CENTRO UNIVERSITÁRIO PRESIDENTE ANTÔNIO CARLOS - UNIPAC

CURSO DE DIREITO

MARIANA WENDLING LOPES

INFLUÊNCIA DA LGPD NAS RELAÇÕES DE TRABALHO

JUIZ DE FORA - MG

2021

MARIANA WENDLING LOPES

INFLUÊNCIA DA LGPD NAS RELAÇÕES DE TRABALHO

Monografia de conclusão de curso apresentada ao curso de Direito do Centro Universitário Presidente Antônio Carlos - UNIPAC, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Carmem Lúcia Machado Ribeiro

JUIZ DE FORA – MG

2021

MARIANA WENDLING LOPES

INFLUÊNCIA DA LGPD NAS RELAÇÕES DE TRABALHO.

Monografia de conclusão de curso apresentada ao curso de Direito do Centro Universitário Presidente Antônio Carlos - UNIPAC, como requisito parcial para obtenção do título de bacharel em direito.

Aprovada em: / /

BANCA EXAMINADORA

Prof. Carmem Lúcia Machado Ribeiro (Orientador)

Centro Universitário Presidente Antônio Carlos - UNIPAC

Centro Universitário Presidente Antônio Carlos - UNIPAC

Centro Universitário Presidente Antônio Carlos - UNIPAC

Dedico esse a minha querida mãezinha, que onde é que estiver, sei que estará torcendo pela minha vitória. Sem você eu não teria conseguido, te amo!

AGRADECIMENTOS

Agradeço inicialmente ao meu pai, por ter me ajudado e me incentivado por todos esses anos e em todos os momentos, sejam eles bons ou nem tão bons assim.

Agradeço ao meu esposo, por ter aturado todos os meus surtos nesses 13 anos, mas mais especificamente nesses últimos 5 anos, e por reconhecer que a partir de agora, não irá ganhar mais nenhuma discussão comigo. Agora com cunho jurídico!

Agradeço meus professores, em específico aos professores Alexandre Bonoto, Maria Amélia da Costa e a coordenadora Luciana Braga, muito obrigado pelas inúmeras vezes que vocês me salvaram.

Agradeço a minha Mestra/Musa/Chefe Christiane Polini por estar ao meu lado e por me orientar tão bem nesses últimos tempos, seja quando o assunto é o mundo do Direito, seja em nossas longas conversas no café.

Agradeço aos meus amigos (lá vem a lista):Ana Luiza Wendling, Michelle Rizzo, Amanda Nunes, Aline Emanuela, Victor Guedes, Gustavo Pascoalini. Sem vocês esses 5 anos teriam sido muito pior. Amo vocês!

RESUMO

O presente trabalho analisará a lei nº 13.709/18, iniciando-se por contexto histórico internacional de países que elaboraram normas para a proteção de dados em seu território e com isso influenciaram diretamente a criação da Lei Geral de Proteção de Dados no Brasil. O trabalho abordará as principais definições trazidos pela LGPD, sejam eles: o conceito de dado e de dados sensíveis, o conceito de tratamento de dados e os principais agentes envolvidos, seja como controladores, seja como encarregado de dados – aqui chamado de DPO – *Data Protection Officer*. Após isto, iremos apresentar os nortes legais trazidos pelo art. 7º LGPD, que servirão para enquadramento nas bases legais, justificando, portanto, o seu tratamento pelos agentes envolvidos. Passados tais momentos, iremos utilizar os conhecimentos apresentados, dentro de um panorama da seara trabalhista, aonde percorreremos todos os momentos contratuais: como a fase pré-contratual, ao qual o empregador deverá analisar a real necessidade de captação de dados de eventuais colaboradores, assim como a necessidade de manutenção de banco de currículos. Em uma fase já contratual, iniciada pela efetivação do colaborador, torna-se necessário um zelo maior quanto as informações mantidas, principalmente no que tange os dados sensíveis. Já na fase pós contratual, iremos abordar principalmente o prazo o qual torna-se necessário que o empregador mantenha os dados captados a fim de se resguardar de eventuais ações trabalhistas. Por fim, analisa-se a responsabilidade do empregador na conjuntura desses momentos e as possíveis sanções aplicáveis pela ANPD – Agência Nacional de Proteção de Dados a cada caso.

Palavras-Chave: Direito. LGPD. Tecnologia. Direito do Trabalho.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho **justifica-se** pelo cenário atual de grande fluxo de informações em um mundo globalizado e a atual necessidade de adequação das empresas na utilização dos dados captados, assim como as possíveis sanções a serem aplicadas, cabendo a tal novo diploma legal conceituar e exemplificar os pilares da regimentação, sustentando princípios elementares.

No atual cenário globalizado é claro o crescimento diário ao acesso à tecnologia e internet em todo o mundo. Tratando-se de mecanismo mais rápido e de fácil acesso, fomenta uma série de preocupações relativas à segurança e à privacidade dos indivíduos que optam por essa ferramenta. Assim, como necessidade de adequação das empresas na utilização dos dados captados e as possíveis consequências pelo mau uso, coube à Lei nº 13.709/2018 - Lei Geral de Proteção de Dado conceituar e exemplificar os pilares dessa regimentação, sustentando princípios elementares, tais como a finalidade e a não discriminação.

Na atualidade, com a mudança do perfil de consumo, muitas empresas tiveram de recorrer a vendas on-line para que pudessem se manter no mercado consumidor. Neste contexto, a questão relativa à segurança dos dados de cada usuário, a maneira como são armazenados suas informações e o risco que isso pode gerar à privacidade de cada indivíduo. Um pequeno deslize de uma empresa com os dados de um usuário pode causar danos irreversíveis a sua imagem.

Neste sentido, com o intuito de fiscalizar a maneira como as organizações lidam com os dados pessoais de seus usuários e trazer maior segurança à proteção desses, a Lei nº 13.709/2018 dispõe sobre a proteção de dados pessoais no país, tendo como missão a proteção do cidadão por intermédio da proteção de seus dados naturais.

Sua aplicação irá atingir pessoas físicas e pessoas jurídicas que realizam a captação e armazenamento de dados pessoais de terceiros, acarretando impactos em diversas esferas do direito como por exemplo contratos, responsabilidade dos empresários, com foco principal nas relações trabalhistas.

Com isso, dada a grande relevância jurídica de uma nova legislação, o trabalho possui como objetivo abordar o tema, sob um prima trabalhista, onde, nesse especial nicho jurídico, ocorre volumoso fluxo de manejo de dados pessoais e sensíveis em todos os momentos da relação de trabalho, seja no período de pré-contratual, contratual ou pós-contratual

Ocorre que, informações íntimas do empregado como por exemplo, opinião política, dados de saúde, opção sexual, entre outras, devem ser mantidas em sigilo, uma vez que não há interesse vinculado ao trabalho quanto a essas informações.

Torna-se, assim, necessária uma adaptação nas empresas e demais empregadores para uma proteção tanto nas relações de emprego como nas demais relações de trabalho. Sendo assim, tal tratamento e a sua devida proteção, será realizada a partir aplicação as bases legais constantes nas leis, como alternativa para àqueles que precisarem lidar com os dados, de modo a se resguardarem das possíveis consequências da não observância da legislação no âmbito trabalhista.

Deste modo, mostraremos como a sua criação tem impacto direto na estruturação das empresas no que diz respeito ao armazenamento dos dados de colaboradores. Tal impacto corresponde principalmente à questão da proteção e privacidade dos titulares de dados, que a cada dia cresce frente ao ambiente tecnológico.

2 INFLUÊNCIA DO MODELO EUROPEU NA CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

O direito à privacidade, que fora trazido pelo art. 12 da Declaração Universal dos Direitos Humanos, compreendido como direito à intimidade do indivíduo, à proteção de sua vida privada, direito à honra e à imagem das pessoas, entendido como um direito diretamente relacionado à esfera pessoal, possui a função de guardar a vida privada frente ao contato com a esfera pública.

Neste contexto de preocupação com a esfera pessoal, devido ao crescente desenvolvimento da tecnologia, durante as décadas de 60 e 70, a Alemanha, de forma pioneira, instaurou no Estado de Hesse, a então chamada *Hessisches Datenschutzgesetz* (Lei de Proteção de Dados de Hessian), visando o maior cuidado das informações pessoais de indivíduos armazenadas em meios eletrônico, o estado de *Rhineland-Palatine*, também na Alemanha, seguiria seu modelo em 1974.

Segundo Monteiro, et al. (2020, p.7):

> O Ato de Proteção de Dados de Hesse foi criado tendo em vista a necessidade de tratar com maior cuidado as informações pessoais de indivíduos armazenadas em meios eletrônicos. A lei, assim, foi pioneira ao tratar da coleta e tratamento de dados de indivíduos, ainda que não o fizesse de maneira objetiva e segmentada. (Monteiro, et al, 2020)

Anos mais tarde, na Suécia no ano de 1973, foi aprovada a primeira lei de proteção de dados *Sw. Datalagen* (Lei nº 289, de 11 de maio de 1973 - Lei de Informação Sueca) objetivando trazer ao Estado a função de guarda e proteção de dados dos cidadãos. Assim como anteriormente em Hesse, as coletas de dados ocorriam de forma genérica e aleatória, não regulamentando quais os dados poderiam ou não ser coletados e a qual finalidade seria aplicada. Entretanto, fora a primeira legislação, que entregou as mãos do governo tal obrigação de regulamentação, dispondo que essa coleta, apenas poderia ocorrer, com a prévia autorização da agência governamental competente.

Seguindo esta tendência, nos anos que se seguiram, outras nações como a França, Espanha, Portugal e Dinamarca também adotaram sistemas de proteção de seus dados. Cumpre aqui destacar que, para diversos países, a proteção de dados fora considerada como um direito fundamental em suas constituições e tratados internacionais, demonstrando assim, a grande importância tratada ainda na década de 70.

Na década seguinte, o Conselho da Europa aprovou, o que então se pode considerar o primeiro marco legal sobre a proteção de dados, a Convenção 108, tendo como função precípua, a proteção à vida privada, levando-se em consideração o grande fluxo de informações e dados de caráter pessoal, sendo posteriormente atualizada e modernizada, sendo então conhecida como Convenção 108+.

Em 1995, 25 anos após a criação Lei de Hesse, a então União Europeia, inspirada pelo desenvolvimento do modelo de negócios da economia digital, gerada através do crescente fluxo internacionais de bases de dados gerados pelos avanços tecnológicos oriundos da globalização, aprovou a Diretiva 95/46/CE, regulamentando dentro do campo de seu bloco, o tratamento de dados, o direito dos usuários - assunto até então inédito frente aos seus antecessores.

Ademais, a Diretiva além de estabelecer como ocorreria a captação e o tratamento dos dados coletados, apresentava os princípios norteadores a serem seguidos em tais coletas, do qual, pode se destacar aqui, a licitude na captação, a limitação a quantidade de dados a serem coletados e a sua adequação à necessidade e à transparência nas informações que visam frear possíveis abusos por parte dos responsáveis pelas mesmas.

A Diretiva 95/46/CE vigorou até maio de 2018, quando foi substituída pelo Regulamento n° 2016/679, aprovado em 27 abril de 2016 e implementado em 25 de maio de 2018 pelo Parlamento Europeu, amplamente conhecida como, *General Data Protection Regulation* (‘GDPR’) ou Regulamento Geral de Proteção de Dados (‘RGPD’).

A GDPR, em seu preâmbulo, informa possuir em seu condão de aplicação, não apenas o tratamento de dados de pessoas naturais localizados na União Europeia, mas sim, todo o fluxo de dados relativos aos países membros e aos países ao redor do mundo que possuem conexão com o mercado europeu, bem como a exportação de dados pessoais para fora da UE e do EEE – a chamada transferência internacional de dados, com foco na responsabilização das organizações e das empresas que realizam a captação e o processamento de dados, assim como a ampliação dos direitos do usuário, a garantia da segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos da sociedade como um todo.

A implantação da GDPR trouxe consigo a previsão de adequação dos agentes em até dois anos, findando em maio de 2018, quando então, iniciou-se a aplicação das penalidades impostas.

Tal previsão ocasionou um ‘efeito cascata’ nos demais países que possuíam conexão com a União Europeia, onde a proteção de dados passou a ser elemento relevante de observação nas tratativas de novos acordos econômicos, sem prejuízo da revisão daqueles já firmados, visto que passou-se a exigir dos demais países e empresas que buscassem relações comerciais com o

bloco o mesmo nível de regulamentação imposta, caso contrário, ocorreria o bloqueio econômico e comercial com os países integrantes da UE.

Neste sentido, segundo a autora Patrícia Peck Pinheiro (2020, não paginado):

> Os efeitos da GDRP são principalmente econômicos, sociais e políticos. Trata-se de apenas uma das muitas regulamentações que vão surgir nesta linha, em que se busca trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras.

Neste sentido, nasce a relevância da atuação das Autoridades Nacionais de Proteção de Dados ou *Data Protection Authorities* (DPA), entidades que buscam garantir o direito de todos à privacidade e proteção de seus dados.

Neste contexto, o Brasil, tendo como principal fonte de inspiração a lei geral de proteção de dados da União Europeia, passou a fazer parte do rol dos países com políticas de proteção de dados. Inicialmente, com o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), disciplinando o uso da internet no Brasil, tendo como fundamento o respeito à liberdade de expressão, compelindo às ilicitudes nas esferas civis e criminais, praticadas sob o manto da privacidade na internet e também na Lei do Cadastro Positivo (Lei complementar nº 166). Entretanto, em ambos os casos, o assunto ainda era tratado de forma obscura acerca dos critérios a serem considerados adequados para o tema, como os conceitos básicos, o manuseio e guarda de dados.

Tais lacunas somente vieram a ser sanadas em 14 de agosto de 2018, com a aprovação da Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (‘LGPD’), que posteriormente seria submetida a diversas alterações, principalmente no que tange ao período de vacância da lei, que em seu projeto inicial, teria como prazo 18 meses. Entretanto, em 27 de dezembro de 2018, após alterações legislativas, por meio da Medida Provisória nº 869 (e a sua posterior conversão na lei 13.853/19), culminou na criação da Autoridade Nacional de Proteção de Dados (ANPD) e alterou o prazo de vigência para 24 meses.

O art. 2º da Lei nº 13.709 de 14 de agosto de 2018 - LGPD, apresenta um rol de fundamentos, incluindo:

> I - O respeito à privacidade; II - a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasília, (DF), 2018)

Atualmente, cumpre ressaltar que as sanções administrativas aos agentes que não se adequarem a nova regulamentação somente poderão ser aplicadas a partir de 1º de agosto de 2021.

Deste modo, pode-se observar que, ocorrendo a evolução histórica da sociedade, de modo diretamente ligado ao aumento do fluxo de informações entre os países, houve também o crescimento da necessidade de se regulamentar os dados que ali transitavam, tornando-se uma obra de políticas públicas internas, que refletiam nos vários setores da economia interna e nos relacionamentos externos, políticos e comerciais.

3 PRINCIPAIS CONCEITOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº13.709/2018, tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, uma vez que os dados pessoais ganham importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opiniões, entre outras atividades.

Atualmente, mais de 126 países do mundo possuem leis para a proteção de dados pessoais, visando à regulamentação do tratamento de dados das empresas, evitando assim, o mal uso destas informações, bem como a pôr incidentes e acidentes com os dados pessoais.

Quanto à territorialidade, a LGPD, se aplica aos dados pessoais de indivíduos localizados no Brasil, assim como quando o tratamento desses dados ocorrer no Brasil e quando houver a oferta de bens e serviços para indivíduos, não se aplicando, porém, quando os dados forem provenientes e destinados a outros países que estejam apenas transitando no território nacional. Não se aplicará também para o uso pessoal, para uso não comercial, para fins jornalísticos, acadêmicos ou de segurança pública.

3.1. O que são dados pessoais?

Os dados pessoais são definidos na LGPD, em seu art. 5º, como sendo aqueles que permitem identificar seu titular ou torná-lo identificável. Como exemplos, tem-se: nome, endereço, números únicos identificáveis (CPF, ID, CNH), exames médicos e dados referentes a sua saúde, biometria, entre outros.

Dentro deste conceito, há uma subclassificação de dados pessoais, denominada dados pessoais sensíveis, que, devido a sua importância, demandam mais proteção em comparação aos dados pessoais comuns. Como exemplos tem-se a orientação sexual, a filiação sindical, a opinião política e os dados referentes à origem étnica e racial.

3.2. O que pode ser entendido como tratamento de dados pessoais?

O tratamento de dados pessoais - comuns ou sensíveis, pode-se entender como toda a operação realizada efetivamente com os dados pessoais, referindo-se a sua coleta, sua produção, sua receptação, classificação, utilização, acesso, transmissão, distribuição, processamento, arquivamento, entre outros.

Esses dados serão manuseados pelos agentes de tratamento, pessoas que, segundo a lei, são classificadas como controladores e operadores dos dados pessoais. O controlador, é a pessoa física ou jurídica, de direito público ou privado, a quem compete a tomada de decisões referente aos tratamentos dos dados pessoais. Já ao operador de dados pessoais, que também pode ser uma pessoa física ou jurídica, de direito público ou privado, compete a realização propriamente dita do tratamento destes dados em nome do controlador.

Em caso de ato contrário aos termos da LGPD, tanto o operador como o controlador irão responder diretamente, de forma subjetiva e solidária com a empresa para a qual atuam sobre o incidente envolvendo dados pessoais.

A lei também previu a criação do cargo de encarregado ou DPO – *Data Protection Officer*, que poderá ser a pessoa física ou jurídica, empregado já contratado ou uma nova contratação. Entretanto, O DPO precisa ter autonomia, independência e acesso ao mais alto nível da direção da empresa, ou seja, no exercício da função a organização precisa apoiá-lo e conferir-lhe todas as informações necessárias em relação ao tratamento de dados pessoais, pois será o responsável por realizar todo possível esclarecimento aos titulares dos dados e às autoridades. O DPO terá a sua identidade disponibilizada aos titulares e às autoridades, devendo o seu contato estar disponibilizado de forma simples e de fácil acesso.

Para se adequar a este novo cenário, as empresas deverão providenciar documentos essenciais a fim de que estejam em conformidade com a LGPD. Dentre estes documentos, as empresas deverão possuir um relatório de impacto à proteção de dados pessoais, documentação esta que será de responsabilidade do controlador e que conterá a descrição dos processos de tratamento de dados pessoais, chamado de ciclo de dados, que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas e mecanismos de mitigação de riscos, tais como alterações de contrato e criação de políticas de proteção de dados.

3.3. Quais são as bases legais para o tratamento de dados?

Atualmente, para cada finalidade de uso de dados, o tratamento deve estar justificado em uma das bases legais previstas no art.7º da LGPD, dos quais são:

- O consentimento pelo titular: Conforme disposto no art.8, o consentimento do titular, será o meio pelo qual o titular dos dados pessoais poderá determinar o nível de proteção e garantir a extensão do fluxo de seus dados, através de sua anuência clara e expressa,

devendo estar destacado das demais cláusulas contratuais, a fim de que não se passe despercebido. Tal consentimento poderá ser revogado a qualquer momento pelo titular e deverá a ele ser garantido a sua facilidade a revogação, assim como, ocorrer de modo gratuito.

- Cumprimento de obrigação legal ou regulatória pelo controlado: Ocorrerá quando, diante da própria natureza jurídica da relação, torna-se obrigatória a captação de dados, não dependendo do consentimento do titular. Como exemplo dessa base legal tem-se a coleta de dados para a emissão de nota fiscal, ou ainda, a captação de dados pessoais do trabalhador para envio à Caixa Econômica Federal para cadastro junto ao FGTS.
- Execução de políticas públicas: Ocorrerá quando o tratamento de dados tiver como objetivo o cumprimento de execuções públicas do Estado, tais como a verificação de qualidade de ensino em instituições ou ainda em projetos públicos de campanhas de saúde.
- Estudo por órgãos de pesquisa e desenvolvimento: Será destinado a órgãos que, possuíam como intuito, a elaboração de pesquisas e estratégias de desenvolvimento de setores, devendo, sempre que possível, ocorrer com anonimação dos dados pessoais. Tem-se como principal exemplo dessa base legal, a realização do Censo, estudo estatístico realizado pelo governo para identificar suas características e revelar como vivem os brasileiros, produzindo informações para a definição de políticas públicas.
- Execuções de contratos: Será lícito o tratamento de dados pessoais, quando tornar-se necessário para a execução de obrigações contratuais, no qual o titular dos dados é parte ou para a realização de procedimentos preliminares a sua constituição.
- Exercício regular de direitos em processo legal, arbitral ou administrativos: Nesta base legal, será autorizado o tratamento de dados pessoais que integrem o curso do processo legal, sendo possibilitado o seu tratamento para o fornecimento para a produção de provas.
- Para a proteção da vida, da integridade física e a tutela da Saúde: Os dados tratados no âmbito da saúde podem servir para garantir a proteção da vida ou integridade física pelos agentes de saúde, como médicos, enfermeiros e agentes sanitários. Assim como garantir a qualidade de vida da sociedade e a redução de riscos ao adoecimento. Em relação à autoridade sanitária, recorda-se a Lei nº 9.782/99, que define o Sistema Nacional de Vigilância Sanitária e cria a Agência Nacional de Vigilância Sanitária.

- Legítimo interesse: O legitimo interesse é a hipótese legal que, dentro de um caso concreto, quando presente situações relevantes entre o titular dos dados e o responsável pelo tratamento, onde esteja presente uma razoabilidade esperada e um limite de uso, poderão ser tratados os dados através de um teste legítimo de interesse. Mostrar que há um interesse legítimo significa que o controlador (ou um terceiro) deve terá algum benefício ou resultado claro e específico em mente. Não basta afirmar a existência de interesses comerciais vagos ou genéricos.
- Para a proteção do crédito: Os dados pessoais podem ser tratados para a proteção ao crédito de forma a tornar a economia do país mais segura e conceder mais benefícios a quem cumpre com as suas obrigações. Nesse caso, a base deverá restar em constante diálogo com normas como o Código de Defesa do Consumidor (Lei nº 8.078/90), a lei do cadastro positivo (Lei nº 12.414/11) e portarias do Ministério da Justiça.

3.4. A Autoridade Nacional de Proteção de Dados (ANPD)

Com a promulgação da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), através da Medida provisória nº 869, com a sua posterior conversão na Lei nº 13.853 de 14 de agosto de 2019, tendo sua competência estabelecida pelo art. 55-J, sendo suas principais funções o zelo pela aplicação da lei, fiscalização, comunicação com os controladores e fixação de sanções caso verificadas irregularidades.

A ANPD não possui autonomia ainda, pois encontra-se vinculada à Presidência da República, possuindo 2 anos de prazo para uma possível transformação em órgão da Administração indireta, na forma de Autarquia. Referida Autoridade será composta pelo Conselho Diretor, Corregedoria, Ouvidoria, órgão de assessoria jurídica, unidades necessárias à aplicação da LGPD e um Conselho Nacional.

Segundo a autora Patrícia Peck Pinheiro (2020, não paginado):

> Mas é importante ter em mente que não basta ter a lei de proteção de dados pessoais, é preciso educar, capacitar. Por isso, a importância do papel orientativo da autoridade (ANPD), e a relevância de sua atuação proativa junto à sociedade e às instituições, para encontrar medidas viáveis de implementação da nova regulamentação, que gerem menor impacto possível nos setores produtivos e que sejam adaptados e aderentes aos usos e costumes.

3.4.1. Direitos do titular

Os direitos dos titulares de dados, presentes nos artigos 17 ao 22 da Lei nº 13.709/2018, possuem uma grande gama de especificidades, dentre as quais podem ser destacar: o acesso facilitado às informações que as empresas possuem do usuário, que, ao ser exigido, deverá ser prestado de forma clara e precisa, o direito a anonimização, correção, bloqueio e eliminação de dados incorretos, informação sobre eventual compartilhamento de dados entre empresas, e a mais importante: a revogação a qualquer tempo de eventual consentimento para utilização, que deverá ocorrer de forma expressa, em um processo gratuito e facilitado.

3.4.2. Tratamento irregular e as sanções aplicáveis

A aplicação das sanções e penalidades pela ANPD entraram em vigor a partir de 1º de agosto de 2021, iniciando-se com um processo administrativo que possibilite a ampla defesa. As penalidades vão de advertência, multas com limite de R$ 50.000.000,00 (cinquenta milhões de reais) até a proibição total ou parcial de toda execução de atividades relacionadas ao tratamento de dados.

Sobre o tema, diz o site oficial da ANPD (2021, não paginado):

> Nos termos da Lei, a aplicação de sanções requer, ainda, criteriosa apreciação e ponderação de inúmeras circunstâncias, dentre as quais a gravidade e a natureza das infrações e dos direitos pessoais afetados, a condição econômica do infrator, o grau do dano, a cooperação do infrator, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas.

Verifique-se que as Empresas deverão tratar com seriedade a conformidade com a LGPD, sempre atentando aos seus princípios norteadores, sob o risco de sofrerem graves punições.

Assim, a partir do que foi apresentado neste capítulo, pode-se entender que a interpretação da LGPD, com a sua posterior aplicação nos mais diversos ramos do direito, não poderá ser realizada sem a observação de seus princípios e conceitos basilares, sendo essencial entender a forma com a qual a privacidade alterou-se diante da sociedade informacional, moldando-se para dar ao indivíduo o poder de controle e a devida informação acerca da coleta e tratamento de seus dados pessoais.

4 A LGPD E OS REFLEXOS NAS FASES DO CONTRATO DE TRABALHO

A LGPD vem provocando significativas mudanças nas rotinas empresariais, principalmente no que tange ao tratamento dos dados de seus empregados, assim como prestadores de serviços contratados, parceiros, sócios e as pessoas físicas que, de alguma forma, precisem ter seus dados disponibilizados entre organizações. Diante disto, torna-se fundamental a revisão de todos seus procedimentos para a coleta de dados, de forma a compatibilizá-los com as atuais previsões da LGPD.

No que tange à contratação de colaboradores, as empresas deverão estar atentas a todos os momentos contratuais, pois os cuidados com o tratamento dos dados deverão ocorrer desde a fase pré-contratual, fase contratual e pós-contratual.

Logo, torna-se digno de nota que a legislação brasileira não excluiu, ao contrário do GDPR europeu, os dados laborais da necessidade de proteção e tratamento, quanto em seu artigo terceiro deixa claro que a LGPD “aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados”, não excluindo, portanto, as relações jurídicas existentes neste cenário.

Neste sentido aborda, Adriana Giutini (2021, p.7):

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

Vale destacar que não existe um manual para a adequação à LGPD, devendo cada empresa aplicar internamente os processos e procedimentos, com uma equipe multidisciplinar, composta, dentre outras, pelas áreas jurídica, de tecnologia e departamento pessoal, para identificar a necessidade de alteração de algum procedimento, levando-se em consideração o perfil empresarial presente em suas ações, seu tamanho e a quantidade de colaboradores e fornecedores.

4.1. Fase Pré-contratual

A fase pré-contratual abrange todo o processo de seleção, isto é, abertura de vaga, recebimento de currículos com sua triagem e entrevistas, até a realização da contratação. Nesta fase é natural de compreender-se que as empresas necessitam coletar diversos dados para cumprimento de obrigações legais ou regulatórias, tais como envio de dados para Ministério da Economia, INSS, E-social. Sendo assim, devido ao fato de tratar-se de cumprimento de obrigações legais, não requer a necessidade de autorização expressa do titular, desde que tais dados sejam usados para a finalidade obrigacional.

Neste ponto, torna-se usual as empresas acumularem grande volume de currículos, formando um pequeno banco de dados, para serem utilizados posteriormente em outras vagas, neste sentido, deve-se também aplicar os preceitos trazidos pela LGPD no que tange a este armazenamento, devendo, portanto, os empregadores adotarem medidas as quais, solicitem apenas as informações estritamente necessárias para a avaliação e seleção do candidato, assim como, informar ao candidato o tratamento que será dado às informações ali presentes e verificar se há interesse em manutenção do currículo em banco de dados, necessário, portanto, na captação de autorização expressa para isso.

Todavia, torna-se estritamente necessário o cuidado para não solicitar qualquer informação, limitando-se somente a coleta de dados necessários para os devidos cumprimentos legais.

Não obstante, para situações como fornecimento de vale alimentação, contratação de planos de saúde, cartão transporte, dentre outros, o colaborador deverá autorizar claramente a utilização e compartilhamento de seus dados com as demais instituições.

4.2. Fase Contratual

A fase contratual inicia-se com a efetiva admissão do empregado ou a formalização do contrato com prestador de serviços. A partir deste ponto, todos os dados coletados pela empresa terão um fluxo maior e, portanto, deverá haver uma maior cautela, com a instauração de procedimentos específicos, de acordo com a realidade de cada empresa.

Outro aspecto importante de se observar, é referente à coleta dos dados biométricos para registro do controle de jornada de trabalho. Agora, com a LGPD, este dado também é protegido, sendo considerado um dado sensível, requerendo, portanto, um maior cuidado com o seu tratamento. Assim, diante desta proteção, o empregado terá que ser claramente comunicado

sobre a finalidade da coleta, devendo emitir um consentimento expresso e específico para utilização dos dados biométricos pela empresa ou prestadora de serviço.

As empresas que oferecem aos seus funcionários plano de saúde, por tratar-se também de um dado sensível, precisará revisar com extrema cautela o seu contrato com a seguradora que presta os serviços, já que poderá ser responsabilizada por incidentes de segurança incorridos pelos operadores por ela indicados.

Empresas que realizem a contratação de menores de idade, assim como a indicação de dependentes menores de idade do empregado, os responsáveis legais deverão, nos termos da lei, autorizar expressamente o tratamento, além de serem mantidos a par de todos os tratamentos realizados com os dados pessoais dos menores, assim como eventuais compartilhamentos.

Vale ressaltar ainda que, o empregado como titular desses dados, a qualquer momento, poderá solicitar que o empregador informe os dados que possui e destinação destas informações, bem como que o empregador efetue a eliminação dos mesmos quando a rescisão contratual, exceto para cumprimento de obrigações legais e regulatórias, como veremos logo a frente.

4.3. Fase Pós-contratual

Pode-se entender como fase pós-contratual a fase caracterizada pelo desligamento de um funcionário ou colaborador dos quadros da empresa. Neste momento, nasce o dever de informação de finalização do uso de dados ao titular, ora pela determinação legal, ora por solicitação do próprio titular.

Entretanto, em relação ao uso de dados na seara trabalhista, nascem obrigações legais de guarda de documentos, tais como as obrigações de cunho fiscalizatório, logo, podem acarretar o afastamento da solicitação do titular do direito, em eventual uso de dados no futuro, tal como a sua exclusão, devendo ser analisado sua destinação, envolvida no caso concreto.

Neste cenário, surgem questionamentos sobre quanto tempo necessário que as empresas poderão ter a guarda de dados pessoais do empregado, após a rescisão do contrato de trabalho, de modo a amparar sua defesa em eventuais reclamações trabalhistas. Diante do fato que o empregado possui o prazo prescricional de 2 (cinco) anos, contados do fim da relação de trabalho, para os últimos 5 (cinco) anos pretéritos do contrato de trabalho para propor reclamação trabalhista, entende-se que é defeso a guarda de dados igual período, visto que, o trabalhador só pode propor ação visando seus direitos trabalhistas durante este tempo.

Entretanto, poderá ocorrer casos especiais, como determinadas questões que envolvam acidentes e doenças do trabalho, diante disto, este prazo pode variar, devido ao fato que, o prazo

prescricional somente começará a contar a partir do conhecimento da doença, fato este que poderá ocorrer após a extinção do contrato de trabalho, gerando portanto, a necessidade de armazenamento das dados pessoais do empregado um maior tempo.

Fato este que torna tal guarda uma questão importante, diretamente ligado ao fato de ainda não existir regulamentação normatizada quanto ao tempo que as empresas devem armazenar os dados dos ex-colaboradores. Contudo, embora ainda não haja resposta correta a esta questão, torna-se recomendável, porém que as empresas tratem os casos de maneira centrada, delimitando os locais de possíveis demandas trabalhistas.

Caberá aqui também pontuar que, em decorrência do contrato de trabalho, ocorrerá a obrigação do empregador na guarda de dados para compartilhamento com planos de saúde em caso de aposentadoria ou desligamento sem justa causa, tal como elucidado por Leandro Sampaio Correa de Araújo (2021,p.25), tal como nos casos que por exemplo “envolvam doenças e/ou acidentes, pois o marco prescricional tem como ponto de partida a data do efetivo conhecimento do titular (diagnóstico e extensão dos danos) ou quando do evento morte (titular), sendo os herdeiros menores, caso em que não é deflagrado de imediato o prazo”.

Portanto, para todos os momentos que necessitem da autorização do empregado para a utilização desses dados, é imprescritível que o documento informe, de forma clara e específica, para qual finalidade destina-se os dados solicitados, assim como, prever as necessidades de compartilhamento, bem como conste a assinatura do empregado. Vale destacar que, afim de evitar qualquer nulidade do documento, as autorizações não poderão ser genéricas e inseridas aleatoriamente no documento, deverão, portanto, estar presentes de forma explicita e destacada dos demais tópicos presentes no documento.

Ainda referente aos prazos prescricionais, no que tange ao titular dos dados, trazemos relevantes contribuições de Leandro Fernandez (2021, p.12):

> I) Só se pode falar em prescrição a partir de uma conduta de inércia do titular do direito, e para tanto é fundamental que ele tenha tido ciência inequívoca de houve a violação/lesão ao seu direito. II) Sob o prisma do direito constitucional classifica-se como um direito fundamental e sob a ótica do direito civil os direitos do titular dos dados enquadram-se como direito da personalidade; III) Em ambos os casos (direito constitucional ou civil) podemos enquadrá-los como imprescritíveis, assim ainda que os titulares deixem de exercê-los por um longo período de tempo, eles não perdem esses direitos, entretanto isso não significa que eles possam a qualquer momento exercer o direito de pleitear a reparação em razão de eventual ofensa a esses direitos; IV) De igual modo, se alguém vem seguidamente violando determinado direito ele não adquire para si o direito de continuar violando tal norma jurídica, podendo o titular do direito pleitear que essa violação seja cessada, a qualquer tempo; V) Feitos esses esclarecimentos, deve se aplicar no âmbito das relações trabalhistas em regra os prazos prescricionais especificamente estatuídos na Carta Magna e na CLT, quais sejam dois anos após a extinção do contrato, retroagindo cinco anos, devendo se observar a hipótese de ciência inequívoca da violação por parte do ex-colaborador após grande lapso temporal, sendo neste caso iniciado o prazo prescricional de dois anos a partir do conhecimento da lesão. VI) Entretanto, para lesões ocorridas na fase pré-contratual, deve se aplicar o prazo de cinco anos após a ciência inequívoca da violação aos ditames da LGPD; VII) Por fim, deve se destacar que a maioria dos direitos dos titulares dos dados não podem ser limitados temporalmente, eis que pela própria essência deles são atemporais, podendo ser exercidos a qualquer momento, tal como se observa do rol constantes dos artigos 9 e 18 da LGPD.

No mesmo sentido, aborda Carloto (2020, p. 202):

> Os dados deverão sempre ser eliminados após o fim do tratamento. Em regra, os dados poderão ser guardados durante o prazo prescricional trabalhista, mas quando coletada a biometria digital, por exemplo, estes dados deverão ser eliminados assim que acabar o tratamento, ou seja, com a extinção do contrato de trabalho, já que os mesmos eram apenas utilizados para o Registro Eletrônico de Ponto.

Diante disto, observa-se que o art. 8º acima referenciado, estabelece em seu parágrafo segundo, que será incumbido à empresa o ônus da prova de que o consentimento do empregado fora coletado em conformidade com o regulamentação da LGPD, criando portanto, para proteção dos dados pessoais, uma regra processual especial, normatizando o procedimento ordinário no âmbito probatório diante da importância do objeto do processo.

Isto posto, em conformidade com a regra da especialidade, a legislação especial desloca no caso em concreto, a aplicação da regra geral do ônus estático da prova, presente no art. 818 da CLT, considerando que, a LGPD traz um regramento mais recente, em relação ao tratamento dessa matéria em aplicação a consolidação laboral, mesmo considerando a reforma trabalhista de 2017.

4.4. A responsabilidade do empregador

Na vigência do contrato de trabalho, o empregador como parte hiperssuficiente, responsável pela tomada de decisões, possui consigo a função de controlador de dados de seus empregados, cabendo a ele, portanto, a responsabilidade pelos dados coletados, assim como a forma que serão usados e como serão descartados.

Logo, possui dentre outros deveres, o de fornecer, de forma clara e de forma contínua aos seus colaboradores, informações sobre o tratamento dos dados pessoais que transitarem na empresa, indicar medidas técnicas e administrativas para prevenir o vazamento de informações; oferecer treinamentos e atualizações sobre o tema, para permitir a criação da cultura de proteção de dados dentro da empresa e cuidar para que a transferência dos dados dos colaboradores seja realizada de forma segura, ainda que para o cumprimento de obrigações legais ou regulatórias.

Com relação às sanções administrativas, uma vez comprovadas, a empresa ficará sujeita à advertência, estipulando prazo para adoção de medidas corretivas, bem como multa simples de até 2% (dois por cento) do faturamento da empresa, limitada a R$ 50.000.000,00 (Cinquenta milhões) por infração.

Deste modo, é evidente que a LGPD veio para causar impactos positivos na proteção dos dados pessoais, contudo a empresa deve se atentar às regras previstas na legislação, a fim de que as sanções previstas na Lei não sejam causadoras de impactos ainda maiores e devastadores aos negócios da empresa infratora, especialmente à de menor porte e capital, por mero descuido ou desatenção à Lei.

5 CONCLUSÃO

Diante de todo o exposto neste trabalho, conclui-se que, que com o advento da Lei nº 13.708/18 - Lei Geral de Proteção de dados, no que tange às relações de trabalho, torna-se necessária uma efetiva adequação dos contratos de trabalho, pois, grande parte do fluxo dos dados ocorrerão fundamentadas no art. 7, inciso II, que trata da base legal para cumprimento de obrigação legal ou regulatória, ou ainda, no art.7, inciso V, para execuções de contratos.

Portanto, a captação e o tratamento de dados deverão ocorrer de forma responsável, sendo observado seriamente a tênue distinção entre o que será um dever jurídico, o poder diretivo do empregador e as previsões da LGPD, devendo ser priorizadas pelas empresas daqui por diante.

Com isto, pode-se constatar que, o advento da LGPD trouxe a necessidade de mudanças importantes nas rotinas das empresas, inicialmente no que se refere à forma do tratamento dos dados de toda pessoa física que possua relação com a organização. As adequações tornam-se necessárias ao passo de evitar a aplicação de sanções, que podem variar de advertências, até aplicação de multa de até 50 milhões de reais, quantia bastante impactante em uma rotina financeira empresarial.

Entretanto, em todos os casos, é de extrema importância que seja realizada a adequação de normas internas e a adequação desses contratos com cláusulas claras relacionadas a privacidade e a proteção desses dados, seja por cláusulas destinadas a este fim, seja por meio de aditivos contratuais.

Dessarte, na vigência da Lei Geral de Proteção de Dados, as partes, titular dos dados e operador, devem manter a observância e cumprimento das regras quanto à proteção de dados, principalmente no que se refere ao tratamento de dados pessoais e sensíveis, mediante aditivos e termos específicos, de acordo com as necessidades e/ou obrigações legais para a coleta dos dados e com destinações relacionadas ao compartilhamento de dados com terceiros, como é o planos de saúde, operadoras do estado ou sindicatos, que, em regra, necessitam de autorização expressa do titular, de forma livre, informada, inequívoca e relacionada a uma determinada finalidade.

REFERÊNCIAS

AGUIAR, Antônio Carlos. **A proteção de dados no contrato de trabalho**. Revista Ltr: legislação do trabalho, São Paulo, SP, v. 82, n. 6, p. 655-661, jun. 2018.

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

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. 4. ed. São Paulo: Saraiva, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 de setembro de 2021

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de DadosPessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: SenadoFederal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em:14 de setembro de 2021

BOMFIM, Vólia C. **Direito do trabalho**. 9. ed. rev. e atual. São Paulo: Método, 2014. p.1332.

CARLOTO, Selma. **Lei geral de proteção de dados**: enfoque nas relações de trabalho. São Paulo: Ltr. 2020 p.212.

CONI JR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. **A lei geral de proteção de dados pessoais e seus impactos no direito do trabalho.** Salvador. Revista Direito UNIFACS – Debate Virtual. Número 239.2020.

GOVERNO FEDERAL (Brasil). Autoridade Nacional de Proteção de Dados. In: **Perguntas Frequentes**. [S. l.], 14 out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c1. Acesso em: 14 out. 2021.

LGPD nas relações de trabalho [livro eletrônico] / Adriana Giuntini... [et al.]. – 1.ed. – Salvador, BA : Motres, 2021.Disponível em: https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf. Acesso em: 14 de novembro de 21

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriane Loureiro; MORIBE; Gabriela. CAMARA; Dennys Eduardo Gonsales; GHERINI, Pamela Michelena de Marchi. **Lei Geral de Proteção de Dados e GDPR:** Histórico, análise e impactos. São Paulo, Baptista Luz Advogados, 2020. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 14 de set. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários a Lei nº 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento dedados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Data de acesso.14 out. 2021.