessoais que podem ser acessados pelo empregado. Trabalhar em casa ou em um ambiente público pode permitir que terceiros que não possuem autorização para conhecer certas informações (incluindo familiares e amigos do empregado), possam acessar respectivos dados pelo simples fato de estarem perto do empregado, seja ao ouvirem uma conversa de uma conferência telefônica, seja por poderem olhar a tela do computador do empregado livremente.

A confidencialidade é um dever implícito do empregado dentro da relação empregatícia pautada por um padrão ético de confiança mútua, cuja violação constitui justa causa para rescisão do contrato de trabalho, nos termos da alínea G do artigo 482 da CLT. No mesmo sentido, a Lei 9.279, que regula os direitos e obrigações inerentes à propriedade intelectual, classifica como crime de concorrência desleal a divulgação, exploração ou utilização, sem autorização, de informações e dados confidenciais que não sejam de conhecimento público, cujo acesso decorreu da relação empregatícia, mesmo após a rescisão do contrato de trabalho.

Para endereçar essas situações, duas recomendações são relevantes: (i) incluir cláusulas de confidencialidade ou elaborar NDAs com os empregados, reforçando a sensibilidade das informações que eles terão acesso e a sua responsabilidade de não divulgá-las para terceiros em qualquer cenário, sob pena de imposição de sanções administrativas; e (ii) ampliar a conscientização sobre o tema segurança da informação, que deve ser frequente e recorrente, para que os empregados saibam da relevância desse tema para a organização, das suas responsabilidades pela proteção das informações e das melhores práticas para evitar eventos que possam resultar numa violação à LGPD.

**Este artigo foi escrito por nosso sócio Felipe Palhares, da área de Proteção de Dados e Cybersecurity, e pela advogada Julia Soave Garcia da área Trabalhista. A publicação foi veiculada pelo Estadão em 30/10/2021. Clique aqui e confira o artigo na íntegra.*

***Este conteúdo também faz parte do e-book "Dilemas Trabalhistas Atuais: fim da pandemia e novas formas de trabalho". Clique aqui para ler a publicação da íntegra.*

Leia também:

- E-book | Sanções Administrativas da LGPD: O que você precisa saber
- Informativo de Proteção de Dados e Cybersecurity: confira as novidades

da área de outubro de 2021.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares