COMITÊ DE RELAÇÕES TRABALHISTAS NO DIGITAL

ANADD
Associação Nacional de
Advogadas e Advogados de Direito Digital

Comitê ANADD RTD
* COMITÊ DE RELAÇÕES TRABALHISTAS NO DIGITAL *

LGPD e as Relações de Trabalho

Coautores:

Elis Xavier
Hilda Cavalcanti
Júlia Medeiros
Maria Santos
Renata Proximo
Valéria Ribeiro

Coordenação:
Maria Santos

Arte e Design:
Ricardo Castro Cajazeira

Revisão:
Maria Santos e Ricardo Castro Cajazeira

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital
Registro ISBN nº 978-65-999397-1-6

Sumário

Introdução

Este Ebook tem o objetivo de transmitir as experiências dos(as) autores(as) conduzindo consultorias e projetos de Privacidade e Proteção de Dados nas Empresas, principalmente com relação às relações do Trabalho, entre empregados, empregadores e prestadores de serviços.

Percebemos que a cada dia novos desafios surgem visando a proteção de dados pessoais. E as Transformações Digitais estão revolucionando o Direito do Trabalho, fazendo com que as empresas se adaptem ainda mais rápido, e desta forma nosso sistema judiciário brasileiro precisa acompanhar estas transformações com critérios específicos e orientados às inovações tecnológicas da nossa sociedade.

Estamos à caminho da Sociedade 5.0, onde buscamos mais serviços Inteligentes, eficientes e sustentáveis.

Neste sentido, esperamos que este trabalho desenvolvido pelo nosso Comitê de Relações Trabalhistas no Digital, traga a você conhecimento a partir de nossas experiências e estudos profundos sobre o tema.

Maria Santos - Diretora da ANADD e do Comitê RTD
Ricardo Castro Cajazeira - Presidente da ANADD

Sumário

Capitulo 1 e 2

Por Elis Xavier, Advogada

Advogada. Mestranda em Direito Privado pela PUC/MG. Pós graduada em Direito, Tecnologia e Inovação pela Univale. Sócia do escritório Elis Xavier Advocacia e Soluções Jurídicas.

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

1. Fundamentos da LGPD e Princípios

A LGPD possui conceitos fundamentais para compreensão e aplicação da norma, sendo elas:

- Dado pessoal: É toda informação relacionada a pessoa natural identificada ou identificável, como por exemplo: CPF, PIS, NIT, Nome, dados biométricos, etc.

- Aplicação: A lei é aplicável a qualquer pessoa, natural ou jurídica, de direito público ou provado, que realize o tratamento de dados de pessoas para fins econômicos, podendo ser online ou offline, incluindo os dados dos empregados e prestadores de serviço (art. º1);

- Local da aplicabilidade: Desde que qualquer fase da operação (início ao fim) de tratamento dos dados pessoais seja realizada em território nacional, mesmo que sua sede seja fora do país, a LGPD seja aplicada (art. 3º);

- Base legal para o tratamento: A Lei prevê, em seu artigo 7º, 10 hipótese que permitem o tratamento de dados, que será objeto de análise futura;

- Dados sensíveis: 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 (art 5º,II);

1. Fundamentos da LGPD e Princípios

- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Agentes de tratamento: o controlador e o operador;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado de dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Tratamento: Toda operação realizada com 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;

1. Fundamentos da LGPD e Princípios

- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

1. Fundamentos da LGPD e Princípios

- Relatório de impacto à proteção de dados: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

- Órgão de pesquisa: Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

- Autoridade Nacional de Proteção de dados: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

1. Princípios

- Boa fé: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

- Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

1. Princípios

- Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

- Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

- Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

2. Atendendo os princípios da LGPD nas relações de trabalho, na Etapa pré-contratual (Algoritmos - IA, recrutamento e seleção)

A LGPD não possui previsão, específica, quanto às relações de trabalho, mas sua base principiológica ratifica o que as normas trabalhistas expressam, quanto à responsabilidade jurídica que o empregador detém em relação aos dados de seus empregados, a finalidade desses com as cláusulas contratuais e a existência de boa-fé no tratamento de dados dos empregados pelo empregador e também aprimorar quanto à segurança no armazenamento de dados, sejam esses por meios digitais ou físicos.

Cumpre dizer que, ao contrário do que muito se pensa, a LGPD não protege apenas os dados armazenados digitalmente, sendo abrangente protegendo, também, os dados armazenados em meio físico.

Na aplicação da norma de proteção de dados deve ser utilizada durante todo o fluxo contratual, ou seja, desde a fase pré-contratual – processo seletivo – observando sempre a finalidade dos dados solicitados para os requisitos da vaga disponibilizada e até a rescisão do contrato, verificando quais dados podem permanecer arquivados e qual a justificativa legal para o arquivamento, conforme prevê referida lei no artigo 7º, II.

.

2. Atendendo os princípios da LGPD nas relações de trabalho, na Etapa pré-contratual (Algoritmos - IA, recrutamento e seleção)

Diante da quantidade de dados pessoais e pessoais sensíveis que são compartilhados com os órgãos públicos, bem como circulam dentro da própria organização, é imprescindível que a empresa esteja em conformidade em todas as fases de relacionamento entre empregador e empregados.

Por este motivo, se faz necessário que os departamentos da organização estabeleçam um plano de ação, iniciando pelo mapeamento de dados, estudo das bases legais, cuidados com o processo seletivo, inclusão de novas cláusulas contratuais, treinamento aos colaboradores, por exemplo.

Não se pode esquecer do armazenamento dos dados pessoais dos prestadores de serviço, pois abre precedentes na esfera trabalhistas.

Sumário

Capitulo 3

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Por Maria Santos, Advogada

Advogada e Data Protection Officer.
Atuando na Advocacia Chizzolini
Certificada DPO ITCERTS. Membro da Diretoria Associação Nacional dos Advogados de Direito Digital - ANADD.
Responsável Comitê Relações Trabalhistas no Digital,
Especialista em Direito Empresarial e Direito do Trabalho, atuando a mais de 30 anos no Mercado Corporativo. Pós-Graduanda em Direito Digital pela EBRADI
MBA e Pós Graduação, Controladoria, Auditoria e Compliance pela FMU - Pós Graduação em Direto Processual Trabalho -Anhembi Morumbi

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

LGPD nas relações de trabalho

Não há dúvidas que em qualquer seguimento de empresa, o maior volume de dados se concentra no departamento pessoal e recursos humanos, haja vista que não podemos esquecer que muito embora exista funções atribuídas a inteligência artificial, a gestão desta área e feira de pessoas,

A LGPD trouxe regras, que abrange a todos, assim o tratamento de dados irá envolver operações dos empregadores, pessoas físicas ou pessoas jurídicas, em todos os âmbitos públicos ou privados. União, Estados e Municípios estão sujeitos a Lei, e estão se adequando a ela . A proteção de Dados deve ser assegurada a todos, sem nenhuma exceção.

Lembrando que o tratamento de dados, regulado pelo artigo 5º. da LGPD, é toda forma de operação que utiliza dados pessoais, ou seja, desde sua coleta, produção, classificação, acesso, reprodução, distribuição, comunicação, transferência, arquivamento, eliminação, dentre outros.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

O tratamento de dados é um dos conceitos mais abrangentes da Lei Geral de Proteção de Dados. Essa expressão da lei que serve como um guarda-chuva para vários procedimentos envolvendo dados, como:

Coleta, Produção, Recepção, Classificação, Utilização, Acesso, Reprodução, Transmissão, Distribuição, Processamento, Arquivamento, Armazenamento, Eliminação, Avaliação, Controle, Modificação, Comunicação, Transferência, Difusão, Extração

Exemplos pertinente à fase contratual, pertinentes Livros e ficha de registros de empregados, jornada, valor do salário, descontos, faltas, motivos das faltas, doenças, acidentes, situações conjugais e familiares que podem ter reflexos em providências da empresa, como o pagamento de pensão, inclusão de dependente no plano de saúde, rescisão contratual, inclusive exame médico demissional dentre outros.

Dados sensíveis pertinentes a criança e adolescentes, quando da qualificação dos filhos, estes dados geralmente serão necessários para fins do salário-família, havendo, portanto, obrigação legal legitimadora para tanto

Muitos dados constantes de documentos, são extremamente questionáveis e devem ser revistos.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Além disso a gama de dados que circulam no departamento pessoal e recursos humanos, são enormes, dados de documentos, dados pessoais de filhos e outros dependentes, dados sindicais, informações de raças e etnias.

Iniciamos nosso ebook, com o estudo dos princípios, trazidos pela LGPD e podemos perceber que para cada dado coletado, necessária uma finalidade . Ou seja, esse princípio está relacionado com o propósito para a realização do tratamento de dados. Portanto, o fim a que se destina o dado precisa ser legítimo, específico, explícito e devidamente informado ao titular.

Percebemos, portanto, que a LGPD, trouxe um questionamento extremamente importantes.

T*odos esses dados são importantes ??*
Necessários a atividade desenvolvida?
Podem ser compartilhados?

Seguimos relacionando o nosso tema com os princípios já estudados, temos a importância de entender o princípio da adequação, que exige a compatibilidade entre o tratamento do dado pessoal e a finalidade informada ao trabalhador.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Nesse entendimento o CONTROLADOR ou EMPREGADOR não está livre para armazenar e/ou transferir todos os dados pessoais de seus colaboradores de acordo com seus interesses, deve utilizar somente aqueles que sejam compatíveis com a finalidade declarada na coleta.

Não podemos esquecer que os funcionários, colaboradores, diretores, prestadores de serviços, representantes, contratados, os chamados PJ, também são titulares, perante a LGPD, e devem ter seus dados pessoais e sensíveis protegidos.

Assim, conscientizara equipe , ou os responsáveis a planejar a forma que será realizada o tratamento de dados, considerando que ao coletar dados o faça com o minimamente possível, estipulando e limitando os dados que efetivamente serão necessários para alcançar o objetivo desejado. Coletar dados desnecessários é colocar a empresa em um nível de risco desnecessário e imprudente , lembre-se no caso de vazamentos de dados a multa é extremamente alta.

Outro ponto fundamental é revisar os procedimentos e os formulários da coleta de dados, adequando-os aos requisitos e princípios norteadores da LGPD.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

De quais dados estamos falando ?

o próprio nome, endereço, escolaridade, currículo, nome dos genitores, idade, e-mail, estado civil -, além de dados pessoais sensíveis como a filiação a sindicatos ou às organizações de caráter religioso, filosófico ou políticos e dados referentes à saúde, que devem ser protegidos, e assegurando ao titular a garantia prevista pela LGPD;

Como já vimos, temos como os principais personagens:

Titular *– empregado ou prestador de serviços que fornece a informação ao empregador; e*
Controlador/Operador de dados *– é o empregador, que deve tomar as decisões necessárias sobre o tratamento.*

Importante frisar que o tratamento de dados o mundo corporativo, e nas relação de trabalho inicia-se muito antes do início da prestação de serviços, inicia na prospecção de candidatos, como veremos TODAS as etapas da relação contratual o tratamento de dados está presente.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Iniciamos pela **Fase pré-contratual,** captação de candidatos, o recebimento do Curriculum Vitae, preenchimento de cadastro de sites, ou situações similares, preenchimento de ficha de solicitação de emprego.

As empresas devem tomar todo cuidado, a fase de recrutamento e seleção como análise do currículo, entrevistas, dinâmicas e posterior escolha do candidato selecionado.

Em situações normais entenderíamos que inexiste qualquer relação jurídica formal, *o candidato ainda não é funcionário, não assinou contrato....*

Contudo, a LGPD não entende assim, se esses dados não forem tratados de maneira adequado, a empresa poderá responder judicialmente por eventuais danos morais, além de receber a multa prevista na LGPD, se não tiver procedimentos, fluxos de trabalho, a informação clara ao candidato da finalidade, as tratativas e o descarte desses dados. .

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Ressaltamos que é proibida a coleta de dados que possam gerar qualquer critério discriminatório entre os candidatos, como, por exemplo, solicitação de exames de gravidez, toxicológico, exames de sangue, atestado de antecedentes criminais e análise de crédito, dados inclusive considerados “sensíveis” , a teor do art. 5º. Da Lei 13709/2018, que devem ser tratados com todo cuidado possível.

Já existe jurisprudência nesse sentido, proferida pelo Tribunal Superior Trabalho em acórdão publicado em 22/09/2017, no julgamento do Recurso Repetitivo (RR) 243000-58.2013.5.13.0023, com a fixação da tese jurídica prevalecente que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais, em virtude da existência de lei, natureza do ofício ou elevada fidúcia.

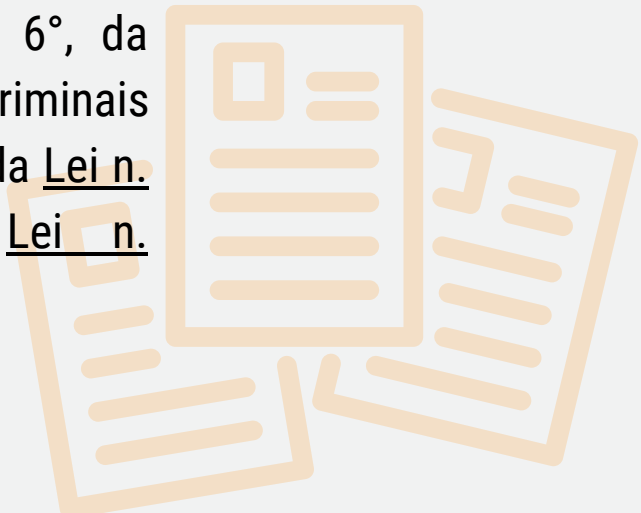
Uma sugestão, como tratamento do dados constante dos Curriculos e a Fichas de solicitação de emprego, que muitas empresas se utilizam, principalmente nas empresas de prestação de serviços, é criar políticas, processos e procedimentos para gerenciá-lo, assim como seu acesso e auditoria, com atenção ao descarte dos documentos não utilizados.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Uma sugestão de boa prática seria reduzir as informações constantes das "fichas de solicitação de emprego", quanto mais informações maior o risco, principalmente se tais informações não sejam essencialmente necessárias e autorizados pelo candidato.

Outra elaborar um documento que o candidato anua seu consentimento expresso acerca da coleta e da utilização dos dados pela pretensa contratante.

Dentre as analises prévias existem exceções como é o caso do exame toxicológico para o motorista profissional (artigo 168, § 6°, da CLT) e do atestado de antecedentes criminais para os vigilantes (artigos 12 e 16, VI, da Lei n. 7.102/1983 c/c art. 4°, I da Lei n. 10.826/2003).



3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Importante ressaltar que a Lei define que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios LGPD:

- *ADEQUAÇÃO*
- *FINALIDADE*
- *LIVRE ACESSO*
- *NÃO DISCRIMINAÇÃO:*
- *NECESSIDADE:*
- *PREVENÇÃO:*
- *QUALIDADE DOS DADOS*
- *RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS*
- *TRANSPARÊNCIA*

Em hipótese em que se faça entrevista for realizada por videoconferência importante adotar cuidados com o armazenamento do vídeo gravado em razão da possibilidade de conter inúmeros dados sensíveis.

Sendo o candidato dispensado do processo seletivo, o contralador/empregador , deve estipular um período de armazenamento desses dados e principalmente INFORMAR o candidato (art. 5º, XIV, LGPD).

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Se houver A mesma regra vale para o compartilhamento de currículo com outras possíveis empregadoras, caso em que o titular dos dados pessoais precisa saber e anuir expressamente (art. 5º, XVI, LGPD).

Encerrando a etapa de seleção os responsáveis, devem ser transparentes com os candidatos não selecionados quanto o que irá ocorrer com os dados, dai a importância da diugação massiva pela organização da a política de privacidade onde constará a maneira que haverá a utilização dos dados , bem como, o que será feito com os dados pessoais e com os documentos por eles apresentados.

Recomenda-se o descarte. Contudo, caso haja necessidade de mantê-los armazenados por um propósito legítimo, é obrigatório que o recrutador informe ao titular dos dados a razão pela qual não os descartará de imediato.

A Implementação correta da prerrogativas da LGPD devem ser feitas de maneia minuciosa, e requer o envolvimentos de todas as áreas da empresa, sendo fundamental o treinamento dos funcionários da empresa constantemente.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Fase contratual, candidato contratado, primeiros passos

EXAME ADMISSIONAL - CONTRATO DE TRABALHO - FICHA DE REGISTRO

Exame admissional, é um dado sensível, e requer cuidados importantes e exclusivos, lembre-se que muitos departamentos estão envolvidos, sendo este documento compartilhado pelas clinicas, prestadores de serviços de segurança do trabalho, e as vezes clientes.

Tudo isso deve ser mapeado e executado com uma gestão peculiar e de suma importante.

Importante o empregador informá-lo a respeito da política de tratamento de dados da empregadora/controlador.

Aos elaborar os documentos, importante frisar que, o consentimento do funcionário deve ser expresso e as cláusulas que versarem sobre a política de tratamento de dados da empresa devem vir destacadas no documento, de forma a garantir a observância dos princípios da finalidade, transparência e segurança, assim a reavaliação dos contratos de trabalho é primordial.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Os mesmos devem ser regularmente adequados. Como sugestão, refaça novo contrato e peça para o colaborador assinar, evite solicitar a assinatura em documento apartado, como termo de consentimento, uma vez que este poderá ser revogado a qualquer momento.

Ficha de registro: na ficha de registro é comum que contenha dados pessoais e dados sensíveis, a exemplo da filiação a sindicato, e dados dos filhos menores. Nesse aspecto a LGPD prevê expressamente a necessidade de tratamento desses dados com a limitação de acesso à ficha de registro do funcionário.

Atestados admissionais, atestado médico com ou sem identificação de CID, caso haja identificação da doença e/ou o motivo do afastamento, a LGPD considera estas informações sensíveis e, portanto, precisarão de política de tratamento específica de guarda e acesso, e monitoramento das pessoas que efetivamente terão acessos , devendo essas serem limitadas.

3. Tratamento de Dados (art. 5°) e Tipos de Dados quando da relação contratual

Como bem explica Voila Bonfim e Iuri Pinheiro:

Como exemplo prático no cotidiano das relações de trabalho, podemos citar o caso da entrega de atestados médicos, nos quais tenha constado a indicação de uma doença (CID10).

É inequívoco que o empregado possui o direito de que a informação sobre seu estado de saúde não seja compartilhada entre os demais trabalhadores até mesmo pelo elevado potencial discriminatório, mas, por outro lado, a empresa tem o dever de guarda da documentação de seus empregados inclusive para fins de reflexos previdenciários.

É fundamental, assim, que a empresa esteja preparada para criar rotinas seguras. Os atestados médicos devem, preferencialmente, ser armazenados em setor específico de segurança e medicina ocupacional, mas esse procedimento deve ser feito com proteção adequada para não incorrer em violação à privacidade.

Para a guarda segura, pode-se citar como possibilidade o armazenamento digital com a utilização de criptografia, anonimização ou pseudonimização, recursos esses cogitados pela própria LGPD e que demandarão o trabalho conjunto com a tecnologia da informação.
Todos os empregados devem ser informados e alguns treinados para o armazenamento, descarte e demais formas de tratamento de dados pessoais e sensíveis, inclusive os que aparentemente não lidam com dados, como a faxineira, o contínuo ou o garçom, pois podem ter acesso fortuito a um documento esquecido no ambiente de trabalho. Compete ao empregador (controlador) a adoção das medidas de precaução e proteção aos dados de todos os trabalhadores.

Sumário

Capitulo 4

4. Personagens da LGPD na Relação de Trabalho

Por Hilda Cavalcanti, Advogada

CEO da Cavalcanti Lima Verde Sociedade de Advocacia, advogada militante há mais de 20 anos no Piauí; experiência e formação no magistério superior e como orientadora em monitorias, treinamentos e TCC. Participa na elaboração de artigos jurídicos publicados em revistas eletrônicas e organizações e em obras literárias coletivas com temáticas de direito digital, trabalhista, tributário e proteção de dados.

4. Personagens da LGPD na Relação de Trabalho

Nas últimas décadas, as relações de trabalho têm sido impactadas de uma forma acelerada pelo pelas decisões dos empregadores uso de tecnologias de informação e comunicação, dados biométricos, monitoramento dos trabalhadores através do GPS, ou aplicativos como wase, google maps , instalados em celulares corporativos e de uso dos colaboradores ou até a realização de exames médicos no processo seletivo ou para manutenção do emprego, a novidade é que além dessa transformação digital do trabalho, a forma de tratamento de dados pessoais pelos empregadores passaram a ter limites legais para garantia dos direitos de liberdade, privacidade e do livre desenvolvimento da personalidade dos empregados a partir da Lei Geral de Proteção de Dados, na fase pré-contratual, contratual e até pós-contratual.

É importante destacar que traçar limites de atuação dos agentes de tratamento de dados no direito do trabalho mesmo sem previsão na LGPD é possível pela inspiração no modelo europeu de proteção de dados. O direito comparado é utilizado como fonte supletiva segundo o artigo 8º da CLT e por isso se aplica o art. 88 do GDPR que permite a pactuação de normas específicas no ordenamento jurídico e nas convenções coletivas para o tratamento de dados pessoais no contexto laboral regulando o recrutamento, execução do contrato de trabalho e as obrigações trabalhistas durante e após a extinção do contrato de trabalho.

É difícil existir relações de trabalho sem tratamento de dados do empregado pelo empregador, inclusive, antes mesmo de se firmar o contrato de trabalho, na fase de seleção e recrutamento, há um manuseio das informações daquela pessoa, na fase que antecede o vínculo empregatício, porém a proteção de dados também é devida a esses candidatos na forma da lei.

4. Personagens da LGPD na Relação de Trabalho

Isto é, candidatos e empregados (titulares de dados) passam a ter mais um direito fundamental a ser tutelado pelo Estado, segundo o artigo 5º, inciso LXXIX ao artigo 5º, CF - "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" - e os empregadores (controladores) bem como os fornecedores e prestadores de serviços que façam uso também desses dados (operadores)passam a ter obrigações de segurança contra o mau uso deles e prevenção contra possíveis danos.

O cuidado com a pessoa, com os recursos humanos de uma organização, e com os seus dados na forma da lei (nome, idade, sexo, profissão, filiação, endereço, telefone, email, etc) vem acompanhado do dever de prestação de contas desse tratamento diante dos próprios titulares de dados e perante órgão público fiscalizador e sancionador (ANPD) que é intermediada pelo trabalho da pessoa física ou jurídica contratada para estabelecer uma comunicação entre os agentes de tratamento dos dados (controladores e operadores) e os titulares de dados e a autarquia federal Autoridade Nacional de Proteção de Dados que é chamada de encarregado de dados ou de Oficial de Proteção de Dados ou DPO.

Por isso, adaptando-se o artigo 5º da LGPD, os Controladores nas relações de trabalho são os empregadores que tomam as decisões sobre o tratamento dos dados pessoais de seus colaboradores e a sua finalidade enquanto que os Operadores nas relações de trabalho são terceiros que executam por ordem do empregador o processamento de dados pessoais em algumas situações singulares e; já os Controladores por equiparação são os empregados que tratam os dados pessoais de forma diversa da orientada pelo empregador/controlador.

4. Personagens da LGPD na Relação de Trabalho

No Direito do Trabalho pode-se dizer que os controladores, por exemplo, são os empregadores que têm o direito de acesso e tratamento dos dados pessoais de seus empregados e prestadores de serviços pessoa física e que devem tratar esses dados de forma adequada se quiser ter legitimidade para conservá-los em sua base de dados ou até compartilhar com terceiros.

Segundo o Guia Orientativo da ANPD não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta.

Já os terceiros chamados **operadores** são pessoas físicas ou jurídicas para quem é transmitido esses dados pessoais decorrentes da relação de trabalho. Eles precisam estar aderentes ao programa de conformidade à LGPD dos controladores de dados, para garantir a proteção de dados pessoais e prestar as informações necessárias aos interessados (controladores) que têm o dever de prestá-las ao titular de dados pessoais e à ANPD, sob pena de responder administrativamente, civilmente e até penalmente pelo mau uso dos dados pessoais que estão sob sua gestão de forma solidária.

4. Personagens da LGPD na Relação de Trabalho

Em contrapartida o empregado/titular de dados fica mais forte com a previsão na lei dos princípios do livre acesso a seus dados que o empregador detém; da transparência de todo o fluxo dos dados e da finalidade do tratamento do dado para um fim específico e o mínimo necessário, dentre outros princípios elencados no artigo 6º da lei, busca mais esclarecimentos e controle sobre os seus dados mesmo em mão de terceiros.

O agente de tratamento - empregador ou médico do trabalho -, por exemplo, devem ter legitimidade para coletar, armazenar, compartilhar e até conservar os dados pessoais do empregado/titular de dados - enquanto que o empregado pode resistir a um tratamento de seus dados por outrem se não tiver enquadrado nas hipóteses legais de tratamento.

Por isso, identificar os personagens da LGPD que estão presentes em todas as relações de trabalho tem sua relevância num programa de adequação, pois os agentes de tratamento de dados –Controladores e os Operadores –devem ser facilmente identificados para a devida apuração de responsabilidades; ou os titulares de dados devem ter clareza sobre os seus direitos e de como exercê-los de forma expressa (nos contratos de trabalho, em normas convencionais, códigos de conduta e políticas internas da organização). Ainda, a lei obriga a escolha de oficial de proteção de dados pessoa física ou pessoa jurídica (antigo encarregado de proteção de dados) que tenha conhecimentos e habilidades que o capacite atuar com autonomia sem qualquer conflito de interesses dentre seus colaboradores ou por terceirização desse serviço.

4. Personagens da LGPD na Relação de Trabalho

Essa tarefa de bem identificar os personagens da LGPD nem sempre foi fácil, até mesmo os tribunais já cometeram equívocos quanto aos controladores e operadores e por isso a ANPD já regulamentou essa matéria no Guia Orientativo sobre Agentes de Tratamento de Dados e Encarregado que além de estabelecer diretrizes não-vinculantes aos agentes de tratamento, explica quem pode exercer a função do controlador, do operador e do encarregado; com as definições legais; os respectivos regimes de responsabilidade.

Esse trabalho de conformidade com as novas normas de proteção de dados previstas na LGPD se aplica a todas as organizações que adotam tratamento de dados pessoais dos empregados, por isso os empregadores e os terceiros contratados estão obrigados a manter a segurança ao adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas com a adequação dos seus procedimentos internos e contratos de acordo e a prevenção contra a ocorrência da danos em virtude do tratamento de dados pessoais sob pena de sofrer sanções administrativas, salvo se as suas operações estejam previstas nas exceções do artigo 4º.

De fato, a apresentação dos personagens da LGPD nas relações de trabalho precede a atribuição de responsabilidade civil por culpa do controlador e do operador que causou dano ao titular de dados. Vale ressaltar que o operador só será responsabilizado solidariamente caso seja comprovado o dano causado ao empregado por sua culpa, no caso por exemplo, do banco/operador que faça a gestão da folha de pagamento do empregador não realizar a adequação à LGPD de seus processos ou tenha descumprido orientações de tratamento de dados do empregador/controlador

4. Personagens da LGPD na Relação de Trabalho

Conclui-se pelo exposto que a caracterização adequada de cada personagem e a responsabilidade de cada um desses personagens protetores de dados pessoais é necessário para estabelecer o polo ativo e passivo da reclamação trabalhista, a começar pela do controlador, que deve estipular os objetivos que justificam a realização do tratamento dos dados pessoais dentro das hipóteses legais.

Se o empregador viola o artigo 6º, I, da LGPD, um dos princípios que deve orientar as atividades de tratamento de dados pessoais - o princípio da finalidade - compreendido como a *"realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*", está passível de condenação indenizatória.

Alguns julgados no Brasil já condenou o controlador de dados pessoais (empregador) a reparação por danos morais, a exemplo (**Processo: 0010010-89.2021.5.03.0186** do TRT 3ª Região) por prática que viola esse princípio da LGPD; e até mesmo sujeito a pagamento de multa administrativa devido o empregador se recusar a apresentar informações do trabalhador ao sindicato que comprova legitimação de representação da categoria profissional, pois Lei Geral de Proteção de Dados (LGPD) não exime o empregador do dever de informar previsto em lei (Processo 0000876-17.2021.5.12.0015 - TRT-12ª Região).

Sumário

Capitulo 5

5. Consentimento na Relação de Trabalho

Por Valéria Ribeiro, Advogada

Advogada Fundadora e Titular do escritório Valeria Ribeiro – Sociedade de Advogados. Escritório no Metaverso. Especialista em Compliance pela KPMG. Auditora líder das Normas ISO 19.600:2014 e 37.001:2017 pela CBG Certificadora. Pós-graduada em Direito do Trabalho e Processo do Trabalho Pós Reforma Trabalhista pela EJUTRA. Mestre e Doutora em Ciências Jurídicas pela Universidade Autónoma de Lisboa. Técnica em Coletas e Processamento de Registro de Provas Digitais na forma Criptografada com a tecnologia Blockchain e ICP-Brasil.

5. Consentimento na Relação de Trabalho

Inicialmente pretende-se destacar que o trabalho ora proposto não objetiva esgotar o tema, mas apenas trazer reflexões, tomando como ponto de partida a necessidade da demonstração do consentimento sem vício, simulação e/ou fraude.

A tecnologia e a globalização trouxeram uma necessidade de regular os dados pessoais e os dados pessoais sensíveis que fomenta as atividades comerciais e econômicas.

Assim, no Brasil foi publicada a lei n. 13.709/2018, Lei Geral de Proteção de Dados, com finalidade de nortear o tratamento dos dados pessoais e dados pessoais sensíveis, a fim de possibilitar ao titular dos dados a acompanhar, ter ciência, consentir ou não, revogar o consentimento para o tratamento dos dados pessoais.

Nas relações trabalhistas há grande fluxo de dados pessoais decorrente do pré-contrato de trabalho, durante o contrato de trabalho e pós-contrato de trabalho. Há dados que são autorizados pela LGPD e há dados que necessitam o atendimento aos requisitos e princípios dispostos na LGPD. Considerando o desequilíbrio existente entre o empregado e empregador nas relações de trabalho, principalmente econômico, nem sempre o consentimento será revestido de legitimidade, bem como o legítimo interesse justificará o termo de consentimento fornecido.

5. Consentimento na Relação de Trabalho

IDentro das relações laborais, e empregador não só será o responsável pela realização das atividades de tratamento das informações de seus empregados, como terá o ônus de provar que o consentimento foi dado de forma livre e transparente. Por sua vez, os empregados possuem o direito de obter informações de como ocorrerá o tratamento e revogar o consentimento em qualquer época.

Dessa forma, pretende-se, através da análise doutrinária e prática, demonstrar que o consentimento e o legítimo interesse devem preencher os requisitos e princípios dispostos na LGPD, sob pena de ser considerado nulo. No mesmo liame, a não comprovação do consentimento livre.

5. Consentimento na Relação de Trabalho

DA PROTEÇÃO DOS DADOS PESSOAIS E A RELAÇÃO DE TRABALHO

O Regulamento Geral sobre a Proteção de Dados – RGPD dispõe no artigo 4º, n. 1, que dados pessoais são dados e/ou informações relativas a uma pessoa singular identificada ou identificável – titular dos dados-.

A Lei Geral de Proteção de Dados publicada em 13.709/18 regulamenta o tratamento dos dados pessoais no Brasil e aduz que a informação relacionada à pessoa natural identificada ou identificável são dados pessoais e tem por finalidade proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD em seus artigos 7º e 11º traz as bases legais para tratamento dos dados pessoais, sendo o artigo 11º os dados pessoais sensíveis.

A lei brasileira não contempla expressa disposição sobre o direito do trabalho, diversamente da GDPR – General Data Protection Regulation.

O que se observa que o Brasil adotou um conceito mais amplo para definir os dados pessoais para que fosse considerado todas as hipóteses de manuseio de dados, independente do meio utilizado, ou seja, físico ou digital.

5. Consentimento na Relação de Trabalho

Se observa pela leitura do inciso I do artigo 5º da LGPD que são considerados dados pessoais o nome, RG, CPF, estado civil, religião, profissão e gênero, dentre outros.

No tocante aos dados pessoais sensíveis, a LGPD, conceitua como sendo uma informação "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".

O inciso X do artigo 5º da LGPD aduz a definição de tratamento dos dados pessoais e de dados pessoais sensíveis como sendo:

"(...) toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (...)."

5. Consentimento na Relação de Trabalho

O artigo 7º aponta a base legal para o tratamento de dados, sendo o rol taxativo e que corresponde às 10 (dez) bases legais que autorizam o tratamento de dados pessoais dos titulares que são: consentimento; cumprimento de obrigação legal; execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n. 9.307/96; para a proteção da vida ou da incolumidade física do titular ou de terceiros; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; 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 ou para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;

O consentimento como base legal para o tratamento dos dados pessoais no âmbito das relações trabalhistas trouxe um debate acadêmico, haja vista a existente subordinação jurídica entre empregador e empregado.

5. Consentimento na Relação de Trabalho

O consentimento deve ser livre, informada, de forma inequívoca e com a transparência da finalidade da coleta e uso dos dados. Ausente um dos requisitos, a manifestação de vontade e consequentemente o consentimento será considerado viciado e nulo. O consentimento deve ser coletado para uma finalidade determinada, o que os consentimentos genéricos também serão considerados nulos.

Dentro desse contexto, passamos a analisar a aplicabilidade do consentimento nas relações trabalhistas.

APLICABILIDADE DO CONSENTIMENTO NAS RELAÇÕES TRABALHISTAS

O consentimento está disposto no artigo 7º, inciso I, da LGPD, no qual destaca que a vontade deve ser livre, informada, inequívoca e com finalidade. Assim, o titular dos dados concorda com o tratamento dos dados para uma finalidade específica, sob pena de ser considerada nula.

O controlador dos dados possui o ônus da prova de que o consentimento preenche todos os requisitos, quais sejam: vontade livre, inequívoca informada e com finalidade anunciada. (artigo 7º, § 2º da LGPD).

5. Consentimento na Relação de Trabalho

Segundo Maria Picolo, (2021) a proteção dos dados está relacionada ao direito à autodeterminação informativa, no qual fundamenta as atividades de processamento das informações no ordenamento jurídico brasileiro na forma do inciso II do artigo 2º da LGPD. E que é compreendido como forma de garantir o controle do titular sobre suas informações, mesmo que o tratamento de seus dados seja válido ou legítimo

Por essa razão o consentimento deve ser sempre coletado para uma finalidade específica, para que seja possível ao titular dos dados emitir autorizações de forma consciente e acompanhar sobre o que deve ou não ser disponibilizado e utilizado.

É assegurado ao titular dos dados o poder de revogar o consentimento.

A LGPD tem impacto significativo nas relações trabalhistas, posto que visa disciplinar e resgatar o equilíbrio dentro das relações entre o empregador e o empregado.

Decerto que existe um fluxo considerável de dados pessoais no tocante ao contrato de trabalho como filiação em sindicato, autorização de descontos, controle de jornada de trabalho, entre outras.

5. Consentimento na Relação de Trabalho

Nas relações de trabalho, o controlador corresponde ao empregador, no qual, realizará atividades de processamento dos dados pessoais do empregado em seu nome. E, por consequência, esse terá o ônus de provar que o consentimento preenche os requisitos para a sua validade.

Nas relações de trabalho há a subordinação do empregado para com o empregador e a superioridade econômica deste sobre aquele, tem como consequência desequilíbrio nas relações de trabalho, e por este fato, o consentimento é visto como uma parte sensível a privacidade, liberdade pessoal e aos direitos de personalidade dos trabalhadores titulares de dados.

O artigo 8º da LGPD aduz que o consentimento seja fornecido por escrito ou outro meio que demonstre a manifestação de vontade do titular, ou seja, não é necessariamente ser por escrito. No entanto, o inciso XII do artigo 5º do mesmo diploma legal, segue o mesmo entendimento do RGPD europeu, no qual impõe que a vontade seja explícita.

O Código Civil ao tratar do defeito dos negócios jurídicos trata do consentimento, no qual prevê expressamente que a manifestação de vontade do indivíduo de forma seja “livre e consciente” e sem uma das hipóteses de vício na forma prevista nos artigos 138 a 165 do CC/2002.

5. Consentimento na Relação de Trabalho

Na hipótese da ocorrência de vício na declaração de vontade, estará caracterizado o “vício de consentimento” o que tornará o negócio jurídico anulável. Dentro desse contexto, a LGPD faz remissão expressa à vedação do tratamento dos dados mediante vício do consentimento, à luz dos defeitos do negócio jurídico previsto no Código Civil brasileiro.

A manifestação de vontade inequívoca e a especificidade são um dos requisitos que tem o condão de impedir que a vontade do titular seja realizada de maneira generalista.

Os requisitos são cumulativos.

Considerando que o consentimento previsto pelo inciso I do artigo 7º da LGPD, não trata das relações de emprego, o que traz uma insegurança jurídica na aplicabilidade do consentimento nestas relações, principalmente pelo tratamento dos dados pessoais englobar todas as fases da relação de trabalho, quer do processo seletivo, da formalização do contrato de trabalho até após o término da rescisão do contrato de trabalho.

Temos assim que o tratamento dos dados pessoais está presente nas fases pré-contratual, contratual e pós-contratual.

5. Consentimento na Relação de Trabalho

Alcântara (2021, 0.17) destaca que a expressão “livre” pressupõe que a opção do titular dos dados pessoais foi legítima. Entretanto, esta suposição suscita dúvidas sobre sua legitimidade no contexto de uma relação trabalhista, posto que essa é caracterizada pelo desequilíbrio de poder e, em regra, pela dependência econômica. Nesse cenário, as alegações de que o empregado não teve legítima escolha deverão ser frequentes, sob pretexto de que o consentimento foi utilizado como moeda de troca para a manutenção do vínculo empregatício.

O contrato de trabalho é pactuado por manifestação livre das partes, no entanto, o desequilíbrio entre as partes, empregado e empregador, o consentimento do empregado fundado em legítimo para o tratamento dos dados será revestido de presunção relativa da manifestação de vontade, em virtude da dificuldade de o empregado recusar a fornecer o consentimento sem perder a vaga de emprego.

O termo de consentimento não tem o mesmo tratamento que o contrato de adesão. O termo de consentimento deve ser autônomo ao contrato de trabalho.

O empregador pode utilizar da base leal do consentimento para fundamentar o tratamento dos dados pessoais, no entanto, deverá demonstrar que o consentimento foi manifestado de forma livre, sem coação, bem como adesão ao termo como requisito para o preenchimento da vaga, bem como a finalidade da utilização dos dados pessoais.

5. Consentimento na Relação de Trabalho

Caso o empregador utilize o consentimento no próprio contrato de trabalho, deverá constar a cláusula respectiva de forma destacada das demais cláusulas, não sendo dispensável o preenchimento de todos os requisitos para o tratamento dos dados.

Decerto que algumas atividades de tratamento de dados pessoais dentro do contexto das relações de trabalho estão autorizadas o tratamento por parte da LGPD, podendo-se citar a admissão ou desligamento, normas de segurança do trabalho, exames admissionais, periódicos, demissionais, treinamento e capacitação, comunicação à Previdência Social quanto a acidente do trabalho, CAGED, RAIS, E-social.

Entretanto, isso não significa que o empregador poderá realizar o tratamento dos seus dados de forma livre e sem o termo de consentimento com a finalidade.

Outro fundamento que o empregador pode utilizar para o tratamento dos dados pessoais é o legítimo interesse, a exceção é sobre direitos, interesses e liberdades fundamentais do trabalhador.

5. Consentimento na Relação de Trabalho

O legítimo interesse se justifica para as hipóteses da existência de interesse do controlador ou de terceiros, a existência de finalidades legítimas e a proteção dos direitos do titular. O controlador deverá verificar se seu interesse é legítimo e legal, ou seja, finalidade legítima sem contrariar leis esparsas e legislação infralegal e que respeite as leis normas infralegais aplicáveis a situação específica, o que se pode citar a hipótese de violação o exame de gravidez ou HIV em situações de trabalho, para fins de exames admissionais.

O legítimo interesse não justifica a validade do consentimento.

CONCLUSÃO

A LGPD prevê inúmeras bases legais que autorizam o tratamento dos dados pessoais, sendo o consentimento e o legítimo interesse algumas delas. O empregador deverá observar as hipóteses expressas de cabimento e os requisitos previstos no inciso XII do artigo 5º da LGPD para o tratamento dos dados pessoais do empregado. Deve ser avaliado se atendido os requisitos de validade do consentimento e finalidade para verificar a base legal ao tratamento dos dados, haja vista que o não atendimento caracterizará vício na manifestação de vontade do titular, no caso o empregado, tornando nulo os efeitos de autorizações concedidas para o correspondente tratamento dos dados.

5. Consentimento na Relação de Trabalho

Ressalva posições diametralmente opostos, a desigualdade econômica, e por consequência, de poder e a subordinação jurídica existente na relação laboral é impedimento ao reconhecimento pleno da validade do consentimento preenchido os requisitos exigidos para sua validade. Ressaltando que o legítimo interesse não é fundamento para justificar o tratamento dos dados.

O consentimento realizado de forma objetiva e transparente, especificando a finalidade, com opção de recusa no fornecimento pelo empregado, a exceção dos dados baseados no legítimo interesse (para fins de E-social, FGTS, INSS, etc), que irá validar o termo de consentimento nas relações laborais.

O empregador ao realizar o tratamento dos dados pessoais do empregado deverá seguir os princípios estipulados no artigo 6º da LGPD, quais sejam: finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A relação laboral e o tratamento dos dados pessoais continua e continuará sendo um dos pontos de maior sensibilidade da proteção de dados.

Sumário

Capitulos 6 e 7

Por Maria Santos, Advogada

Advogada e Data Protection Officer.
Atuando na Advocacia Chizzolini
Certificada DPO ITCERTS. Membro da Diretoria Associação Nacional dos Advogados de Direito Digital - ANADD.
Responsável Comitê Relações Trabalhistas no Digital,
Especialista em Direito Empresarial e Direito do Trabalho, atuando a mais de 30 anos no Mercado Corporativo. Pós-Graduanda em Direito Digital pela EBRADI
MBA e Pós Graduação, Controladoria, Auditoria e Compliance pela FMU - Pós Graduação em Direto Processual Trabalho -Anhembi Morumbi

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

6. Tratamento de dados após o término do contrato de trabalho

O término do tratamento de dados tem uma importância digna de destaque porque é preciso compreender até que momento seria possível continuar o tratamento dos dados pessoais para fazer a sua devida gestão.

Assim prescreve o art. 15 da Lei Geral Proteção de Dados nos seguintes termos:

> ***Art. 15.*** *O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:*
>
> *I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;*
> *II - fim do período de tratamento;*
> *III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou*
> *IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.*

6. Tratamento de dados após o término do contrato de trabalho

O art. 16 da Lei Geral Proteção de Dados estipula a necessidade de eliminação dos dados pessoais após as causas do art. 15, mas autoriza a sua conservação em quatro hipóteses:

> ***I - cumprimento de obrigação legal ou regulatória pelo controlador;***
> ***II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;***
> ***III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou***
> ***IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.***

O inciso I, é claro quanto a devida permanência dos dados durante o prazo prescricional principalmente pela possibilidade de defesa em interposição jurídica, a fim de instrução judicial.

6. Tratamento de dados após o término do contrato de trabalho

Observe-se que o prazo prescricional trabalhista de dois anos após fim do contrato ou dos cinco últimos anos do ajuizamento de uma ação (art. 7º, XXIX, da CF/88), ou outrem que a Lei estabeleça nos casos especificas.

Concluímos, portanto, que nas relações de trabalho, a conservação dos dados pessoais dos colaboradores com a finalidade de cumprir uma obrigação legal ou regulatória pela empresa ou para seu uso exclusivo, neste último caso desde que os dados sejam anonimizados. Dado anonimizado é o dado que não identifica nem torna identificável uma pessoa natural, resultando na inaplicabilidade da LGPD.

A anonimização é resultado de um procedimento para que um dado pessoal perca, de maneira irreversível, a possibilidade de identificar uma pessoa natural.

Frisemos que, os dados pessoais coletados somente podem ser utilizados para uma nova finalidade se ela for compatível com a finalidade original, ou deverá adequá-la a outra base legal, ou solicitar novo consentimento ou a necessidade de cumprimento de uma obrigação legal ou o legítimo interesse.

As empresas devem criar políticas de segurança dentre elas a de eliminação de dados pessoais, nessa situação estarão de acordo com a lei, bem como evitando custos excessivo com armazenamento, bem como gerenciamento de dados pessoais, além de estarem minimizando riscos de roubo de informações.

7. Descarte dos Dados

Eliminação dos Dados

Caso não se aplique nenhuma das hipóteses mencionadas, deve ocorrer a eliminação.

A eliminação refere-se a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. Inclui-se os dados de backups, múltiplos acessos, servidores diferentes, armazenamento em nuvem, entre outros.

Esses dados serão eliminados segundo os limites técnicos encontrados, situação esta que gera um importante debate acerca da eliminação completa dos dados, é fundamental garantir que os dados excluídos não possam ser recuperados por cibercriminosos.

Nessa situação, o responsável pelo tratamento deverá informar os outros agentes com os quais tenha realizado o uso compartilhado de dados para que repitam o procedimento de eliminação dos dados. Ele só ficará isento disso caso comprove que a comunicação é impossível ou que exige um esforço desproporcional.

7. Descarte dos Dados

Neste caso, deverá o controlador do dado estabelecer mecanismos de controles eficazes para ajustar seus procedimentos internos e eliminar completamente os dados assim que os prazos legais se extingam.

Havendo situação de finalização do uso de dados ao titular, seja por determinação legal, seja por solicitação, do próprio titular a teor do artigo 4 da LGPD.

Contudo como mencionado nas relações trabalhistas, há obrigações de guarda de documentos que decorrem de imposição legal, e isso pode acarretar o afastamento da solicitação do titular do direito, e tais situações devem ser mapeadas para que a decisão correta seja tomada.

Considerando o efetivo descarte, e especial atenção ao descarte de documentos físicos, haja vista que o histórico de utilização de "cópias" de documentos para rascunho, é mais corriqueiro que imaginamos

Recomenda-se utilizar triturador de papel a fim de destruir o documento por completo, A fragmentação garante que as informações sigilosas não sejam vazadas.

Informações, por meios digitais em Nuvem devem ser excluídos e e os HDs físicos, formatados para garantir que os dados não sejam mais acessados, mas é preciso criar uma política clara para isso e cumpri-la.

Sumário

Capitulo 8

8. MAPEAMENTO

Por Renata Proximo, Advogada

Renata Proximo - Advogada Empresarial, especializada em compliance, consultoria e auditoria trabalhista estratégica e relações trabalhistas e sindicais. Especializada em Privacidade e Proteção de Dados (GDPR e LGPD), atuação como DPO as a Service. Diretora do Comitê Mulher, Inclusão e Diversidade da ANADD. Membro do Comitê de Relações Trabalhistas no Digital - ANADD. Membro efetivo das Comissões de Direito Digital e Privacidade e Proteção de Dados da OAB Campinas. - Instagram: @renataproximo_consultoria - Linkedin: https://www.linkedin.com/in/renata-proximo/

8. Mapeamento

Antes de falar sobre mapeamento de dados nas relações de trabalho, precisamos entender, o que é mapeamento de dados.

Também conhecido como Data Mapping ou Data Flow, o mapeamento de dados é documento essencial para implantação do programa de proteção e privacidade de dados. Sendo uma avaliação para entender como é o fluxo de tratamento de dados dentro de uma empresa.

Devendo ser realizado no início da implantação e sempre renovado, já que os processos e procedimentos mudam com frequência e essas informações também farão parte do RIP (Relatório de Impacto).

Toda empresa é um organismo vivo, que sofre mudanças, a depender de quem trata do dado, inclusive do empregado em si, responsável pelo tratamento. Sendo assim, o mapeamento deve fazer parte de uma constante manutenção de informações, já que influencia em toda a cadeia do programa de proteção de dados, governança e compliance.

8. Mapeamento

Para começar, é importante observar o que diz o artigo 5º da LGPD, que considera tratamento de dados, as operações como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avalição ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim, é de suma importância para toda empresa, conhecer esse fluxo no tratamento de dados, e mapeá-los de forma a desenvolver estratégias de controle de segurança.

O objetivo do mapeamento é diagnosticar a forma como a empresa trata a privacidade e a segurança das informações obtidas de seus empregados, com o objetivo de cumprir com as exigências do artigo 37 da LGPD, que estipula que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais.

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

8. Mapeamento

Para exemplificas, segue algumas análises feitas no mapeamento:

Na fase pré-contratual, podemos mapear:

- Guarda de currículo – consentimento do candidato e estipulação de prazo para guarda.
- Ficha de contratação – somente solicitar dados relevantes para a seleção, evitando, por exemplo, número de CTPS, RG, CPF, nome dos filhos, cônjuge etc.

Na fase contratual e registro, podemos mapear:

- Solicitação de documentos – somente o que é obrigatório para registro, conforme regras do e-Social e órgãos públicos, forma de recebimento, arquivo e compartilhamento.
- Exames admissionais – Verificar quais informações são compartilhadas com o médico do trabalho e, se terceirizado, se este profissional também está em processo de adequação ao programa de privacidade e proteção de dados.
- Identificação de dados sensíveis tratados, sua necessidade e consentimento correspondente.

8. Mapeamento

Na fase pós-contratual, podemos mapear:

- Forma de armazenamento das informações contratuais que contenham dados.

- Exclusão/interrupção de compartilhamentos necessários na constância do contrato.

- Prazo e forma de descarte dos dados já tratados.

Lembrando que aqui trazemos os exemplos e diretrizes básicas do mapeamento, que deve ser desenvolvido juntamente com as áreas de Recursos Humanos, Departamento Pessoal e Gestão de Pessoas como um todo.

8. Mapeamento

Ainda, quando falamos em área de Gestão, devemos observar que os coordenadores, supervisores, gerentes de área, também participam do tratamento de dados de empregados subordinados, e devem ser envolvidos no mapeamento dos dados nas relações de trabalho.

O mapeamento além de ser um trabalho constante é um trabalho que deve ser realizado em conjunto com diversas áreas da empresa, para coleta de informações fidedignas de tratamento de dados, que se tornam valiosas no momento de avaliar a segurança.

Sumário

Capitulo 9 e 10

Por Maria Santos, Advogada

Advogada e Data Protection Officer.
Atuando na Advocacia Chizzolini
Certificada DPO ITCERTS. Membro da Diretoria Associação Nacional dos Advogados de Direito Digital - ANADD.
Responsável Comitê Relações Trabalhistas no Digital,
Especialista em Direito Empresarial e Direito do Trabalho, atuando a mais de 30 anos no Mercado Corporativo. Pós-Graduanda em Direito Digital pela EBRADI
MBA e Pós Graduação, Controladoria, Auditoria e Compliance pela FMU - Pós Graduação em Direto Processual Trabalho -Anhembi Morumbi

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

9. Bases legais para tratamento de dados nas relações de Trabalho

A Lei Geral de Proteção de dados, em seu ***artigo 7º***. define as dez bases legais para o a utilização dos dados pessoais de maneira compatível a atender aos princípios da própria lei.

Para cada finalidade atribuída ao uso de um dado pessoal, o controlador, ira empregador deve indicar uma base legal como justificativa.

Segundo a Lei temos as seguintes bases legais:

9. Bases legais para tratamento de dados nas relações de Trabalho

Como vimos o tratamento de dados pessoais de colaboradores, o empregador deverá justificar o tratamento daquele dado com base em uma hipótese prevista no ***art. 7º. na LGPD***. Essas hipóteses podem ser de vários tipos: para cumprir uma exigência legal ou regulatória, para executar um contrato, para utilizar judicialmente, entre outras.

Havendo a utilização de dados pessoais sensíveis, as possibilidades de justificar o tratamento são reduzidas – e, se a justificativa for o consentimento, ele terá de ser concedido de forma destacada, transparente , ressaltando a necessidade de temporalidade também expressa.

Como restará demonstrado o tratamento dos dados, na relação de trabalho, decorre primordialmente de obrigação legal ou para execução do contrato.

Passamos a tecer alguns comentários acerca das principais, bases legais utilizadas pelos dados pessoais que trafegam no departamento pessoal e recursos humanos. com especial atenção ao tratamento de dados pessoais sensíveis, como a biometria.

Reforçamos a importância de se ter em mente os princípios advindos do ***art. 5 da LGPD,*** o qual serão balizadores na utilização dos dados capaz de justificar a coleta de dados dos empregados de forma irrestrita: os dados coletados devem ser necessários e adequados à finalidade da execução do contrato.

9. Bases legais para tratamento de dados nas relações de Trabalho

Lembrando sempre de considerar o princípio da minimização dos dados, que pode ser extraído dos princípios da adequação, necessidade e finalidade, previstos no artigo 6º da Lei.

Como sabemos, no contexto da relação de emprego, inevitavelmente serão tratados dados pessoais sensíveis dos empregados, incluindo dados de saúde, filiação a sindicato e dados biométricos.

Consentimento do titular:

Essa base legal demanda certo cuidado no âmbito do Direito do Trabalho, como já sobejamente demonstrado no capítulo X.
obrigação legal ou regulatória

Para o cumprimento de obrigação legal ou regulatória pelo empregador/controlador: em alguns casos, o agente trata determinados dados não por uma vontade própria, mas sim porque existe uma lei ou uma normativa própria do seu setor que o impõe. Por exemplo, o empregador é obrigado pelo artigo 911A da CLT a recolher o INSS dos empregados

9. Bases legais para tratamento de dados nas relações de Trabalho

Lembrando sempre de considerar o princípio da minimização dos dados, que pode ser extraído dos princípios da adequação, necessidade e finalidade, previstos no artigo 6º da Lei.

Como sabemos, no contexto da relação de emprego, inevitavelmente serão tratados dados pessoais sensíveis dos empregados, incluindo dados de saúde, filiação a sindicato e dados biométricos.

Consentimento do titular:

Essa base legal demanda certo cuidado no âmbito do Direito do Trabalho, como já sobejamente demonstrado no capítulo X.

Obrigação legal ou regulatória

Para o cumprimento de obrigação legal ou regulatória pelo empregador/controlador: em alguns casos, o agente trata determinados dados não por uma vontade própria, mas sim porque existe uma lei ou uma normativa própria do seu setor que o impõe. Por exemplo, o empregador é obrigado pelo artigo 911A da CLT a recolher o INSS dos empregados

9. Bases legais para tratamento de dados nas relações de Trabalho

A LGPD permite o tratamento de dados quando esse for necessário para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária ***(art. 7º, VIII),***

Observe que, para os casos de dados pessoais sensíveis ***(art. 11, "f")***, o controlador/empregador utilizasse por vezes de um médico do trabalho (saúde ocupacional), que realiza diversos exames, como os admissionais, demissionais, de retorno de função.

Ou situações em que a empresa proporciona, aos seus colaboradores atendimentos terapêuticos, de massagistas etc, no interior das empresas, proporcionando de alguma forma bem-estar aos colaboradores, mas que notadamente fazem registros de dados sensíveis.

Temos ainda a atuação da equipe de segurança do trabalho que elabora o Programa de Controle Médico de Saúde Ocupacional (PCMSO), conforme a NR 7.

Importante comentarmos acerca do tratamento dos dados biométricos podemos utilizar como base legal de ***"cumprimento de uma obrigação legal ou regulamentar"***, visto que, as empresas com mais de 20 funcionários são obrigadas a controlar o horário de trabalho de seus funcionários, conforme previsão do parágrafo 2º do artigo 74 da Consolidação das Leis Trabalhistas – CLT.

9. Bases legais para tratamento de dados nas relações de Trabalho

A Legislação vigente é ampla quando se fala em tratamentos de dados pessoais no âmbito trabalhista , considerando que estar “de acordo” com a Lei Geral de Proteção de Dados” não significa cumpri-la, apenas, mas cumprir também outras normas setoriais, por exemplo: a Constituição Federal, a Consolidação das Leis Trabalhistas, as Convenções da Organização Internacional do Trabalho, as Normas Regulamentadoras expedidas pelas autoridades competentes, entre outras.

Especificamente na Consolidação das Leis Trabalhistas, alguns artigos tratam de documentos dos empregados, veja:

“[...] existem disposições legais que estabelecem a necessidade ou a possibilidade de lidar com as informações do empregado, tais como: as anotações na CTPS (art. 29 da CLT), os livros de registro de empregados (art. 41 da CLT), os exames médicos (art. 168 da CLT), a obrigatoriedade de notificação de doenças profissionais (art. 169 da CLT), e a obrigatoriedade de entrega do Documento de Informações Sociais (art. 360 da CLT). Recente alteração do art. 6.º da CLT reconhece o uso de meios telemáticos e informatizados para o exercício do poder diretivo do empregador (Lei n.º 12.551, de 15 de dezembro de 2011), mas não estabelece as condições de seu exercício, nem seus limites.”14

9. Bases legais para tratamento de dados nas relações de Trabalho

Temos ainda, a Portaria 1.510, emitida pelo Ministério do Trabalho e Emprego em 2009, denominada “Lei do Ponto Eletrônico”, regulamenta o sistema eletrônico utilizado para o controle do horário de trabalho e, devido às exigências inerentes a este controle, é considerado mais seguro e menos suscetível a fraudes.

E finalmente neste aspecto temos a Portaria 373, também emitida pelo Ministério do Trabalho e Emprego, em 2011, permite que as empresas utilizem sistemas alternativos de controle de jornada de trabalho autorizados por uma Convenção Coletiva de Trabalho.

Execução de contrato

Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular.

Tendo em vista que a relação de trabalho está definida dentro dos termos do contrato individual do trabalho, qualquer processo com tratamento de dados que decorra deste pacto está justificado por ele.

9. Bases legais para tratamento de dados nas relações de Trabalho

Importante, trazermos a pauta uma situação singular, os contratos de trabalho são considerados verdadeiros “contratos de adesão” afinal, considerado a “ parte vulnerável da relação”, os empregados não possuem autonomia e liberdade para discutir, rever e modificar as cláusulas contratuais que definem as condições em que os serviços serão prestados, notadamente quando estão sendo contratados, em algumas situações sequer sabem o que estão assinando.

Nesse sentido o colaborador é hipossuficiente no contexto da relação de emprego, as normas trabalhistas objetivam proteger o empregado, de forma a reduzir a desigualdade fática no campo jurídico.

Exercício regular de direitos em processo judicial

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral: o empregador/controlador tem a prerrogativa legal da LGPD para armazenar dados que possam resguardá-lo no caso de uma ação judicial.

9. Bases legais para tratamento de dados nas relações de Trabalho

PRAZO PRESCRICIONAL DOS CRÉDITOS TRABALHISTAS

Prescrição é a perda do direito de ação ocasionada pelo transcurso do tempo, em razão de seu titular não o ter exercido. Portanto, haverá prescrição quando, por inércia do titular do direito de ação (trabalhador), este deixar de escoar o prazo fixado em lei, em exercê-lo.

A prescrição está prevista no art. 7º, inciso XXIX da Constituição Federal:

"Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social:

.....

XXIX - ação, quanto aos créditos resultantes das relações de trabalho, com prazo prescricional de cinco anos para os trabalhadores urbanos e rurais, até o limite de dois anos após a extinção do contrato de trabalho;"

O prazo prescricional foi estabelecido pela Emenda Constitucional - EC 28/2000, equiparando os trabalhadores urbanos e rurais no que concerne à prescrição de créditos resultantes das relações de trabalho.

9. Bases legais para tratamento de dados nas relações de Trabalho

TRABALHADOR RURAL

Para o trabalhador rural, o prazo prescricional antes da EC 28/2000 era de 2 (dois) anos após a extinção do contrato, retroagindo seus créditos e direitos até o começo do pacto laboral, ou seja, poderiam reclamar os créditos referentes a todo o período lesado.

A partir da publicação da EC, só poderiam reclamar os últimos cinco anos trabalhados, até o limite de dois anos da extinção do contrato, sendo que esta última deve prevalecer sobre a anterior, tendo em vista que a mudança foi ditada pelo Poder Público e abrange todos os contratos de trabalho e relações trabalhistas.

9. Bases legais para tratamento de dados nas relações de Trabalho

DO PRAZO PRESCRICIONAL

O prazo prescricional atual para o empregado urbano e rural exigirem seus créditos e direitos trabalhistas derivados das relações de trabalho é de 5 (cinco) anos, até o limite de 2 (dois) anos após a extinção do contrato.

Conforme dispõe a Súmula 362 do TST, o prazo prescricional para reclamação do FGTS deve ser observado os dois critérios abaixo:

FGTS. PRESCRIÇÃO (nova redação) - Res. 198/2015, republicada em razão de erro material – DEJT divulgado em 12, 15 e 16.06.2015

I – Para os casos em que a ciência da lesão ocorreu a partir de 13.11.2014, é quinquenal a prescrição do direito de reclamar contra o não-recolhimento de contribuição para o FGTS, observado o prazo de dois anos após o término do contrato;

II – Para os casos em que o prazo prescricional já estava em curso em 13.11.2014, aplica-se o prazo prescricional que se consumar primeiro: trinta anos, contados do termo inicial, ou cinco anos, a partir de 13.11.2014.

9. Bases legais para tratamento de dados nas relações de Trabalho

Interesse legítimo

Quando necessário para atender aos interesses legítimos do controlador empregador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

A LGPD igualmente estabelece parâmetros, para a utilização do interesse legítimo como requisito autorizativo para o tratamento de dados sem o consentimento do titular, conforme se depreende de seu artigo 10:

> ***Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:***
> ***I - apoio e promoção de atividades do controlador; e***
> ***II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.***
> ***§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.***
> ***§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.***
> ***§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.***

9. Bases legais para tratamento de dados nas relações de Trabalho

Os dispositivos da LGPD que tratam dos interesses legítimos ***(arts. 7º, IX, e 10)*** possibilitam a transposição de parte do mencionado teste para avaliar a existência de legítimo interesse no caso concreto.

O Art. 10, em seu caput e inciso I, traz a necessidade de avaliação da existência de uma finalidade legítima e de uma situação especifica, diante disso, percebe-se a importância e o cuidado de classificar o tratamento de dados, pelo legitimo interesse.

Trazemos situação exemplificativa extraído do livro Thomson Reuters ProView - Reflexos da LGPD no Direito e no Processo do Trabalho - Ed. 2022

> ***Visualizemos o caso em que o empregador, objetivando garantir segurança aos seus funcionários e à empresa, decide instalar sistema de câmeras em ambiente do estabelecimento que abriga grandes valores financeiros. A nosso ver, não há se falar em tenham suas imagens captadas, filmadas, recomendando-se tão somente que sejam notificados da existência do dispositivo e da não utilização das imagens para fins diversos daqueles legitimamente aduzidos. Citemos, também, o caso de determinado empregado que presta serviços à distância, sendo monitorado através da geolocalização. Pensamos não haver qualquer tipo de violação de dados ou mesmo do direito à privacidade, desde que sejam respeitados os princípios da razoabilidade e da proporcionalidade quando da operacionalização do serviço.***

9. Bases legais para tratamento de dados nas relações de Trabalho

Destaque-se que a Lei nº 13.709/2018 expressamente dispõe que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil, poderá requerer ao controlador (empregador) um relatório de impacto à proteção de dados pessoais (RIPD) quando o tratamento realizado pela empresa for baseado no legítimo interesse do empregador. Trata-se de documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, conforme reza a literalidade do art. 5º, XVII, da LGPD.

Outro exemplo, do tratamento, considerando o legitimo interesse temos o monitoramento de redes sociais:

O GT29 aponta exemplo concreto sobre o tema: "Um empregador monitoriza os perfis de antigos empregados no LinkedIn que estão envolvidos durante a vigência das cláusulas de não concorrência. A finalidade desta monitorização consiste em controlar a conformidade com essas cláusulas. A monitorização é limitada a estes antigos empregados. Enquanto o empregador puder provar que tal monitorização é necessária para proteger os seus interesses legítimos, que não existem outros meios menos invasivos disponíveis e que os antigos empregados tenham sido devidamente informados da extensão da observação regular das suas comunicações públicas, o empregador pode invocar o fundamento jurídico do art. 7.º, alínea f), da Diretiva" (cfr. ponto 5.2 do Parecer 2/2017 do GT29).

9. Bases legais para tratamento de dados nas relações de Trabalho

Em entendimento particular, tenho a ressaltar três pontos que entendo ser de sua importância :

1º. A utilização de bases legais como o consentimento e o legítimo interesse deve ser utilizada como última opção, ante as suas peculiaridades na esfera legal trabalhista.

2º. Substitua cláusulas especificas de consentimento nos contratos de trabalho, para documentos específicos em apartado, isso garante a transparência, e legitimidade do documento.

3º. Entendo não ser viável, para um mesmo tratamento, indicar duas ou mais bases legais, posto isso cabe ao empregador identificar cuidadosamente as bases legais que autorizam o tratamento e, havendo mais de uma hipótese, optar pela mais segura, específica e concreta.

9. Bases legais para tratamento de dados nas relações de Trabalho

As bases legais e O tratamento de dados pessoais sensíveis

A LGPD , traz em seu artigo 11, as bases legais pertinentes aos dados sensíveis:

> ***Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas***
> ***seguintes hipóteses:***
> ***I – quando o titular ou seu responsável legal consentir, de forma específica e***
> ***destacada, para finalidades específicas;***
> ***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 n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro;***

9. Bases legais para tratamento de dados nas relações de Trabalho

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

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. 9° desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1° Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2° Nos casos de aplicação do disposto nas alíneas a e b do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3° A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4° É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

9. Bases legais para tratamento de dados nas relações de Trabalho

Os empregadores deverão analisar todos os departamentos que possuem acesso aos dados de colaboradores e prestadores de serviços, a fim de dar maior atenção a utilização dos dados sensíveis.

Quando da captação e dados, deve-se evitar a formulação de exigências relacionadas ao gênero, estado civil, existência de filhos, pretensão de contrair matrimonio, religião, doenças prévias, patrimônio genético, antecedentes criminais e investigação de vida financeira, essas devem ser subtraídas se efetivamente necessárias.

Quando falamos de bases legais para tratamentos de dados sensíveis, importante ressaltamos que excluem-se ao tratamento de dados sensíveis as seguintes bases legais: *a execução de contrato, com base em interesses legítimos e para a proteção ao crédito*, permanecendo as demais possibilidades.

E nesse sentido me reporto as argumentações expostas anteriormente às demais bases legais.

10. Compliance e Governança

Em um sentido geral, compliance é seguir um conjunto de regras

A LGPD preconiza que as atividades de tratamento de dados pessoais deverão observar as boas práticas e padrões de governança em privacidade de dados e segurança da informação

10. Compliance e Governança

Os empregadores na figura de agente de tratamento são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, para isso segundo previsão da própria LGPD, caput do art. 46, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

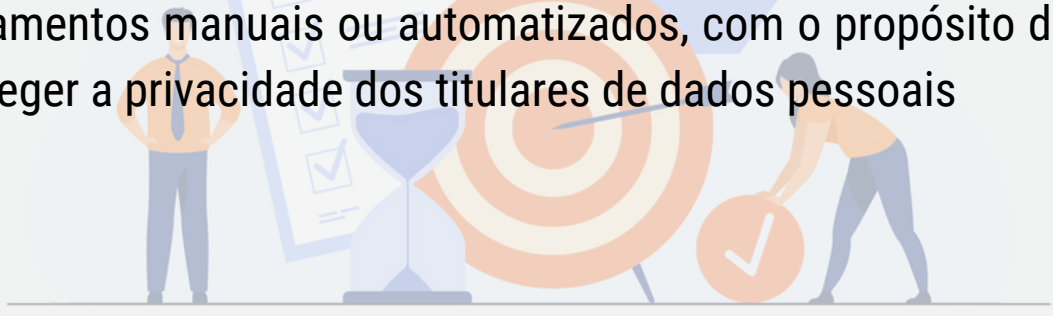
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

10. Compliance e Governança

O artigo 50 da LGPD estabelece que os controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização.

> ***Art. 50, LGPD. "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...]."***

O Programa de Governança em Privacidade - PGP, deve definir diretrizes para a gestão da segurança do tratamento dos dados pessoais, nos meios físicos e digitais, em tratamentos manuais ou automatizados, com o propósito de proteger a privacidade dos titulares de dados pessoais



10. Compliance e Governança

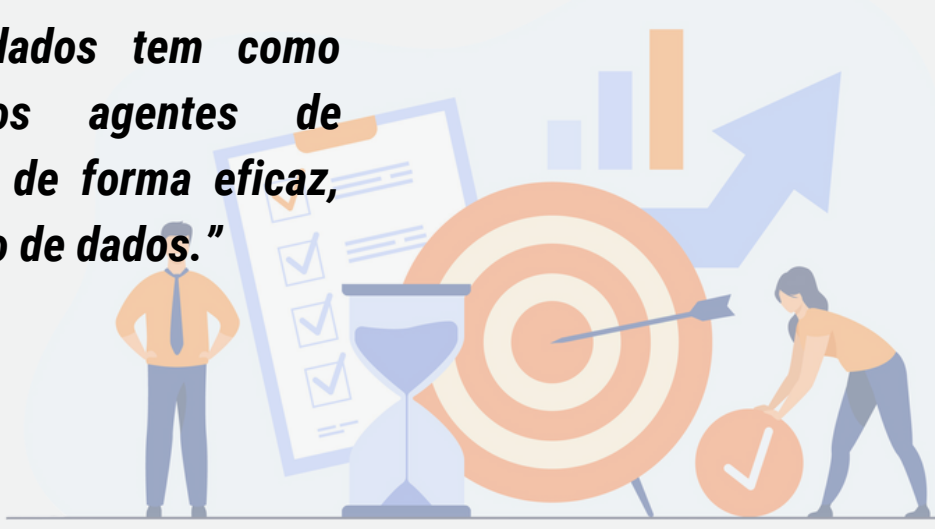
Nesse sentido importante a elaboração e implantação de um conjunto de medidas para fazer cumprir as normas legais, regulamentares e políticas, com a finalidade de evitar a aplicação de sanções, bem como, detectar e tratar qualquer desvio ou desconformidade.

A definição de compliance para Rossetti e Pitta (2017, p. 42),

"é um conjunto de ações que uma empresa deverá adotar para estar de acordo com certa legislação, prevenindo assim a ocorrência de infrações."

Para Frazão, Oliva e Abilio (2019, p. 694)

"o compliance de dados tem como objetivo auxiliar os agentes de tratamento a aplicar, de forma eficaz, as normas de proteção de dados."



10. Compliance e Governança

Estabelecer GOVERNANÇA DE DADOS

Ficará a cargo da equipe de governança de maneira contínua exercer e fiscalizar os mecanismos de controle sobre todas as atividades da empresa, que envolvam tratamento de dados pessoais, segurança da informação, incidentes de reputação digital e compliance.

Mapeamento de Processos e Dados

Uma atividade importante é o mapeamento de processos e em consequência o mapeamento dos dados pessoais tratados pelo empregador, como a figura do controlador, consolidando assim o inventário de dados pessoais.

O mapeamento deverá constar a finalidades do tratamento, base legal e tempo de armazenamento, bem como quais os departamentos e colaboradores que terão acesso a esses processos, dentre outras informações, apresentadas no ***capítulo 8***

10. Compliance e Governança

Revisão de Contratos e Documentos

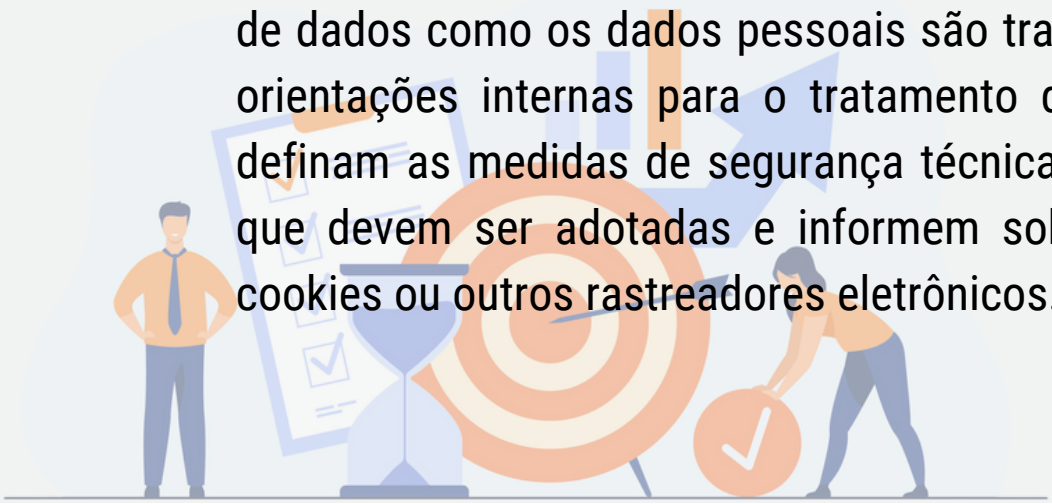
Ressalta-se a necessidade da revisão dos documentos internos das empresas para garantir a informação e conscientização dos empregados sobre dados pessoais.

Aditivos contratuais, Códigos de Conduta, Políticas de Segurança da Informação e Privacidade; Políticas de Privacidade Externa, Termo de Confidencialidade, Termo de Responsabilidade, Política de utilização de e-mails, etc.

Documentos que deverão prever não só as questões trabalhistas, mas também as obrigações a serem cumpridas pelos colaboradores para resguardar os dados cuja responsabilidade de proteção ficam a cargo do empregador.

A melhor prática indica até mesmo punições aos empregados que descumprirem tais normas, passiveis inclusive de desligamento por justa causa, a teor do art. 482 da CLT.

As políticas devem informar aos colaboradores , ou titulares de dados como os dados pessoais são tratados, estabeleçam orientações internas para o tratamento de dados pessoais, definam as medidas de segurança técnicas e administrativas que devem ser adotadas e informem sobre a utilização de cookies ou outros rastreadores eletrônicos.



10. Compliance e Governança

Limitação de Acesso de conteúdo e sites

Atendendo ao princípios oriundos da LGPD, o empregador deve usar o recurso de permissões de acesso para restringir as ações de cada usuário e limitar o conteúdo a ser acessado de acordo com os dados necessários para a realização do trabalho dentro de suas atribuições. Ideal a elaboração de Instruções de Trabalho, refletindo as atribuições de cada cargo da empresa.

Implementar conjunto de medidas restritivas que impedem práticas como prints da tela de sistemas para envio por chats, envio de banco de dados em planilhas para trabalho em computadores pessoais ou em modo offline; o bloqueio de informações para que não sejam salvas no computador.

Ideal ainda, criptografar dados confidenciais, realizar backup das informações e permitir o acesso apenas por dispositivos devidamente seguros.

10. Compliance e Governança

Mapear os fatores de risco e executar um plano de ação imediato

Depois de compreender a lógica de circulação dos dados pela empresa, chega a hora de mapear os riscos e definir as providências a ser tomadas. Aqui, a noção de risco está associada, especialmente, às chances de uma informação vazar, ou de ser conhecida por quem não deveria. O capítulo demonstra o funcionamento do mapeamento.

Medidas de Segurança Tecnológicas

Deverão ser implementadas medidas de segurança cibernética para a guarda e transmissão segura dos dados pessoais dos colaboradores. Para tanto, é importante a participação de profissionais de Tecnologia da Informação.

Relatório de Impacto à Proteção de Dados (RIPD);

O relatório de impacto à proteção de dados pessoais, avalia a possibilidade de um tratamento de dados e o risco que ele acarreta para o titular dos dados conforme disposto no artigo 38 da LGPD, sendo que poderá ser exigido pela autoridade, mas dará maior compreensão sobre o impacto do tratamento de dados, ao próprio empregador.

Canais de Comunicação;

Designar o Encarregado de Dados;

10. Compliance e Governança

A estrutura organizacional da Governança, deve ser montada da seguinte forma: Comitê Executivo de Privacidade e Proteção de Dados; Grupo de Trabalho; Executivos gestores de negócio; Usuários chaves e especialistas.

O Comitê tem a função de acompanhar o programa de implementação e tomar as decisões sobres os planos de ações e riscos; o Grupo de Trabalho é a ponte entre o Comitê e as áreas de negócios da empresa (RH, Marketing etc.) e é composto pelo DPO e pelo Jurídico, Compliance, Sistemas da Informação e Tecnologia da Informação.

Portanto, as empresas terão que adotar boas práticas, através do compliance trabalhista, que consiste na aplicação de programas de integridade, além do relatório de impacto à proteção de dados pessoais, códigos de ética e conduta e regulamentos empresariais, com intuito primordial de garantir a segurança dos dados dos empregados.

Caso as medidas mencionadas não sejam adotadas ou não são suficientes para salvaguardar os dados pessoais, os bancos de dados dos controladores de tratamento estarão sujeitos aos incidentes de segurança. Nessas situações, a LGPD estabelece procedimento a ser seguido de modo a minimizar os potenciais riscos e danos desse incidente, o que serão analisados no **capítulo 12**

10. Compliance e Governança

Como se percebe a adoção de boas práticas e de governança é essencial para que todos os requisitos necessários e os princípios estabelecidos pela LGPD quanto à proteção dos dados pessoas sejam efetivos e garantidos em sua integralidade.

Os artigos 40, 41, 42 e 43, estipulam as medidas de boas práticas que envolvem um sistema amplo e complexo de relações e previsões como instituição de mecanismos de educação e prevenção em face da segurança da informação, atuação de organismos de certificação e treinamento de equipes junto à atuação das autoridades supervisoras.

Recomenda-se a utilização de algum framework, boa prática ou norma técnica aplicável como a ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 Técnicas de segurança — Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 - Guidelines for privacy impact assessment.

Sumário

Capitulo 11

11. Compartilhamento de dados com terceiros e Transferência internacional

Por Renata Proximo, Advogada

Renata Proximo - Advogada Empresarial, especializada em compliance, consultoria e auditoria trabalhista estratégica e relações trabalhistas e sindicais. Especializada em Privacidade e Proteção de Dados (GDPR e LGPD), atuação como DPO as a Service. Diretora do Comitê Mulher, Inclusão e Diversidade da ANADD. Membro do Comitê de Relações Trabalhistas no Digital - ANADD. Membro efetivo das Comissões de Direito Digital e Privacidade e Proteção de Dados da OAB Campinas. - Instagram: @renataproximo_consultoria - Linkedin: https://www.linkedin.com/in/renata-proximo/

11. Compartilhamento de dados com terceiros e Transferência internacional

Em primeiro plano precisamos entender o que é, afinal, compartilhamento de dados. O compartilhamento de dados, nada mais é que a possibilidade do controlador enviar os dados pessoais coletados para outra instituição.

Nos termos da LGPD o compartilhamento de dados, pode ser entendido como o momento em que os dados pessoais são difundidos, transferidos internacionalmente ou interconectados.

Assim, a LGPD tem, inegável relevância na sociedade moderna, já que se tornou comum compartilhar, muitas vezes sem a ciência do titular, seus dados pessoais.

Observe-se que o titular de dados tem direito a informação, ou seja, o controlador deve informar ao titular sobre as situações que envolvem o tratamento de seus dados, inclusive quando há compartilhamento de dados, momento em que deve ser esclarecido a existência do compartilhamento, além de sua finalidade, é o que determina o artigo 9º da LGPD.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

11. Compartilhamento de dados com terceiros e Transferência internacional

É certo que, o controlador deve obter consentimento específico do titular, para compartilhar seus dados, conforme vemos no artigo 7º, §5º, observando que esse consentimento é específico, não podendo ser utilizado, no futuro, para finalidades diversas, mesmo no tempo de guarda.

> ***"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:***
> ***§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei."***

No entanto, na esfera trabalhista observamos que o controlador deve cumprir uma série de obrigações legais, o que obrigada o controlador a realizar transferência e compartilhamento de dados, mesmo a margem de um consentimento obtido do titular.

Assim, podemos trazer como exemplo de autorização de compartilhamento de dados, sem a necessidade de obtenção de consentimento, nas hipóteses do artigo 7º, incisos II, V, VI, VII:

11. Compartilhamento de dados com terceiros e Transferência internacional

> ***"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:***
> ***II - para o cumprimento de obrigação legal ou regulatória pelo controlador;***
> ***V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;***
> ***VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;***
> ***VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro***

Devemos sempre observar que no compartilhamento de dados estamos sujeitos a fatores de risco, principalmente no que diz respeito ao incidente de segurança.

Por essa e outras razões, o controlador deve garantir que será compartilhado somente os dados essenciais para a operação desejada, respeitando a finalidade para a qual foi solicitado o consentimento do titular de dados.

Outra precaução importante é a análise das cláusulas contratuais, que, no mínimo, delimitem o papel de cada agente de tratamento de acordo com a atividade desenvolvida, que contenha cláusula de segurança da informação, proíba o compartilhamento, com outra instituição, sem prévia e expressa autorização do titular e ainda que garanta a destruição dos dados assim que concluída a atividade de tratamento.

11. Compartilhamento de dados com terceiros e Transferência internacional

Para além do consentimento, o controlado deve garantir ao titular dos dados uma política de privacidade, inclusive política de privacidade para empregados, com informações claras sobre seus direitos, facilitando o acesso aos dados e qualquer desejo de cancelamento de consentimento para compartilhamento, ou seja, o titular de dados deve ter autodeterminação informada.

Já quando falamos em transferência internacional de dados, temos um cenário diferente do compartilhamento interno entre corporações ou instituição governamental.

A transferência internacional de dados pode ocorrer devido à natureza de operação do controlador, por necessidade de compartilhar o tratamento de dados pessoais com empregados situados em outro país, departamentos ou até órgãos e instituições estrangeiras, ou seja, os dados pessoais serão transferidos para país diverso do qual foi coletado. Aqui estamos falando em compartilhamento de dados, nos termos do artigo 5º, XV e XVI da LGPD.

Em primeiro plano devemos observar que a transferência internacional de dados apresenta maior risco aos direitos e liberdades dos titulares, uma vez que, como já falamos, os dados serão enviados para país distinto do qual foi coletado.

11. Compartilhamento de dados com terceiros e Transferência internacional

Ainda, a preocupação com a segurança da informação deve ser redobrada, já que as chances de ocorrência de incidentes de segurança são grandes.

As operações que envolve transferência de dados de forma internacional, o responsável deve respeitar os princípios de proteção de dados e salvaguardar os direitos dos titulares.

Podemos destacar aqui, o princípio da transparência, ou seja, o titular deve ter informações claras, precisas, claras e acesso facilitado sobre o tratamento aplicado aos dados fornecidos. Nas relações de trabalho tal transferência ocorre, geralmente, entre empresas do mesmo grupo econômico, para controle de filiais, entre outras necessidades.

A LGPD enumera um rol taxativo, de situações em que os dados pessoais coletados no Brasil podem ser transferidos internacionalmente.

O artigo 33 da LGPD, enumera esse rol com as permissões para a transferência internacional de dados:

11. Compartilhamento de dados com terceiros e Transferência internacional

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

11. Compartilhamento de dados com terceiros e Transferência internacional

Para melhor compreensão trago exemplos extraídos do Guia de Proteção de Dados Pessoais – Transferência Internacional - Versão 1.0 - Outubro, 2020, disponível em https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf

5.4. QUANDO A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS É PERMITIDA CONFORME A LGPD?

De acordo com a LGPD (Art. 33), a transferência internacional de dados pessoais somente é permitida, alternativamente, quando:

(a) Os países ou organismos internacionais proporcionarem grau de proteção de dados pessoais adequado ao previsto na LGPD (Art. 33, I, da LGPD). Está previsto que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela ANPD (Art. 34 da LGPD), de modo que as pessoas jurídicas de direito público, no âmbito de suas competências legais, e seus responsáveis, no âmbito de suas atividades, poderão requerer à ANPD a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional (Art. 33, parágrafo único da LGPD).

(b) O Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD. É de responsabilidade do Controlador garantir a segurança dos dados e proteção dos direitos e garantias dos titulares de dados. Esta hipótese é abordada em mais detalhes na seção “Transferência para países de regime diferente do Brasil”.

11. Compartilhamento de dados com terceiros e Transferência internacional

(c) A transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (Art. 33, III, da LGPD).

(d) A transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros (Art. 33, IV, da LGPD). Nesse caso, estudos envolvendo o COVID-19, algoritmos sobre o comportamento de sistemas epidêmicos poderiam ser enquadrados.

(e) A autoridade nacional autorizar a transferência (Art. 33, V, da LGPD).

(f) A transferência resultar em compromisso assumido em acordo de cooperação internacional (Art. 33, VI, da LGPD). Aqui, a transferência pode ser realizada mediante acordo bilateral entre Ministérios de diferentes países, por exemplo.

(g) A transferência for necessária para a execução de política pública ou atribuição legal do serviço público (Art. 33, VII, da LGPD).

(h) O titular tiver fornecido o seu consentimento específico e em destaque para a transferência (Art. 33, VIII, da LGPD), com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta e outras finalidades; ou

(i) É necessária para atender as hipóteses previstas nos incisos II, V e VI do Art. 7º da LGPD (Art. 33, IX, da LGPD), isto é respectivamente: para o cumprimento de obrigação legal ou regulatória pelo Controlador, quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

11. Compartilhamento de dados com terceiros e Transferência internacional

Ressalte-se que o nível de adequação, contido o inciso I do artigo 33, deverá ser avaliado pela ANPD (Autoridade Nacional de Proteção de Dados). Essa avaliação será feita considerando:

I. as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II. a natureza dos dados;
III. a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV. a adoção de medidas de segurança previstas em regulamento;
V. a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI. outras circunstâncias específicas relativas à transferência.

A transferência internacional só poderá ser admitida para países em que houver tratado de cooperação em matéria cível, visto que a inexistência do tratado dificultaria eventual medidas por parte dos titulares.

Assim, além do país que receberá a transferência contar com legislação e fiscalização efetiva sobre proteção de dados pessoais, deve fazer parte de tratado em matéria cível.

O importante, na transferência internacional é a garantia de proteção dos dados compartilhados, a informação clara ao titular e a garantia dos direitos do titular no que diz respeito aos dados compartilhados, lembrando que os dados estão em outro país as precauções devem ser dobradas.

Sumário

Capitulo 12

12. Plano de Contingencia e Incidente de Segurança

Por Julia Medeiros, Advogada

Advogada, especialista em Direito Digital. Pós-graduada em Direito Digital e LLM em Direito Empresarial. Membro da ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados). Membro da ANADD (Associação Nacional de Advogados do Direito Digital) - Comitê de Relações Trabalhistas no Digital. Membro da Comissão de Direito de Proteção de Dados da OAB/PE. Certificada DPO.

12. Plano de Contingencia e Incidente de Segurança

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

O Incidente de Segurança da Informação é qualquer evento adverso confirmado que ocorra a violação de algum dos pilares da Segurança da Informação: a confidencialidade, a integridade e a disponibilidade, tais como acesso não autorizado, ilícito que resulte em destruição, perda, alteração, vazamento de informação.

Com a chegada da Lei Geral de Proteção aos Dados (LGPD), aprovada em 14 de agosto de 2018 e sancionada em 18 de setembro de 2020, traz como objetivo a garantia da proteção dos dados pessoais além de criar diretrizes para a tratamento dos dados, que se faz desde a coleta até o descarte dos dados.

Dentro deste gênero de incidentes, estão os incidentes de segurança de dados pessoais indicado pela Lei Geral de Proteção de Dados - LGPD, isto é, aqueles que envolvam especificamente dados pessoais de pessoas naturais.

Portanto, nem todo incidente de segurança envolverá dados pessoais, mas todo incidente de dados pessoais será um incidente de segurança.

12. Plano de Contingencia e Incidente de Segurança

Assim, conforme definição da Autoridade Nacional de Proteção de Dados – ANPD - um incidente de segurança de dados pessoais

"(...) é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

O art. 46 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

12. Plano de Contingencia e Incidente de Segurança

Como exemplos de incidentes de segurança de dados pessoais temos:

- *Vazamento ou sequestro de dados pessoais após um ataque hacker;*
- *Acesso a dados pessoais por qualquer pessoa não autorizada;*
- *Exposição acidental de dados pessoais em sites, comunicados ou redes sociais;*
- *Perda de dados devido a catástrofes naturais, queda de energia e atualizações de sistemas;*
- *Eliminação indesejada de dados pessoais;*
- *Alteração indevida de dados pessoais por parte de um colaborador, etc.*

12. Plano de Contingencia e Incidente de Segurança

MEDIDAS DE SEGURANÇA ADOTADAS

Um incidente de segurança numa Organização pode levar a perdas financeiras, danos à reputação, sanções administrativas e ações judiciais individuais e coletivas.

Deste modo, é fundamental que as organizações estabeleçam medidas de Segurança da Informação para mitigar riscos de incidentes de segurança, através de tratamento de riscos de forma preventiva, tais como:

·Ter implementada a Política de Segurança da Informação na Organização;

·Ter controle técnico de segurança, através de aplicação de criptografia, utilização de VPN, política de senhas com complexidade de senhas, firewall, backup;

·A realização do due diligencie de parceiros comerciais que tenham acesso a dados pessoais;

·A conscientização e treinamentos de todos os colaboradores;

12. Plano de Contingencia e Incidente de Segurança

·Controle de acesso lógico, garantindo que os usuários acessem apenas o que lhe é autorizado e, controle de acesso físico, este voltados a fechaduras, portas, leitor de biometria, entre outras medidas;

·Plano de Resposta a Incidente no qual prepara a organização para agir rapidamente diante de uma situação adversa, convocando os responsáveis previamente estabelecidos para agir; e,

·Ter um Plano de Contingência. As ações de contingências previstas no plano não têm natureza preventiva, mas sim serem utilizadas como recurso quando as medidas de segurança preventivas não forem suficientes para impedir o efeito indesejável. Sua função é minimizar os danos decorrentes de forma a que se preserve ao máximo as características essenciais do planejamento original da Organização.

12. Plano de Contingencia e Incidente de Segurança

PLANO DE CONTINGÊNCIA DE SEGURANÇA (PC)

O Plano de Contingência de Segurança (PC) é definido como um documento formal no qual contém um processo de planejamento prévio com objetivo e ações para ser acionado de forma rápida e efetiva em caso de um estado de incerteza de segurança por uma Organização, quando as medidas de segurança adotadas previamente não são capazes de evitar um evento indesejado, a fim de responder a uma anormalidade/emergência de segurança.

O Plano de Contingência tem por objetivo fazer com que os processos vitais da organização não sejam atingidos, ou se atingidos, que voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos a organização, buscando assegurar a continuidade operacional da organização e reduzir anular as consequências de um sinistro, reduzindo ao mínimo o perigo potencial de lesões, mortes, prejuízos, danos a propriedade, ao meio ambiente e a toda coletividade.

Todas as Organizações devem ter um Plano de Contingência de Segurança atualizado, baseado em uma avalição de risco, e considerá-lo como uma ferramenta valiosa para sua existência, uma vez que é impossível garantir que um risco jamais se concretizará.

12. Plano de Contingencia e Incidente de Segurança

Exemplos de Plano de Contingência de Segurança com ações preliminares para resposta a situações e eventos indesejados:

- *Plano de Contingência para falta de energia elétrica ou de água;*
- *Plano de Contingência para falhas sistemas de comunicação, a exemplo, queda de acesso a Rede e a Internet;*
- *Plano de Contingência para ataques virtuais;*
- *Plano de Contingência para falhas em Backups;*
- *Plano de Contingência para acidentes de trabalho;*
- *Plano de Contingência para invasões e assaltos;*
- *Plano de Contingência para greves e paralisações*.

O Plano de Contingência também é denominado de “Plano B”, porque também pode ser usado como uma ação alternativa se os resultados esperados não se concretizarem. O planejamento de contingência é um componente do Plano de Continuidade do Negócio (PCN) e do Plano de Recuperação de Desastres (PRD).

O PC é ativado logo após a ocorrência do evento indesejável, a fim de mitigar consequências do risco. Se as ações do plano de contingência forem insuficientes para restaurar as operações em sua normalidade, pode ser declarado um desastre e iniciar o PCN de longo prazo, bem como o PRD.

12. Plano de Contingencia e Incidente de Segurança

ELABORAÇÃO DO PLANO DE CONTINGÊNCIA (PC)

Para fazer o plano de contingência é importante que a alta administração juntamente com o gestor de segurança ou Comitê de Segurança constituído na Organização entenda que se refere a uma atividade multidisciplinar para que envolva todos que serão atingidos pelo Plano e assim, torna-se mais efetivo, vez que:

- *Amplia a compreensão dos envolvidos acerca dos riscos e das ações de gestão, gerando uma postura de corresponsabilidade;*
- *Reforça a credibilidade do gestor e de sua equipe, pois as pessoas sentem-se parte integrante do processo de tomada de decisão;*
- *Favorece o cumprimento de exigências legais em relação à participação e controle social;*
- *Há maior probabilidade de corresponder às necessidades reais e ser eficientes;*
- *As decisões e os programas são enriquecidos pelo conhecimento e experiência de muitas pessoas;*
- *As pessoas que cooperam na elaboração ou nas decisões tornam-se mais interessadas e envolvidas na sua execução e não precisam ser convencidas.*

12. Plano de Contingencia e Incidente de Segurança

É importante garantir que o plano de contingência forneça orientações claras para os seguintes itens:

- *·A identificação, avaliação e classificação dos riscos que possam vir a afetar o funcionamento da Organização, através de uma gestão de ativos, com análise detalhada da infraestrutura de TI da empresa, incluído dados, hardwares e softwares, mapeando as ameaças e vulnerabilidades existentes;*
- *·A definição das estratégias de mitigação dos riscos, estabelecendo um plano de ação diante do acontecimento de cada risco, sincronizando as ações/atividades e recursos necessários para implementação, inclusive no que se refere a comunicação do incidente de segurança de dados pessoais trazido pela LGPD;*
- *·Documentar o plano de contingência que deve incluir etapas claras a seres seguidas, caso qualquer um dos eventos identificados ocorra;*
- *·A conscientização e treinamento dos envolvidos no planejamento. Tratar sobre a conscientização do posicionamento, agilidade, eficiência, conformidade com as leis, normas e doutrinas de segurança;*
- *·Avaliar o desempenho do Plano de Contingência, estabelecendo uma comparação entre o desempenho esperado e o apresentado, conforme ciclo PDCA. Para cada simulado ou execução real do plano, verifica-se se os objetivos foram alcançados. Caso negativo, deve-se corrigir os erros;*
- *Revisão e auditoria, no qual o plano de contingência de segurança deve ser atualizado regularmente para se manter atualizado com as melhores práticas de segurança, bem como garantir que o mesmo atenda às necessidades operacionais da Organização.*

12. Plano de Contingencia e Incidente de Segurança

COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS

Caso algum incidente de dados pessoais ocorra, a LGPD estabelece que o controlador deve primeiro avaliar se o incidente pode acarretar risco ou dano relevante aos titulares. Se ocasionar um risco ou dano relevante, o controlador deverá comunicar a ocorrência do incidente à ANPD (Autoridade Nacional de Proteção de Dados) e ao titular dos dados.

Conforme definição da ANPD, risco ou dano relevante é:

"(...)pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados."

12. Plano de Contingencia e Incidente de Segurança

A comunicação preliminar à ANPD deve ser feita no prazo de 02 dias úteis e por meio de peticionamento eletrônico, devendo conter, no mínimo:

- *A descrição da natureza dos dados pessoais afetados;*
- *As informações sobre os titulares envolvidos;*
- *A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;*
- *Os riscos relacionados ao incidente;*
- *Os motivos da demora, no caso de a comunicação não ter sido imediata; e*
- *As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo*.

Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente, desde que informe que serão realizadas posteriormente, bem como quais meios estão sendo utilizados para obtê-las. A ANPD também poderá requerer informações adicionais a qualquer momento.

Após, a ANPD vai avaliar a gravidade do incidente e poderá determinar a adoção de algumas providências, a exemplo, medidas para reverter ou mitigar os efeitos do incidente.

12. Plano de Contingencia e Incidente de Segurança

CONCLUSÃO

Visto que no mundo corporativo não há algo 100% (cem por cento) protegido de problemas como ameaças e vulnerabilidades (eventos externos e internos), quem podem ocasionar diversos danos à Organização.

Porém, é possível se preparar com antecedência para eventos adversos e incidentes de segurança por meio de planos de contingências. O Gerenciamento de risco auxilia a reduzir impactos e probabilidades de eventos que causaria perdas e danos a Organização.

O plano de contingência, portanto, é parte essencial da gestão de risco e deve ser bem elaborado, de forma clara e, identificando os possíveis riscos que a empresa pode correr, além dos recursos disponíveis para resolver os problemas.

Investir no desenvolvimento de um planejamento estratégico possibilita definir as melhores soluções para resolver os diversos tipos de problemas existentes e, consequentemente, reduzir ou até eliminar, perdas de dados e outros prejuízos, a exemplo, uma paralisação prolongada dos negócios de uma Organização.

Sumário

Capitulo 13

13. LGPD e TERCEIRIZAÇÃO

Por Renata Proximo, Advogada

Renata Proximo - Advogada Empresarial, especializada em compliance, consultoria e auditoria trabalhista estratégica e relações trabalhistas e sindicais. Especializada em Privacidade e Proteção de Dados (GDPR e LGPD), atuação como DPO as a Service. Diretora do Comitê Mulher, Inclusão e Diversidade da ANADD. Membro do Comitê de Relações Trabalhistas no Digital - ANADD. Membro efetivo das Comissões de Direito Digital e Privacidade e Proteção de Dados da OAB Campinas. - Instagram: @renataproximo_consultoria - Linkedin: https://www.linkedin.com/in/renata-proximo/

13. LGPD e Terceirização

A Lei Nº 13.429/2017, também conhecida como Lei da Terceirização, sancionada no dia 31 de março de 2017 autoriza a terceirização de serviços para todas as atividades da empresa, inclusive atividade fim ou principal.

Utilizando-se dessa premissa, muitas empresas terceirizam atividades internas, contratando empresas especializadas para prestação de serviços.

A partir do momento em que há um contrato de prestação de serviços, com fornecimento de mão-de-obra e compartilhamento de dados de pessoa natural todas as empresas envolvidas devem observar as diretrizes trazidas pela Lei Geral de Proteção de Dados aplicada ao contrato.

Como é de conhecimento geral, a partir do momento em que a prestadora de serviços passa a fornecer mão-de-obra, as tomadoras solicitam uma série de documentos e identificação dos empregados que estarão a sua disposição. Tal procedimento é importante, já que identificar os indivíduos que prestam serviços e circulam dentro da empresa é essencial, além disso, identificar cada empregado terceirizado ajuda no monitoramento e no jus vigilandi, que é responsabilidade da empresa tomadora de serviços.

13. LGPD e Terceirização

A empregadora/prestadora de serviços deve observar a lei em sua completude, inclusive quanto ao compartilhamento de dados de seus empregados com seus clientes.

Assim, a empresa prestadora de serviços deve observar o princípio da transparência e da informação, deixando seus empregados cientes de que alguns dados, essenciais, serão compartilhados com outras empresas, denominadas clientes ou tomadores de serviços, conforme determina o artigo 9º, inciso V.

"Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;"

Outro cuidado importante a ser observado pela empresa empregadora/prestadora de serviços é exigir que seu cliente/tomador esteja também adequado a Lei.
A exigência deve ser imposta no próprio contrato de prestação de serviços, com cláusula específica e elaborada de forma adequada as necessidades e ao tipo de contrato.
No contrato de prestação de serviços deve ser observado, inclusive, condições e obrigações quanto ao tratamento de dados recebidos e compartilhados.

13. LGPD e Terceirização

Passado a averiguação, de adequação ao programa de privacidade de dados, a empresa empregadora/prestadora de serviços deve analisar quais são os dados a serem compartilhados, minimizando ao máximo o compartilhamento de dados de seus empregados.

Ainda é muito comum nos depararmos com empresas clientes/tomadoras que exigem diversos documentos e dados que não se justificam, dados que não serão utilizados, ignorando a finalidade e adequação, nos termos do artigo 6º.

Assim, tal fiscalização deve ser feita pela empresa empregadora/prestadora de serviços, já que é a responsável pelo compartilhamento e inclusive deve, como dito acima, informar seu empregado sobre o compartilhamento e justificá-lo, nos termos da Lei.

Sempre que a empresa cliente/tomadora solicitar dados que possa ser entendido como desnecessário, cabe a empregadora/prestadora de serviços questionar a necessidade da informação, buscando a finalidade específica do tratamento.

Em contrapartida, a empresa cliente/tomadora deve atentar para que seu fornecedor de mão-de-obra também comprove sua adequação a lei, fornecendo evidências de cumprimento da legislação trabalhista como um todo, além da legislação previdenciária, exigindo ainda idoneidade e averiguação da saúde financeira.

13. LGPD e Terceirização

Quanto aos termos da Lei Geral de Proteção de Dados, deve evidenciar sua adequação na condução dos contratos de trabalho, apresentar o consentimento fornecido pelo empregado, quando necessário, demonstrar que seu empregado tem livre acesso informado quanto aos seus direitos.

Como exemplo, podemos citar:

- *Receber informações sobre os dados coletados e tratados pela, incluído as hipóteses de compartilhamento;*
- *Ter acesso aos dados facilitado, sempre que solicitado;*
- *Solicitarretificação e atualização dos dados tratados, sempre que imprecisos, incompletos e desatualizados;*
- *Se opor ao tratamento que não seja a finalidade informada, solicitar anonimização e eliminação de dados, em circunstâncias especificas;*
- *Solicitar portabilidade, quando aplicável;*
- *Revogar consentimento a qualquer momento;*
- *Requerer revisão de decisões automatizadas que possam afetar seus interesses.*

Também chamados de pilares e compondo ainda o conceito de segurança da informação a Confidencialidade, Integridade e Disponibilidade são os princípios críticos da Segurança da Informação que podem variar de acordo com cada modelo de negócio o nível de segurança a ser empregado para cada um destes princípios.

13. LGPD e Terceirização

Observar as políticas internas de seus parceiros de negócio é sempre importante, cabendo as empresas, tanto a cliente/tomadora quanto a empregadora/prestadora de serviços observar a coleta, tratamento, guarda, compartilhamento e descarte de dados, conforme determina a legislação.

As empresas devem agir de forma conjunta, como parceiras para garantir a qualidade e proteção dos dados tratados e compartilhados, dos empregados terceirizados, já que a responsabilização é solidária, nos termos do artigo 42, §1º, incisos I e II, na ocorrência de vazamento de dados.

Os departamentos de Compliance e Governança das contratantes devem unir forças para fiscalizar, solicitar informações e melhorias necessárias para cumprir a legislação de forma completa, sem risco de causa incidentes que prejudique seu parceiro de negócios ou seus empregados, já que as atividades de tratamento de dados pessoais, como coleta, uso, armazenamento, compartilhamento e até a exclusão devem estar de acordo com a norma legal, sob pena de acarretar, entre outras penalidades, a responsabilização civil.

Sumário

Capitulo 14

14. Responsabilidade Civil

Por Maria Santos, Advogada

Advogada e Data Protection Officer.
Atuando na Advocacia Chizzolini
Certificada DPO ITCERTS. Membro da Diretoria Associação Nacional dos Advogados de Direito Digital - ANADD.
Responsável Comitê Relações Trabalhistas no Digital,
Especialista em Direito Empresarial e Direito do Trabalho, atuando a mais de 30 anos no Mercado Corporativo. Pós-Graduanda em Direito Digital pela EBRADI
MBA e Pós Graduação, Controladoria, Auditoria e Compliance pela FMU - Pós Graduação em Direto Processual Trabalho -Anhembi Morumbi

14. Responsabilidade Civil

O novo Código aperfeiçoou o conceito de ato ilícito ao dizer que o pratica quem “violar direito e causar dano a outrem” (art. 186), substituindo o “ou” (“violar direito ou causar dano a outrem”) que constava do art. 159 do diploma de 1916. Com efeito, o elemento subjetivo da culpa é o dever violado.

Assim, entendemos que a responsabilidade é uma reação provocada pela infração a um dever preexistente.

No entanto, ainda mesmo que haja violação de um dever jurídico e que tenha havido culpa, e até mesmo dolo, por parte do infrator, nenhuma indenização será devida, uma vez que não se tenha verificado prejuízo. Se, por exemplo, o motorista comete várias infrações de trânsito, mas não atropela nenhuma pessoa nem colide com outro veículo, nenhuma indenização será devida, malgrado a ilicitude de sua conduta. A obrigação de indenizar decorre, pois, da existência da violação de direito e do dano, concomitantemente.

14. Responsabilidade Civil

O art. 186 do Código Civil consagra uma regra universalmente aceita: a de que todo aquele que causa dano a outrem é obrigado a repará-lo. Estabelece o dispositivo legal, informativo da responsabilidade aquiliana:

> ***"Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".***

A análise do artigo supratranscrito evidencia que quatro são os elementos essenciais da responsabilidade civil: ação ou omissão, culpa ou dolo do agente, relação de causalidade, e o dano experimentado pela vítima.

Na mesma situação estão todos os demais prepostos (empregados ou não) do controlador. Se eles, por ato próprio, de natureza ilícita, causam danos ao titular dos dados em face da violação à LGPD, logo, o autor da lesão e o empregador ou comitente respondem de forma solidária perante do ofendido. Se o controlador, porém, não concorreu para o dano, ele poderá se ressarcir regressivamente do ofensor seu preposto (art. 934 do CC).

14. Responsabilidade Civil

Assim, todo o empregado poderá responder pessoalmente pelos danos, materiais ou morais, que vier a causar, dolosa ou culposamente, em relação a terceiros, independente da responsabilidade do seu empregador.

A responsabilidade civil contratual do empregado, em havendo negligência, imperícia ou imprudência tem como base legal, para ressarcimentos dos prejuízos causados ao empregador vide que o que descreve o § 1º do art. 462 da CLT , que assim descreve:

"Art. 462 - Ao empregador é vedado efetuar qualquer desconto nos salários do empregado, salvo quando este resultar de adiantamentos, de dispositivos de lei ou de contrato coletivo."

Além disso, também caberá dependendo do causa a rescisão do contrato por justa causa, a teor do art. 482, da CLT, situação essa ratificação perante o Tribunal Regional do Trabalho , quando devidamente caracterizada que o vazamento de dados ocorreu, em conduta inadequada do colaborador, bem como ter a empregadora ter adotado todas as medidas de treinamentos, conscientizar e proteção dos dados para o exercício da atividade dos colaboradores.

14. Responsabilidade Civil

Vide caso recente:

Assim, todo o empregado poderá responder pessoalmente pelos danos, materiais ou morais, que vier a causar, dolosa ou culposamente, em relação a terceiros, independente da responsabilidade do seu empregador.

EMPREGADO VIOLA LGPD EM PEDIDO DE RESCISÃO INDIRETA E É PUNIDO COM JUSTA CAUSA

Em sentença proferida na 81ª Vara do Trabalho de São Paulo-SP pela juíza Edite Almeida Vasconcelos, um enfermeiro teve o pedido de rescisão indireta do contrato de trabalho prejudicado por ter juntado provas aos autos que violam a Lei Geral de Proteção de Dados. Para a magistrada, a atitude do trabalhador configura falta grave.

Na ação, o homem alega que a empresa praticou diversas faltas e descumpriu obrigações. Dentre as situações relatadas estão a exigência de realizar dobra de plantões, cuidar de pacientes em número superior ao determinado pelo Conselho de Enfermagem e efetuar pagamentos "por fora". Com o intuito de provar alguns fatos, o profissional juntou planilhas do Sistema de Gerenciamento de Internação.

14. Responsabilidade Civil

Em defesa, o hospital argumenta que ao tomar conhecimento do processo constatou que o autor "cometeu falta gravíssima ao apropriar-se indevidamente de documentos confidenciais", aos quais ele só teve acesso em razão do cargo que exercia. Em vista disso, a instituição fez um pedido liminar de tutela de proteção de dados e os documentos foram excluídos dos autos. Diante do fato, a empresa requereu também a conversão da rescisão contratual em dispensa por justa causa.

A análise da julgadora considerou que "o autor violou a intimidade e a privacidade de terceiros, pessoas naturais clientes da reclamada, e infringiu a Lei Geral de Proteção de Dados - LGPD, utilizando dados sensíveis de forma ilícita. Ainda, fez com que a empresa infringisse a LGPD, pois esta era a responsável pela guarda dos dados sensíveis de seus clientes. Por fim, o reclamante descumpriu norma expressa da reclamada, da qual o reclamante foi devidamente cientificado."

Com isso, o pedido de rescisão indireta do trabalhador foi julgado improcedente e ele foi responsabilizado pela falta praticada, sendo punido com a dispensa por justa causa. Cabe recurso.

14. Responsabilidade Civil

Isso porque o não cumprimento de regra na empresa pelo empregado, ante aos treinamentos realizados e a existência de políticas e normas de segurança. Evidenciado a negligencia ou imprudência, resta claro a falta de confiança e a boa-fé, que devem existir na relação empregatícia, tornando assim, impossível o prosseguimento da relação, culminando com eventual desligamento por justa causa.

Importante que os fatos sejam evidenciados e comprovados, se possível através de sindicância interna e investigação dos danos causados, bem como procedimento acometidos pelo empregado, evidenciado os prejuízos causados à empresa, que evidenciado o ato de improbidade.

A quebra da confiança na relação empregatícia pode se dar independentemente da aferição de prejuízo real pela empresa, se, caracterizado a falta de cuida, e o risco gerado.

Já no caso de o dano decorrer de ato praticado por terceiro não preposto do controlador e do operador, somente àquele se deve imputar a responsabilidade (inciso III do art. 43 da LGPD).

14. Responsabilidade Civil

Doutrinariamente assim, nos ensinam os mestres;

Inicialmente relatamos a doutrina a esse respeito e conforme a lição de Rui Stoco:

"A noção da responsabilidade pode ser haurida da própria origem da palavra, que vem do latim respondere, responder a alguma coisa, ou seja, a necessidade que existe de responsabilizar alguém pelos seus atos danosos. Essa imposição estabelecida pelo meio social regrado, através dos integrantes da sociedade humana, de impor a todos o dever de responder por seus atos, traduz a própria noção de justiça existente no grupo social estratificado. Revela-se, pois, como algo inarredável da natureza humana" (STOCO, 2007, p.114)

(citado em http://www.ambitojuridico.com.br/site/?n_link=revista_artigo_leitura&artigo_id=11875).

Ensina, neste contexto, Washington de Barros Monteiro que:

"Em face, pois, da nossa lei civil, a reparação do dano tem como pressuposto a prática de um ato ilícito. Todo ato ilícito gera para seu aturo a obrigação de ressarcir o prejuízo causado. É de preceito que ninguém deve causar lesão a outrem. A menor falta, a mínima desatenção, desde que danosa, obriga o agente a indenizar os prejuízos consequentes de seu ato." (Curso de Direito Civil, vol. 5, p. 538)

14. Responsabilidade Civil

O princípio da responsabilização e prestação de contas (accountability) estabelece que os(as) agentes de tratamento devem ser capazes de demonstrar o cumprimento e o respeito à LGPD, apresentando as medidas adotadas e a eficácia delas. Para isso, a lei apresenta uma série de instrumentos que podem ser utilizados.

A responsabilidade civil pelo descumprimento à LGPD está disciplinada a partir do artigo 42, informando que o Controlador ou o Operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

O Operador responde solidariamente junto com o Controlador quando descumprir a LGPD ou quando não tiver seguido as instruções do Controlador. O Controlador que estiverem diretamente envolvidos nas atividades de tratamento que causarem danos aos titulares serão solidariamente responsáveis.

14. Responsabilidade Civil

Isento portanto o Operador atue em conformidade com a LGPD e dentro das exigências do Controlador, não sendo assim responsabilizado solidariamente por eventuais danos causados pelo Controlador.

Assim como, o Controlador que não participa do tratamento do qual decorra danos ao titular não será solidariamente responsável por danos causados.

Assim, importante que através de contrato formal seja estabelecido de maneira clara e transparente as atribuições de cada parte e das limitações de responsabilidade.

Os agentes de tratamento (Controlador ou Operador) só não serão responsabilizados quando provarem:

> I - ***que não realizaram o tratamento de dados pessoais que lhes é atribuído;***
> ***II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou***
> ***III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. Daí advém a necessidade de adequação dos Contratos entre o Controlador e o Operador.***

14. Responsabilidade Civil

A fim de impor compulsoriamente novas regras de segurança, a LGPD previu sanções às empregadoras, como controladoras. que ao descumprirem as previsões legais.

Embora a eficácia dessas sanções administrativo por parte da Autoridade Nacional de Proteção de Dados (ANPD) esteja vigente desde 1º de agosto de 2021, fato é que outras modalidades de demandas podem surgir até então.

São elas as ações judiciais trabalhistas que visem ressarcir o empregado de eventuais danos sofridos pelo vazamento de dados sensíveis a terceiros, e uso indevido de seus dados.

Os artigos ***42 a 45 da Lei 13.709/18*** tratam da responsabilidade civil patrimonial e extrapatrimonial do controlador e operador, no tratamento de dados.

É prevista legalmente a advertência, a multa simples no importe de 2% sobre faturamento da empresa, multa diária, o bloqueio, a eliminação ou a suspensão total ou parcial do funcionamento do banco de dados.

14. Responsabilidade Civil

No que diz respeito à modalidade de responsabilidade civil a ser adotada, há uma tendência doutrinária em se adotar a responsabilidade subjetiva com culpa presumida por força da aplicação do artigo 42 e incisos II e III do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele que não violou a lei.

Contudo importante, considerar a responsabilidade civil objetiva é prevista no Código Civil e assim como a LGPD não trouxeram a culpa como elemento necessário para configuração de responsabilidade.

Referências bibliográficas

https://radarlegislativo.org/projeto/1/
https://www.27001.pt/iso27001_2.html
https://www.abnt.org.br/
https://www.abntcatalogo.com.br/normagrid.aspx
https://www.gov.br
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/legislacao-federal
https://www.iso.org/home.html
https://www25.senado.leg.br/web/atividade/materias/-/materia/113947
https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca - Acessado em 25/10/2022;
https://www.lgpdbrasil.com.br/como-lidar-com-um-incidente-de-seguranca-da-informacao/ - Acessado em 25/10/2022;
https://gestaodesegurancaprivada.com.br/plano-de-contingencia-de-seguranca-o-que-e-7--passos-elaborar/ - Acessado em 25/10/2022;
https://getprivacy.com.br/plano-de-resposta-a-incidentes/ - Acessado em 25/10/2022;
https://4future.com.br/index.php/2021/10/24/medidas-de-seguranca-da-informacao/ - Acessado em 26/10/2022.
https://www.gov.br/anpd/pt-br - Acessado em 26/10/2022.

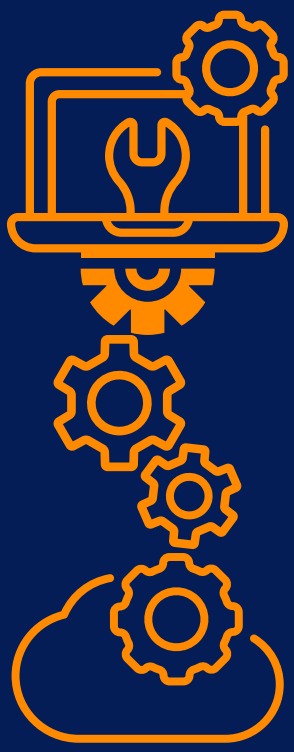
Referências bibliográficas

hALCASSA, Flávia. A Lei Geral de Proteção de Dados Pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. Revista do Tribunal Regional do Trabalho da 10ª Região, Brasília, v. 24, n. 02, p. 145-151, jul./dez. 2020. Disponível em: https://revista.trt10.jus.br/index.php/revista10/article/view/419. (acessado em 10 de janeiro de 2023)

BOMFIM, Vólia; PINHEIRO, Iuri; LIMA, Fabrício; MIZIARI, Raphael. LGPD e seus impactos nas relações de trabalho subordinado. São Paulo: IBJUR, 2020. p. 1-47.

BRASIL. Tribunal Superior do Trabalho. Recurso de Revista n. 613/2000-013-10-00.7. Brasília, 18 de maio de 2005. Primeira Turma. Relator: Min. João Oreste Dalazen. Brasília, 10 jun. 2005. Disponível em: https://tst.jusbrasil.com.br/jurisprudencia/1724843/recurso-derevista-rr-613002320005100013-61300-2320005100013/inteiro-teor0792867?ref=juristabs. Acesso em: 17 mai. 2023.

Referências bibliográficas



CANOTILHO, JJ Gomes. Direito Constitucional e Teoria da Constituição. Coimbra: Almedina, 2003.

CASSAR, Vólia Bomfim; BORGES, Leonardo. Comentários à Reforma Trabalhista. São Paulo: Gen, 3ª Ed, 2019.

CASSAR, Vólia Bomfim. Direito do Trabalho. São Paulo: Gen, 17ª Ed. 2020.

LIMA, Fabírcio; PINHEIRO, Iuri. Manual do compliance trabalhista: teoria e prática. Salvador: Ed. JusPodivm, 2020.

MOREIRA, Teresa Coelho. A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um estudo dos limites do poder de controlo electrónico do empregador. Coimbra: Almedina, 2010.

SCHWAB, Klaus. A quarta revolução industrial. São Paulo: Edipro, 2016.

ALCANTARA, Clayton Deodoro G. de. Impactos da Lei Geral de Proteção de Dados nas Relações de Trabalho. Pontifícia Universidade Católica de Goiás: Goiânia, 2021.

ALVES, Lurdes Dias. Proteção de Dados Pessoais no Contexto Laboral. O direito à privacidade do trabalhador. Editora Almedina. 2020.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

COMITÊ DE RELAÇÕES TRABALHISTAS NO DIGITAL

ANADD
Associação Nacional de
Advogadas e Advogados de Direito Digital

Comitê ANADD RTD
* COMITÊ DE RELAÇÕES TRABALHISTAS NO DIGITAL *

GT RTD - Relação Trabalhista Digital

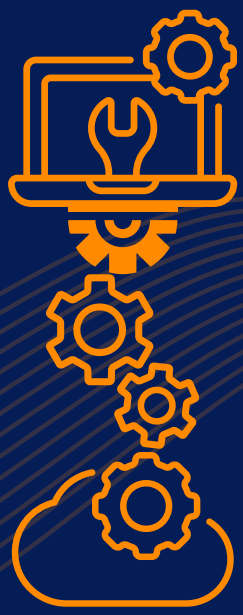
Coautores:

Elis Xavier
Hilda Cavalcanti
Júlia Medeiros
Maria Santos
Renata Proximo
Valéria Ribeiro

Coordenação:
Maria Santos

Arte e Design:
Maria Santos e Ricardo Castro Cajazeira

Revisão:
Maria Santos e Ricardo Castro Cajazeira



Título: LGPD e as Relações de Trabalho
Formato: Livro Digital
Veiculação: Digital
Versão 1.0 - junho/2023

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital
Registro ISBN nº 978-65-999397-1-6