OpiniÃ£o: Riscos cibernÃ©ticos e dados pessoais na Ã¡rea trabalhista

A entrada em vigor da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), em setembro de 2020, potencializou o direito à privacidade e à vida privada e abriu caminho para a consolidação do princípio da autodeterminação informativa. Contudo, a adequação à lei ainda não é vista como prioridade por parte de muitas empresas, tornando-as vulneráveis aos riscos cibernéticos inerentes à era

A mudança de percepção cultural em relação ao tratamento de dados pessoais e às medidas de segurança aplicadas a esses dados vem aos poucos fazendo parte do dia a dia de empresas e colaboradores. No contexto pandêmico, tivemos de nos adaptar à rotina do trabalho remoto em tempo bastante curto, o que aumentou as vulnerabilidades inerentes ao mundo *online* e, entre elas, o potencial de ataques cibernéticos.

Segundo pesquisa do Fórum Econômico Mundial, *"The Global Risk Report 2019"*, o risco cibernético figura em quarto lugar como o mais provável nos próximos dez anos. Esse risco se refere aos *"potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais"* (*International Organization of Securities Commissions*), princípios básicos da segurança da informação.

Nesse contexto, não apenas os empregadores, mas também os empregados são responsáveis pela gestão do risco e das vulnerabilidades decorrentes do ambiente digital. Empregadores devem adotar medidas técnicas e administrativas para resguardar os dados pessoais e dados pessoais sensíveis decorrentes da relação de trabalho e os empregados devem observar as normas de segurança e proteção de dados adotadas pela empresa.

Mas quais são os cuidados que os empregadores podem adotar para melhor gerenciar o risco que envolve o tratamento de dados de seus colaboradores e mitigar os danos que podem ocorrer em eventual vazamento de dados? Vejamos abaixo algumas medidas que podem ser adotadas em âmbitos pré-contratual, contratual e pós-contratual.

Dados pré-contratuais
Aqui estamos diante da fase preliminar do contrato de trabalho. É nessa fase que o empregador tem o primeiro contato com os dados do candidato (titular de dados). É de conhecimento geral que as empresas recebem dezenas de currículos e que, geralmente, os currículos contêm dados pessoas, tais como: nome, endereço, filiação, idade, estado civil, RG e CPF, ou seja, uma gama de dados pessoais (artigo 5º, inciso I da LGPD).

Geralmente, os processos seletivos são realizados e nem todos os candidatos são contratados, o que leva a empresa a "armazenar" currículos para eventual oportunidade. Algumas empresas chegam a compartilhar o currículo do candidato com outras empresas, justamente com o intuito de alguma forma ajudar esse candidato. Contudo, de acordo com a LGPD, tal conduta requer o consentimento do candidato. Portanto, orienta-se que as empresas, quando da não contratação, descartem imediatamente os dados desses candidatos e não compartilhem sem o consentimento do titular, sob pena de incorrer em sanções previstas na LGPD.

As empresas devem ainda se atentar ao anunciar uma vaga ou solicitar informações, visto que é proibida a coleta de dados sensíveis que possam gerar qualquer critério discriminatório entre os candidatos. O artigo 5º, inciso II, da LGPD considera dado sensível *"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"*.

Dessa forma, recomenda-se a adoção do princípio da minimização da coleta de dados, que nada mais é do que solicitar a menor quantidade possível de dados para a realização das finalidades pretendidas, justamente para reduzir eventuais riscos.

Dados contratuais
Após o candidato ser selecionado e contratado, o empregador passa a ter contato quase diário com diversos dados, muitas das vezes sensíveis, referentes a esse colaborador. Dessa forma, deverá adotar medidas adequadas e seguras para o tratamento desses dados. Apenas para exemplificar: a LGPD considera os dados biométricos como sendo sensíveis. Ocorre que muitas empresas utilizavam o sistema de controle de jornada através de ponto biométrico, portanto, passando a ter acesso a um dado sensível desse funcionário. Outro exemplo é o recebimento de atestados médicos e exames que constam na Classificação Internacional de Doenças (CID), ou identificação da doença. Tais dados também são sensíveis e demandam um tratamento seguro, respeitando os princípios e bases legais da LGPD. Vale destacar que a exigência de CID em atestados médicos é um tema polêmico na jurisprudência do Tribunal Superior do Trabalho, que tem entendimento no sentido de que a inserção da sigla no atestado pode violar o direito fundamental à privacidade e à intimidade do trabalhador (Informativo nº 114 do TST). Além das situações já mencionadas, é comum que as empresas tenham fichas de registro de empregados, as quais, geralmente, contém dados pessoais e pessoais sensíveis, tais como: afastamentos por motivos de saúde, filiação sindical, advertências e suspensões, portanto, tais dados devem ser corretamente armazenados e tratados pelas empresas, limitando o acesso à ficha desses funcionários.

No que diz respeito à base legal para o tratamento de dados do empregado, é preciso avaliar a finalidade para a qual foram coletados. A coleta de dados biométricos para o acesso à empresa, por exemplo, poderá ser feita mediante consentimento do empregado, informando-o a respeito da finalidade expressa de utilização, vedada utilização para outra finalidade sem o seu consentimento. Dados relativos à saúde, sensíveis, portanto, podem ser coletados independentemente do consentimento, quando em cumprimento à obrigação legal a qual o empregador esteja sujeito, como aquela disposta no artigo 168 da Consolidação das Leis Trabalhistas (CLT).

Por outro lado, o compartilhamento de dados relacionados à saúde com seguradoras e planos de saúde requer a expressa concordância do titular, motivo pelo qual é necessário elaborar um termo de consentimento para o compartilhamento das informações para finalidades específicas.

Deve-se notar que a regra geral estipulada na LGPD é que os dados pessoais e pessoais sensíveis dos funcionários não podem ser fornecidos a terceiros, sob pena de possibilitar prejuízos e discriminação, o que, por sua vez, pode ensejar uma reparação indenizatória. Importante salientar, ainda, que é direito do empregado ter acesso a todos os seus dados decorrentes do contrato de trabalho, podendo ele requerer, a qualquer tempo, que a empresa informe a natureza e a destinação das informações, podendo inclusive solicitar o descarte desses dados quando da rescisão contratual.

Em recente decisão, a 6ª Turma do TRT da 3ª Região (MG), com base na LGPD, julgou procedente pedido feito por trabalhadora em produção antecipada de provas para determinar à empresa a apresentação de registros de ponto, ficha de empregado atualizada, demonstrativos de pagamento e ficha financeira. Ao julgar procedente o pedido, a turma enfatizou que a LGPD é uma lei geral, de indiscutível transversalidade, que reflete, profundamente, nas relações jurídicas de emprego. Afinal, é grande o fluxo de dados pessoais nas relações de trabalho, desde a fase pré-contratual até a pós-contratual, sendo o empregador o responsável pelo tratamento dos referidos dados (controlador — artigo 5º, VI, LGPD).

Para a turma, os documentos requeridos pela autora contêm informações pessoais da empregada relacionados à sua vida laboral, sendo a reclamante, portanto, a titular dos mencionados dados pessoais (artigo 5º, V, LGPD). E, como titular dos dados pessoais dispostos em documentos mantidos pela ex-empregadora, a parte autora tem o direito legal de livre acesso aos mesmos, de forma facilitada, ainda que após o término da relação laboral (artigo 6º, IV, LGPD). Sustentou ainda que a empregadora, como controladora dos dados pessoais de sua ex-empregada, tem o dever de atender os direitos da titular dos dados pessoais elencados no artigo 18 da LGPD, bem como de, entre outras inúmeras obrigações legais, agir com transparência (artigo 6º, VI, LGPD).

Portanto, rejeitou o argumento defensivo no sentido de que *"não há, no ordenamento jurídico pátrio, qualquer dispositivo que obrigue a reclamada a exibir os documentos pretendidos pela autora"*. Por fim, decidiu que os dados pessoais da ex-empregada contidos nos documentos requeridos, bem como em outros que a ex-empregadora ainda armazene, pertencem àquela e é obrigação legal da parte ré permitir o livre acesso a eles, de forma facilitada e em segurança.

A decisão aqui comentada é inédita e demonstra que a LGPD já é uma realidade e deve, portanto, ser observada e respeitada.

Dados pós-contratuais
Com o término do contrato de trabalho, a pergunta que surge é: preciso armazenar os dados? Posso descartar? Quanto tempo devo armazenar? Esses são alguns questionamentos que surgem no dia a dia e que os empregadores devem ter atenção.

Primeiramente, é importante verificar a real necessidade de manter determinado dado. Se não houver finalidade específica, é melhor eliminá-lo. Na seara trabalhista, vale a pena destacar a hipótese de conservação dos dados pessoais dos trabalhadores com a finalidade de cumprir uma obrigação legal ou regulatória pela empresa, como é o caso dos documentos relativos ao Fundo de Garantia do Tempo de Serviço (FGTS) e previdenciários, que devem ser armazenados por 30 anos.

Destaca-se que muitos desses dados das fases contratual e pós-contratual são armazenados em dispositivos informáticos, o que demanda dos empregadores a adoção de medidas técnicas e administrativas para a proteção dessas informações de ataques de agentes mal-intencionados. A gestão do risco cibernético passa pela conscientização de funcionários quanto às ações que podem adotar para diminuir os riscos de ataque e comprometimento de suas informações e da empresa.

É importante ter em mente que a gestão de riscos deve ser prioridade de todos os funcionários da empresa, e não apenas da área de tecnologia da informação (TI), pois esta é responsável pela infraestrutura de segurança e dos meios técnicos para a proteção das informações. A proteção de dados e da privacidade é realizada no dia a dia operacional dos trabalhadores e estes devem observá-las como parte integrante do seu trabalho.

Algumas medidas objetivas podem ser tomadas por parte de todos da empresa para mitigar a possibilidade de ocorrência de ataques cibernéticos, tais como: não clicar em links suspeitos recebidos por e-mail; sempre verificar a identidade do remetente de e-mails corporativos; não utilizar o e-mail corporativo para finalidades pessoais; ao se ausentar da mesa, bloquear a tela; não deixar documentos em cima da mesa, onde todos podem ver; não entrar em sites impróprios para o local de trabalho; não clicar em links suspeitos, entre outras.

Até 1977, o empresariado brasileiro não tinha a cultura de fornecer equipamentos de proteção individual aos trabalhadores, os chamados equipamentos de proteção individual (EPIs). Tal prática passou a ser obrigatória com a edição da Lei. 6.514 de 22 de dezembro de 1977. No entanto, a adaptação cultural ocorreu somente após diversas tragédias envolvendo acidentes de trabalho e, por consequência, milhões de reais em multas pelo descumprimento. Hoje, após 44 anos, é raro encontrar empregadores que não forneçam tais equipamentos. A efetiva proteção de dados deve ser entendida como o EPI do século 21 e a mudança cultural não pode demorar mais 44 anos…