MANUAL PRÁTICO DE ADEQUAÇÃO À

LGPD

COM ENFOQUE NAS
RELAÇÕES DE TRABALHO

AUTORIA
SELMA CARLOTO
ELAINE GUERRA

LTr®

MANUAL PRÁTICO DE ADEQUAÇÃO À LGPD

COM ENFOQUE NAS
RELAÇÕES DE TRABALHO

2ª EDIÇÃO
2024

LTr Editora Ltda.

Rua Jaguaribe, 571
CEP 01224-003
São Paulo, SP — Brasil
Fone (11) 2167-1101
www.ltr.com.br
Setembro, 2024

Produção Gráfica e Editoração Eletrônica: PIETRA DIAGRAMAÇÃO
Projeto de capa: DANILO REBELLO
Impressão: LOG & PRINT GRÁFICA E LOGÍSTICA

Versão impressa — LTr 6416.9 — ISBN 978-65-5883-304-8
Versão digital — LTr 9918.0 — ISBN 978-65-5883-305-5

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Carloto, Selma

Manual prático de adequação à LGPD [livro eletrônico]: com enfoque nas relações de trabalho/Selma Carloto e Elaine Guerra. – 2. ed. – São Paulo: LTr, 2024.

PDF

Bibliografia.

ISBN 978-65-5883-305-5

1. Direito à privacidade 2. Direito do trabalho – Brasil 3. Proteção de dados – Leis e legislação 4. Proteção de dados pessoais 5. Relações de trabalho I. Guerra, Elaine. II. Título.

24-203791 CDU-342.721:331(81)

Índice para catálogo sistemático:
1. Brasil: LGPD: Proteção de dados pessoais: Direito do trabalho
342.721:331(81)
Cibele Maria Dias – Bibliotecária – CRB-8/9427

SUMÁRIO

INTRODUÇÃO

Neste livro, mergulharemos de forma prática e abrangente no complexo universo da Lei Geral de Proteção de Dados (LGPD) no contexto das relações de trabalho no Brasil. As empresas enfrentam hoje uma série de desafios e incertezas quando se trata de garantir a conformidade com essa legislação, especialmente no que diz respeito à coleta, tratamento e proteção dos dados de seus empregados.

Com a evolução tecnológica acelerada, as dúvidas são muitas e as armadilhas são constantes. A crescente necessidade de obter o consentimento adequado (livre, informado e inequívoco), incluir cláusulas contratuais específicas e evitar tratamentos excessivos de dados torna-se uma tarefa cada vez mais crítica. Nesse cenário, é imperativo que as empresas adotem medidas corretas e abrangentes.

Nosso foco principal é nas relações de trabalho, mas reconhecemos que os empregados desempenham um papel essencial na gestão de dados pessoais e sensíveis de clientes, bem como dos próprios colegas de trabalho. Portanto, esta obra aborda a LGPD com um enfoque amplo, abrangendo todas as práticas recomendadas e regulamentações aplicáveis que impactam a empresa como um todo.

Não se trata apenas de uma adequação parcial, seja no âmbito trabalhista ou nas relações de consumo. A LGPD exige uma abordagem holística e abrangente, englobando todas as áreas da empresa. Isso inclui não apenas os departamentos de Recursos Humanos, Jurídico Trabalhista e Contabilidade, mas também a área de Segurança da Informação. Todos desempenharão um papel direto ou indireto na busca pela conformidade com a LGPD.

À medida que exploramos os processos envolvidos nas relações laborais, destacaremos a importância dos questionários e da colaboração interdepartamental na fase 2 do nosso projeto. O objetivo é fornecer orientações práticas e soluções para que as empresas possam enfrentar os desafios da LGPD com confiança e eficácia.

Capítulo 1

OBJETIVO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

O objetivo e ideia central da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Figura 1 – Objetivo central da LGPD

O art. 1º aduz que "esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".(1)

Fonte: Do autor,2021.

A nova legislação veio para proteger os direitos fundamentais, principalmente a privacidade dos titulares, pessoas naturais e para devolver-lhes o controle dos dados**.** A empresa

(1) BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF. 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 3 mar. 2021.

possui um banco de dados, mas não é mais a dona destes dados, assim deverá informar detalhadamente tudo o que faz com os mesmos, cuidar e dar-lhes segurança a estes, já que não lhe pertencem e apenas tratá-los quando houver de fato necessidade para uma determinada finalidade, além de assegurar sempre e de fato a transparência no tratamento destes dados, os quais, hoje, com a evolução tecnológica, passam a ter um valor inestimável, sendo equiparados a diamantes e valendo mais que petróleo.

Capítulo 2

Conceitos essenciais: dados pessoais, dados pessoais sensíveis, anonimização e pseudonimização

2.1. Dados pessoais

Os dados pessoais consistem em uma informação relacionada à pessoa natural identificada ou identificável, logo, a Lei Geral de Proteção de Dados não se aplica a dados de pessoas jurídicas de forma direta. No entanto, existirá aplicação indireta porque todas as pessoas jurídicas possuem dados de pessoas naturais, inclusive sócios, empregados e outros trabalhadores. Dessa forma, a Lei Geral de Proteção de Dados se aplica a todas as empresas públicas ou privadas e todas as empresas precisarão fazer a sua adequação porque terão ou empregados ou clientes, além de sócios, entre outros titulares.

Por exemplo, uma empresa contrata um representante comercial como pessoa jurídica, o contato será com a pessoa natural do representante comercial e mesmo sendo uma contratação de um representante comercial, pessoa jurídica, haverá uma intensa volumetria de dados de pessoa natural e que demandam conformidade com a Lei Geral de Proteção de Dados.

Conforme mencionado anteriormente, o dado pessoal está vinculado a uma pessoa natural identificada ou identificável. Para uma compreensão mais detalhada, é importante elucidar e exemplificar o que são dados pessoais identificados e identificáveis na prática.

Os dados pessoais identificados referem-se diretamente à pessoa identificada, como nome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, telefone, entre outros. Em contraste, os dados pessoais identificáveis são informações que, indiretamente, podem identificar o titular, exigindo dados adicionais para essa identificação. Por exemplo, a placa de um veículo: ao observar apenas a placa, não é possível identificar imediatamente o titular dos dados; são necessárias informações suplementares para determinar o proprietário do veículo.

É essencial notar essa distinção, pois os dados identificados são facilmente vinculados à pessoa, enquanto os dados identificáveis demandam outros elementos para estabelecer essa conexão com o titular.

Tabela 1 – Dados Pessoais

Dado pessoal-direto	**Dados pessoal indireto**	**Dado anonimizado**	**Dado pseu-do-nimizado**
Quando a pessoa já é diretamente identificada pelo dado: nome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, número da OAB, número do CRM, número do COREN, número de CRECI, telefone etc.	Identificam o titular indiretamente, demandando informações adicionais como exemplo, a placa de um veículo.	Perde-se a possibilidade da associação, considerando-se a utilização de meios técnicos disponíveis e razoáveis no momento do tratamento.	Identificação apenas com informação adicional e mantida separadamente pelo controlador em ambiente controlado e seguro.

Fonte: Do autor, 2021.

2.2. Dados pessoais sensíveis

Os dados pessoais sensíveis são aqueles que demandam uma maior proteção, e precisam de proteção qualificada, como dados 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, nos termos da LGPD.

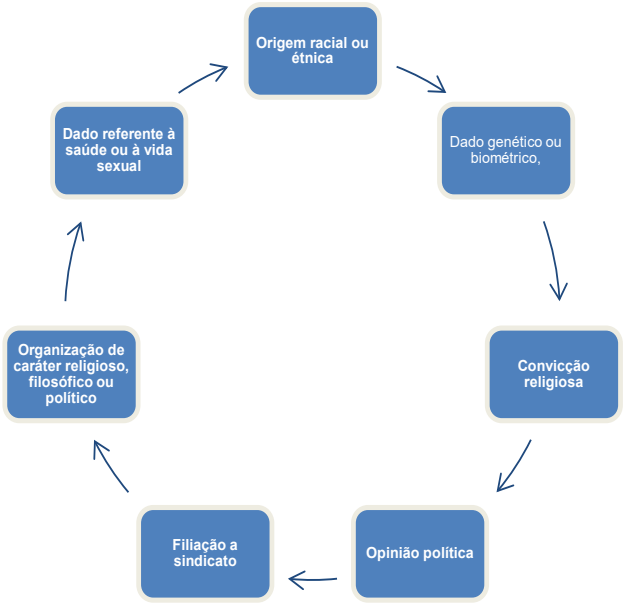
Quando temos tratamento de dados pessoais sensíveis, um incidente ou desconformidade poderá gerar prejuízo maior ainda ao titular dos dados e, por essa razão, esses dados são categorias especiais de dados e se denominam de sensíveis.

Nas relações de trabalho, sempre existirá o manuseio de dados pessoais sensíveis, de forma legítima, por obrigação legal, principalmente de dados de saúde, entre outros, muitas vezes necessários.

É também comum o processamento de dados biométricos para o registro eletrônico de ponto, por meio dos quais as empresas deverão ter mais cuidado para prevenir incidentes relacionados a esses dados, já que estes identificam o titular de forma inequívoca e uma falha de segurança poderá gerar um prejuízo irremediável ao titular.

Se classificarmos o risco de tratamento, sempre será elevadíssimo ao serem tratados ou processados dados pessoais sensíveis e, por essa razão, será importante a elaboração de um RIPD (relatório de impacto à proteção de dados) que explicaremos em capítulo próprio.

Figura 2 – Dados Pessoais Sensíveis



Fonte: Do autor, 2021

Durante as relações laborais e na extinção do contrato de trabalho, as empresas estão sempre recebendo atestados médicos e em muitos casos há necessidade de tratar dados sensíveis para um processo seletivo, o que não poderá ter caráter discriminatório, caso o tenha, a empresa ferirá o princípio da não discriminação.

No processo seletivo, não ofenderia a LGPD coletar dados sensíveis e tratá-los quando a empresa decidir fazer um processo, por exemplo, só para grupos que sofrem regularmente discriminação, já que aqui estaríamos diante de uma discriminação positiva ou reversa, como, por exemplo, um processo seletivo só para deficientes e que consiste em

uma ação afirmativa, com o objetivo de ser preenchida a cota de deficientes, nos termos da Lei da Previdência.

Figura 3 – Dados Sensíveis nas Relações de Trabalho

Fonte: Do autor, 2021

Exemplos de dados sensíveis nas relações de trabalho são dados relativos à saúde (como exames ocupacionais, atestados médicos), biometria, orientação sexual porventura em alguma ficha cadastral, ou sistema eletrônico, religião,

dentre outros. Dessa forma, recomenda-se, por exemplo, que não sejam coletados dados quanto à origem racial do colaborador, a não ser, que seja uma obrigação legal ou regulatória, como no caso do e-Social e da Lei n. 14.553, de 2023. Nesses casos, a empresa coletará os dados, mas aplicará medidas técnicas e administrativas para resguardar os dados pessoais, além da elaboração do relatório de impacto à proteção de dados pessoais (RIPD).

2.1.1. Dados médicos

As empresas sempre irão precisar tratar dados médicos de empregados, já que os exames médicos admissionais, periódicos e demissionais são obrigatórios, nos termos da lei. Ocorre ser muito comum também a coleta e tratamento de atestados médicos.

Esses tratamentos não precisarão de consentimento, mas a empresa deverá restringi-los a quem deva realmente tratá-los, caso contrário, a empresa estará em desconformidade com a LGPD, sendo um incidente ou uma falha de segurança, caso alguém, que não deveria ter acesso, venha a tê-lo, ou até mesmo, por um ataque cibernético.

É importante adotar medidas de precaução rigorosas para garantir a segurança das informações. A primeira delas é evitar deixar atestados visíveis em mesas ou em qualquer local de fácil acesso a qualquer pessoa. Em todas as circunstâncias, as mesas devem estar sempre limpas, sem qualquer informação de empregados ou clientes visível, a fim de proteger a confidencialidade dos dados.

Essa mesma precaução deve ser aplicada quando se trata de documentos em formato digital. É fundamental que os atestados digitais não sejam acessíveis a colegas ou a titulares de setores que não tenham a incumbência de

acessá-los. A confidencialidade das informações deve ser mantida de forma intransigente em todos os meios, físicos e digitais, para assegurar a segurança dos dados.

Cabe à empresa adotar medidas não apenas técnicas, mas também administrativas, para mitigar o risco, como: política de segurança da informação, política de mesa e tela limpas, bloqueio automático de tela quando o usuário sai do computador, proibição de outras pessoas, alheias ao tratamento necessário, acessarem o local noa qual os dados sensíveis são manuseados, entre outras medidas de segurança.

2.1.2. Dados biométricos

A biometria, classificada como um dado pessoal sensível, requer um tratamento especialmente cuidadoso, abrangendo tanto a avaliação da necessidade desse tratamento quanto a implementação de medidas de segurança rigorosas na empresa.

No contexto das práticas de RH, a utilização da biometria, incluindo o reconhecimento facial, pode desempenhar um papel importante na segurança e no controle de acesso às instalações das empresas. Isso se torna evidente ao considerarmos a importância de proteger o direito à vida e à integridade física do titular, bem como de terceiros, além da segurança patrimonial e das informações. Em processos de identificação e autenticação de cadastros em sistemas eletrônicos, a biometria oferece uma camada adicional de segurança.

Vale destacar que, mesmo quando a empresa se baseia em uma base legal que justifica a dispensa de consentimento, isso não a isenta da obrigação de seguir os 10 princípios de proteção de dados, incluindo a transparência no tratamento. Portanto, é fundamental que os trabalhadores sejam devidamente informados sobre como ocorre esse tratamento e quais finalidades são atendidas.

Conforme destacado pelo Grupo de Trabalho do Artigo 29, em seu Parecer 13 de 2011, sobre geolocalização, ao citar o Parecer 8 de 2001 sobre o tratamento de dados pessoais no contexto laboral, a obtenção de consentimento pode ser problemática, especialmente quando os trabalhadores enfrentam potenciais perdas de oportunidades de emprego ao recusar o consentimento. Em vez de solicitar o consentimento, os empresários devem avaliar a necessidade legítima de controlar a localização exata de seus empregados e ponderá-la com os direitos e liberdades fundamentais dos trabalhadores, o que se refere à hipótese legal de tratamento do legítimo interesse.

Um exemplo prático do uso da biometria, como o reconhecimento facial, no controle de acesso seria a implementação de sistemas que utilizam essa tecnologia para permitir que os funcionários acessem áreas restritas da empresa. Essa medida, além de garantir a segurança das instalações, também preserva a privacidade e protege os dados pessoais dos trabalhadores.

No entanto, é importante ressaltar a necessidade de evitar o desvio de finalidade. Embora a biometria, incluindo o reconhecimento facial, possa ser empregada ainda para o controle de jornada, dos trabalhadores, o que se enquadra em cumprimento de obrigação legal ou regulatória, é fundamental que a vigilância contínua da frequência e dos horários de entrada e saída não seja justificada se esses dados forem utilizados para finalidades diferentes das originalmente informadas, como a avaliação de desempenho.

Por exemplo, a empresa pode implementar um sistema de registro de ponto biométrico, onde os funcionários registram suas entradas e saídas usando suas impressões digitais ou o reconhecimento facial. Esses dados são coletados exclusivamente para o controle de jornada, garantindo que os funcionários cumpram seus horários de trabalho.

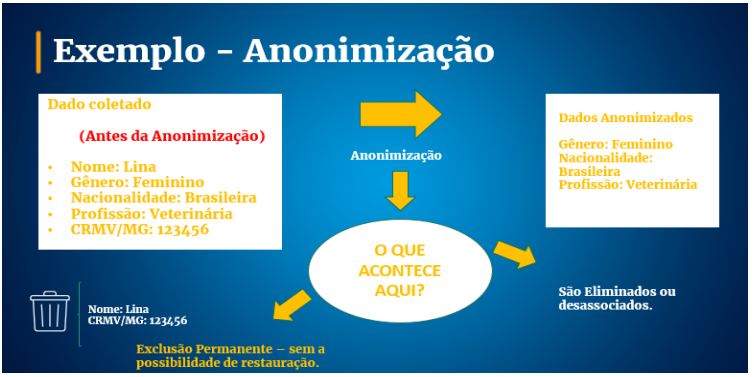
Qualquer uso adicional desses dados, incluindo o reconhecimento facial, para avaliação de desempenho ou outros fins não declarados seria considerado um desvio de finalidade e estaria em desacordo com a LGPD. Portanto, é fundamental que as empresas mantenham a integridade e a transparência em todas as etapas do tratamento de dados biométricos, incluindo o reconhecimento facial.

2.3. Dados anonimizados

A Lei Geral de Proteção de Dados não se aplica, por via de regra, aos dados anonimizados, entretanto, se houver a possibilidade de identificação ou reversão do processo e a pessoa for identificada, passamos a ter dados pessoais, ainda que diante da necessidade de informações adicionais.

Um dado será anonimizado, não sendo dado pessoal, quando se perde a possibilidade da associação, seja direta ou indireta, considerando-se a utilização de meios técnicos disponíveis e razoáveis no momento do tratamento.

Abaixo, um exemplo de anonimização.

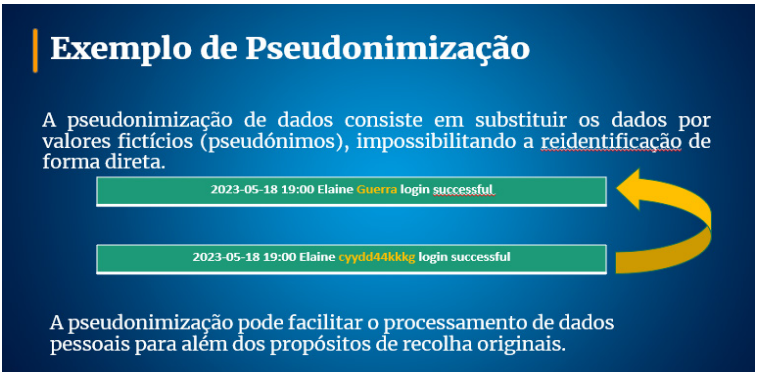


Fonte: Do autor, 2024

2.4. Dados pseudonimizados

Temos ainda os dados pseudonimizados que consistem apenas na possibilidade de identificação do titular com a utilização de informação adicional e mantida separadamente pelo controlador em ambiente controlado e seguro.

Abaixo, um exemplo de pseudonimização.



Fonte: Do autor, 2024