

ASSOCIAÇÃO NÃO TERÁ QUE CUMPRIR ACORDO COLETIVO QUE FERE A LGPD



O TST rejeitou recurso do Sindicato dos Empregados em Instituições Benéficas, Religiosas e Filantrópicas de São Paulo (Seibref/SP), que exigia que a Associação Cristã de Moços (ACM) enviasse a uma empresa administradora de cartão de descontos dados pessoais de seus empregados. Segundo o colegiado, a medida fere a Lei Geral de Proteção de Dados Pessoais, por se tratar de privacidade, direito fundamental indisponível.

As convenções coletivas determinavam que as empresas enviassem ao sindicato dados como nome completo, CPF, telefone, e-mail, data de nascimento e nome da mãe de cada empregado para a emissão de um cartão de

benefícios, o que não vinha sendo cumprido pela ACM, sob alegações de que o envio massivo dessas informações era contrário às disposições da LGPD.

Após sucessivas derrotas nas instâncias inferiores, o Seibref buscou o TST que julgou improcedente seu pleito, alegando que as convenções coletivas não tem o poder de sobrepor-se aos direitos fundamentais dos trabalhadores, dos quais a privacidade é um deles. Adicionalmente, o TST corretamente pontua que o envio e tratamento dos dados requer o consentimento de cada um dos colaboradores da ACM, não podendo ser realizado em massa.

DISPONIBILIZAÇÃO INDEVIDA DE DADOS PESSOAIS NÃO SENSÍVEIS GERA DANO MORAL PRESUMIDO

Em recentes julgamentos, o STJ firmou um precedente muito importante no que diz respeito à Lei Geral de Proteção de Dados: a disponibilização indevida de dados pessoais gera dano moral presumido, independente de prova do prejuízo, ao titular afetado.

O caso dos autos versava sobre a disponibilização de dados não sensíveis (nome, CPF, endereço, telefone, etc.) por instituições financeiras a terceiros, por meio de consulta à banco de dados. Embora os dados fossem não

sensíveis, as instituições financeiras não dispunham do consentimento dos titulares para o repasse dessas informações aos terceiros.

As decisões respeitam o permissivo da LGPD para o tratamento de dados para a proteção ao crédito, reconhecendo a possibilidade, mas condiciona esta hipótese à consulta de score de crédito e ao histórico de crédito apenas, excluindo a consulta de dados cadastrais, cujo compartilhamento indevido gera dano moral presumido.

RESPONSABILIDADE DOS BANCOS DIGITAIS NOS GOLPES VIRTUAIS



O STJ julgou improcedente um recurso no qual o recorrente buscava indenização por danos morais contra um banco virtual. O recorrente foi vítima de um golpe do leilão falso, e alegava que a facilidade para criar contas virtuais oferecida pela instituição teria sido fator preponderante para que tivesse sido vitimado pelo golpe.

Os tribunais alegaram que o banco digital cumpriu integralmente com os requisitos legais para a abertura de conta

digital, de maneira que não se pode alegar falha na prestação do serviço. Ademais, o recorrente sequer era correntista do banco digital, o que torna a relação entre as partes indireta.

A decisão aponta no sentido de que os consumidores devem revestir-se de cautela ao negociar, sendo descabida a responsabilização dos bancos digitais por toda e qualquer irregularidade que aconteça com as transações feitas em suas plataformas.

MANTIDA JUSTA CAUSA A EMPREGADA QUE ENVIOU DADOS PESSOAIS DE CLIENTES PARA E-MAIL PESSOAL

A justa causa por violação da Lei Geral de Proteção de Dados pode ser aplicada quando um funcionário descumprir as normas estabelecidas pela legislação, como acesso não autorizado a dados pessoais, divulgação não autorizada de informações e falta de segurança na proteção de dados.

Neste sentido, uma funcionária foi demitida por justa causa, ao ser flagrada pelo departamento de segurança corporativa de sua empresa enviando dados pessoais de clientes de seu e-mail corporativo para seu e-mail pessoal.

Embora a funcionária tenha alegado que o envio se deu em função das altas pressões sofridas no ambiente de trabalho, que alegadamente a forçariam a trabalhar em casa, a justificativa não foi aceita e a demissão foi mantida.

A funcionária admitiu que tinha passado por treinamentos relativos à LGPD e, portanto, tinha consciência da ilegalidade de sua conduta. O caso reforça a necessidade de seguir a Lei Geral de Proteção de Dados mesmo internamente nas empresas.

COMPLIANCE: ALÉM DA LGPD

Podemos entender por compliance “estar adequado”. Neste sentido, um número cada vez maior de empresas está em compliance com a Lei Geral de Proteção de dados, com seus DPOs nomeados, sites e documentos adequados e mapeamento em dia.

Ocorre que o compliance é muito mais do que a LGPD. As empresas precisam estar adequadas às legislações setoriais, municipais, estaduais, tributárias, trabalhistas, ambientais e muitas outras, sem contar com as necessidades específicas ditadas por seus clientes, fornecedores e parceiros.

Neste sentido, não basta ter um robusto código de ética. É preciso estabelecer controles de governança sobre todos os requisitos legais mencionados, mas também quanto à conduta dos colaboradores, canais de denúncia, regras para due diligence, comitê de ética, treinamentos e muito mais.

Não se pode esperar que um trabalho tão minucioso seja feito corretamente a partir de modelos gratuitos disponíveis na internet. A condução dessas atividades deve ser feita por um corpo competente e especializado.