

LGPD

NAS RELAÇÕES
DE TRABALHO



Lei Geral de Proteção
de Dados Pessoais



DISTRITO FEDERAL
COMISSÃO DE PRIVACIDADE E
PROTEÇÃO DE DADOS PESSOAIS

COMISSÃO DE PRIVACIDADE
E PROTEÇÃO DE DADOS PESSOAIS

LGPD nas relações de trabalho

Autores

Adriana Giuntini
Ana Sylvia da Fonseca Pinto Coelho
Camila Mickievicz
Cinthia Tufaile
Dayane Mendonça
Julie Maria Figueira Vittone
Kelly Santoro
Ilderlândio Teixeira
Marcela Calazans
Natália Saucedo Perez Costa

Revisão final: Jefferson Azevedo

Projeto editorial: Editora Motres

CIP BRASIL - CATALOGAÇÃO NA PUBLICAÇÃO

L534	LGPD nas relações de trabalho [livro eletrônico] /
1.ed.	Adriana Giuntini...[et al.]. – 1.ed. – Salvador, BA : Motres, 2021. PDF. Vários autores. Bibliografia. ISBN : 978-65-89765-07-3 1. Direito à privacidade - Brasil. 2. Direitos fundamentais. 3. Proteção de dados - Legislação - Brasil. I. Título.
08-2021/48	CDD 342.721

Índice para catálogo sistemático:

1. Lei Geral de Proteção de Dados : Direito à privacidade 342.721

Bibliotecária - Aline Grazielle Benitez CRB-1/3129.



Comissão de Privacidade e
Proteção de Dados Pessoais

Conteúdo

Apresentação	4
Prefácio	5
1. Impacto da LGPD nas Relações de Trabalho Adriana Giuntini	7
2. Sujeitos da LGPD na relação de emprego Julie Maria Figueira Vittone	9
3. Dados pessoais e Dados sensíveis Kelly Christina Rangel Santoro Camila Mickievicz Faria	12
4. Principais documentos trabalhistas e prazos de guarda Natália Saucedo Perez Costa	15
5. Responsabilidade do empregador e do empregado à luz da LGPD Marcela Calazans Medeiros Silva	20
6. Autodeterminação informacional Ilderlândio Teixeira	24
7. Ponto Eletrônico Biométrico e a LGPD Cinthia Tufaille	27
8. Treinamento e boas práticas Dayane Mendonça Ana Sylvia da Fonseca Pinto Coelho	31
Saiba mais	35
Autores	36

| Apresentação

A Lei Geral de Proteção de Dados (LGPD) é um novo marco legislativo que produz relevantes impactos nas instituições públicas e privadas. Por se aplicar indistintamente às operações de tratamento de dados pessoais, inevitavelmente também afeta as relações de trabalho e emprego, suscitando questões fundamentais sobre as medidas a serem adotadas pelos empregadores com o objetivo de proteger os direitos de seus empregados.

Idealizado pela Grupo de Trabalho da Comissão de Privacidade e Proteção de Dados Pessoais da OAB-DF, o presente guia foi elaborado com o objetivo de contribuir com o desenvolvimento de uma cultura de privacidade e proteção de dados em nosso país.

Escrito em uma linguagem simples e acessível, ele traz uma coletânea de artigos que contemplam temas voltados à melhor compreensão da aplicação da LGPD no contexto das relações de trabalho não apenas pelos operadores do direito, mas por todos aqueles que se interessam pelo tema.

Além de coautoras, sentimo-nos honradas com a missão de coordenar essa obra coletiva e agradecemos a cada um dos participantes deste tão relevante projeto por todo seu empenho e dedicação.

À Kelly Santoro, nosso especial agradecimento por colaborar com a organização e execução do guia.

Boa leitura!
Adriana Giuntini
Ana Sylvia Coelho

| Prefácio

Desde a sua entrada em vigor, a Lei Geral de Proteção de Dados (Lei nº 13.709/18) vem ocupando, cada vez mais, espaços de grandes debates e discussões técnicas nos mais diversos ambientes profissionais de das organizações, sejam eles ligados à área do Direito, da Tecnologia, da Segurança da Informação ou da própria Administração. Não importa, já que todas elas estão não só relacionadas ao novo diploma legal, mas também constituem atores sem os quais não se enxerga a possibilidade de uma efetiva implementação, educação, avaliação e contínuo monitoramento de todos os quesitos e determinações que passaram a ser exigidos desde o dia 18 de setembro de 2020.

Como não poderia deixar de ser, a área de Recursos Humanos é uma das mais (se não a mais) impactada pela LGPD. Não importa se a empresa tem 6 ou 6 mil funcionários: o tratamento de dados pessoais e de dados sensíveis é sempre muito maior do que nas outras áreas e, justamente por isso, pensou-se em abordar alguns aspectos-chaves nesse contexto.

Os autores da presente obra trabalharam em pesquisas e acompanharam os mais recentes entendimentos no cenário LGPD e Direito do Trabalho. Além de membros permanentes da Comissão de Privacidade e Proteção de Dados Pessoais da Ordem dos Advogados do Brasil, seção Distrito Federal, cada um deles possui formação específica e atuação direta na área trabalhista, o que possibilitou uma abordagem vista de “dentro para fora”, ou seja, de como se apresenta a realidade das empresas no aspecto trabalhista quando se fala de Lei Geral de Proteção de Dados.

Tais realidades, assim, se transformaram em inspirações, pois os temas ora trazidos variam entre o próprio conceito de privacidade nas relações de trabalho até, por exemplo, uma tabela de prazos de retenção de documentos que, ousado dizer, é a mais apropriada no momento, e que pode ser usada por qualquer empresa, de qualquer tamanho. Esta coletânea é, de fato, não apenas uma leitura obrigatória para todos os *stakeholders* de uma organização, mas também constitui um verdadeiro guia que vai ajudar a

compreender o processo de implementação dos programas de privacidade e proteção de dados na empresa.

Sendo assim, eu estimo e recomendo veementemente a leitura e a consulta permanente desta obra, ao mesmo tempo em que me orgulho de ter contribuído para a finalização deste projeto, realizado por pessoas tão incríveis e comprometidas com o ensino e a advocacia na nossa sociedade.

Adriana Antunes Winkler, CIPP/E, CDPSE, CDPO, L.L.M.

Presidente da Comissão de Privacidade e Proteção de Dados Pessoais
Ordem dos Advogados do Brasil – Distrito Federal

1. Impacto da LGPD nas Relações de Trabalho

Adriana Giuntini

A rápida evolução tecnológica e a globalização criaram desafios em matéria de proteção de dados pessoais. O recolhimento e a partilha dos dados registraram um aumento significativo. As novas tecnologias permitem às empresas privadas e públicas a utilização de dados dessa natureza em uma escala sem precedentes no desempenho de suas atividades. Os indivíduos cada vez mais disponibilizam as suas informações pessoais de forma pública e global. O desenvolvimento tecnológico vem transformando a economia e a vida social.

Nesse cenário, a relação entre trabalhadores e empregadores se transformou de maneira vertiginosa com a inserção de novas formas de comunicação e informação com as quais os marcos regulatórios não estavam preparados e não ofereciam alternativas.

Questões relacionadas à privacidade e aos dados pessoais nas relações de trabalho têm sido objeto de debates, e tem sido questionado em que medida um empregador, no cumprimento de suas prerrogativas e direitos no âmbito de uma relação de trabalho, pode estar envolvido no conhecimento e disposição das informações da pessoa – trabalhador.

Estas e outras questões estão sendo construídas nos últimos anos no mundo do direito do trabalho, na tentativa de encontrar novos caminhos para fazer face às novas tecnologias.

Para essas questões, o Brasil promulgou, em 2018, a Lei nº 13.709/2018, denominada **Lei Geral de Proteção de Dados – LGPD**, vigente desde setembro de 2020, que tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade dos cidadãos. Essa lei visa trazer segurança jurídica aos atores envolvidos na coleta, armazenamento e uso de dados (digitais ou físicos) e, ainda, estabelecer regras de proteção de dados e critérios no tratamento dos dados pessoais.

A LGPD não foi pensada para as peculiaridades das relações de trabalho, é uma lei de caráter genérico e amplo, mais voltada para questões consumeristas, como expresso em seu art. 2º atua para defender a privacidade, a autodeterminação informativa, a liberdade de expressão, de informação e de opinião.

Entretanto, sua aplicação deve ser efetuada a “qualquer operação de tratamento” (art. 3º), sem ressalva ao contrato de trabalho, sendo certo que o art. 4º, ao tratar das hipóteses em que ela própria não se aplica, não fez menção às relações de trabalho como excludente.

Portanto, a Lei Geral de Proteção de Dados deve ser observada em cada um dos momentos em que uma relação de trabalho se desenvolve, isto é, antes de começar, na celebração do contrato, durante o seu desenvolvimento e ao final da sua conclusão ou na dissolução.

Existem também outros tipos de situações que podem surgir no desenvolvimento e execução da relação de trabalho, em que podem existir dados e informações a que o empregador tem acesso e que devem ser tratadas com discrição e cuidado observando a Lei.

POR EXEMPLO, os dados necessários para acessar certos benefícios legais ou extralegais, com o seguro de despesas médicas e pensões em que o trabalhador deve fornecer dados pessoais e familiares. Nesta linha, temos o prontuário do trabalhador, com os exames médicos e atestados, entre outros.

Outro fator relevante a ser observado são as contratações de terceiros para prestação de serviços para questões específicas de suporte contábil, preparação da folha de pagamento, consultoria de tecnologia, exames médicos etc. Nestes casos, é normal que as informações relativas aos trabalhadores possam circular entre as empresas. Essas informações, em princípio, devem ser objeto de tratamento especial, e seria conveniente que as obrigações relativas à proteção de dados das pessoas envolvidas fosse objeto de cláusulas contratuais.

Como se pode verificar, o desenvolvimento da relação de trabalho é espaço propício e amplo, no qual o tema da gestão da informação pode ser sensível, quer as informações que as partes prestam no decorrer da própria prestação, quer as que são geradas em resultado da celebração de um contrato de trabalho.

2. Sujeitos da LGPD na relação de emprego

Julie Maria Figueira Vittone

A proteção de dados pessoais está inserida na sociedade como uma forma de tutela aos indivíduos perante os riscos que o tratamento de dados pode causar a sua personalidade, pois, caso alguns limites não sejam estabelecidos e respeitados, o titular dos dados poderá enfrentar incidentes capazes de provocar prejuízos em diversos aspectos de sua vida.

Os ditames da LGPD são aplicados a qualquer operação de tratamento de dados realizada por pessoa natural ou pessoa jurídica de direito público ou privado, levando em consideração que o tratamento de dados seja realizado em território nacional, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Quando tratamos de proteção de dados pessoais na relação de emprego, os principais destinatários serão os funcionários e os prestadores de serviços, seja qual for o setor em que estejam desenvolvendo suas atividades. Os meios de garantir a adequação de uma empresa, de forma que sejam preservados os direitos dos empregados como titulares de dados pessoais, podem ser a construção de políticas internas de tratamento de dados pessoais, adequação dos contratos e formulários de coleta de dados, entre outros.

A LGPD possui ainda três sujeitos no processo de tratamento de dados pessoais: Controlador, Operador e Encarregado.

- Primeiramente, o Controlador é a pessoa natural ou jurídica, de direito público ou privado, responsável pelo tratamento dos dados pessoais, pode-se dizer que as próprias empresas que recebem os dados dos titulares assumem esse papel, cabendo a essa função a preparação da estrutura adequada para fazer a recepção, tratamento, destinação e eliminação dos dados.

- Já o Operador é também a pessoa natural ou jurídica, de direito público ou privado, mas seu papel é realizar o tratamento de dados pessoais em nome do Controlador, esse sujeito pode ser um funcionário da empresa receptora dos dados, uma empresa terceirizada ou um prestador de serviço autônomo, dentre suas funções está a responsabilidade de realizar o tratamento dos dados conforme as instruções fornecidas pelo Controlador.
- Por fim, tem-se o Encarregado, este será a pessoa indicada pelo Controlador para atuar como sua ponte de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) de modo a permitir a fiscalização e respectivas adoção de medidas para regularização de desconformidades com a LGPD.

Correlacionando os sujeitos da LGPD com a relação de trabalho, podemos identificar que, inicialmente, os empregadores assumem o papel dos Controladores que coletam os dados pessoais dos seus funcionários. Dentro dessa relação devem ser respeitados os princípios e garantias de proteção à privacidade dos titulares dos dados, devendo haver uma implementação de métodos seguros em todo o processo de tratamento de dados, o que ocorre desde o recebimento de um currículo até o desligamento do empregado, podendo haver casos em que mesmo desligado, os dados de um funcionário poderão ser guardados para cumprimento de obrigações legais ou regulatórias, devendo a proteção das informações continuar obedecendo os critérios da LGPD.

No caso do Operador, poderá constituir em uma empresa terceirizada ou prestador de serviço autônomo contratado pelo Controlador. Nessa situação pode ocorrer a preocupação com o funcionário que realiza o tratamento de dados para a prestação do serviço, que mesmo não sendo um empregado direto da empresa, assume responsabilidades perante a implementação da lei quando recebe os dados para serem utilizados na prática, assim, deve ser observado pelo Controlador se suas instruções estão sendo obedecidas corretamente e se o Operador possui todos os mecanismos necessários para garantir a segurança e os ditames legais da proteção dos dados pessoais.

Quando falamos do Encarregado nos aspectos da relação empregatícia, pode-se concluir que se trata justamente de um funcionário do Controlador designado para tal função, em razão de exercer um canal de comunicação adequado para o correto fluxo de dados e resolução de exigências que podem ser requeridas pelos titulares dos dados ou pela própria ANPD.

Identificados os sujeitos da LGPD e suas respectivas funções na seara trabalhista, pode-se demonstrar a responsabilidade desses agentes caso os critérios da lei não sejam obedecidos. Isso ocorre quando o Controlador ou Operador, durante a atividade de tratamento de dados pessoais, causem danos aos dados pessoais fornecidos pelos titulares, como vazamentos de informações, perda, compartilhamento indevido, dentre outras situações. Esse tipo de inadequação culmina em uma responsabilização (conforme artigo 42 da LGPD). Nesse caso, o Operador pode responder solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do Controlador, hipótese em que o operador equipara-se ao Controlador, salvo nos casos de exclusão previstos na lei. Nos casos de responsabilidade, é sempre importante aos sujeitos do tratamento de dados aplicarem métodos de registro de tratamento capazes de comprovar todos os seus atos no processo de adequação à LGPD, para que, quando questionados, possam comprovar a lisura dos métodos adotados e a prevenção diante da proteção de dados pessoais.

Pode-se observar, portanto, como as obrigações das empresas e de seus funcionários estão definidamente ligadas ao papel dos sujeitos trazidos pela LGPD. Isso evidencia uma total mudança de paradigma no que diz respeito à forma de tratamento dos dados pessoais, sendo importante a adoção de toda uma nova estrutura operacional para atendimento às garantias e princípios devidos aos titulares das informações na prestação de serviços ou produtos.

3. Dados pessoais e Dados sensíveis

Kelly Christina Rangel Santoro
Camila Mickiewicz Faria

Ao falar de dados pessoais, estamos nos referindo a direitos que protegem as pessoas de intromissões alheias, como por exemplo, por meio do sigilo das correspondências e pela privacidade.

Portanto, a proteção dos dados pessoais é a proteção da personalidade, ou seja, de um conjunto de elementos fundamentais que formam a pessoa.

Enquanto dados pessoais sensíveis, além de ser pessoais, são dados que podem trazer algum tipo de discriminação quando do seu tratamento. Isto é, são dados pessoais que poderão implicar riscos e vulnerabilidades aos direitos e liberdades dos titulares.

Dados pessoais	Dados pessoais sensíveis
É a informação relacionada a uma pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, RG, CPF, códigos de identificação, endereços. (artigo 5º, I)	É o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, 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. (artigo 5º, II)

Vamos exemplificar esses dados pessoais!

- Nome
- RG
- Número de telefone
- Registros de acesso à aplicações de internet
- Contas de email
- *Cookies*

Dados pessoais sensíveis

- Dados biométricos: imagens faciais, impressão digital.
- Dados genéticos: relativos às características genéticas, hereditárias ou adquiridas de uma pessoa que tragam informações únicas sobre a sua fisiologia ou saúde.

Dados pessoais na rotina de trabalho

O tratamento de dados pessoais está presente durante toda a execução do contrato trabalhista, desde sua fase pré-contratual, até após a sua finalização. Portanto, a Lei Geral de Proteção de dados também é aplicável nas relações trabalhistas:

- a) **pré-contratação:** com a obtenção de dados de identificação, currículo, referências do candidato à vaga de emprego, dentre outros;
- b) **durante o contrato de trabalho:** dados para registro de empregados, dados bancários para pagamento de salários, filiação sindical, dados relativos à saúde, como exames ocupacionais, atestados médicos, dentre outros;
- c) **após o término do contrato de trabalho:** com o armazenamento das informações dos antigos empregados para fins trabalhistas, previdenciários e para disponibilização aos órgãos públicos de fiscalização¹.

Na hora da coleta desses dados é de suma importância que a empresa verifique a finalidade e a base legal correspondente, para que não haja um acúmulo de dados e uma desconformidade com a legislação.

As empresas que empregam funcionários menores de idade precisam de uma atenção extra em relação a esses dados. Uma vez que a LGPD dispõe, em seu artigo 14, que dados de crianças e adolescentes devem ser tratados em seu melhor interesse e por meio de consentimento específico e em destaque dados por pelo menos um dos pais ou responsável legal.

Quanto à coleta de dados pessoais sensíveis à observância da finalidade, ou seja, o motivo do recolhimento desses dados, é ainda mais importante, já que a lei nº 13.709 indica um tratamento mais rigoroso dessa categoria de informação devido a sua possibilidade de causar discriminação ao titular.

¹ **Fonte:** <https://www.meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-direito-trabalho>. **Acessado em** 23/02/2021

No entanto, existirão situações em que será imprescindível o tratamento desses dados, por exemplo, informações relacionadas a religião, uma vez que existem algumas que proíbem o labor em determinados dias da semana. Ou das informações sobre filiações sindicais.

A regra geral para que uma empresa trate qualquer dado pessoal deve ser da observância da finalidade, já que quanto maior a quantidade de dados coletados, maior será o dinheiro investido em seu tratamento e segurança.

4. Principais documentos trabalhistas e prazos de guarda

Natália Saucedo Perez Costa

As relações de trabalho pressupõem o acúmulo e guarda de documentos que formalizam a relação entre o trabalhador e seu empregador, que requerem novos cuidados por parte do contratante a partir da entrada em vigor da Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD).

O objetivo aqui não é esgotar o tratamento a ser dado aos documentos que deverão ser mantidos pelo empregador durante e após a conclusão do contrato de trabalho, mas dar orientações quanto ao devido tratamento dos dados pessoais contidos nestes documentos, bem como trazer uma breve orientação quanto à gestão dos mesmos documentos e seus respectivos prazos de guarda.

Importante destacar que é legítimo o direito de o empregador coletar dados de seus empregados e candidatos ao emprego, desde que esses dados tenham finalidades legítimas (diretamente relacionada à relação trabalhista) e estritamente necessários para as finalidades informadas – ainda que redundante, importante lembrar que esses dados estão contidos em algum tipo de documento.

No contexto da Lei Geral de Proteção de Dados (LGPD), os documentos trabalhistas devem ser analisados nas relações laborais sob a ótica do intenso fluxo de dados pessoais, que se estende desde a fase pré-contratual, até a pós-contratual, passando, inevitavelmente, por aqueles durante a fase de vigência do contrato de trabalho.

A fase pré-contratual, habitualmente conhecida como “processo de recrutamento e seleção”, necessariamente envolve a coleta e o tratamento de dados pessoais dos candidatos. A LGPD, em seu art. 7º, V, permite a utilização desses dados, quando necessário, para a execução do contrato

ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular.

Todavia, as empresas devem solicitar o consentimento expresso do candidato e informá-lo de maneira clara que seus dados serão utilizados para recrutamento, avaliação e seleção. Da mesma forma: se a empresa vier a utilizar esses dados para outra finalidade, isso deve ser claramente informado e ter expresso consentimento do titular do dado.

Importante destacar que se a empresa, durante o processo de recrutamento e seleção, contratar agências especializadas, essas devem ser claramente identificadas aos candidatos e explicar a eles como seus dados pessoais serão utilizados.

E, finalmente, mas não por fim, ressalta-se que na elaboração dos documentos trabalhistas é necessária a adequação das cláusulas contratuais que impliquem no tratamento de dados pessoais. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados no artigo 6º.

Necessário se faz ressaltar os cuidados que o empregador deve ter com a guarda de documentos envolvendo a segurança do seu armazenamento, incluindo backups de segurança, especialmente no caso de documentos eletrônicos.

No que toca aos prazos de guarda desses documentos, a tabela 1 abaixo exemplifica (sem ser exaustiva) os documentos trabalhistas, correlacionando com o prazo legal em que deve ser mantida sob a guarda do empregador:

Tabela 1: Guarda de Documentos – Prazos

Documento	Período	Fundamentação Legal
Acordos de Compensação de Horas	05 anos	CF - artigo 7º, inciso XXIX
Advertência e Suspensão	05 anos	CF - artigo 7º, inciso XXIX
Alvará	Permanente	-o-
Apólice de Seguro	01 ano	Lei 10.406/02 – artigos 206 e 1.194
Atas de Assembleias e Conselho de Administração	Permanente	-o-
Atestado Médico/Abono de Falta	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Balancetes	05 anos	Lei 5.172/66 – artigos 174 e 195
CAGED	03 anos	Portaria MTE 235/2003
Cartão de Ponto	05 anos	CF - artigo 7º, inciso XXIX
Comprovante de Ticket-Refeição	05 anos	CF - artigo 7º, inciso XXIX
Comprovante de Vale-Transporte	05 anos	CF - artigo 7º, inciso XXIX
Comunicado de Dispensa	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Comunicado de Dispensa	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Conciliação Bancária	05 anos	Lei 5.172/66 – artigos 174 e 195
Conhecimento de Frete	05 anos	Lei 5.172/66 – artigos 174 e 195
Contrato de Leasing	10 anos	Lei 10.406/02 – artigos 205 e 1.194
Contrato de Locação de Bem Imóvel	03 anos	Lei 10.406/02 – artigos 206 e 1.194
Contrato de Prestação de Serviço	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Contrato de Trabalho	Permanente	-o-
Contrato Social e alterações	Permanente	-o-
Cópia de Certidões do Empregado	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Cópia de Certidões do Empregado	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
DARF (demais tributos)	05 anos	Lei 5.172/66 – artigos 174 e 195
DARF (PIS/COFINS)	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
DARJ, inclusive ICMS	05 anos	Lei 5.172/66 – artigos 174 e 195
DARM-RIO	05 anos	Lei 5.172/66 – artigos 174 e 195
DECLAN-IPM	05 anos	Lei 5.172/66 – artigos 174 e 195
Declaração de Imposto de Renda Pessoa Jurídica (DIPJ)	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Declaração de Opção	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Demais Declarações SRF	05 anos	Lei 5.172/66 – artigos 174 e 195
Demais Livros Fiscais	05 anos	Lei 5.172/66 – artigos 174 e 195
Depósitos FGTS, inclusive através de GFIP	30 anos	Lei 8.036/90
Duplicatas	05 anos	Lei 5.172/66 – artigos 174 e 195

Escritura de Compra e Venda	Permanente	-o-
Escritura de Compra e Venda	Permanente	-o-
Estatuto	Permanente	-o-
Extrato Bancário	05 anos	Lei 5.172/66 – artigos 174 e 195
Folha de Pagamento	30 anos	Lei 8.036/90
GIA-ICMS	05 anos	Lei 5.172/66 – artigos 174 e 195
Guia de Recolhimento da Contribuição Sindical (GRCS)	05 anos	Lei 5.172/66 – artigos 174 e 195
Guia de Recolhimento da Previdência Social (GPS)	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Inscrição Estadual/Municipal	Permanente	-o-
Inscrição no CNPJ	Permanente	-o-
Livro de Acionista	Permanente	Lei 6.404/76 - artigo 177
Livro de Apuração do Lucro Real (LALUR)	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Livro de Inspeção no Trabalho	Permanente	-o-
Livro de Registro de Inventário	10 anos*	Lei 8.212/91 – artigos 45 e 46Decreto 3.048/99 – artigo 225, § 5º
Livro de Registro de Saídas	10 anos	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Livro Diário	Permanente	Lei 6.404/76 - artigo 177
Livro ou Ficha de Registro de Empregados	Permanente	-o-
Livro Razão	Permanente	Lei 6.404/76 - artigo 177
Nota Fiscal (Ativo Imobilizado)	Permanência do bem na empresa	-o-
Nota Fiscal de Saídas de Mercadorias	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Nota Fiscal de Serviços	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
PAT	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
PCMSO	20 anos	Norma Regulamentadora 7
Pedido de Dispensa/Aviso Prévio	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
PRA	20 anos	Norma Regulamentadora 9
RAIS	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Recibo de Pensão Alimentícia	05 anos	Lei 5.172/66 – artigos 174 e 195
Recibo de Pró-Labore	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Recibos de Salário, Férias e 13º	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
RPA	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Salário Educação	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Salário Família	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Salário Maternidade	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º
Termo de Rescisão de Contrato	10 anos*	Lei 8.212/91 – artigo 46Decreto 3.048/99 – artigo 225, § 5º

Fonte: http://www.boletimcontabil.com.br/conteudo/novo/tabelas_praticas/guarda_doc.php acessado em 08/04/2021 às 14:57.

Observação 1: A lista não é exaustiva, necessitando análise detalhada das particularidades documentais e aspectos culturais de cada empresa. Deve ser observada, também, a existência de autos de infração, e de ações judiciais ou trabalhistas, para os quais é recomendável o prazo de guarda dos documentos até a decisão administrativa ou judicial correspondente. Para os documentos exigidos por mais de um órgão fiscalizador, deve-se observar o maior prazo existente na legislação.

Observação 2: Mediante o julgamento do Recurso Especial nº 616.348-MG, a Corte Especial do Superior Tribunal de Justiça (STJ) declarou, por unanimidade, no dia 21/08/2007, a inconstitucionalidade do artigo 45 da Lei 8.212/91, que autorizava o INSS a apurar e constituir créditos pelo prazo de 10 anos. Esta decisão pode ser considerada como uma das maiores disputas tributárias envolvendo o Instituto Nacional do Seguro Social (INSS). Embora o texto estabeleça o prazo de dez anos para a decadência de tributos, o STJ concluiu que a regra só poderia ser criada por lei complementar e não ordinária, conforme previsto na alínea “b”, inciso III, artigo 146 da Constituição Federal. Sendo assim, deve-se considerar o prazo do Código Tributário Nacional (CTN), que é de 5 anos, conforme é previsto nos artigos 174 e 195. Assim, o destino final dos documentos coletados e usados durante a vigência da relação trabalhista pode ser sua eliminação (dependendo de autorização ou da legislação vigente - citadas na tabela 1 acima, de forma exemplificativa) ou a guarda (provisória ou permanente) por razões administrativas, legais e/ou fiscais (constituição de créditos ou eventuais ações judiciais, por exemplo).

5. Responsabilidade do empregador e do empregado à luz da LGPD

Marcela Calazans Medeiros Silva

Na relação de trabalho, o empregador, enquanto controlador dos dados pessoais de seus colaboradores, é o responsável por tomar todas as decisões sobre a forma como os dados serão coletados, usados, armazenados e descartados. O empregador pode ainda, dependendo das atividades que a empresa desempenha, ser considerado operador de dados de seus clientes e parceiros comerciais.

Com isso, surge para a empresa a necessidade de regulamentar e repassar aos seus colaboradores a forma como o tratamento de dados deve ser realizado. Isso porque, ao processar dados pessoais, os colaboradores o fazem em nome da própria empresa.

A relação abaixo não tem a pretensão de esgotar o tema, servindo apenas como parâmetro inicial do que se espera que o Empregador execute para garantir a integridade, a disponibilidade e confidencialidade das informações.

Das responsabilidades do empregador:

- fornecer informações claras e de forma contínua aos seus colaboradores sobre como tratar os dados pessoais que transitarem na empresa;
- indicar medidas técnicas e administrativas para prevenir o vazamento de informações;
- oferecer treinamentos e atualizações sobre o tema, para permitir a criação da cultura de proteção de dados dentro da empresa;
- incentivar as práticas de mesa e tela limpa e a adoção de medidas mitigatórias de exposição indevida de informações;
- garantir que os colaboradores possam contribuir com a construção de boas práticas de proteção de dados, na medida em que conhecem a ro-

tina do trabalho a ser desempenhado, e a realidade deve transparecer na documentação de governança de dados;

- orientar e direcionar cada colaborador na conduta a ser adotada, de acordo com as suas atribuições, sobre os cuidados necessários para evitar prejuízos aos titulares de dados, para atender às solicitações que envolvam dados pessoais e realizar o descarte seguro de informações.
- utilizar os dados pessoais de seus colaboradores apenas se amparados por uma base legal que os justifiquem e garantir que os dados estejam adequados à finalidade a que se destinam;
- ser transparente com o colaborador, indicando quais e quando os dados estão sendo coletados, se há monitoramento de equipamentos, prazo de retenção dos dados e outras informações relevantes;
- realizar avaliação prévia de impacto à privacidade para os casos em que houver riscos razoáveis aos interesses do titular;
- avaliar e sopesar os casos em que o tratamento de dados, pautado no legítimo interesse da empresa, for passível de extrapolar as expectativas razoáveis de privacidade do empregado;
- manter rigoroso controle de acesso aos dados pessoais dos colaboradores, especialmente dos dados sensíveis a que tiver ciência, tais como: atestados médicos, dados de filiação sindical e outros previstos na legislação;
- cuidar para que a transferência dos dados dos colaboradores seja realizada de forma segura, ainda que para o cumprimento de obrigações legais ou regulatórias;
- fazer avaliação prévia do nível de maturidade dos fornecedores que terão acesso aos dados pessoais dos seus colaboradores e firmar contratos que prevejam garantias mínimas para preservar a segurança dos dados;
- não usar os dados pessoais de seus colaboradores para fins discriminatórios ou que possam causar qualquer tipo de prejuízo ao titular.

Por sua vez, aos empregados também competem responsabilidades para assegurar que os dados pessoais a que tiverem acesso para o exercício de suas atividades, sejam utilizados conforme o previsto na legislação e indicações realizadas pelo empregador. Assim, tem-se que cabe ao empregado:

- contribuir para a disseminação da cultura de proteção de dados na organização;

- prestar os seus serviços com zelo, diligência e colaboração, atendendo-se para empregar as melhores práticas na condução de sua rotina laboral;
- ser fiel às regras e recomendações fornecidas por seu empregador na execução de suas atividades;
- zelar pela qualidade da informação, pelo fluxo do tratamento de dados e pela privacidade dos titulares de cujos dados tiver ciência para o exercício de suas atribuições;
- reportar ao seu superior hierárquico qualquer violação ou vazamento de informações de que tiver ciência, para que este possa avaliar a gravidade e verificar as medidas a serem adotadas no caso concreto;
- indicar ajustes ou melhorias que reputar necessárias à garantia da qualidade dos dados pessoais, para que o empregador possa avaliar a implementação da sugestão na prática.

5.1. Top Down dos Gestores

Considerando que a proteção de dados é um tema com o qual muitas pessoas ainda estão começando a ter contato, é de suma importância que as empresas se comprometam a fomentar e incentivar a criação da cultura à privacidade e proteção de dados.

No modelo de gestão *top down*, as decisões são tomadas por um núcleo central, geralmente composto pelos cargos de maior hierarquia dentro da organização, que tem o dever de definir as diretrizes e estratégias que serão adotadas como um todo no ambiente corporativo em adequação às determinações da Lei Geral de Proteção de Dados.

Dessa forma, é essencial que os gestores e líderes provoquem suas equipes a refletir sobre o tema e a incorporar às atividades do setor as melhores práticas para garantir que todo o fluxo de ações seja amparado pelos conceitos de *privacy by design* e *privacy by default*.

O referencial e direcionamento deve sempre vir de cima para baixo, em um verdadeiro efeito cascata, em que os níveis superiores provoquem alterações nos níveis inferiores e assim por diante, até que todos estejam aculturados e firmes no propósito de proteger as informações que lhe foram confiadas para o exercício de suas atividades.

A abordagem *top down* não impede que os colaboradores possam contribuir com suas expertises e apresentar subsídios para que os gestores, conhecendo melhor a realidade do labor, considerem as necessidades da equipe e criem instruções com base no que efetivamente acontece na prática. Esse cenário, aliás, é o mais recomendado, considerando que as Políticas da empresa devem representar a realidade cotidiana, e não mera expectativa de tratamento de dados.

Por fim, ressalta-se a importância da gestão *top down* como forma de esclarecer eventuais medidas que a empresa poderá adotar no caso de descumprimento das normas definidas pela organização e necessidade de penalização dos responsáveis.

6. Autodeterminação informacional

Ildefrândio Teixeira

“A autodeterminação do indivíduo é o que parametriza a licitude ou ilicitude de qualquer atividade de tratamento de dados pessoais”.

Bruno Bioni

A autodeterminação informacional aparece na Lei Geral de Proteção de Dados como **autodeterminação informativa**. Trata-se, em verdade, da mesma coisa, ela é uma das bases jurídicas da proteção e privacidade de dados pessoais.

O fluxo informacional interno e externo deve ser de conhecimento de todos os agentes envolvidos no ciclo, que se inicia na coleta, passa pela transmissão e armazenamento e finaliza no descarte.

O fluxo informacional deve ter como pano de fundo **a autodeterminação informacional** com as garantias principiológicas, e bases legais de tratamento como forma de licitude para os controladores e operadores, agentes de tratamento.

Segundo Laura Schertel, muitos outros direitos fundamentais tendem a ser afetados ou influenciados pelo fenômeno da informação caracterizada exatamente pelo **fluxo intenso de informações**.

O contexto informacional nas relações trabalhistas são diversos, a saber: produtividade, saúde, familiar, escolaridade, visual e experiência. Tais contextos envolvem vários atores no processo de tratamento.

É dever do empregador, sindicatos e confederações sindicais **limitar o fluxo de informação** dos colaboradores e afiliados, respectivamente, limitando-se à sua finalidade, necessidade e adequação em todo o ciclo de vida dos dados pessoais.

A autodeterminação informacional é denominada por alguns autores como liberdade da informação, a qual Danilo Doneda estabelece ser a *proteção de dados pessoais* baseada nos princípios da publicidade (ou

da transparência), da exatidão, da finalidade, do livre acesso, da segurança física e lógica, todos assegurados por normas positivadas.

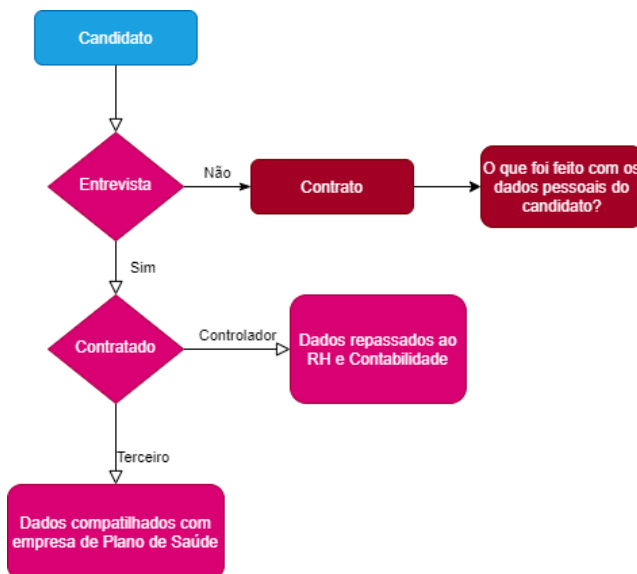
No *compartilhamento de dados com terceiros*, seja para cumprimento de obrigação legal ou regulatória, execução de contratos ou mediante o fornecimento de consentimentos não adjetivados e adjetivados, é dever assegurar a autodeterminação informacional.

Segundo Bruno Bioni, a autodeterminação informacional é sinônimo de **CONTROLE** do cidadão sobre seus dados pessoais. A própria noção do que seja um tratamento de dados pessoais justo e lícito é *vinculada ao consentimento do indivíduo*.

Logo, antes mesmo da Lei Geral de Proteção de Dados ser editada, o ordenamento jurídico pátrio e trabalhista já os assegurava esse controle, o que a LGPD tenta proporcionar é um maior alcance, tais como: *quais dados estão sendo tratados; se tem dados a serem tratados; poder ter acesso aos dados; exigir que se corrija sua anonimização, seu bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade e a portabilidade*.

Praticando, a figura 2 abaixo traz um fluxo informacional de **processo seletivo** de uma determinada organização.

Figura 2 - Esquema elaborado pelo autor



O candidato é o titular dos dados pessoais, detentor do controle da informação, destarte, a autodeterminação da informação lhe é assegurada. Infere-se que ele deve saber o que vai ser feito com os seus dados quando não contratado, assim como quais dados serão levados ao RH e à Contabilidade (interna ou externa) e o porquê do seu compartilhamento com o plano de saúde sem o seu consentimento adjetivado.

Prontamente, as boas práticas e governança aplicadas ao processo de conformidade na organização objetivada nos princípios e bases legais no ciclo de tratamentos dos dados pessoais devem ter como fundamento a autodeterminação informacional.

7. Ponto Eletrônico Biométrico e a LGPD

Cynthia Tufaille

Um dos temas que vem gerando bastante polêmica quanto à aplicação da Lei Geral de Proteção de Dados no contexto trabalhista é o uso do ponto eletrônico biométrico. Isso porque a LGPD considera os dados biométricos como dados sensíveis, requerendo, portanto, maior cuidado no seu tratamento.

Em primeiro lugar, destacamos que a biometria não se limita à impressão digital e à íris, voz e face também são considerados dados biométricos. E o tratamento desses dados, categorizados como sensíveis, somente podem ocorrer nas hipóteses elencadas no art. 11 da LGPD:

- consentimento do titular, de forma específica e destaca e para finalidades específicas;
- cumprimento de obrigação legal ou regulatória;
- execução de políticas públicas;
- realização de estudos por órgãos de pesquisa, com a anonimização dos dados, sempre que possível;
- exercício regular de direitos, inclusive em contrato e processos judiciais, administrativos e arbitrais;
- proteção da vida ou segurança física do titular ou terceiro;
- tutela da saúde (apenas por profissionais de saúde, serviços de saúde ou autoridade sanitária);
- prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Nessa última hipótese, incluiu o legislador, a observância do art. 9º da LGPD, que determina o direito dos titulares ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara e adequada e no mínimo:

- finalidade do tratamento de dados;
- forma e duração;
- identificação do controlador;
- contato do controlador;
- informações sobre a existência de uso compartilhado de dados e sua finalidade;
- responsabilidade dos agentes que realizarão o tratamento;
- menção explícita dos direitos do titular.

Já o § 2º, do art. 74 da CLT, dispõe que “Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso”.

Por sua vez, a Portaria 1.510/09 do extinto Ministério do Trabalho regula o uso de Sistemas de Registro Eletrônico de Ponto, enquadrando a biometria no ponto eletrônico. A Portaria 373/11, também do MTE, dispõe sobre o uso de sistemas alternativos de controle da jornada de trabalho, como o ponto eletrônico biométrico por aplicativo.

Neste cenário, poderíamos argumentar que a coleta do dado biométrico para registro de ponto se enquadraria na hipótese do art. 11, II, “a” – obrigação legal ou regulatória pelo controlador –, já que a CLT determina a obrigatoriedade do registro para empresas com mais de 20 funcionários, **ou**, na hipótese do art. 11, II, “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”.

No entanto, o debate que vem sendo travado especificamente sobre essa atividade de tratamento é a possível ofensa ao do Princípio da Necessidade, uma vez que existem no mercado outros meios de registro de ponto, sem a utilização de um dado sensível.

Certamente existem outros mecanismos de registro de jornada laboral, mas seriam tão eficazes quanto a biometria para garantir a fidedignidade das informações dos horários lançados e quem os fez?

Entendemos que a credibilidade desses registros traz segurança tanto para o empregador quanto para o empregado, evitando a ocorrência de fraudes e garantindo o efetivo registro das horas trabalhadas.

No entanto, se de um lado temos garantida a lisura dos registros, por outro, as empresas devem adotar medidas técnicas e organizacionais que garantam a segurança dos dados biométricos coletados, além de se limitarem a usar esses dados somente para a finalidade declarada, qual seja, o controle da jornada.

Já se sabe que a LGPD sofreu grande influência do GDPR, que é a legislação aplicável na União Europeia (EU) sobre proteção de dados. Assim, o entendimento da UE sobre o uso da biometria no contexto laboral, poderá auxiliar nas medidas a serem adotadas no Brasil.

O GT 29, em seu Parecer nº 02/2017, que aborda o Tratamento de Dados no local de trabalho, opinou pela utilização da biometria no caso de controle de ponto desde que esses dados sejam utilizados exclusivamente para essa finalidade, mas reconhece que “embora tais sistemas possam constituir uma importante componente de uma pista de auditoria de um empregador, colocam também o risco de proporcionar um nível de conhecimento e controlo invasivo das atividades do empregado no local de trabalho”².

A Lei nº 58/2019 de Portugal traz, em seu art. 28, item 6, a seguinte redação:

“O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados”³.

² https://www.uc.pt/protecao-de-dados/suporte/20170608_parecer_2_wp249_gt29 Consultado em 15.07.2021

³ <https://dre.pt/pesquisa/-/search/123815982/details/maximized> Consultado em 15.07.2021

No mesmo sentido, a Agencia Española de Protección de Datos (AEPD), considerou válida a coleta de dados biométricos para fins de controle de jornada⁴.

E no Brasil? Bom, aqui a ANPD ainda não se posicionou a respeito e não há previsão de manifestação sobre o uso da biometria no contexto laboral. Com fundamento nas opiniões emitidas na União Europeia, acreditamos que o uso da biometria para controle da jornada continuará permitido, observadas as medidas de segurança pertinentes e a respectiva finalidade. Inclusive por ser uma forma validada pelo extinto Ministério do Trabalho e em consonância com a CLT. Caberá a cada empresa, após a realização do Relatório de Impacto, decidir se adotará ou não outro mecanismo de controle.

⁴ <https://www.aepd.es/es/documento/td-01755-2009.pdf> Consultado em 15.07.2021

8. Treinamento e boas práticas

Dayane Mendonça

Ana Sílvia da Fonseca Pinto Coelho

Conforme anteriormente mencionado, a LGPD conceitua o titular de dados pessoais como a “*pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*”. No contexto do contrato de trabalho, o titular de dados pessoais será, em regra, o empregado.

No contexto da relação de emprego, sob o enfoque do tratamento realizado no âmbito das relações mantidas entre o empregado e o empregador, que, no âmbito dessas relações faz as vezes de controlador, verifica-se um intenso fluxo de dados pessoais, que se estende desde a fase pré-contratual e alcança a pós-contratual. Cumpre esclarecer que o tratamento de dados pessoais não se encerra com o término do contrato de trabalho.

Vale também ressaltar que, em média, de acordo com o relatório da *Kaspersky Lab e B2B International*, “O Fator Humano na Segurança de TI: como os funcionários tornam as empresas vulneráveis de dentro para fora” cerca de 46% dos incidentes são causados pelos próprios funcionários, o que gera uma fragilidade nas empresas, que deve ser resolvida em vários níveis, não apenas pelo departamento de segurança de TI, o que evidencia a importância da empresa investir também na conscientização do seu quadro de colaboradores e em mecanismos de segurança para garantir que seja estabelecida uma verdadeira cultura de proteção de dados dentro da empresa.

Partindo desta realidade, a ideia desta cartilha é indicar, de maneira exemplificativa, boas práticas nas relações de trabalho com enfoque na Lei Geral de Proteção de Dados, a saber:

a. Elaboração ou revisão do Código de Ética e Conduta e do Regulamento Interno de Empresa segundo a Política de Privacidade e Proteção de Dados Pessoais.

É importante que sejam elaborados ou revisados o Código de Ética e de Conduta e o Regulamento Interno da Empresa, segundo a Política de Privacidade e Proteção de Dados Pessoais, com linguagem simples e acessível, já que sua finalidade é ser compreendido por todos os colaboradores da empresa, dos mais diversos cargos ali existentes, devendo ser apresentado de maneira atrativa, interessante e, se possível, com exemplos práticos.

No Regimento Interno é recomendável que sejam estabelecidas regras internas, como por exemplo, as relacionadas ao uso seguro dos equipamentos da empresa como telefone e computadores comerciais; cuidados com a segurança dos acessos e senhas; abertura de *e-mails* e mídias removíveis, e ainda deverá conter regras ligadas à segurança no trabalho realizado de forma remota, eventual descarte de papéis, acompanhamento da entrada de visitantes, impedimento de acesso a estranhos, entre outros.

b. Termo de Confidencialidade e sigilo entre empregador e empregado.

É importante que o empregador firme com seus colaboradores um Termo de Confidencialidade e Sigilo no ato das contratações, documento esse que garantirá que informações estratégicas e confidenciais do seu modelo de negócio não sejam repassadas a terceiros ou até mesmo utilizadas pelo empregado. A violação de segredo da empresa é, inclusive, uma das hipóteses de demissão por justa causa elencadas no artigo 482 alínea “g” da legislação trabalhista.

c. Treinamento para conscientização sobre a privacidade e proteção de dados.

Um projeto de adequação eficaz é aquele que inclui um treinamento e conscientização de toda a equipe de colaboradores sobre privacidade e proteção de dados, informando a todos acerca da importância de se respeitar a legislação, tanto na jornada interna e diária dos colaboradores, quanto para o seu público externo.

A efetiva conscientização viabiliza as mudanças de comportamentos e a existência de colaboradores engajados em prol da cultura de privacidade e proteção de dados.

O tema “treinamento e conscientização” é tão importante que ganhou papel de destaque na LGPD, no capítulo destinado à adoção de boas práticas e medidas de governança de dados, e está previsto em diversos documentos relevantes que o abordam, tais como i) o Guia de Boas Práticas elaborado pela Secretaria de Governo Digital; ii) o Decreto n. 10.222/2020, do Gabinete de Segurança Institucional da Presidência da República - Estratégia Nacional de Segurança Cibernética (E-Ciber) e iii) as regulamentações de padrão internacional ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27701.

d. Canal de Comunicação que permita o exercício dos direitos dos titulares.

Ao falarmos na Lei Geral de Proteção de Dados, a primeira ideia que parece surgir está relacionada à adoção de medidas que garantam a privacidade dos dados dos consumidores e usuários dos serviços finais. Contudo, como anteriormente mencionado, enquadrado o empregado como titular de dados pessoais, faz-se imprescindível que os empregadores controladores lhes assegurem o exercício dos direitos legalmente previstos por meio de canal de comunicação efetivo.

Do exposto acima, compreende-se como obrigação do empregador assegurar a manutenção de um canal de comunicação que viabilize também ao empregado o exercício desses direitos dentro do prazo previsto em lei ou regulamentado pela ANPD.

e. Adequação dos contratos de trabalho com cláusulas específicas sobre a LGPD.

Nas relações de trabalho, grande parte das operações de tratamento ocorrerão com esteio nas bases legais de cumprimento de obrigação legal ou regulatória (art. 7, II, LGPD) ou execução de contrato (art. 7, V, LGPD). De todo modo, é de extrema importância que seja realizada a adequação dos contratos de trabalho com cláusulas específicas relacionadas à privacidade e proteção de dados, por meio de aditivos contratuais e as cláusulas destinadas a esse fim. Destaca-se, ademais, que as cláusulas contratuais que

visem regulamentar aspectos específicos do tratamento de dados pelo empregador devem vir destacadas no documento, de forma a garantir a observância dos princípios da finalidade, transparência e segurança.

Considerando a Lei Geral de Proteção de Dados, as partes se obrigam à observância e cumprimento das regras quanto à proteção de dados, inclusive no tratamento de dados pessoais e sensíveis, mediante aditivos e termos específicos, de acordo com a necessidade e/ou obrigação legal de coleta dos dados e com previsões específicas relacionadas ao compartilhamento de dados com terceiros, como é o caso das seguradoras, operadoras de planos de saúde ou entidades sindicais, que, em regra, necessitam de autorização expressa do titular, de forma livre, informada, inequívoca e relacionada a uma determinada finalidade.

O empregador se compromete à correta conservação dos dados pessoais e demais dados pertinentes à relação de emprego, na vigência e após o seu eventual término para cumprimento de obrigação legal ou regulatória do controlador, respeitando os prazos legais trabalhistas, previdenciários e fiscais para guarda de tais dados, nos termos do art. 16, I da Lei 13.079/2018.

f. Investimento em cibersegurança, tanto no ambiente corporativo da empresa quanto no trabalho *home-office*.

Para efetivação de uma política de privacidade e proteção de dados, faz-se imprescindível, por fim, que os controladores (em nosso recorte os empregadores) invistam em tecnologia e em campanhas educativas e ações que priorizem a cibersegurança de sistemas e aplicações, tanto internamente quanto aos funcionários que trabalham *home-office*.

Investimento em criptografia, instalação de programas de antivírus, utilização de rede virtual privada - VPN, implemento de *softwares* de rastreamento, entre outros, são algumas das medidas que poderão minimizar a ocorrência de *cibercrimes* e viabilizar a proteção efetiva dos dados pessoais.

| Saiba mais

ARAÚJO, Leandro Sampaio Correa de. **Impactos da Lei Geral de Proteção de Dados nas relações de trabalho** Disponível em: <https://www.conjur.com.br/2020-mar-14/leandro-araujo-impactos-lgpd-relacoes-trabalho> Acesso em: 29 de março de 2021.

F-Reynoso Castillo C, Los derechos humanos laborales. México, Tirant lo Blanch, UNAM, UAM, 2015.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo. Saraiva. 2014.

PAMPLONA FILHO, Rodolfo; CONI JUNIOR, Vicente Vasconcelos. A Lei Geral de Proteção de Dados Pessoais e seus impactos no Direito do Trabalho. **Revista Direito Unifacs: debate virtual**, Salvador, n. 239, p. 1-42, maio 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/7108>. Acesso em: 31 de março de 2021.

Sáenz Torre de Torre. “El derecho a la intimidad personal en el ámbito laboral”. Facultad de Ciencias Jurídicas y sociales, Universidad de la Rioja, año académico 2014-2015, trabajo para grado académico, La Rioja, España.

https://www.kaspersky.com.br/about/press-releases/2017_em-40-das-empresas-do-mundo-todo-funcionarios-escondem-incidentes-de-seguranca-de-ti acessado em 05.04.2021.

http://www.boletimcontabil.com.br/conteudo/novo/tabelas_praticas/guarda_doc.php acessado em 08/04/2021 às 14:57.

| Autores



Adriana Giuntini

Advogada, Consultora em Proteção de Dados. Professora do MBA do IESB para DPO. Membro da Comissão de Privacidade e Proteção de Dados da OAB/DF. Sócia fundadora da 2Innovate Consultoria Empresarial e Treinamentos Ltda e da Giuntini Advocacia. Possui Pós-graduação em *Compliance* e Proteção de Dados pela Universidad Católica de San Antonio de Murcia - UCAM/ Espanha. Delegada de Protección de Datos – DPD/DPO em General Data Protection Regulation – GDPR pela Escuela de Negócios – EDEU – Madri/Espanha e Pós graduação em Gestão de Negócios pela Fundação Dom Cabral.



Ana Sylvia da Fonseca Pinto Coelho

Advogada e Sócia do Fischgold Benevides Advogados. Professora de Direito do Trabalho há quase 10 anos. Mestre em Direito do Trabalho e Processo do Trabalho pela PUC Minas. Professora de cursos de pós-graduação - Os impactos da LGPD nas relações de trabalho. Certificada em Privacidade e Proteção de Dados pela Data Privacy Brasil.



Camila Mickiewicz

Advogada, consultora com expertise em Lei Geral de Proteção de Dados. Pós-graduanda em Direito Digital pela Escola Brasileira de Direito. Integrante da Comissão de Direito Digital, Tecnologias Disruptivas e Startups e da Comissão de Privacidade e Proteção de Dados da OAB-DF.



Cinthia Tufaile

Advogada, Encarregada pelo Tratamento de Dados Pessoais. Mestre pela UnB – Universidade de Brasília. Membro da Comissão de Privacidade e Proteção de Dados da OAB/DF. Pós-Graduanda em Direito Digital e Proteção de Dados pela Ebradi e cursando MBA em Data Protection Officer pelo IESB.



Dayane Mendonça

Advogada, empresária, consultora especialista em privacidade e proteção de dados. Pós-graduanda (MBA) para Data Protection Officer – DPO (LGPD & GDPR) pelo Centro Universitário IESB. Integrante da Comissão Especial de Privacidade e Proteção de Dados da OAB-DF para o triênio 2019/2021, com forte atuação junto aos micros e pequenas empresas, com forte atuação junto aos micros e pequenas empresas e como encarregada de dados.



Julie Maria Figueira Vittone

Advogada e pesquisadora em Direito Digital. Membro da Comissão de Direito Digital, Tecnologias Disruptivas e Startups e da Comissão de Privacidade e Proteção de Dados Pessoais na Ordem dos Advogados Seccional do Distrito Federal. Pós-Graduada em Direito Digital e Pós-Graduada em Lei Geral de Proteção de Dados.



Kelly Santoro

Sócia do Escritório R. Santoro Advogados. Mediadora de Conflitos do Tribunal de Justiça do RJ, com certificação do CNJ. Consultora jurídica e instrutora no direito empresarial e na proteção de dados e privacidade, com forte atuação junto os micros e pequenas empresas. Especialista em Gestão de Crise e Conflito nas organizações públicas e privadas pela AVM/RJ. MBA em Direito da Economia e da Empresa pela FGV/RJ. Membro da Comissão Especial de Proteção de Dados Pessoais da OAB/DF. Membro da Comissão de Mentoria da OAB/RJ. Membro do Grupo Jurídico B, do Sistema B.



Ilderlândio Teixeira

Advogado, DPO | CPO | Vice-Presidente CPPDP® OAB/DF | Especializando em Segurança da Informação | Especialista em Advocacia Civil e Processual Civil. | Graduado em Sistemas de Telecomunicações.



Marcela Calazans

Advogada, Encarregada de Proteção de Dados, com certificação DPO pela EXIN. Consultora Jurídica em Privacidade e Proteção de Dados. Especialista em Direito Digital e *Compliance*. Atuação em projetos de adequação à LGPD, governança corporativa e gestão de riscos. Membro da Comissão de Privacidade e Proteção de Dados da OAB/DF e da ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados.



Natália Saucedo Perez Costa

Advogada, Pós-Graduada em Direito do Tributário pelo Instituto IDP. Assessora do Gabinete do Presidente da Companhia Nacional de Abastecimento. Membro da Comissão de Lei Geral de Proteção de Dados da OAB/DF.



Lei Geral de Proteção
de Dados Pessoais



Todo o conteúdo dos textos é de inteira
responsabilidade de seus autores.

ISBN 978-65-89765-07-3



9 786589 765073

