UNIVERSIDADE FEDERAL DE SERGIPE
CAMPUS SÃO CRISTÓVÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

JOHNATAN DOUGLAS ANDRADE DE JESUS

A NOVA REALIDADE DO TRATAMENTO E DA PROTEÇÃO DE DADOS DOS TRABALHADORES FRENTE A LGPD E O *COMPLIANCE* JURÍDICO

SÃO CRISTÓVÃO
2021

JOHNATAN DOUGLAS ANDRADE DE JESUS

A NOVA REALIDADE DO TRATAMENTO E DA PROTEÇÃO DE DADOS DOS TRABALHADORES FRENTE A LGPD E O *COMPLIANCE* JURÍDICO

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito da Universidade Federal de Sergipe, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientadora: Profª. Drª. Clara Angélica Gonçalves Cavalcanti Dias

SÃO CRISTÓVÃO

2021

Há, então, dois princípios contrários, um bom e outro mau? Perguntaram os discípulos de Manés. Não, os dois princípios do equilíbrio universal não são contrários ainda que opostos em aparência, porque é uma sabedoria única a que opõe um ao outro. O bem está à direita, o mal à esquerda; porém a bondade suprema se acha acima de ambos e ela se servirá do mal para o triunfo do bem, e do bem para a reparação do mal.
(Eliphas Levi)

RESUMO

O presente trabalho busca compreender a nova realidade do tratamento e da proteção de dados dos trabalhadores frente a Lei Geral de Proteção de Dados, e apresenta o *compliance* jurídico como uma ferramenta que o empregador encontra a disposição para auxiliar na adaptação da empresa. Baseado no método dedutivo e por meio da análise bibliográfica e da legislação sobre o tema, este trabalho se divide em três partes. Em um primeiro momento se faz um apanhado histórico de como as novas tecnologias impactaram o mundo do trabalho. Também é abordado o conceito de indústria 4.0 e o surgimento das leis de proteção de dados. A segunda etapa aborda o impacto da Lei Geral de Proteção de Dados nas relações de trabalho. A terceira e última parte busca mostrar como o *Compliance* jurídico é uma ferramenta eficaz no processo de adequação das empresas aos impactos da LGPD. Constatou-se que a Lei Nº 13.709/2018 influi diretamente no Direito do Trabalho e altera a forma com que o empregador deve tratar os Dados dos seus empregados, bem como o *compliance* jurídico sendo uma ferramenta efetiva no processo de adequação da empresa e que pode proporcionar a redução do passivo trabalhista e o aumento da credibilidade perante o mercado.

Palavras-chave: Revolução 4. 0. Direito do Trabalho. LGPD. Compliance.

ABSTRACT

This study focuses in a search to understand the new reality of the treatment and protection of workers' data face of the Data Protection Law, and introduces legal compliance as a device that the employer finds available to assists him in the adaptation of the company. Based on the deductive method and through bibliographic analysis and legislation of the subject, this study was divide in three parts. At first, a historical overview of how new technologies have affected the world of work, with the addressment to the concept of industry 4.0 and the emergence of data protection laws. The second part addresses the impact of the Data Protection Law on labor relations. The third and final part examined that Legal Compliance is an effective device in the process of adapting companies to the impacts of the LGPD. The Law No. 13.709/2018 directly influences the Labor Law and changes the way the employer must handle the Data of his employees. Also legal compliance is an effective device in the process of adaptation of the company what brings benefits such as the reduction of labor liabilities and the increase of credibility in the market.

Key words: Industry 4. 0. Labor Law. LGPD. Compliance.

.

SUMÁRIO

1 INTRODUÇÃO 6

2 A REVOLUÇÃO 4.0 8

3 A IMPORTÂNCIA DA PROTEÇÃO DE DADOS E A CRIAÇÃO DE NORMAS 13

3.1 LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) 16

4 O TRATAMENTO DE DADOS PESSOAIS E O SEU IMPACTO NAS RELAÇÕES DE TRABALHO 19

4.1 AS FASES DO TRATAMENTO DE DADOS NAS RELAÇÕES TRABALHISTAS 23

4.2 DO MANUSEIO DE DADOS SENSÍVEIS NAS RELAÇÕES TRABALHISTAS 24

4.3 O PAPEL DO ENCARREGADO DE DADOS NAS EMPRESAS 26

5 O *COMPLIANCE* JURÍDICO 30

5.1 OS MODELOS DE *COMPLIANCE* E SUA RELEVÂNCIA PRÁTICA 33

6 O *COMPLIANCE* TRABALHISTA E A INFLUÊNCIA DA LGPD 37

6.1 O PROCESSO DE ADEQUAÇÃO DA EMPRESA 38

6.2 AS CONSEQUÊNCIAS DO DESCUMPRIMENTO DA LGPD 42

7 CONCLUSAO 45

REFERÊNCIAS 47

1 INTRODUÇÃO

Não se pode afirmar o que vai acontecer no futuro, mas uma coisa é certa: a necessidade de estar preparado para ele. Atualmente a empresa que não investe em tecnologia fica para trás em rentabilidade e na qualidade do serviço prestado. O que convencionou-se chamar de indústria 4.0 muda completamente a relação das pessoas com o consumo e coloca em evidência a problemática em torno da proteção de dados pessoais.

O presente trabalho se debruça em explorar as mudanças advindas a partir da Lei Geral de Proteção de Dados (LGPD), no que diz respeito ao tratamento de dados dos empregados. A lei foi sancionada em agosto de 2018 e teve inspiração na GDPR (General Data Protection Regulation). É um conjunto de normas válidas para o território brasileiro sobre como as empresas, as pessoas e os órgãos públicos devem guardar, proteger e usar informações pessoais coletadas dos usuários.

Dado Pessoal é toda e qualquer informação da qual se possa tornar o titular de direito identificado ou identificável. Na prática, o tratamento de dados se refere a todas as operações realizadas com os dados pessoais dos titulares. O procedimento de tratamento possui algumas fases e a depender do dado que esteja sendo tratado podem existir mais ou menos processos.

Muito embora não exista nenhum artigo expresso na lei direcionando a sua aplicação ao direito do trabalho, possui intrínseca conexão com o direito trabalhista. Os dados e as informações dos empregados devem ser preservados e protegidos, as empresas deverão se atualizar de acordo com a nova realidade ao levar em consideração que nas relações de trabalho os empregadores lidam constantemente com os dados pessoais de seus empregados.

Diante da complexidade das demandas empresariais e das relações jurídicas que envolvem as empresas, surge a importância da adesão a um programa de adequação (*compliance)*, a fim de estabelecer a cultura de estar de acordo com as exigências legais vigentes atrelada a perspectiva da governança corporativa.

A intenção do advogado que presta orientações ou consultorias no sentido do parágrafo anterior é mitigar riscos e evitar problemas. Um programa de *compliance* deve sempre atender às necessidades específicas da empresa, levando em consideração que a depender da atividade explorada estarão sujeitas a riscos diferentes. Assim, antes de criar um programa de *compliance*, deve ser feita uma análise de risco, com o objetivo de verificar quais são as reais necessidades da empresa.

Portanto, criar uma cultura de respeito à proteção de dados capacitando profissionais, ajustando os equipamentos eletrônicos, fortalecer o programa de *compliance*, sempre se assegurar acerca do consentimento do titular de dados é a maneira mais eficaz de reduzir os riscos e contribuir com a efetivação do direito à privacidade no meio virtual.

> Consentimento do titular de dados é a forma mais conhecida de tratamento legal de dados e deve ser livre e o mais consciente possível, ou seja, o titular deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocidade do consentimento. (TEIXEIRA, ARMELIN, 2019).

O dado desnecessário coletado e armazenado de forma irregular representa apenas um risco para a empresa. Por vezes, não só os dados são desnecessários, mas sim todo o processo e as ferramentas de coletagem podem ser considerados desnecessários ou inadequados.

Este trabalho, através de um método direcionado a pesquisa bibliográfica e análise da legislação, parte da perspectiva de que todo o processo de contratação, manutenção e demissão de empregados, no que diz respeito ao armazenamento e tratamento de dados, deverão ser readequados de acordo com a LGPD. Sendo assim, fará parte da análise a cautela sobre quais dados são realmente necessários de coleta e a maneira como serão armazenados e tratados na seara trabalhista.

Ademais, o objetivo desse trabalho é apresentar uma discussão acerca do tratamento e armazenamento de dados trabalhistas, introduzir a ideia de que um processo de *compliance* jurídico é uma ferramenta eficaz contra o aumento de passivo trabalhista decorrentes da inadequação das empresas às normativas da Lei Geral de Proteção de Dados.

2 A REVOLUÇÃO 4.0

De início, as modificações que os homens produziam na natureza eram muito pequenas, sobretudo antes do desenvolvimento da atividade agrícola. Com o passar do tempo, principalmente tendo em vista o crescimento populacional e o desenvolvimento de novas técnicas, o domínio de novas tecnologias e o uso de novos instrumentos de produção, as intervenções humanas no ambiente foram sendo cada vez mais intensas e amplas.

Nesse sentido, após um longo período de adaptação e evolução do ser humano vivendo em conjunto e em sociedade. As revoluções industriais representaram grandes marcos na relação sociedade-natureza e no estabelecimento de novas formas de produção.

Segundo Eric Hobsbawm (2014), as Revoluções Industriais culminaram em modificações econômicas e tecnológicas que solidificaram o sistema capitalista e permitiram a exploração de novas formas de organização da sociedade. Essas transformações foram vividas principalmente na Europa Ocidental, de início limitadas à Inglaterra, nos primórdios do século XVIII e tiveram diversos desdobramentos ou "fases". Esses momentos corresponderam ao processo evolutivo das tecnologias desenvolvidas e as consequentes mudanças socioeconômicas.

Inicialmente, é oportuno abordar as três primeiras fases da revolução industrial. A Primeira Revolução Industrial se refere ao processo de evolução tecnológica vivido a partir do século XVIII na Europa Ocidental, entre 1760 e 1850, na qual se estabeleceu uma nova relação entre a sociedade e o meio ambiente laboral. Possibilitou, também, o surgimento de novas formas de produção. Transformando, principalmente, o setor industrial e dando início a um novo modelo de consumo.

Foi uma fase marcada especialmente pela substituição da energia produzida pelo homem por energias alternativas. Como exemplo, podem-se citar a energia a vapor, eólica e hidráulica. Começou, assim, um processo de substituição da produção artesanal (manufatura) pela indústria (maquinofatura). Logo, surgiu uma nova dinâmica nas relações de trabalho.

A primeira revolução Industrial foi iniciada de maneira pioneira na Inglaterra, a partir da segunda metade do século XVIII. É comum atribuir esse pioneirismo aos ingleses pelo fato de que foi lá onde surgiu a primeira máquina a vapor, em 1698, construída por Thomas Newcomen e aperfeiçoada por James Watt, em 1765. O historiador Eric Hobsbawm (2014),

inclusive, acredita que a Revolução Industrial só foi iniciada de fato na década de 1780. Nascendo, assim, o que hoje chamamos de indústria 1.0.

A produção se reinventou de maneira a possibilitar a diminuição do tempo e o aumento da produtividade. Houve um melhor aproveitamento de matérias-primas, bem como de consumidores, e também favoreceu a distribuição dos bens produzidos.

Contudo, com o passar dos anos a técnica se aperfeiçoou criando novas formas de produção e um segundo modelo de mercado. A Segunda Revolução Industrial se refere ao período entre a segunda metade do século XIX até meados do século XX, findando-se durante a Segunda Guerra Mundial. A industrialização avançou os limites geográficos da Europa Ocidental, espalhando-se por países como Estados Unidos, Japão e outros países da Europa. Os avanços tecnológicos foram considerados ainda maiores que os vivenciados na primeira fase, bem como o aperfeiçoamento de tecnologias que já existiam. O mundo pôde, então, vivenciar uma gama de novas criações das quais aumentaram ainda mais a produtividade e consequentemente os lucros das indústrias.

Os pontos chaves dessa nova fase estão intrinsicamente associadas ao uso do petróleo como fonte de energia. Foi nesse momento que surgiu o primeiro motor a combustão. A eletricidade, que antes servia apenas para desenvolvimento de pesquisas em laboratórios, começou a ser utilizada para o funcionamento de motores, com destaque para elétricos e à explosão. O ferro, que antes era largamente utilizado, passou a ser substituído pelo aço.

A Terceira Revolução Industrial, que também ficou conhecida como Revolução Tecnocientífica, teve início na metade do século XX após a Segunda Guerra Mundial. Segundo Hobsbawm (2014) esse momento representa uma revolução não só no setor industrial, uma vez que passou a relacionar não só o desenvolvimento tecnológico voltado ao processo produtivo, mas também ao avanço científico que deixa de ser algo limitado a apenas alguns países e se espalhando por todo o mundo.

As transformações advindas pelos avanços tecnocientíficos são facilmente observáveis até os dias atuais, e também cada nova descoberta representa outro patamar alcançado dentro dessa fase da revolução. Surgindo, assim, o que ficou conhecido como capitalismo financeiro. A introdução da biotecnologia, robótica, avanços na área da genética, telecomunicações, eletrônica, transporte, entre outras áreas, transformaram não só a produção como também as relações sociais, o modo de vida da sociedade e o espaço geográfico.

Todos esses desenvolvimentos proporcionados pelos avanços obtidos nas diversas áreas científicas relacionam-se ao que se convencionou chamar de globalização. Tudo converge para

a diminuição do tempo e das distâncias, interligando pessoas, integrando lugares, transmitindo informações na velocidade da luz. Superando, assim, os desafios e obstáculos naturais das localizações geográficas, diferenças culturais, físicas e sociais.

> Há um tempo falava-se em globalização, que era a quebra de barreiras entre países. Chegamos na era digital, em que as informações transitam em velocidade instantânea e há comunicação direta entre as pessoas, sem limites de tempo e espaço, estamos falando na quarta revolução industrial e na indústria 4.0. (FERREIRA, 2017)

Hoje, a conexão entre mundo real e mundo virtual (a chamada virtualização) é algo comum. Utilizando um computador ou *smartphone*, pode-se conectar pessoas por meio das redes sociais, além de ter acesso instantâneo a uma infinidade de serviços. A indústria 4.0 é o momento da digitalização dos processos industriais.

Após a terceira revolução industrial, que foi a responsável pela automação dos processos de produção, nesse novo momento são retirados dados dessa automação através de processos de análise e processamento de dados. Por meio de sistemas como a realidade aumentada, realidade virtual e otimizações *online*, por exemplo. Desse modo, as fábricas e a indústria de modo geral passaram a digitalizar todos os processos, tirando vantagens daquilo que já se tem automatizado a partir da terceira revolução.

> Nesse contexto, o uso de tecnologias para a objetivação e facilitação de informações por parte de empresas privadas e entes públicos, à nível mundial, fez surgir diversos conceitos multidisciplinares, inéditos no âmbito jurídico, até então, o que deu origem ao o que é para alguns um novo ramo, e, para outros, uma nova releitura do Direito tradicionalmente conhecido, sob a ótica dos impactos e reflexos tecnológicos: o Direito Digital. (SANTOS, 2019)

O principal aspecto da indústria 4.0 são os Dados. A partir da análise de diversas variantes de dados é que se obtém a informação, a qual pode ser utilizada de acordo com o interesse do seu detentor. Desse modo, essas novas tecnologias possibilitam um novo modelo de negócios, novos serviços, novas experiências e, também, novos modelos de automatização e digitalização de processos.

> Na Quarta Revolução Industrial todos os produtos pensados e criados nas pretéritas Revoluções Industriais foram otimizados através do uso da internet, sendo que seu principal sustentáculo é o aprimoramento que o computador recebeu, adicionando potência, capacidade, velocidade e novas funções através da internet e dos aplicativos antes não existentes. Junto a este contexto as novas formas e tecnologias facilitaram o transporte e logística, inclusive, como é o caso do surgimento do notebook, do smartphone (quando o telefone se tornou também um computador em um único aparelho) e do tablet. (ROCHA; PONTINI, 2021)

Não é somente a questão da automação. Se trata de todo um novo arranjo das empresas e indústrias para comprar, cativar o cliente, produzir e vender os seus produtos. É uma mudança radical de como a indústria é organizada.

Dentre processos para se considerar uma indústria como 4.0 podem-se citar:

1- Transparência do chão de fábrica: é o começo da sensorização do chão de fábrica. As maquinas começam a gerar relatórios e extrair dados. Com esses dados se passa a construir o *BigData*, onde se possibilita a visualização dos dados.

2- A visualização é a segunda etapa no processo de construção de uma indústria 4.0. Visualizar e tomar decisões. Contudo, essas decisões ainda são decisões humanas tomadas por um técnico que esteja presente na fábrica, por exemplo.

3- A terceira etapa vem a partir da utilização desse *BigData*, dessa massa de dados armazenada, para começar a colocar algoritmos de inteligência a fim de que a tomada de decisão a partir desse momento passe a ter o auxílio de uma inteligência artificial

4- A quarta etapa diz respeito ao processo de inserção da inteligência cognitiva. Assim a empresa não precisa mais programar a inteligência, uma vez que a inteligência artificial aprende por si só.

A indústria 4.0 Permite que empresas repensem completamente suas relações com seus clientes e deixem de apenas vender produtos específicos para vender serviços e resultados. Ao fazer isso, elas conseguem ter uma relação mais próxima e pessoal com seus clientes, podendo aumentar sua margem de lucro a longo prazo ao mesmo tempo em que fascinam seus consumidores com novos produtos e serviços.

Ademais, é importante salientar que ao mesmo passo que surgem novas soluções e oportunidades no mercado, também aumentam a quantidade de problemas advindos e relacionados com a indústria 4.0, principalmente se tratando de aspectos da segurança da informação. É certo que a cada vez que se está *online*, se está exposto a algum tipo de ataque malicioso ou roubo de informações.

> O mundo, especialmente ao longo da última década, foi moldado para extrair dados dos usuários da Internet em escala massiva. Estes dados, reunidos e processados através do que se convencionou chamar de Big Data, que permite a obtenção de informações e o poder de influenciar condutas, em escalas até o presente momento ainda não inteiramente esclarecidas. Assim, os dados pessoais são transformados em importante ativo comercial das grandes empresas de tecnologia do mundo, com o claro objetivo de obtenção de capital, além de outros até o momento não tão claros assim. (REQUIÃO, 2020)

No momento em que se conecta máquinas a rede de internet se passam a ter as mesmas vulnerabilidades de quando um computador é conectado à rede de internet. Se abrem novas formas de ameaças cibernéticas, novas formas de riscos à segurança, não só da informação, mas de todo o processo produtivo.

Aqueles tipicamente considerados fornecedores de produtos, agora passarão a ser administradores dos dados de seus clientes. Surge uma responsabilidade de respeitar a privacidade individual, os segredos comerciais dos seus clientes, bem como seus dados sensíveis. Na atualidade é imperioso garantir que o administrador esteja guardando seus dados de forma segura, seja em seus servidores ou quando são transferidos de um lugar para o outro.

Desse modo, no bojo da indústria 4.0, é importante salientar que empresas que estão passando por uma transformação digital não apenas precisam alterar suas próprias operações, mas também a maneira como tratam e respeitam os dados dos seus clientes.

> A atividade empresarial teve uma evolução desde o surgimento da Revolução Industrial a partir de 1750, na Inglaterra, até se concretizar como Indústria 4.0, nos dias atuais, a saber: 1ª Revolução Industrial (1750-1850), tinha como fundamento a mecânica; A 2ª Revolução Industrial (1850-1950), tinha como fundamento a elétrica; A 3ª Revolução Industrial (1950 até o final do Século XX), tem como fundamento a automação; e; finalmente, a 4ª Revolução Industrial (início do Século XXI), tem como fundamento inteligência artificial e a robótica Big Data Analytic.(DELLAGNEZZE, 2020)

É certo que a Indústria 4.0, resulta do uso integrado de tecnologias avançadas da automação, do controle, da tecnologia da inovação e da inteligência artificial em processos industriais e comerciais. Tais mudanças envolvem questões como o uso da robótica, de novos materiais tecnológicos, de biotecnologia, de armazenamento de energia, da *BigData analytic*, entre outros. Para este estudo a perspectiva a ser abordada é a problemática da proteção dos dados pessoais nesse momento da sociedade, principalmente com relação à proteção dos dados pessoais dos empregados.

3 A IMPORTÂNCIA DA PROTEÇÃO DE DADOS E A CRIAÇÃO DE NORMAS

Likes em redes sociais, cliques em vários websites, conversas por telefone com a atendente da operadora de celular, um gerente do banco, um cadastro na farmácia no qual trocamos o número do CPF por descontos, ou até mesmo os vários aplicativos que são acessados nos smartphones ao longo dos dias, meses, anos. Em todas essas situações estamos deixando para trás dados. Os dados pessoais não são apenas o nome, RG, CPF, endereço, foto, mas todos esses e outros rastros vinculados ao indivíduo e que são capazes de o identificar.

Essas migalhas de informação juntas vão compor um retrato sobre quem somos. Os gostos, predileções, características. Enfim, uma fotografia bastante precisa sobre a nossa personalidade. E é com base nisso que uma série de decisões são tomadas a nosso respeito. A sociedade atual é completamente movida pelos dados. Os dados que são coletados sobre nós têm impacto sobre o que vai acontecer nas nossas vidas. Assim, neste capítulo será feito um cotejo sobre importância da tutela aos dados pessoais e sensíveis e a criação de leis específicas sobre o tema.

Observa-se, portanto, como bem aludido por Laura Schertel (2014), que:

> "A proteção dos dados pessoais se insere na sociedade de informação como uma possibilidade de se tutelar o indivíduo diante dos potenciais riscos que o tratamento de dados poderia causar à sua personalidade, pois o que se visa proteger não são os dados em si, mas sim o seu titular, que poderá ser afetado em sua privacidade caso alguns limites não sejam estabelecidos.

Por exemplo, atualmente não é simplesmente o gerente do banco quem vai decidir a aprovação ou não do crédito de um de seus clientes. Na verdade, é bem provável que um programa (algoritmo) processe uma série de dados sobre o cliente, a exemplo das contas que foram pagas em atraso ou em dias, se há algum tipo de negativação ou restrição, de modo a traçar um perfil a partir do cruzamento de informações disponíveis em um banco de dados sobre esse indivíduo "identificável". A partir da análise dessas informações é que se avaliará a possibilidade de autorizar ou não o aumento de crédito para aquele cliente. É apenas um programa de computador que vai aprovar ou negar o crédito e fixar a taxa mais adequada para o perfil de bom (ou mau) pagador.

A todo momento estamos sendo monitorados. Desenvolver sistemas de proteção de dados é fundamental, uma vez que fazem parte da nossa identidade. A capacidade de

autodeterminação do usuário é cada vez mais calibrada pelos usos que são feitos com os seus dados na cultura do informacionismo.

> Assim sendo, este deixou de ser entendido como uma disciplina vertical, relacionada unicamente ao Direito da Informática, da Tecnologia ou Cibernético, para tornar-se um Direito muito mais amplo e presente no cotidiano, visto que trata de uma Sociedade Digital, que para tudo se utiliza da tecnologia, e, muitas vezes, até mesmo depende incondicionalmente desta. [...]
>
> [...] o informacionismo trata das informações dos indivíduos (dados pessoais) e das demais informações gerais, bem como a forma como tais elementos são retratados e manuseados no mundo prático. (SANTOS, 2019)

Proteger os dados pessoais significa estabelecer regras para que todo o tratamento de dados, todo o fluxo de informações, seja íntegro e apropriado. Não só para proteger a integridade dos indivíduos, mas também para oferecer segurança e confiança entre os cidadãos, organizações públicas e privadas que se valham e que fazem usos desses dados para os seus modelos de negócios, para suas atividades comerciais, para a formulação de políticas públicas.

A Lei Geral de Proteção de Dados (LGPD) foi sancionada em agosto de 2018 e teve inspiração na GDPR (General Data Protection Regulation). Essa lei trata de um conjunto de normas sobre como as empresas, pessoas e os órgãos públicos devem guardar, proteger e usar as informações pessoais coletadas dos usuários.

Basicamente, a LGPD serve para garantir o direito de privacidade da população e impedir que seus dados circulem livremente entre empresas e pessoas que não estão autorizadas a utilizar essas informações.

A principal função de uma lei de proteção de dados é determinar como que será o tratamento de dados. Dessa forma, a Lei estabelece parâmetros de como esses dados serão coletados, armazenados, processados e destruídos. Conforme exposto no artigo 1º, Lei Nº 13.709, de 14 de agosto de 2018, *in verbis:*

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

A partir de então, as empresas terão uma série de obrigações como informar o porquê elas estão coletando dados e qual a utilidade daquelas informações em específico. A transparência deve ser bastante alta, com indicação até de quem é o responsável por aquele

servidor que os armazena. As sanções para o descumprimento podem ser apenas simples advertências ou multas de até dois por cento do faturamento, por exemplo.

> A escolha brasileira, por seu turno, como já referido, aproximou-se do modelo europeu, privilegiando uma legislação por princípios, o que se identifica a partir da redação do artigo 6º da Lei nº 13.709/2018, segundo o qual as atividades de tratamento de dados pessoais, além de observar a boa-fé, devem se pautar pelos princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas. (REIS, 2019)

A lei também possui exceções. Pessoas físicas que usam dados para objetivos pessoais, acadêmicos, artísticos ou jornalísticos, não precisam montar toda a estrutura imposta pela lei para o tratamento de dados. Contudo, para a utilização desses dados os mesmos devem passar por um processo de anonimização. Casos de segurança pública, ou investigação criminal também possuem regras específicas. Vide artigo 4º da Lei em comento, *in verbis:*

> Art. 4º Esta Lei **não** se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) **jornalístico e artísticos**; ou
>
> b) **acadêmicos**, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; (BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Grifo nosso)

Ademais, as empresas devem apagar os dados que não são mais necessários, como contas que foram excluídas, mas existem situações em que a lei obriga a manutenção dos dados.

Para garantir a lisura, a devida aplicação e fiscalização da nova lei, a sua aprovação envolveu a criação de um órgão federal chamado ANPD (Autoridade Nacional de Proteção de Dados), em seu artigo 55-A. Esse grupo é subordinado à presidência da República e será o responsável por fiscalizar, investigar, avaliar denúncias e orientar a sociedade. Ademais, além do conselho diretor, são 23 titulares com dois anos de mandato que incluem desde membros setores do país, do Executivo a instituições científicas. Esse órgão poderá requerer documentos, relatórios de riscos de exposição de dados, aplicar sanções administrativas nas empresas e expedir recomendações.

> No Brasil, a figura da Autoridade Nacional de Proteção de Dados (ANPD), prevista no PLC nº 53/2018, foi vetada no texto final da LGPD, sancionado pelo Presidente Temer, sob o argumento de que o Poder Legislativo não poderia criar órgãos que resultassem em novos gastos ao orçamento do Executivo. Posteriormente, a Lei nº 13.853, de 08 de julho de 2019, criou a ANPD (considerada autoridade nacional), como órgão da administração pública federal, vinculada à Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil, assim como elaborar a Política Nacional de Proteção de Dados e da Privacidade, entre outras competências previstas no artigo 55-J da Lei nº 13.709/2018. (CAVALCANTI; SANTOS, 2018).

Com o crescimento, tratamento e armazenamento do grande volume de dados, de forma a acompanhar a evolução social, houve uma necessidade de reação legislativa no sentido de criar leis que protegessem as pessoas do próprio sistema capitalista que explora essa estrutura de forma a invadir a privacidade dos indivíduos. Atualmente existem algoritmos que conseguem realizar o cruzamento de diversos dados e traçar perfis de consumo e de comportamento, o que representa um afronte a individualidade e privacidade do usuário que não concedeu sua permissão para esses fins.

3.1 LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O debate sobre proteção de dados no país já acontecia há um bom tempo antes do sancionamento da LGPD. A título de exemplo, pode-se citar o projeto de lei apresentado em 2012 pelo deputado Milton Montes, no qual falava sobre proteção de dados pessoais. Contudo, o projeto não chegou a evoluir. Em 2015 o tema voltou as ser debatido, porém sem muito sucesso.

Nesse meio tempo, em 2014 foi aprovado o Marco Civil da Internet que foi considerado um avanço principalmente pelas empresas de telecomunicações. Ademais, essa lei ainda era deficitária no que se refere à proteção de dados. “Destaca-se que, no Brasil, apesar de a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil e o Marco Civil da internet protegerem de alguma forma direitos relacionados aos dados e à privacidade” (REIS, 2019).

Dentro das problemáticas trazidas frente a geração digital, está a questão da proteção de dados. Notadamente, a Constituição Federal de 1988 já traz em seu bojo normativo um sistema garantidor de proteção e inviolabilidade a personalidade e a intimidade dos sujeitos de direito.

A constituição tem um papel fundamental de legislar de forma geral a nortear o ordenamento jurídico. Assim como também autoriza que por lei ordinária sejam reguladas matérias mais específicas, de forma mais detalhada.

> [...] o nível de desenvolvimento tecnológico e a necessidade de se garantir maior segurança jurídica às relações exigia uma legislação que tratasse da proteção dos dados pessoais e sensíveis compatível com a de outros países, sendo que em 2018 foi aprovada pelo Congresso Nacional Brasileiro a Lei nº 13.709/18, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD). (REIS, 2019)

A Lei Geral de Proteção de Dados, foi baseada no Regulamento Geral sobre a Proteção de Dados (GPDR) europeia, que é um conjunto de leis de proteção de dados que foi aprovado em 2016. Além disso, a Explosão do caso da *Cambridge Analytica,* que usou de forma ilegal dados do *facebook* de modo que se aproveitaram de dados pessoais para traçar perfis psicométricos, acelerou as discussões sobre a importância da criação de uma lei que versasse sobre a proteção de dados em todo o mundo.

Foi também pensando na perspectiva aludida anteriormente que em 2018 surgiu a Lei Geral de Proteção de Dados Pessoais (LGPD), como sendo uma legislação que tem o objetivo de proteger a liberdade e a privacidade das pessoas no meio digital e dar mais participação aos usuários no tratamento de seus dados. Prevista para entrar em vigor de forma plena em maio de 2021, ela demanda que empresas e órgãos públicos mudem a forma de coletar, armazenar e tratar os dados das pessoas.

> A LGPD é um marco normativo no Brasil, porquanto introduz uma nova engenharia jurídica para a gestão e proteção de informações pessoais das pessoas físicas no ordenamento jurídico pátrio, inserindo um conjunto de normas e princípios que buscam tutelar direitos fundamentais constitucionais. (ROCHA; PONTINI, 2021)

Existem quatro figuras básicas para entender a LGPD: o **dado** em si, que nada mais é que a informação que diz respeito a alguém; o **titular** do dado, esse é aquele à quem a informação se refere; o **controlador** dos dados, que é quem decide o que vai ser feito com as informações, se os dados vão ser coletados ou não, onde serão armazenados, processados, analisados, destruídos, etc.; a última figura é o **operador ou encarregado**, que é quem vai lidar diretamente com os dados e vai executar na prática o tratamento das informações.

A depender da empresa, o controlador e o operador podem ser a mesma pessoa, ou funcionários diferentes, ou até mesmo empresas prestadoras de serviços.

A LGPD vigora para todas as empresas, de todos os portes. A lei vale para todos que de alguma forma realizem tratamento de dados pessoais. Esses devem adequar os seus procedimentos internos e externos para proteger os dados que são utilizados. Desde o cadastro de um cliente em uma loja à coleta de dados pessoais de um funcionário para preencher a sua ficha de registro, são práticas que envolvem o tratamento de dados.

4 O TRATAMENTO DE DADOS PESSOAIS E O SEU IMPACTO NAS RELAÇÕES DE TRABALHO

A fim de contextualizar melhor o tema, é importante salientar que o Direito Digital é uma área recente, mas que em contrapartida está interligada com praticamente todas as áreas do direito. Para o presente trabalho, a perspectiva a ser abordada é a problemática do tratamento e armazenamento de dados no que vertem para as relações trabalhistas. Neste capítulo, se introduz a perspectiva de que a LGPD não foi criada com enfoque no direito do trabalho, mas tem vasta aplicação voltada para a área.

A lei não vem para atrapalhar as empresas, mas apenas para oferecer um padrão mínimo de tratamento de dados. Dessa forma se tem, então, que mudar a estrutura do tratamento de dados a fim de evitar possível responsabilização que potencialmente afete a empresa negativamente.

> A LGPD não traz nenhum dispositivo expresso que se refere especificamente à proteção de dados pessoas nas relações de trabalho, o que poderia suscitar discussões quanto ao seu alcance na seara trabalhista. No entanto, o próprio art. 1º da LGPD deixa claro que a lei é voltada para proteger os dados pessoais de pessoas naturais que sejam tratados por pessoas físicas ou jurídica de direito público ou privado. (CORREIA; BOLDRIN, 2020).

Dado Pessoal é toda e qualquer informação da qual se possa tornar o titular de direito identificado ou identificável. Desse modo, uma pessoa natural é considerada titular desses direitos. Assim, todo e qualquer dado que possibilitar a identificação de um sujeito é considerado Dado Pessoal e é amplamente protegido pela LGPD. Esses, possuem um conceito expansivo podendo ser tanto o que identifica diretamente o titular de direito quanto o que possa a vir identifica-lo, pelos dados em si ou ainda por meio de interesses em comum.

Os Dados Pessoais estão destacados na LGPD em duas categorias. Na primeira são os Dados Identificados, que são aqueles que se têm por senso comum, tais como o número do Registro Geral, Cadastro de Pessoa Física, endereço, ou seja, referentes à identificação direta do titular. A outra categoria é referente aos Dados Identificáveis, que são aqueles que possibilitam identificar o titular de dados quer seja por sua cor, religião, compleição física, vestimenta, etc. Logo, tratam-se de informações que vão além dos documentos considerados e identificados.

Na prática o tratamento de dados se refere a todas as operações realizadas com os dados pessoais dos titulares. Se inicia com a coleta do dado no momento em que ele chega no sistema. Começando, assim, o ciclo do tratamento manipulando essas informações até a sua utilização para algum fim.

O tratamento de dados possui algumas fases e a depender do dado que esteja sendo tratado podem existir mais ou menos processos. A primeira etapa lastreia a fase de coleta dos dados (também chamada de obtenção/aquisição). É nesse momento que as informações passam a existir dentro do banco de dados e passam a ser de responsabilidade do detentor. As origens dessas informações podem ser variadas. Podem chegar a partir de um contrato de trabalho, de uma relação de consumo, de uma parceria entre empresas, etc.

A segunda etapa é quando os dados já se encontram armazenados. Os mesmos precisam ser analisados e classificados para que cada um receba o tratamento adequado. Podem ser considerados como sensíveis, nos casos especificados no Art. 5º, II, da LGPD, ensejando uma proteção ainda maior. Adotar procedimentos diferentes para cada espécie de dados é fundamental.

A terceira etapa é a utilização dos dados para o fim que justificou a sua coleta.

A última etapa é a da exclusão dos dados. Nesse momento eles serão reanalisados a fim de averiguar se ainda possuem alguma viabilidade, ou seja, se podem ser reutilizados ou se devem ser excluídos do banco de dados.

Entre todas essas fases, a partir da LGPD, ficou determinado que o titular dos dados deve consentir com os procedimentos que foram realizados em todas as etapas do tratamento. Além disso, deve ser explicado ao titular qual é a finalidade dos procedimentos adotados. Esse consentimento deve ser feito preferencialmente por escrito.

> Nessa perspectiva, o titular dos dados pessoais tem direito à confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e a revogação do consentimento. (REIS, 2019)

Dessa forma, as empresas devem ajustar seus formulários e termos de privacidade, quando no meio virtual, e imprimir seus termos de consentimento quando for necessário presencialmente, como é o caso das relações de trabalho.

Quanto mais claros e detalhistas forem esses termos de consentimento, mais informações terá o titular para controlar o que é feito com seus dados e menor é a chance que empresas tenham algum tipo de problema. Assim, a LGPD se dedicou a dar mais autonomia e participação ativa do titular dos dados durante todo o processo de tratamento através do poder do seu consentimento.

O direito do trabalho, surgiu para proteger direitos mínimos, bem como as leis de proteção de dados. Não existe na Lei Geral de Proteção de Dados uma especificação direta relacionando a aplicação da lei no direito do trabalho.

> A incidência da LGPD no Direito do Trabalho é questão fundante e imperiosa, porquanto a existência de circulação de dados pessoais nas relações de trabalho, não apenas nas fases de seleção e contratação, mas durante a vigência e término do contrato, e também após o fim dele, uma vez que os dados continuam armazenados no sistema da empresa por certo lapso de tempo. (ROCHA; PONTINI, 2021)

Com relação ao porte das empresas, como já aludido anteriormente, a lei deverá ser aplicada independentemente do tamanho da empresa ou do seu faturamento. Todas as empresas deverão cumprir a nova legislação. Não basta que somente os empregadores se adaptem, deverão demonstrar que estão cumprindo as obrigações impostas pela nova legislação. Quando da autuação por parte da ANPD, as empresas deverão ter toda a documentação e relatórios de forma comprobatória para afastar qualquer tipo de penalização.

Muito embora não haja nenhum artigo expresso na lei de que a LGPD seja aplicável ao direito do trabalho, essa lei tem intrínseca conexão com o direito trabalhista. O próprio artigo 1º estabelece que o intuito dessa legislação é proteger os dados de pessoas naturais. Ou seja, o empregado, assim como qualquer titular de direitos, também está protegido pela LGPD. Assim, as empresas devem observar as exigências que constam na nova lei e cumpri-las.

As empresas devem colher o menor número de informações possível sobre seus empregados, visto que o armazenamento desses dados traz um risco. A exemplo do momento da contratação, tem-se que nem todos os dados são realmente necessários e que estão lá por mero costume ou desinformação.

As empresas deverão se adaptar, uma vez que os dados e as informações dos empregados devem ser preservados e protegidos. Nas relações de trabalho, os empregadores lidam constantemente com os dados pessoais de seus empregados. Desde o ato da contratação,

perpassando pela vigência do contrato de trabalho e, até mesmo, no término da relação contratual. Para compreensão da perspectiva apresentada, vide, *in verbis*, o artigo 7º da LGPD:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> 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;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Na seara do direito do trabalho podem-se vislumbrar três situações especificadas no artigo 7º da LGPD:

a) Cumprimento da obrigação legal: neste caso, a empresa tem o dever de exigir do empregado algumas informações para constar no seu registro. Ex: qualificação civil, tipo de relação de emprego, período do gozo de férias, acidentes de trabalho, etc. Todas essas informações não precisam do consentimento prévio do empregado, uma vez que a empresa tem o direito de obtê-las;

b) os dados necessários para a execução do contrato de trabalho: nestas situações, a empresa poderá usar os dados do empregado, por ele autorizados, para a execução do seu contrato de trabalho;

c) o interesse legitimo do controlador: a empresa poderá utilizar alguns dados do empregado sem o seu consentimento quando houver interesse legítimo. Por exemplo, a empresa não pode exigir do empregado que ele exiba a sua conta de telefone, mas se esse empregado utiliza um aparelho que foi concedido pela empresa e a mesma custeia a conta de telefone, nessa situação específica a empresa terá o interesse legítimo de ter acesso a conta de telefone do empregado.

A lei também dispõe sobre o tratamento de dados sensíveis que são todos aqueles de origem racial ou étnica, convicção religiosa, opinião política, filiação sindical e etc. e ainda há dados relacionados a saúde, vida sexual, genéticos e biométricos, os quais demandam uma proteção especial. Assim, conforme o exposto, é clara e evidente a influência direta dos ditames da LGPD nas relações trabalhistas e empresariais.

4.1 AS FASES DO TRATAMENTO DE DADOS NAS RELAÇÕES TRABALHISTAS

É possível observar três momentos na relação de trabalho: a fase pré-contratual, contratual e pós-contratual. Em todos esses momentos existe um fluxo de coleta, armazenamento, processamento e destruição de dados. Na rotina das relações de trabalho, há constantemente o tratamento de dados dos empregados e demais prestadores de serviços em diversos momentos da contratação, segundo Correia e Martinucci Boldrin (2020).

Ainda segundo os mesmos (2020) as fases apresentam as seguintes características com relação ao fluxo de dados:

a) Pré-contratação: essa fase se perfaz com a obtenção de dados de identificação, currículo, referências do candidato à vaga de emprego, dentre outros; quando uma determinada pessoa fornece um currículo para uma empresa, esta deverá dar o tratamento adequado a este documento. Desse modo, é adequado que as empresas comecem a exigir do candidato o seu consentimento para o armazenamento dessas informações no banco de dados. Mesmo com essa autorização a empresa não poderá comercializar esses dados ou transferi-los para terceiros;

b) durante o contrato de trabalho: dados para registro de empregados, dados bancários para pagamento de salários, filiação sindical, dados relativos à saúde como exames ocupacionais, atestados médicos, dentre outros; são inúmeras as situações nas quais se evidencia o tratamento de dados do empregado. Por exemplo, em casos que envolvem a saúde do trabalhador a CID (classificação internacional da doença) e a coleta de dados biométricos, sendo essas situações tratadas pela LGPD como obtenção de dados sensíveis, cabe a empresa ter uma autorização prévia do empregado para que possa utiliza-las. Assim, a empresa agirá de forma cautelosa e se precavendo em caso de futuras ações judiciais.

c) após o término do contrato de trabalho: com o armazenamento das informações dos antigos empregados para fins trabalhistas, previdenciários e para disponibilização aos órgãos públicos de fiscalização. São informações obrigatórias legais. Exemplos de dados a serem armazenados nessa fase são os registros da saída do empregado, holerites, recibos de férias, folhas de ponto, todos os documentos com relação a vigência do contrato de trabalho devem permanecer armazenadas na empresa, uma vez que a mesma tem a obrigação legal de guardar esses documentos por pelo menos um prazo de 05 anos.

Existem também os dados sensíveis do termino do contrato de trabalho. Um exemplo bem nítido é com relação a rescisão por justa causa. Esta informação do motivo da rescisão não pode ser divulgada pela empresa, sob pena da mesma ser responsabilizada pela divulgação indevida. Desse modo, é cristalina a influência da nova dinâmica no tratamento de dados pessoais frente a realidade imposta pela Lei Geral de Proteção de dados em diversos momentos da relação de trabalho, até mesmo em momentos anteriores a contratação.

4.2 DO MANUSEIO DE DADOS SENSÍVEIS NAS RELAÇÕES TRABALHISTAS

Tendo por dado pessoal a informação que pode ou que identifica uma pessoa, a lei também traz o conceito de dados sensíveis. Esses ensejam uma proteção ainda maior frente a legislação diante da relevância e vulnerabilidade desses dados.

Os dados sensíveis são dados que pela sua sensibilidade natural podem levar a uma maior chance de descriminação da pessoa ou são dados considerados de saúde. Fazem parte dessa categoria os referentes a orientação sexual, convicção religiosa, orientação política, etnia, ou seja, dados que podem levar o titular a sofrer algum tipo de preconceito.

> [..] os dados sensíveis seriam aqueles que indicam particularidades dos indivíduos, revelando questões da intimidade destes, como opiniões políticas ou convicções religiosas, além de dizerem respeito a questões biológicas, o que poderia acarretar, se utilizados de maneira diversa de seu propósito inicial, em discriminação aos seus titulares. (SANTOS, 2019, p.17)

Ademais, alguns dados dos quais originalmente não seriam considerados sensíveis a depender do contexto podem passar a ser considerados como sendo. A exemplo dos dados de geolocalização, esses dados por si só são considerados apenas dados pessoais por conta da sua capacidade de identificar o titular. Contudo seriam considerados sensíveis se trouxessem a informação de que determinado usuário frequentemente vai a uma igreja específica ou sede de partido político. Transformando-se, assim, um dado que essencialmente era apenas pessoal em dado pessoal sensível.

Também são considerados dados sensíveis qualquer dado relacionado com a saúde do titular. A exemplo do tipo sanguíneo, existência de doença hereditário, quadro clínico, vacinação, dado genético. Da mesma forma são considerados os referentes a identificação biométrica, ou facial.

A LGPD traz alguns conceitos, exemplo do artigo 5º, inciso I, ao considerar dado pessoal a "informação relacionada a pessoa natural identificada ou identificável", ou no artigo 12, §2º que também inclui como dados pessoais "aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. " (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

No caso dos dados pessoais sensíveis o consentimento é a principal base legal para justificar o tratamento dos mesmos. Na seara trabalhista o empregado é o titular dos dados pessoais e o empregador o controlador, cabendo ao segundo a obrigação de obter a autorização do primeiro de forma clara, objetiva e direta, para só assim poder fazer o tratamento desses dados.

Na fase pré-contratual da relação de trabalho, surge necessidade quanto à proteção dos dados pessoais contidos nos currículos dos candidatos à vaga de emprego. Antes, os candidatos apenas entregavam o currículo ao empregador de forma arbitrária e direta com diversas informações sobre sua vida pessoal, acadêmica e profissional.

Com a nova lei a dinâmica mudou. Agora é mais que prudente que as empresas exijam o consentimento do candidato quanto a finalidade de uso daqueles dados, o processo de tratamento, a possibilidade de manutenção de seu currículo na base de dados da empresa e deixar claro as hipóteses de exclusão e o procedimento de eliminação das informações.

Na vigência do trabalho podem se identificar os dados sensíveis quando do armazenamento da biometria dos empregados em sistemas de registro de jornada de trabalho. Também é possível verificar o aparecimento dessa classe de dados quando se armazenam informações sobre o tipo sanguíneo do empregado, atestados médicos, comunicados de acidente de trabalho, informações referentes à benefícios previdenciários. Nesses casos é obrigação legal do empregador, informar ao empregado o procedimento de armazenamento e uso desses dados.

Findo o contrato de trabalho, é importante destacar que existem alguns prazos de preservação de documentos trabalhistas e previdenciários que devem ser observados pelas empresas.

Os dados que envolvam atas da Comissão Interna de Prevenção de Acidentes (CIPA), o registro de empregados e o livro de Inspeção do Trabalho devem ser armazenados por prazo indeterminado. Por sua vez, dados envolvendo a relação de emprego como acordos de compensação, recibos de férias, de pagamento de salário, dentre outros, devem ser armazenados pelo período de 5 anos, prazo correspondente à prescrição trabalhista.

> Como se observa, as atividades que abrangem o tratamento de dados são muitas. Em linhas gerais, na dinâmica do Big Data, os dados são coletados das mais variadas formas, como em transações comerciais, pesquisas de mercado e de estilo de vida, censo de registros e interações em meios digitais. O armazenamento se dá em enormes bancos de dados. O processamento, por sua vez, consiste em técnicas de análise e refinamento dos dados, com o intuito de deles extrair informações úteis e valiosas. Por fim, a difusão está associada à ideia de mercado de dados pessoais, que pode ser entendida como interações econômicas voltadas à compra e venda de informações. (REIS, 2019, p.77).

Em todas as fases das relações trabalhistas é importante que o operador trate os Dados Pessoais de maneira compatível com a finalidade original para a qual foram coletados, não podendo ser coletados com um fim e utilizados para outro diferente. Quaisquer outras finalidades devem ser compatíveis com a razão original para qual os Dados Pessoais foram coletados ou então serão passíveis de responsabilização.

4.3 O PAPEL DO ENCARREGADO DE DADOS NAS EMPRESAS

Com a LGPD tendo entrado em vigor e alterando profundamente a forma com que a os dados podem e devem ser tratados nas empresas. É importante ressaltar que essa não é apenas

uma preocupação do setor de TI (tecnologia da informação), mas sim da empresa como um todo, uma vez que os dados são perenes à toda organização. Desse modo, áreas como marketing, recursos humanos, financeiro, comercial, e qualquer outra que lide com dados, a lei se aplica a todas as áreas.

> A LGPD traz quais são os agentes destinados ao tratamento dos dados (art. 5°, IX), sendo estes o controlador e o operador, ambos que desenvolvem papel de destaque no *compliance* trabalhista. O controlador é a pessoa jurídica ou natural, de direito público ou privado que deve tomar as decisões quanto ao tratamento dos dados (art. 5°, VI). (ROCHA; PONTINI, 2021)

Nesse contexto, surge então o papel do encarregado de dados. Esse é o responsável por garantir que as iniciativas de aderência à LGPD sejam criadas, mantidas e aplicadas ao longo de toda empresa.

O encarregado servirá como um canal de comunicação entre o controlador, os titulares de dados e a ANPD. Afinal de contas, as empresas podem ter que apresentar no momento da fiscalização relatórios contendo a descrição dos processos de tratamento dos dados pessoais que possam representar algum risco a privacidade dos titulares.

À luz do artigo 5º, inciso VIII, da LGPD, o encarregado corresponde à "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). " (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Dentro da estrutura organizacional da empresa o encarregado possui responsabilidades que dizem respeito à definição de um comitê de privacidade, o qual deve ser composto por Encarregados de Dados, Executivos Sêniores, igualmente membros com poder diretivos, ou seja, pessoas que tenham alçada de toda organização para tomada de decisão. Isso posto, pois, na adequação à LGPD decisões serão tomadas tais quais impactarão toda organização.

Além disso, segundo § 2º do artigo 41 dispõe que as atividades do encarregado consistem em:

> I – Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II – receber comunicações da autoridade nacional e adotar providências;
>
> III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

> IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

O encarregado, também ajudará a empresa a definir a política de proteção de dados a ser aplicada. E além disso, deve orientar cada setor da empresa a cumprir as exigências da lei. Desse modo, as empresas devem investir em uma política interna de tratamento de dados. Ou seja, é interessante fazer um regulamento que tenha como objetivo orientar os seus colaboradores e também os prestadores de serviço sobre um comportamento padrão, que deve ser adotado naquilo que diz respeito aos dados que circulam na empresa.

A política de proteção e tratamento de dados deve ser discutida e aprovada pelo comitê, só depois o encarregado de dados é responsável por fazer com que essa seja aplicada a todas as áreas da empresa. Apesar de ser o responsável pela implementação das regras de proteção de dados, os encarregados não são pessoalmente responsáveis em caso de descumprimento dos preceitos da lei, uma vez que ter um encarregado de dados não exonera o controlador da responsabilidade em estar de acordo com a norma.

Nesse sentido, o artigo 43 da LGPD dispõe que "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: [...] II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; " (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Após a definição das políticas é o momento de criar treinamentos e difundir a ideia das políticas ao longo da organização. É importante que o encarregado prepare o ambiente e as pessoas para essa nova realidade baseada nos preceitos da LGPD. Essa modificação não deve ser só no âmbito interno da empresa, é igualmente necessário que a parte externa também se adeque. Relacionamentos com fornecedores e com o público, também devem ser levados em consideração.

Assim, o encarregado de dados é o canal de comunicação com órgãos regulatórios, com o público e também é o responsável por resolver crises, incidentes de grande porte, que podem vir a acontecer em relação à dados.

Destarte, com o encarregado de dados envolvido em todas as ações de privacidade e proteção de dados a empresa possui maior assertividade em suas iniciativas, além de que as chances de garantia da continuidade do *compliance* empresarial aumentam significativamente justamente por ter uma pessoa específica a fim de concentrar aquela atividade.

O trabalho de conscientização do time e disseminação da cultura organizacional de privacidade e proteção de dados certamente será mais efetiva. Além da notória contribuição

para a imagem positiva da empresa, uma vez que por observar que se preocupa com a proteção de dados dos seus funcionários e seus clientes, gera, assim, maior confiança com relação à sua visibilidade no mercado, entre todas as partes envolvidas e até mesmo por parte da ANPD.

5 O *COMPLIANCE* JURÍDICO

O termo *compliance* tem origem derivada do verbo inglês "*to comply",* que significa "cumprir"/ "obedecer", e que, no cotejo deste trabalho, pode ser definido como "estar em conformidade com leis e regulamentos". Com a inclusão da **integridade** ao seu sistema o conceito se expande para o objetivo de alcançar a ética.

> [...] à adesão da companhia a normas ou procedimentos de determinado setor. Seu objetivo primordial é o combate à corrupção. Diferentemente da ética, que é assumida com espontaneidade, o *compliance* está relacionado à responsabilidade legal [...]. Ser ético é agir voluntariamente com princípios morais para com a sociedade. Já *compliance* é cumprir com regras e regulamentos; é trabalhar ou agir dentro da lei. [...] formado por leis, decretos, resoluções, normas, atos e portarias, o *compliance* é todo arcabouço regulatório aplicado pelas agências que controlam e regulam o setor no qual a empresa está inserida. As maiores e mais organizadas corporações também criam suas próprias normativas internas para direcionar o comportamento de seus diretores e executivos e, assim, coibir comportamentos negativos, desvios de conduta e inconformidades. (ANTONIK, 2016, p. 976 e 987).

No ambiente corporativo o *compliance* é a forma mais efetiva para a adequação da empresa às normas ao combate a corrupção, fraudes e demais ilicitudes. Os modelos de *compliance* apresentados no mercado possuem três pilares de sustentação: prevenção, detecção e correção.

Diante da complexidade das demandas empresariais e das relações jurídicas que as envolve surge a importância da empresa aderir a um programa de adequação. A finalidade é estabelecer uma cultura de estar de acordo com as exigências legais vigentes atrelada a perspectiva da governança corporativa.

Para o real funcionamento de um programa de *compliance* prático faz-se necessário um envolvimento amplo dos gestores, equipe de comunicação, transparência, treinamento para a força de trabalho, canal de denuncia efetivo, processo de apuração e políticas continuas de boas práticas.

O *compliance* jurídico é um tema que requer um aprendizado contínuo na constante luta pelo enraizamento da ética na gestão. Apesar de ser um instituto de origem estrangeira no Brasil, a título de exemplo, foi publicado o decreto Nº 8.420, de 18 de março de 2015 no qual regulamenta a responsabilização objetiva administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, de que trata a Lei nº 12.846, de 1º de agosto de 2013, a qual traz em seu artigo 41:

> Art. 41. Para fins do disposto neste Decreto, programa de integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira.
>
> Parágrafo Único. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, a qual por sua vez deve garantir o constante aprimoramento e adaptação do referido programa, visando garantir sua efetividade.

Diante do conceito previsto na legislação, o programa de integridade tem como foco medidas anticorrupção adotadas pela empresa, especialmente aquelas que visem a prevenção, detecção e remediação de atos lesivos contra a administração pública nacional e estrangeira.

Um programa de *compliance* é um sistema complexo e organizado composto de diversos componentes que interagem nos mais variados processos e negócios da empresa. Trata-se de um sistema que depende de uma estrutura múltipla que inclui pessoas, processos, sistemas eletrônicos, documentos e ideias.

Como cada organização possui uma estrutura diferente e processos de tomadas de decisão singulares, a busca pela estruturação e implementação de função de integridade e *compliance* de cada instituição é autônoma e independente.

Existem diversos fatores a serem considerados na elaboração de um programa de *compliance*, segundo Mendes (2020) existem seis componentes estruturais a serem observados:

> 1- Suporte da alta administração e instância responsável;
>
> 2- Avaliação de perfil e riscos;
>
> 3- Estruturação das regras e instrumentos referentes a:
>
> - Políticas e procedimentos para mitigar os riscos,
>
> - Padrões de ética e regra de conduta,
>
> - Controles internos,
>
> - Investigações internas,
>
> -Detecção de ilícitos
>
> - Ações de remediação,

- Medidas disciplinares,

- Recrutamento e seleção.

4- Canal de denúncias;

5- Treinamento e Comunicação;

6 – Monitoramento e Auditoria.

Não existe um procedimento padrão de *compliance* a ser aplicado uniformemente a todas as empresas. Contudo, a partir da análise casuística é que serão desenvolvidas ações e medidas que juntas consubstanciarão o plano de adequação da empresa.

Independentemente do tamanho ou tipo da empresa, todas poderão ser diretamente responsabilizadas sobre diversas esferas, seja penal, trabalhista, tributária, administrativa, civil, etc. Ademais, não é somente o funcionário ou a pessoa que praticou o ato que será penalizado, mas também a empresa que teve interesse ou benefício na prática das irregularidades.

Destarte, todas as empresas deverão estar o mais adequado possível às disposições legais. Em se tratando de uma empresa com diversas filiais, é importante que a mesma observe a legislação local sobre impostos, por exemplo, as quais se alteram a depender do Estado que a filial se encontre. Assim é extremamente importante que o setor jurídico da empresa garanta um *compliance* tributário adequado.

Um programa de adequação é a melhor forma de prevenção de problemas legais. Não apenas reduz a possibilidade de que irregularidades ocorram, como também atenua as sanções na eventualidade de a empresa ser responsabilizada.

Complicações podem surgir a partir de diversos fatores a exemplo de erros na declaração de tributos, o não pagamento de impostos ou problemas com repasses obrigatórios para o governo. Desse modo, investir na implementação de modelos eficazes de *compliance* protegerá a empresa contra essas punições. É de bom alvitre salientar que deixar de perder dinheiro com processos e demandas judiciais é na verdade uma forma de aumentar os lucros.

A intenção daquele advogado que presta uma orientação ou consultoria é mitigar riscos e evitar problemas. Um programa de *compliance* deve sempre atender às necessidades específicas da empresa e levar em consideração que a depender da atividade explorada estas estão sujeitas a riscos diferentes. Assim, consequentemente, antes de criar um programa de *compliance*, deve ser feita uma análise de risco, para verificar quais as reais necessidades da empresa.

5.1 OS MODELOS DE *COMPLIANCE* E SUA RELEVÂNCIA PRÁTICA

É inegável que as relações empresariais se tornaram mais complexas aos longos dos anos. Naturalmente o direito se modificou de maneira a acompanhar esses fenômenos. Destarte, é evidente o surgimento de leis que tornam ainda mais rígida a responsabilidade dos empresários nas diversas esferas jurídicas.

Nesse sentido, pode-se afirmar que existem modelos diferentes de *compliance* que são temas constantes no mundo corporativo. Estar de acordo com as normas representa uma estratégia eficaz a fim de garantir redução de custos e aumentar a vantagem competitiva da empresa no mercado. É natural que empresas busquem parceiros que também sigam um programa de *compliance*.

> [...] à adesão da companhia a normas ou procedimentos de determinado setor. Seu objetivo primordial é o combate à corrupção. Diferentemente da ética, que é assumida com espontaneidade, o *compliance* está relacionado à responsabilidade legal [...]. Ser ético é agir voluntariamente com princípios morais para com a sociedade. Já *compliance* é cumprir com regras e regulamentos; é trabalhar ou agir dentro da lei. [...] Formado por leis, decretos, resoluções, normas, atos e portarias, o *compliance* é todo arcabouço regulatório aplicado pelas agências que controlam e regulam o setor no qual a empresa está inserida. As maiores e mais organizadas corporações também criam suas próprias normativas internas para direcionar o comportamento de seus diretores e executivos e, assim, coibir comportamentos negativos, desvios de conduta e inconformidades. (ANTONIK, 2016, p. 976 e 987).

Os tipos de *compliance* tendem a variar conforme o seguimento da empresa. Assim, a empresa que adere a um programa de adequação busca atuar em conformidade com as leis vigentes no país. Também é importante levar em consideração aspectos locais a serem considerados de acordo com o tipo de atividade e a localidade na qual é explorada.

Dentre os tipos de *compliance* podem-se citar:

a) *Compliance* empresarial

Sendo o formato mais “generalista” este tipo de *compliance* se direciona a todas operações e decisões de uma empresa. Sobretudo em ações de expansão de mercado, lançamento de produtos, direito de imagem, relações contratuais, relacionamentos com franquias e fornecedores, fusões e aquisições, etc.

b) *Compliance* fiscal e tributário

Este modelo de *compliance* é mais específico e se volta às finanças e atividades monetárias do negócio. Informações contabilísticas e documentos relacionados a balanços,

folhas de pagamento e afins devem ser monitorados principalmente para atendimento das leis, auditorias da Receita Federal e demais órgãos fiscalizadores. É com esse tipo de *compliance* que também é possível prevenir os crimes e fraudes empresariais.

Já em se tratando de *compliance* tributário, o foco está no cumprimento, pagamento e coleta de juros e outros tributos. O atendimento a todos os tributos municipais, estaduais e nacionais é importante para manter as operações da empresa legalizadas e deve-se levar em consideração a natureza do produto ou serviço oferecido pela companhia.

c) *Compliance* ambiental

Em se tratando de empreendimentos que exploram atividades que podem causar impactos no meio ambiente, a responsabilidade com a comunidade passa também pelo cuidado e a preservação do meio ambiente. No geral, o *compliance* ambiental é cumprido com boas práticas voltadas à reciclagem, descarte correto do lixo, economia de água e energia, entre outras ações, mas também tem por objetivo adequar as operações corporativas conforme as leis vigentes, a fim de que a empresa não seja responsabilizada criminalmente ou civilmente por danos ao meio ambiente.

d) *Compliance* trabalhista

De modo a observar as contratações e o atendimento às normas da Consolidação das Leis do Trabalho, esse tipo de *compliance* atua de forma a desvencilhar todas essas necessidades e também manter a empresa atualizada e isenta de problemas jurídicos desta ordem. Ademais, é avaliar se a empresa está em conformidade com a CLT, Constituição Federal, instrumentos coletivos e portarias do Ministério do Trabalho e emprego. Com um programa de *compliance* dessa espécie, a empresa fica segura para admitir ou demitir um colaborador e gerenciar contratos de emprego, bem como possibilita uma melhora no relacionamento com o empregado.

Esse tipo de *compliance* é importantíssimo devido ao fato de que ações judiciais trabalhistas representam uma enorme perda de lucro da empresa, e que ao aderir um programa dessa espécie o dinheiro pode ser reinvestido no crescimento da empresa.

e) *Compliance* de TI

A segurança da informação tem a função de proteger redes, programas, sistemas, dados e informações de uma empresa contra-ataques cibernéticos, vazamento de dados e ameaças do gênero. Assim, também é levado em consideração a atual preocupação da sociedade com a proteção de dados pessoais. Um procedimento de *compliance* em Tecnologia da Informação tem a função de demonstrar que o programa de segurança do empreendimento atende aos

padrões, normas, regulamentos e legislações específicas de proteção de dados, tais como a LGPD.

Ademais, o artigo 50 da LGPD, previu a implementação de programas de *compliance*, aos quais atribuiu o nome de programas de governança em privacidade, nos seguintes termos:

> Art. 50. 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.
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I – implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
>
> II – Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Por fim, é comum a todos os procedimentos de *compliance* jurídico que a empresa crie políticas e procedimentos claros e específicos ,a fim de que a nova cultura de estar de acordo às regras sejam facilmente absorvidas pela equipe.

As organizações só têm a ganhar do ponto de vista econômico, uma vez que estar em conformidade com a lei através de programas de *compliance* impacta diretamente na reputação e nos lucros do empreendimento.

6 O *COMPLIANCE* TRABALHISTA E A INFLUÊNCIA DA LGPD

Tendo em vista que a lei Nº 13.709/2018 entrou em vigor em setembro de 2020, desde então houveram mudanças nas rotinas das empresas. Se tornou muito importante a implementação de um programa de adequação à Lei Geral de Proteção de Dados. A LGPD não se destina, precipuamente, às relações de trabalho. O objetivo da lei é proteger os direitos fundamentais da liberdade e privacidade, além do livre desenvolvimento da personalidade da pessoa natural.

É evidente que o *compliance* trabalhista tem um enfoque maior em garantir que a empresa esteja de acordo com a normativa vigente no país, seja a CLT, acordos coletivos, decretos municipais, etc.

Nas relações de trabalho também existem situações em que se faz necessário realizar o armazenamento e tratamento de dados pessoais, conforme exposto no capítulo 3 do presente trabalho, demonstrando a necessidade de que o *compliance* trabalhista também aglutine as normas da LGPD. Destarte, "todas as relações jurídicas que tenham como consequência natural o manuseio de dados e informações, entre pessoas naturais e/ou jurídicas, serão afetadas pela LGPD." (SANTOS, 2019, P.43).

A Lei Geral de Proteção de dados, altera de forma direta as relações nos negócios, uma vez que toda empresa utiliza dados pessoais em maior ou menor escala, para cumprir alguma finalidade específica de cunho comercial ou até mesmo o cumprimento de obrigações legais como compartilhar dados com sistemas como o CAGED, planos de saúde dos funcionários, comunicações oficiais de contratações e demissões ao Ministério da Economia, ceder informações a auditorias, dentre outros exemplos.

> Portanto, a LGPD não veio para complicar a relação e as regras trabalhistas. Apesar da Lei gerar impactos, estes poderão ser minimizados com a adoção de práticas que visem maior atenção e cuidado com a coleta de dados pessoais e dados sensíveis, desde a fase de seleção de candidatos, durante a relação contratual, até o término ou rescisão do contrato de trabalho, sejam dos colaboradores terceirizados, celetistas ou prestadores de serviços. (MATTIA, 2021)

Todo o processo de contratação, manutenção e demissão de empregados, no que diz respeito ao armazenamento e tratamento de dados, deverão ser repensados de acordo com a LGPD. Sendo assim, fará parte da nova realidade definir com mais clareza quais dados que são realmente necessários de coleta e a maneira como serão armazenados e tratados.

Existe, hoje mais do que nunca, a necessidade de um *compliance* digital não só por parte dos empregadores, mas também por parte dos funcionários uma vez que o processo de adequação engloba o treinamento das equipes de trabalho em todos os setores das empresas.

> [...] a execução de um programa de *compliance* voltado às disposições da Lei Geral de Proteção de Dados exige, à princípio, uma equipe multidisciplinar, além de investimentos na área, para viabilizar a privacidade dos dados armazenados fisicamente ou digitalmente. (SANTOS,2019, p. 47)

6.1 O PROCESSO DE ADEQUAÇÃO DA EMPRESA

É evidente que um dado desnecessário coletado e armazenado de forma irregular representa apenas um risco para a empresa. Por vezes não só os dados são desnecessários, mas sim todo o processo e as ferramentas de coletagem de dados são desnecessários ou inadequados.

Os dados pessoais que eventualmente seriam tratados não teriam respaldo pela lei caso fossem para usos particulares, porém os dados das relações de emprego são dados compartilhados com órgãos governamentais para finalidades como fundo de garantia, para a Caixa Econômica Federal (CEF) que tem algumas pretensões de cobranças de multas, seguro desemprego, ministério da economia, subsecretaria de trabalho, outras empresas (a exemplo dos planos de saúde), vários dados que possuem correlação com o governo através do E-social. Então não é com fim exclusivamente particular, ou seja, os dados irão perpassar por terceiros.

De modo a viabilizar a plena aplicabilidade dos direitos e garantias fundamentais e da dignidade da pessoa humana, sobretudo aos dados dos empregados, criar uma cultura de respeito à proteção de dados capacitando profissionais, ajustando os equipamentos eletrônicos, fortalecendo o programa de *compliance.* Se assegurar acerca do consentimento do titular de dados no tratamento é a maneira mais eficaz de reduzir riscos e contribuir com a efetivação do direito à privacidade no meio virtual

Desse modo, para evitar problemas com a LGPD a empresa deve escolher um encarregado e investir, dentre outras coisas, em uma política interna de tratamento de dados. Ou seja, é interessante fazer um regulamento que tenha como objetivo orientar os colaboradores e também as prestadoras de serviço, sobre um comportamento padrão que deve ser adotado naquilo que diz respeito aos dados que circulam pela empresa.

> A partir disso, percebe-se que os encarregados pelo tratamento de dados, são fundamentais dentro de uma empresa, desempenhando papel de destaque no tocante ao *compliance* trabalhista, visto que lidam diretamente com o processamento dos dados. Sendo assim, faz-se necessário entender quais as diretrizes e ações são fundamentais para a segurança e as boas práticas da empresa, relacionadas ao tratamento dos dados dentro de todos os departamentos. (ROCHA; PONTINI, 2021)

Investir no treinamento de funcionários e fazer uma auditoria de fluxo de dados em cada setor da empresa para depois fazer um *check-list* de adequação a LGPD também são medidas essenciais no processo de adaptação à proteção de dados. O artigo 50 da LGPD determina que as empresas promovam ações educativas e de treinamento sobre o tratamento dos dados.

Logo, o recomendado é que a empresa realize treinamentos específicos dentro dos setores mais atingidos pela Lei Geral de Proteção de Dados. Os treinamentos devem ser dados por profissionais capacitados e adaptados de acordo com as necessidades individuais do negócio.

> Art. 50. 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. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018)

O que mais preocupa as empresas, principalmente as menores, é o encarregado de dados. Não existe flexibilização das regras entre empresas grandes e pequenas. O encarregado de dados terá de ser diligente a fim de construir, aplicar e monitorar todos os mecanismos de controle interno que garante a conformidade com a lei de proteção de dados, desta forma atua sendo o profissional de *compliance*.

No entanto, a atividade não necessariamente precisa ser realizada por um time jurídico composto basicamente por advogados, visto que a atuação desse profissional é bem ampla. O trabalho também pode ser feito por profissionais formadas em outras áreas como administração de empresas, engenharia e ciências contábeis, dependendo do segmento da companhia.

É indispensável que haja treinamento dos empregados que ficarão responsáveis pelo tratamento dos dados pessoais dos trabalhadores, especialmente nos setores de recursos humanos (RH) das empresas. Além da previsão de confidencialidade, é preciso estabelecer as consequências da utilização incorreta dos dados pelo empregado responsável. “Nesse sentido,

as empresas podem se valer de técnicas de "*compliance*" com o treinamento dos empregados no correto tratamento de dados pessoais. " (CORREIA; BOLDRIN, 2020).

Ademais, o *compliance* deve ser construído gradativamente. Logo no início, na fase pré-contratual, é fundamental repensar quais dados que são realmente necessários de coleta, observando o princípio da finalidade. O dado desnecessário coletado representa apenas um risco para a empresa.

A política de *compliance* deve continuar nas demais fases sempre observando quais dados são realmente essenciais e fazer um mapeamento, observando seu ciclo de vida. A partir desse mapeamento é que se começa a construir uma solução de *compliance* a ser reavaliada periodicamente.

É obrigatório a partir da LGPD que a empresa obtenha documentação de consentimento de uso de dados na qual conste claramente sua finalidade. No processo também há uma determinação de políticas de segurança da informação com o objetivo de obter a conscientização de todo o time sobre o assunto através de treinamentos de boas práticas.

> Outro aspecto relevante é o treinamento da equipe para a adequação as novas regras. Com isso, será possível que os agentes tenham acesso as novas instruções, possam sanar dúvidas e aprendam a melhor forma de aplica-las. Apesar do treinamento, eventuais erros e descumprimentos podem ocorrer, para tanto, um sistema de monitoramento deve ser criado. (ROCHA; PONTINI, 2021)

Por vezes, não só os dados são desnecessários, mas sim todo o processo e as ferramentas de coletagem de dados são desnecessários ou inadequados. São diversas as formas com que uma empresa pode aderir uma política de *compliance*. Atualmente também existem aplicativos e programas de centralização de dados e processos. Constituem condutas que podem ser implementadas a partir do programa de adequação.

Sendo assim, podem ser considerados os seguintes passos para uma proposta de solução de *compliance* levando em consideração as diretrizes da LGPD:

(1) Realizar um mapeamento de dados a fim de identificar os riscos aos quais a empresa está submetida e analisar toda a cadeia de dados apontando criteriosamente os dados que hoje estão em seu poder, os que sejam considerados sensíveis, a utilidade da manutenção dos dados, para quais finalidades foram captados, etc.

De posse dessa análise de dados e com uma visão completa do cenário da empresa é que será possível proceder com adequação dos processos de capitação, tratamento e armazenamento dos dados, mantendo-se apenas aqueles que efetivamente geram algum benefício ou decorrem

de exigências legais, para que na sequência se possa definir quais ações serão necessárias para a adequação e conformidade com novas as exigências legais.

(2) Elaboração e/ou revisão dos contratos referentes aos termos de uso dos serviços, políticas de privacidade das empresas, consentimento de dados sensíveis;

(3) Revisão geral dos contratos de trabalho, termos aditivos e comunicados decorrentes do vínculo empregatício observando todas as fases da relação de trabalho (pré-contratual, contratual, pós-contratual), e também dos contratos de prestação de serviços, tanto como sendo o tomador quanto sendo o prestador da atividade empresarial. Consequentemente também efetuar a revisão dos instrumentos jurídicos correlatos (tais como contabilidade, assistência médica, folha de pagamento, plano de saúde, comunicado de acidente de trabalho, dentre outros), a fim de que a empresa esteja de acordo com a lei e completamente protegida.

(4) Definição da forma de tratamento dos dados já existentes antes da vigência da LGPD (legado).

(5) Elaboração do plano de *compliance* de dados, definindo os métodos e processos para garantir a plena adequação dos procedimentos adotados pela empresa com as regras da LGPD;

(6) Contratar ou definir dentre os membros da empresa quem efetuará as atividades de encarregado e operador, com ampla regulamentação das atividades que serão executadas por cada um deles, bem como elaborar um padrão de atendimento ao titular de dados.

(7) Estabelecer procedimentos de controle do fluxo de dados para adquirir um aparato probatório para uso futuro em eventuais fiscalizações e demandas por parte da ANPD.

Dentre os benefícios observáveis a partir da cultura de *compliance*, pode-citar: a prevenção de riscos, conscientização dos funcionários, redução nos custos, identificação e mitigação prévia de eventuais problemas. Além disso, é evidente a credibilidade e notoriedade no mercado, tanto por parte de fornecedores quanto de clientes e investidores. Uma boa política de *compliance* permite a correta aplicação das normas vigentes e passa credibilidade e confiança nos negócios realizados.

Com a contenção de riscos, um código de conduta e um canal de denúncias bem definidos que sejam eficazes e aplicados dentro da empresa, é provável que ações trabalhistas sejam evitadas e possíveis multas por irregularidades deixadas de ser aplicadas. O que faz com que a empresa deixe de perder parte do seu faturamento com despesas de natureza passiva trabalhista.

6.2 AS CONSEQUÊNCIAS DO DESCUMPRIMENTO DA LGPD

Como visto anteriormente, a LGPD prevê uma série de direitos aos titulares de dados pessoais, bem como obrigações e atividades às empresas receptoras desses dados (controlador). Assim, na hipótese de descumprimento dos mandamentos legais a empresa deverá ser responsabilizada pela reparação dos danos eventualmente causados, sem prejuízo de responder por outras sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

Um dos prejuízos que podem acontecer àquelas empresas que não respeitam os parâmetros da LGPD é a perda da oportunidade de se inserir no mercado. A lei brasileira permite a transferência de dados pessoais apenas para países ou órgãos internacionais que proporcionem um grau de proteção de dados pessoais adequado ao previsto. Sendo assim, na ordem econômica, a empresa estaria perdendo oportunidades de negócios caso não adira aos parâmetros estabelecidos pela lei.

A LGPD estabelece diretrizes genéricas a serem observadas pelas autoridades nacionais. Ademais, tem-se como irregular, por exemplo, o tratamento de dados pessoais quando o controlador deixar de observar a legislação ou quando não fornecer um nível de segurança adequado. É importante levar em consideração o modo pelo qual o tratamento de dados é realizado, o resultado e os riscos que razoavelmente dele se espera, bem como, também, as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Os problemas podem ocorrer quando hipoteticamente uma empresa não possua um procedimento adequado observando requisitos mínimos e elementos de segurança digital. Para uma efetiva proteção dos dados é interessante que a empresa tenha uma política bem definida de coleta e armazenamento de dados. Desde uma simples entrega de currículos ou quando da rescisão do contrato com relação aos dados que precisam ser armazenados por um período legal na própria empresa, são situações em que deve haver um procedimento padrão para o manuseio dos dados.

Nos casos em que a forma de tratamento for inadequada ou ilícita, a empresa coletora dos dados (controlador ou o operador) poderá responder civilmente pelos eventuais danos que der causa em decorrência da violação da devida proteção. Deixar de adotar as medidas de segurança ou técnicas aptas a proteger os dados pessoais de acessos não autorizados, bem como

em situações acidentais ou ilícitas de destruição, alteração, perda ou comunicação, são situações que ensejam a reparação civil pela lesão de direitos.

Existe a possibilidade de que controlador e operador não sejam responsabilizados pelos danos causados aos titulares, com uma tendência de se afirmar que estar-se-ia diante de uma responsabilidade subjetiva, na qual incube ao controlador e/ou operador o ônus da prova em sentido contrário. Para isso, deverão provar de acordo com o artigo 43 da LGPD:

> Art. 43. Os agentes de tratamento 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. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Dentre as sanções administrativas previstas pela LGPD destacam-se as seguintes punições, aplicáveis pela autoridade nacional, previstas nos incisos do artigo 52 da Lei Nº 13.709/2018:

> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - Multa diária, observado o limite total a que se refere o inciso II;
>
> IV – Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - Eliminação dos dados pessoais a que se refere a infração;
>
> VII - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 06 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

> VIII - Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> IX - Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, Lei nº 13.709, de 14 de agosto de 2018).

Assim, é importante destacar que na seara trabalhista, tanto quanto nas outras áreas, também é protegido pela referida lei o direito à privacidade e intimidade dos titulares de dados pessoais (os empregados). É de obrigação das empresas promover o tratamento adequado dos dados dos trabalhadores, uma vez que a violação dos mesmos gera o dever do empregador/controlador de indenizar àquele que foi violado ou prejudicado. Também é possível a empresa estar passível de sansões administrativas por parte da ANPD.

7 CONCLUSAO

Enfim, diante de todas as questões abordadas percebe-se que apesar de o legislador não ter contemplado na LGPD um capítulo específico para regular as relações de trabalho o Direito do Trabalho como o ramo do direito voltado para a relação de emprego, não fica de fora da área de abrangência da lei tendo reflexos em todos os momentos da relação de trabalho.

Considerando que o tratamento de dados se tornou imprescindível para o desenvolvimento da sociedade e do alcance de objetivos pessoais e empresariais, em especial nas relações trabalhistas, cumulativamente com a exposição da visão geral do direito à proteção dos dados pessoais amparada na análise dos regramentos estatuídos pela Lei 13.709/2018 (LGPD), especialmente no que concerne às atividades a serem exercidas na seara trabalhistas, é esperado que, em contrapartida, a extensão considerável de obrigações direcionadas às empresas destinatárias de dados pessoais haja uma fiscalização ostensiva por parte dos titulares dos dados, bem como por órgãos de proteção aos cidadãos e ainda pela Autoridade Nacional de Proteção de Dados (ANPD), culminando na possibilidade de aplicação de severas sanções e responsabilização civil perante o Poder Judiciário.

De fato, a proteção de dados pessoais tonou-se obrigatória e deve ser efetivada em todas as esferas da cadeia operacional e produtiva da empresa. Deve abranger desde aspectos comerciais à procedimentais, tais como a contratação de um simples empregado ou ao seu desligamento, perpassando pela transferência de dados, desde os essenciais para operações como para os enviados a convênios médicos, serviços de contabilidade, folha de pagamento, e também àqueles envolvendo os contratos com demais tomadores dos serviços e empresas que fornecem insumos e matérias primas.

Inclui-se também os órgãos públicos, como INSS e Receita Federal, além do consumidor (cliente) final. Assim, todo o ciclo empresarial deverá estar hermeticamente protegido a fim de evitar vazamentos ou a utilização indevida de dados pessoais, sob pena de responsabilização de qualquer empresa integrante deste ciclo que não adote cautelas necessárias a adequada proteção dos dados pessoais de seus empregados.

Dessa maneira, é necessário observar quais dados pessoais e sensíveis são manuseados pela empresa e qual o percurso por eles traçado desde a contratação até o desligamento do empregado. Ademais, a delimitação e a atuação de forma eficaz dos operadores e controladores são fundamentais, visto que estes são os responsáveis pelo tratamento dos dados. Conforme

exposto em capítulos anteriores, o *compliance* jurídico é a forma mais efetiva para a adequação da empresa às normas, combate a corrupção, fraudes e demais ilicitudes.

Conclui-se, então, que é medida extremamente prudente a imediata implantação de programas de adequação trabalhista (*compliance)* de proteção de dados pessoais de acordo com os regramentos da LGPD, por se tratar de imposição legal e uma necessidade intrínseca ao momento em que vivemos.

Medidas como a análise de riscos, a criação de um código de conduta e de um canal de denúncias, além do treinamento e fiscalização dos funcionários devem ser visualizadas em uma solução de *compliance* trabalhista. Levando, assim, a vantagens como a redução de reclamações trabalhistas e possíveis multas aplicáveis à empresa. Conclusivamente, é possível perceber como o *compliance* trabalhista é importante na adequação das relações trabalhistas as novas regras disciplinadas pela LGPD.

REFERÊNCIAS

ADJUTO, Graça (ed.). **Indústria 4.0 deve atingir 21,8% das empresas brasileiras em uma década**. 2017. Publicado em 12/12/2017 - 06:00 Por Camila Maciel - Repórter da Agência Brasil - São Paulo. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2017-12/industria-40-deve-atingir-218-das-empresas. Acesso em: 11 fev. 2021.

ANTONIK, Luis Roberto. **Compliance, ética, responsabilidade social e empresarial: uma visão prática**. Rio de Janeiro: Alta Books, 2016. Edição do Kindle.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 maio. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (Lgpd). Brasília , Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 17 jun. 2021.

BRASIL. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. **Decreto Nº 8.420, de 18 de Março de 2015**. Brasília, Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2015/Decreto/D8420.htm. Acesso em: 17 jun. 2021.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. A Lei Geral de Proteção de Dados do Brasil na era do Big Data. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (coord.). **Tecnologia jurídica & direito digital:** II Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018.

CORREIA, Henrique; BOLDRIN, Paulo Henrique Martinucci**. Lei Geral de Proteção de Dados (LGPD) e o Direito do Trabalho**. 2020. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/09/25/lei-geral-de-protecao-de-dados-lgpd-e-o-d. Acesso em: 11 jan. 2021.

DELLAGNEZZE, René. **A Industria 4.0**. 2020. Disponível em: https://jus.com.br/artigos/86845/a-industria-4-0. Acesso em: 11 fev. 2021.

EMBRATEL (org.). **Compliance em TI: qual é a sua importância para a segurança da informação?** 2021. Disponível em: https://mundomaistech.com.br/seguranca/compliance-em-ti-qual-e-a-sua-importancia-para-a-seguranca-da-informacao. Acesso em: 22 jun. 2021.

FERREIRA, Paulo Afonso. **O avanço da tecnologia e as transformações na sociedade**. 2017. Disponível em: https://noticias.portaldaindustria.com.br/artigos/paulo-afonso-ferreira/o-avanco-da-tecnologia-e-as-. Acesso em: 16 jan. 2021.

HOBSBAWM, Eric John Ernest. **A Era das Revoluções 1789-1848**. Rio de Janeiro: Paz e Terra, 2014.

MADRANI, Eduardo. **A Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018.

MATTIA, Elaine Renata Sabi. **Os desafios da adequação à LGPD nas Relações de Trabalho**. 2021. Disponível em: https://www.sabi.adv.br/blog/www-sabi-adv-br. Acesso em: 01 jun. 2021.

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

MENDES, Márcio. **O que é compliance?** 2020. Disponível em: https://marciomendes.com.br/o-que-e-compliance/. Acesso em: 25 maio 2021.

REIS, Beatriz de Felippe. **O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias**. 2019. 176 f. Dissertação (Mestrado) - Curso de Direito, Universidade do Extremo Sul Catarinense – Unesc, Criciúma, 2019.

REQUIÃO, Maurício. **Covid-19 e proteção de dados pessoais: o antes, o agora e o depois**. Disponível em https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois. Acesso em 06/05/2021.

ROCHA, Cláudio Jannotti da; PONTINI, Milena Souza. **Compliance trabalhista: impacto da lei geral de proteção de dados (LGPD) no direito do trabalho**. 2021. Desenvolvida pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa. Disponível em: https://www.cidp.pt/revistas/rjlb/2021/2/2021_02_0407_0427.pdf. Acesso em: 01 jun 2021.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral De Proteção De Dados: fundamentos e compliance**. 2019. 55 f. Monografia (Especialização) - Curso de Direito, Universidade Federal do Ceará, Fortaleza, 2019. Disponível em http://www.repositorio.ufc.br/bitstream/riufc/49370/1/2019_tcc_vbmsantos.pdf. Acesso em 22 jun 2021.

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

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais**. Salvador. Juspodivm. 2019.