A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS(LGPD) E A EXPOSIÇÃO DE DADOS SENSÍVEIS NAS RELAÇÕES DE TRABALHO

Flávia Alcassa dos Santos[1]

Resumo

A segurança é um elemento necessário, mas não suficiente, para garantir os direitos e liberdades das pessoas em relação à proteção de dados pessoais, principalmente no que diz respeito às informações sobre dados pessoais e dados sensíveis desde o primeiro contato dos empregadores com seus empregados, na fase pré-contratual no momento de recrutamento e seleção para uma vaga de trabalho, durante a fase contratual com o cumprimento do contrato de trabalho e no pós-contrato com o desligamento da empresa. O objetivo deste artigo não é esgotar a matéria, mas analisar a importância da governança de dados e boas práticas nas relações de emprego, observando os regramentos trazido pela LGPD que não podem conflitar com o ideal da Legislação Trabalhista que defende o equilíbrio da relação do empregado e empregador, tudo para se evitar passivos trabalhistas e fiscalizações de órgãos regulatórios.

Palavras-chave: Lei Geral de Proteção de Dados. Governança de dados. Dados Pessoais. Relação empregado e empregador.

1 Advogada, sócia-fundadora do escritório Alcassa & Pappert.- especializada em Direito Digital Corporativo e Relações de Trabalho, Membro do comitê jurídico da ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados, Membro da ANADD - Associação Nacional de Advogados do Direito Digital, certificada pela EXIN Privacy and Data Protection, Proteção de dados, Segurança Digital e Contratos pela FGV, Colunista, Palestrante e Instrutora de cursos, Membro convidada do Privacy for Peaple.

Introdução

A proteção de dados é um direito humano que nasce vinculado à Declaração Universal dos Direitos Humanos (DUDH), aprovada pela Assembleia Geral das Nações Unidas em 1948, com o objetivo de garantir a dignidade do ser humano e como instrumento de combate à opressão, impunidade e insultos à dignidade humana.

O objetivo deste direito é preservar a dignidade humana contra a invasão de privacidade que envolve a coleta e o tratamento excessivo de dados pessoais. Seu objetivo é estabelecer uma estrutura de garantias que permita exercer os direitos e liberdades fundamentais dos seres humanos e impedir que o uso de informações pessoais seja usado indiscriminadamente contra os direitos e liberdades inerentes ao ser humano.

No Brasil no panorama mundial de

privacidade, encontramos a proteção da privacidade, da intimidade e da vida privada expressa na Constituição Federal CF/88 em seu art. 5º, e outras leis como o "Marco Civil da Internet" e na Lei 12.965/2014 com normas de proteção e segurança a privacidade de dados das pessoas. Com o avanço da tecnologia e necessidade de uma lei especifica mais criteriosa, em 14 de agosto de 2014, após inúmeros debates e emendas, foi publicada a Lei nº 13.709 e alterações da Lei nº 13.853, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) em que buscou-se um equilíbrio na manutenção do desenvolvimento econômico e tecnológico, com a adoção da inviolabilidade dos direitos constitucionais dos cidadãos, representando um importantíssimo marco regulatório para o Brasil sobre o tema.

É objetivo geral deste artigo, analisar a importância da governança de dados e boas práticas nas relações de trabalho e refletir sobre os dados sensíveis nas relações de trabalho.

A IMPORTÂNCIA DA GOVERNANÇA DE DADOS E BOAS PRÁTICAS NAS RELAÇÕES DE TRABALHO.

Considerando que a relação de trabalho constitui uma fonte inesgotável de dados pessoais tratados, é dever do empregador fazer uso correto deles. Isso é aplicável em dados de empregados, prestadores de serviços, fornecedores, clientes, entre outros. O uso adequado dos dados deve ser uma prioridade para qualquer empreendedor, empresa ou instituição. ALei Geral de Proteção de Dados não é aplicável somente na relações de trabalho e sim em todas as relações envolvendo o tratamento de dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O avanço da tecnologia e a privacidade no compartilhamento de dados um tema de grande importância, nesse cenário que a Lei Geral de Proteção de Dados Pessoais (LGPD) é mais uma legislação que tutelará a privacidade.

No direito à proteção de dados pessoais, afirma-se que:

> Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana (SARLET; MARINONI; MITIDIERO; 2018, p.497).

Nas relações de trabalho de acordo com a Lei Geral de Proteção de Dados (LGPD) o empregado figura como o **titular dos dados** e o empregador como o **controlador dos dados**.

> Art. 5º Para os fins desta Lei, considera-se: V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018)

O consentimento do titular(empregado) pode ser excepcionalmente dispensado na hipótese da relação de empresa, desde que para obrigação de cumprimento legal, conforme ordena a própria LGPD no seu art. 7º, V e IX, para atender aos legítimos interesses do empregador para execução do contrato de trabalho em benefício do próprio empregado (ALCASSA; CASTELANI, 2020).

> Art. 7 -V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

Embora o consentimento seja dispensado nas hipóteses de "execução de contrato ou de procedimentos relacionados a contrato do qual seja parte o titular dos dados do empregado" o seu tratamento merece ainda mais cautela, para não ferir a privacidade do trabalhador, ocasionando danos à imagem, danos de natureza moral, além de prejuízos de ordem material ao empregador. As violações previstas poderão ser objeto de reclamação trabalhista e denúncias ao MPT(Ministério Público do Trabalho), bem como sujeitas à fiscalização da ANPD(Autoridade Nacional de Proteção de Dados) com sanções disciplinares previstas no art. 52 da Lei.

Treinamento e conscientização do uso devido dos dados pessoais, aliados ao departamento de Recursos Humanos (RH), tem papel primordial na adequação à LGPD e *compliance*.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IX - não **discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;**(BRASIL, 2015) (grifo nosso).

No campo infraconstitucional do Direito do Trabalho brasileiro, o art. 1º, da Lei nº 9.029/95, proíbe a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de emprego, ou sua manutenção, **por motivo de sexo, origem, raça, cor, estado civil, situação familiar ou idade**, ressalvadas, neste caso, as hipóteses de proteção ao menor, previstas no inciso XXXIII, do art. 7º, da Constituição Federal de 1988. (BRASIL, 1995)

A Constituição Federal brasileira prevê, em seu artigo 5º, X, a inviolabilidade da intimidade e da vida privada, vejamos:

"As violações previstas poderão ser objeto de reclamação trabalhista e denúncias ao MPT(Ministério Público do Trabalho), bem como sujeitas à fiscalização da ANPD(Autoridade Nacional de Proteção de Dados) com sanções disciplinares previstas no art. 52 da Lei."

DADOS SENSÍVEIS NAS RELAÇÕES DE TRABALHO

A relação de trabalho constitui uma fonte inesgotável de dados pessoais e no tocante a proteção de dados pessoais nas relações empregatícias um dos pontos que merecem maior atenção é o atinente à categoria dos dados pessoais sensíveis.

O Art. 5º da LGPD considera que:

> II - Dado pessoal 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 (BRASIL, 2015) (grifo nosso).

O art. 6º dispõe que:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - **são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

O art. 2º da LGPD também dispõe como fundamento a i**nviolabilidade da intimidade, honra e da imagem.**

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

> IV - a inviolabilidade da intimidade, da honra e da imagem; (BRASIL, 2018).

As informações relacionadas à saúde dos empregados são dados sensíveis e, embora já protegidas pelo sigilo médico (o código de ética médica, no art. 73),merecem muita atenção quanto ao armazenamento e divulgação de informações como: divulgação de doenças, atestados, exames médicos, divulgação de informações de compra de medicamentos, convênios e utilização do plano de saúde, por exemplo, além do armazenamento seguro das informações sensíveis por parte do empregador(controlador). Aplica-se a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, no caso em análise(empregado), ressalvado o disposto em legislação específica (ALCASSA, 2020).

Segundo Cartaxo (2010), o Repertório de Recomendações Práticas de Proteção de Dados Pessoais do Trabalhador da Organização Internacional do Trabalho - OIT (1997) sugere que a coleta de dados médicos deve se restringir às informações que são necessárias para determinar se o trabalhador está apto para determinado posto de trabalho; se pode cumprir com os requisitos de segurança e saúde do trabalho; e, mais, se pode ter direito a prestações sociais.

O legislador previu de maneira mais restritiva a coleta e o tratamento destes dados, para legitimar a obtenção e o uso da informação na categoria de dados sensíveis, especificados no art. 11, a seguir:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> **a) cumprimento de obrigação legal ou regulatória pelo controlador;**
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018) (grifo nosso).

Importante destacar que as multas por descumprimento da LGPD podem chegar a 50 milhões de reais , ademais esse não é o único impacto para as empresas, algumas discussões na Justiça do Trabalho envolvem primordialmente as questões de privacidade:

i) pedido de obrigações de fazer ou não fazer por práticas **discriminatórias na obtenção ou no uso da informação relativa ao empregado**; ii) dano moral individual ou coletivo por **práticas discriminatórias quanto as que são de algum modo ilícitas**; iii) justa causa ou de despedida indireta, para cuja aplicação são examinados a obtenção e o **uso da informação pessoal ou a prática de determinada conduta pelo empregado ou pelo empregador**. Nota-se que o foco das demandas trabalhistas está dirigido ao exercício dos poderes do empregador e aos direitos da personalidade do empregado, que indica o uso indevido, práticas discriminatórias e abusivas dos dados sensíveis do empregado.

Neste sentido para que o funcionário se sinta protegido e a empresa isenta de reclamações é preciso à manutenção da confiabilidade dos dados coletados.

> Medical personal data should not be collected except in conformity with national legislation, medical confidentiality and the general principles of occupational health and safety, and only as needed: (a) to determine whether the worker is fit for a particular employment; (b) to fulfil the requirements of occupational health and safety; and (c) to determine entitlement to, and to grant, social benefits (INTERNATIONAL LABOUR ORAGNIZATION, 1997, p.3).

Outro ponto que merece atenção é no momento de seleção de candidatos e o processo adequado de recrutamento e seleção, o que pode ou não ser coletado e o que extrapola a finalidade da contratação.

Não devem ser coletados dados que extrapolam a finalidade do contrato específico, como registro criminal (a menos que o cargo seja justificado), testes psicotécnicos, análises médicas, gravação de entrevistas de seleção (que sempre devem ser expressamente consentidas), histórico comercial (exceto no caso de trabalhadores com poderes para representar o empregador, como gerentes, gerentes adjuntos, agentes ou advogados, desde que, em todos esses casos, sejam dotados, pelo menos, de poderes gerais de administração e de trabalhadores encarregados da cobrança, administração ou custódia de fundos ou valores mobiliários de qualquer natureza, ou antecedentes focados na prevenção criminal, caso não sejam adequados, necessários e proporcionais (como é o caso de consultas nas listas públicas da ONU) (CARTAXO, 2010).

Como exemplo de prática ilícita de exposição de dados pessoais sensíveis de empregados, temos a decisão de Julho de 2020 dos julgadores da Segunda Turma do TRT3-MG, que, sem divergência, mantiveram sentença proferida pela 24ª Vara do Trabalho de Belo Horizonte. A juíza convocada MM. Maria Cristina Diniz Caixeta entendeu que, pelas provas colhidas, ficaram claros os danos morais em virtude da exposição indevida da intimidade do trabalhador.

A Justiça do Trabalho determinou que a empresa pague indenização por danos morais a um ex-empregado do setor administrativo que teve seus dados sigilosos expostos no sistema interno de informação da empresa. Um trabalhador da companhia confirmou, no processo que, ao fazer pesquisa no sistema, **deparou-se com o relatório médico do autor da ação, com a indicação de que ele tinha pensamentos suicidas e era usuário de cocaína.**

Para a juíza convocada Maria Cristina Diniz Caixeta, a conduta da empresa revelou o dano sofrido, já que a exposição de dados de cunho pessoal certamente causou dano moral ao autor. E, diante das provas, a magistrada reforçou que não via elementos capazes de afastar o direito do reclamante à reparação por dano moral. A julgadora manteve o valor fixado para a indenização, de três salários do trabalhador, por entender que o montante atende à finalidade de atenuar as consequências da lesão jurídica e reveste-se de razoabilidade. (TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, 2020).

Neste sentido, no caso de tratamento de dados pessoais sensíveis, com risco elevado no tratamento incluindo dados

médicos de saúde e biometria, a empresa deverá possuir um Relatório de Impacto à Proteção de Dados Pessoais (**Art. 38, parágrafo único, da LGPD**), observando as medidas e salvaguardas para mitigar os riscos no tratamento de dados pessoais.

De modo geral, tanto os dados ordinários como os sensíveis, a empresa deve adotar algumas medidas para assegurar a conformidade com a Lei:

- Revisar ou elaborar Política de Segurança considerando os três pilares: confidencialidade, integridade e disponibilidade e em conformidade com a ISO 27001, 27002 e a extensão ISO 27701;

- Adotar políticas de privacidade de uso de dados dos empregados e terceiros;

- Elaborar termos de autorização de envio de dados a terceiros para finalidade específica;

- Adotar um Código de Ética e Conduta para gerenciar dados dos candidatos às vagas da empresa e dos Contratos de empregados ativos (Delimitar claramente os papéis que cada parte exercerá no tratamento dos dados pessoais, o que impacta diretamente na definição de suas responsabilidades, de acordo com a lei);

- Revisar e incluir cláusulas atinentes à Privacidade nos contratos com empregados de conformidade com a LGPD;

- Elaborar aditivos dos contratos em vigor para adequação às exigências da LGPD;

- Revisar e incluir cláusula nos contratos de prestadores de serviços;

- Revisar fichas e formulários de entrevistas de acordo com o Princípio da minimização de dados (adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados);

- Nomear um Encarregado de dados, conhecido como Data Protection Officer (DPO) perante a GDPR na EU, peça chave para adequação e conformidade com atribuições nos termos da Lei. Art.41,§ 2º.

CONCLUSÃO

Concluiu-se que são necessárias as adoções de segurança e de boas práticas para a governança de dados dos funcionários com o intuito de não os deixarem em uma posição de vulnerabilidade para evitar passivos trabalhistas perante a justiça do trabalho e fiscalizações dos órgãos reguladores.

Todos os esforços devem representar uma verdadeira mudança de paradigma, adaptando a "Cultura" da empresa à nova realidade ditada pela sociedade dos dados, geração 4.0, havendo real mudança de hábitos e costumes de todos os envolvidos no processo, sendo imperiosa a adoção de uma governança de dados dos empregados, evitando prejuízos de ordem moral e material a empresa.

Referências

ALCASSA, Flávia. O papel da Lei Geral de Proteção de Dados Pessoais. (LGPD) nas relações de trabalho. **Revista Síntese**: Trabalhista e Previdenciária. Revista Síntese: trabalhista e previdenciária, v. 31, n. 375, p. 58-65, set. 2020.

ALCASSA, Flávia; CASTELANI, Liliana. Lei Geral de Proteção de Dados Pessoais e o Impacto nas Relações de Emprego. Associação Nacional dos Profissionais de Privacidade de Dados. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 nov. 2020.

BRASIL. Lei n.9.029, de 13 de abril de 1995. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas

discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. **Diário Oficial da União**, 13 abr. 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9029.htm#:~:text=Art.,no%20inciso%20XXXIII%20do%20art. Acesso em: 20 nov. 2020.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 nov. 2020.

SARLET, Ingo Wolfgang. MARINONI, Luiz Guilherme. MITIDIERO, Daniel. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2018.

INTENATIONAL LABOUR ORGANIZATION. **Protection of workers' personal data**. An ILO code of practice. Geneva, ILO, 1997. Disponível em: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang--en/index.htm. Acesso em: 20 nov. 2020.

TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO. **Copasa deverá indenizar trabalhador por exposição de dados na rede interna de informações da empresa**. Belo Horizonte: TRT3, 01 jul. 2020. Disponível em :https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/nj-copasa-devera-indenizar-trabalhador-por-exposicao-de-dados-pessoais-na-rede-interna. Acesso em: 20 nov. 2020.