Valéria Reani: A lei de proteção de dados e as relações de trabalho

21/09/2018

A Lei 13.709/2018[1], sancionada pelo presidente Michel Temer, representa um marco legal para a proteção de dados pessoais e a privacidade no Brasil.

Conhecida como Lei Geral de Proteção de Dados (LGPD), é, assim como o Regulamento Geral sobre a Proteção de Dados (norma europeia que entrou em vigor em maio, também conhecida como GDPR[2]), uma norma baseada em princípios e, ao regular a proteção dos dados pessoais, garante direitos aos cidadãos e estabelece regras claras sobre as operações de tratamento realizadas por órgãos públicos ou privados.

Um princípio básico refere-se à responsabilização do controlador de dados (a quem competem as decisões referentes ao tratamento de dados pessoais), que deverá ser capaz de demonstrar que o processamento é realizado de acordo com a LGPD, de forma eficaz. Adota-se uma perspectiva pela qual a privacidade deve ser respeitada desde a concepção dos serviços/produtos, uma premissa "cultural" para trilhar o caminho da conformidade.

Trocando em miúdos, a LGPD traz princípios que empoderam o cidadão, a ter mais noção de que dados pessoais são tratados, armazenados, transferidos, comercializados, da mesma maneira que o empodera a denunciar práticas nocivas aos órgãos competentes.

Ressalte-se os 10 principais pontos sobre a Lei Geral de Proteção de Dados brasileira:

- afeta qualquer atividade que envolva a utilização de dados pessoais, incluindo o tratamento pela internet, de consumidores e empregados, entre outros;
- o consentimento será umas das 10 possibilidades que legitimarão o tratamento de dados pessoais;
- introduz 10 princípios da proteção de dados, incluindo-se o de demonstrar medidas adotadas para cumprir a lei (prestação de contas);
- titulares dos dados terão amplos direitos: informação, acesso, retificação, cancelamento, oposição e portabilidade, entre outros;
- em caso de incidentes de segurança envolvendo os dados, nas situações aplicáveis;
- aplica-se também a empresas que não possuem estabelecimento no Brasil;
- regras específicas para tratar dados sensíveis, transferência internacional de dados e utilizar dados de crianças e adolescentes;
- realizar avaliação de impacto à proteção de dados (semelhante ao DPIA – *data protection impact assessment*)[3];
- atividades de tratamento de dados devem ser registradas em relatório;
- toda empresa responsável por tratamento de dados deverá nomear um encarregado de proteção de dados pessoais.

A lei ainda determina punição para infrações, como advertência a multa.

Neste contexto, a lei objetiva proteger a privacidade das pessoas e reorganizar a maneira como companhias lidam com dados e segurança da informação. Essa é a ideia central da Lei de Proteção de Dados (Lei 13.709/2018), que entra em vigor em 15/2/2020 e é aplicável a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado. Em linhas gerais, a lei define como dados pessoais quaisquer informações relacionadas a pessoa natural identificada ou identificável e dados sensíveis como qualquer dado pessoal passível de maior potencial discriminatório em relação ao seu titular, estabelecidos na lei como os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biométrica de uma pessoa física.

A lei define ainda dado anônimo ou anonimizado como qualquer dado pessoal que, submetido a meios técnicos razoáveis, passe a não mais identificar ou a proporcionar a identificação de uma pessoa natural, direta ou indiretamente — por exemplo, indicação de que uma pessoa do gênero masculino mora no prédio Oscar Freire.

Mais direitos para o titular de dados, mais obrigações para empresas
Diversos direitos do cidadão, enquanto titular de dados, estão protegidos pela LGPD, de modo que as empresas podem ter que atender às suas solicitações para, por exemplo, retificar dados incorretos, incompletos ou desatualizados, excluir dados ou realizar a sua portabilidade para outro fornecedor de serviço ou produto.

Adaptar-se para conseguir atender a tais solicitações, por parte de inúmeros titulares de dados, será um grande desafio para as empresas de modo geral, sobretudo para aquelas de médio e menor porte.

A nova lei tem importantes impactos nas relações de trabalho e demanda das empresas algumas adequações em seus procedimentos internos e contratos, sob pena de sanções administrativas e multa de até R$ 50 milhões por infração.

Bases legais para o tratamento de dados pessoais
O tratamento de dados pessoais exige um fundamento legal. A LGPD enuncia 10 hipóteses autorizadoras do uso dos dados pessoais, das quais destacam-se:

- o fornecimento de consentimento inequívoco pelo titular dos dados;
- o cumprimento de obrigações legais ou regulatórias pelos agentes do tratamento;
- para a execução de políticas públicas pela administração pública;
- para atender aos interesses legítimos dos agentes de tratamento.

Esta última hipótese permite o uso de dados para finalidades além daquelas originalmente autorizadas, mediante um teste de proporcionalidade que considera os interesses dos responsáveis pelo tratamento e os direitos individuais dos titulares. Essa situação é particularmente importante, pois viabiliza usos inovadores dos dados, utilizando tecnologias como baseadas em *big data*, inteligência artificial, *machine learning* e modelos de negócio inovadores.

O impacto da lei nas relações trabalhistas

Antes mesmo de haver uma relação laboral, entre um cidadão e uma corporação, existe a responsabilidade das empresas, no Direito do Trabalho, que começa na fase antes da contratação (pré-contratual), ou seja, no processo seletivo.

Assim, a empresa, ao fazer o anúncio de emprego, precisa adotar algumas cautelas, como, por exemplo, não fazer discriminação com o candidato. A discriminação no processo seletivo pode ser evidenciada quando a vaga requer injustificadamente algum requisito, tal como: homem, mulher, casado, solteiro, sem filhos, religião, opção sexual ou, ainda, "boa aparência".

Um dos princípios basilares de LGPD é o da não discriminação. Ele determina que uma pessoa não pode ser discriminada, de modo que a prejudique, com base nos seus dados pessoais. Ainda, a LGPD confere ao titular — a pessoa física a quem os dados se referem —, o direito de ter acesso a todos os dados que uma entidade, privada ou pública, tem sobre ela. Assim, o cidadão poderia verificar realmente quais dados sobre ele a empresa tinha em mãos e o que fez com tais dados após o uso dos mesmos.

A LGPD, de forma objetiva, reforça, por exemplo, o que o direito trabalhista já consolidou na Consolidação das Leis do Trabalho, no capítulo específico para proteção do trabalho da mulher, aonde consta expressamente a vedação da discriminação[4].

A discriminação, no processo seletivo, muitas vezes é assombrosa, causando evidente ofensa a direitos humanos do candidato, bem como a princípios constitucionais como a dignidade da pessoa humana (artigo 1º, III) e a direitos fundamentais como a inviolabilidade do direito à vida, à liberdade, à igualdade (artigo 5º, *caput*), a inviolabilidade à intimidade, à vida privada, à honra e à imagem das pessoas (artigo 5º, X); a direitos sociais como: o direito ao trabalho (artigo 6º); constituindo como objetivos fundamentais da República Federativa do Brasil promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV); além de direitos do trabalhador (artigo 7º) como licença à gestante (XVIII), licença-paternidade (XIX), proteção do mercado de trabalho da mulher (xx), proibição de diferença de salários, de exercício de funções e de critério de admissão por motivo de sexo, idade, cor ou estado civil (XXX), proibição de qualquer discriminação no tocante a salário e critérios de admissão do trabalhador portador de deficiência (XXXI), proibição de distinção entre trabalho manual, técnico e intelectual ou entre os profissionais respectivos (XXXII)[5].

Dito isso, ressalte-se a necessidade de cuidadosa revisão por parte dos recursos humanos quanto aos processos seletivos, para contratação laboral, mais especificamente em relação aos dados pessoais que são solicitados aos candidatos, especialmente aqueles considerados sensíveis.

Sugere-se um *checklist* com simples questionamentos: quais informações são necessárias para fins de cumprimento de obrigação legal ou execução do contrato de trabalho de acordo com cada especificidade dos mesmos? Quais requerem o consentimento do candidato? Certamente, tais medidas vão exigir a adoção de formulários claros que comprovem a manifestação livre, informada e inequívoca por meio do qual ele concorda com o tratamento de seus dados pessoais

para uma finalidade e adequação determinada, de forma a atender a lei.

Além disso, ressaltamos aqui uma prática bastante utilizada pelas empresas no que se refere ao armazenamento dos currículos em bancos de dados para futuros processos seletivos, que deve ser reavaliado quanto à necessidade de consentimento do candidato para tanto, visando assegurar a segurança das informações contra vazamento.

Nas sociedades modernas, as relações de trabalho são reguladas por meio de um contrato de trabalho, que estipulam os direitos e as obrigações de ambas as partes. Por exemplo, o contrato laboral prevê uma cláusula de proteção no emprego, segundo a qual o trabalhador (ou assalariado) tem direito a auferir uma indenização caso seja despedido sem causa justa, ou benefícios de plano de saúde, para o titular e seus familiares, onde muitos dados pessoais estão envolvidos.

Da mesma forma, em algumas situações haverá a necessidade de inclusão de cláusulas específicas nos contratos de trabalho. É o caso, por exemplo, de empresas que transmitem dados de seus empregados a terceiros, tais como operadoras de planos de saúde, seguro de vida e empresas de gestão de folha de pagamento, sendo recomendável, nesses casos, a revisão dos contratos com esses prestadores de serviços, a fim de incluir obrigações definidas na LGPD, sobre a forma de tratamento e proteção dos dados transferidos, bem como as responsabilidades em caso de eventual vazamento.

Dentre as obrigações dos agentes de tratamento está o registro de toda atividade de tratamento de dados pessoais; a notificação aos titulares de incidentes envolvendo seus dados; a possibilidade de que se exija um relatório de impacto à proteção de dados (DPIA) e a indicação de um encarregado pela supervisão da aplicação da lei, também conhecido como *data protection officer* (DPO) — encarregado de proteção de dados.

Vale ressaltar que há que se ter muita cautela no envio de informações de empregados aos sindicatos, sendo necessário verificar se já há obrigação prevista em lei ou norma coletiva para tanto, ou, ainda, concordância dos empregados, desde que haja uma finalidade e adequação específica.

Já a transmissão de dados a órgãos públicos, necessários para a execução de políticas públicas, tais como o encaminhamento da Declaração do Imposto sobre a Renda Retido na Fonte (DIRF); do Sistema Empresa de Recolhimento do FGTS e Informações à Previdência Social (Sefip); do Cadastro Geral de Empregados e Desempregados (Caged) e Relação Anual de Informações Sociais (Rais), não exige o consentimento dos empregados, tendo em vista se tratar de hipótese de cumprimento de obrigação legal.

As informações relacionadas à saúde dos trabalhadores também são dados sensíveis e, embora já protegidas em grande parte pelo sigilo médico, merecem especial atenção quanto ao armazenamento e divulgação de atestados e exames médicos, compra de medicamentos por meio de convênios e utilização do plano de saúde.

Além disso, é comum que, em casos de terceirização de atividades, empresas solicitem às prestadoras de serviços documentos comprobatórios de cumprimento das obrigações

trabalhistas, os quais, via de regra, possuem dados pessoais dos trabalhadores terceirizados. Esses dados também devem ser protegidos.

Merece muita atenção por parte das empresas a elaboração ou revisão de suas políticas internas, definindo de forma bastante clara os setores que poderão ter acesso a dados de candidatos, empregados e terceiros, bem como a forma de utilização de tais informações, inclusive estabelecendo penalidades em caso de uso indevido de dados, tais como o envio a e-mails particulares ou empregados e terceiros sem autorização de acesso aos dados. Há que se ter também políticas próprias relacionadas à forma de coleta, atualização e acesso dos dados pelos empregados.

A monitorização do trabalhador face à proteção de dados da LGPD
Os sistemas que permitem aos empregadores controlar quem pode entrar nas suas instalações e/ou certas áreas das mesmas também pode permitir o rastreamento das atividades dos funcionários. Embora esses sistemas já existam há vários anos, têm sido introduzidas novas tecnologias destinadas a controlar/monitorizar a atividade do trabalho, incluindo aquelas que processam dados biométricos.

Muitas empresas coletam os dados biométricos de seus empregados, prestadores de serviços e até mesmo parceiros para controle de acesso às suas dependências. Tais dados são considerados sensíveis pela LGPD e por essa razão, nas relações de trabalho, somente podem ser coletados mediante consentimento do titular para uma finalidade específica ou quando forem indispensáveis para cumprimento de obrigação legal — como é o caso do registro da jornada de trabalho por meio do REP (registro eletrônico do ponto).

No entanto, a monitorização contínua, da frequência e os tempos de entrada e saída exatos dos empregados não podem ser justificados se esses dados também forem usados para outra finalidade.

A importância e responsabilidade do RH frente a LGPD
Note-se que, para proteger a privacidade das pessoas, será preciso reorganizar a maneira como companhias lidam com dados e segurança da informação e que não se trata de opção, e sim o cumprimento de lei.

Mas para que isso aconteça, além das questões técnicas e de adequação de infraestrutura, que são de responsabilidade da área de TI, é essencial que o RH esteja envolvido no projeto. Isso porque a referida área é responsável por grande parte do processamento e do controle de dados pessoais das empresas.

Além da conscientização de todos sobre a importância da mudança, cabe ao RH identificar potenciais falhas em *compliance*, além de se certificar sobre quais são as informações dos funcionários que estão sob sua responsabilidade e de que forma estão armazenadas. Também é importante saber por quanto tempo guardar esses dados e como protegê-los durante a permanência do funcionário na companhia.

Nos processos de recrutamento e seleção, já citados acima, é importante que o líder de TI reestruture as políticas e os acordos de confidencialidade. É preciso contar, desde a primeira

conversa, com termos de consentimento de uso de dados, que devem ser assinados pelos candidatos, num processo transparente de como a empresa usará esses dados e quais serão mantidos em arquivo.

Outro ponto importante é que as informações só poderão ser conservadas se estiverem atualizadas. Assim, a área deve ter como procedimento a eliminação de currículos e documentação complementar (decorrente dos processos de recrutamento). Por isso, para que o processo ocorra de maneira efetiva, é essencial um trabalho conjunto entre RH e TI.

Conclusão
Não há dúvidas de que a LGPD trouxe uma série de obrigações para as empresas, que precisarão adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais e sensíveis obtidos em suas relações de trabalho. A pergunta que não quer calar é: como se adequar à Lei Geral de Proteção de Dados Pessoais?

A sugestão para começar é: conhecer onde, quando e como são coletados dados pessoais de clientes, fornecedores e colaboradores. Isso vai desde cadastro de CPF às informações usadas para a folha de pagamento; descobrir onde os dados são guardados e se há camadas de proteção, como senhas e criptografia; avalie se os colaboradores sabem evitar vazamentos e se têm noção da responsabilidade sobre as informações; enumerar a situação de risco da empresa; priorizar as ações corretivas; buscar consultoria jurídica especializada e um profissional de segurança da informação, para avaliação e diagnóstico preciso para colocar o plano de mudanças focadas na estruturação e adequação da empresa em conformidade com a nova legislação, utilizando para mapeamento de todas as situações internas atingidas pela nova lei, sobretudo na área de recursos humanos, que é o foco deste artigo, para as adequações necessárias a fim de evitar sanções administrativas ou ações de responsabilização civil por eventuais danos causados. Ressalta-se, por fim, que as empresas têm prazo de 18 meses até que a lei passe a vigorar, isto é em, fevereiro de 2020.

[1] Lei Geral de Proteção de Dados (LGPD), disponível em http://www.planalto.gov.br/CCIVil_03/_Ato2015-2018/2018/Lei/L13709.htm.
[2] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
[3] DPIA – Data Protection Impact Assessment, disponível em https://gdpr-info.eu/art-35-gdpr.
[4] Art. 373-A – Ressalvadas as disposições legais destinadas a corrigir as distorções que afetam o acesso da mulher ao mercado de trabalho e certas especificidades estabelecidas nos acordos trabalhistas, é vedado:
I – publicar ou fazer publicar anúncio de emprego no qual haja referência ao sexo, à idade, à cor ou situação familiar, salvo quando a natureza da atividade a ser exercida, pública e notoriamente, assim o exigir;
II – recusar emprego, promoção ou motivar a dispensa do trabalho em razão de sexo, idade, cor,

situação familiar ou estado de gravidez, salvo quando a natureza da atividade seja notória e publicamente incompatível;
IV – exigir atestado ou exame, de qualquer natureza, para comprovação de esterilidade ou gravidez, na admissão ou permanência no emprego;
portador de deficiência (XXXI), proibição de distinção entre trabalho manual, técnico e intelectual ou entre os profissionais respectivos (XXXII).
[5] Constituição Federal, disponível em
http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

Fonte: https://conjur.jumps.com.br/2018-set-21/valeria-reani-alei-protecao-dados-relacoes-trabalho/