UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

UMA PRIMEIRA REFLEXÃO: ELEMENTOS PARA CONSTRUÇÃO DE BOAS PRÁTICAS PARA ATENDER A LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE EMPREGO

ISABELLE STABENOW BATISTA

RIO DE JANEIRO
2022.1
ISABELLE STABENOW BATISTA

UMA PRIMEIRA REFLEXÃO: ELEMENTOS PARA CONSTRUÇÃO DE BOAS PRÁTICAS PARA ATENDER A LEI DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE EMPREGO

Monografia de final de curso no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do título de Bacharel em Direito, sob orientação da Professora: Daniela Silva Fontoura de Barcellos

RIO DE JANEIRO

2022.1

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
FACULDADE NACIONAL DE DIREITO - FND
SECRETARIA DAS COORDENAÇÕES
COORDENAÇÃO DE MONOGRAFIA

ATA DE APRESENTAÇÃO DE MONOGRAFIA DE CONCLUSÃO DE CURSO

DATA DA APRESENTAÇÃO: **14 DE JULHO DE 2022**

Na data supramencionada, a **BANCA EXAMINADORA** integrada pelos (as) professores (as) Daniela Silva Fontoura de Barcellos – Orientadora UFRJ

Vanessa Carvalho Silveira Guterrres - UFRJ

Felipe Bardelotto Pelissa – UFRJ

Társis Nametala Jorge – UERJ

,

Reuniu-se para examinar a MONOGRAFIA do discente: **ISABELLE STABENOW BATISTA**

INTITULADA UMA PRIMEIRA REFLEXÃO: ELEMENTOS PARA CONSTRUÇÃO DE BOAS PRÁTICAS PARA ATENDER A LEI DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE EMPREGO

APÓS A EXPOSIÇÃO DO TRABALHO DE MONOGRAFIA PELO (A) DISCENTE, ARGUIÇÃO DOS MEMBROS DA BANCA E DELIBERAÇÃO SIGILOSA, FORAM ATRIBUÍDAS AS SEGUINTES NOTAS POR EXAMINADOR (A):

	Respeito à Forma (Até 2,0)	**Apresentação Oral** (Até 2,0)	**Conteúdo** (Até 5,0)	**Atualidade e Relevância** (Até 1,0)	**TOTAL**
Prof. Orientador(a)	2,0	2,0	5,0	1,0	10,0
Prof. Membro 01	2,0	2,0	5,0	1,0	10,0
Prof. Membro 02	2,0	2,0	5,0	1,0	10,0
Prof. Membro 03					
				MÉDIA FINAL	10,0

gov.br Documento assinado digitalmente
DANIELA SILVA FONTOURA DE BARCELLOS
Data: 19/07/2022 10:18:34-0300
Verifique em https://verificador.iti.br

PROF. ORIENTADOR (A): NOTA: 10,0

PROF. MEMBRO 01: NOTA: 10,0

PROF. MEMBRO 02: NOTA: 10,0

PROF. MEMBRO 03: NOTA:

MÉDIA FINAL*: 10,0

*O trabalho recebe indicação para o PRÊMIO SAN TIAGO DANTAS? (Se a média final for 10,0 dez)
( ) SIM (X) NÃO

CIP - Catalogação na Publicação

S775p

Stabenow Batista, Isabelle
UMA PRIMEIRA REFLEXÃO: ELEMENTOS PARA CONSTRUÇÃO DE BOAS PRÁTICAS PARA ATENDER A LEI DE PROTEÇÃO DE DADOS NAS RELAÇÕES DE EMPREGO / Isabelle Stabenow Batista. -- Rio de Janeiro, 2022.
68 f.

Orientador: Daniela Silva Fontoura de Barcellos.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2022.

1. LGPD. 2. Direito do Trabalho. 3. Lei Geral de Proteção de Dados. 4. Relações de emprego. I. Silva Fontoura de Barcellos, Daniela , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer à Deus que possibilitou que todos os meus objetivos fossem alcançados, desde a escolha do curso, o sonho de estudar em uma instituição pública e os ensinamentos e desafios durante esses 5 (cinco) anos de curso. Sem Ele, encerrar esse ciclo jamais seria possível.

Aos meus pais, Patricia e Assis, que acompanharam toda a minha trajetória – desde a escolha por cursar direito – o primeiro estágio, período da OAB e até a sonhada efetivação. Eles sempre apoiaram minhas escolhas e nunca deram a entender que eu não poderia ser exatamente quem eu quisesse. Também aos meus avós, Jane e Celso, que foram a minha base, me incentivaram em momentos difíceis, sempre acreditaram em mim e nunca mediram esforços para contribuir para a minha educação. Sem vocês nada disso seria possível.

Agradeço aos profissionais do Mattos Filho que, muitas vezes, foram/são a minha segunda família, escola de vida e a minha base, especialmente ao Domingos Fortunato (Netto) que introduziu o mundo da advocacia e do Direito do Trabalho na minha vida, carreira e matéria que jamais imaginei ter afinidade. Obrigada por direcionar a minha carreira e pela oportunidade. Agradeço muito a Amanda Lins, que foi o meu primeiro contato no trabalho, me acolheu e treinou para que eu fosse uma profissional completa. E mais do que uma grande gestora, tornou-se uma grande amiga. A confiança que vocês depositam em mim me motiva e me faz caminhar rumo a minha melhor versão.

Durante essa trajetória, também não poderia deixar de agradecer aos meus formadores e gestores, excelentes profissionais: Catharina Araujo, Daniel Landim, João Cunha e Julia Freitas. Obrigada por acreditarem no meu potencial, com vocês fui muito além do que as minhas próprias expectativas. Agradeço também pelo acolhimento e parceria nos trabalhos desafiadores, confraternizações de equipe, perrengues de prazos e PJE, e principalmente quando a vida pessoal interferiu no lado profissional. Foi uma longa jornada, com muitas escolhas, muitos obstáculos, mas também com muito crescimento, felicidade e descobertas. O apoio de vocês e dos meus times no trabalho foi essencial e sempre serei grata por esses 3 anos de Mattos Filho.

Agradeço também a minha amiga e base no trabalho, Giovanna. A nossa amizade começou à distância, por conta da pandemia. Foi uma longa jornada e nem acredito que chegamos até aqui. Obrigada por compartilhar os surtos, desesperos, peças e conhecimento. A rotina com você com certeza é mais leve e feliz. Termino esta etapa ciente de que a vida e as nossas oportunidades são muito mais bem aproveitadas quando compartilhadas com quem amamos.

Também não poderia deixar de agradecer as excelentes profissionais que passaram na minha vida e que, com certeza, deixaram muitos ensinamentos, Clarissa Mello e Ana Carolina Santana. Vocês são um exemplo de profissionais e de resiliência, que, consciente ou inconscientemente, tornaram a minha jornada mais alegre e tranquila. Admiro muito vocês e obrigada por todo o apoio, exemplo e pelas oportunidades de desenvolvimento.

Agradeço também à Faculdade Nacional de Direito, aqui fui desafiada em todos os níveis. Também pude fazer amizades sinceras ao longo desses anos, em especial a Bruna, Beatriz e ao Luiz Felipe. Começamos a faculdade juntos e, mesmo com a minha ausência durante o período de estágio/trabalho, vocês nunca deixaram de me apoiar e sempre me ajudaram.

Agradeço, por fim, a todos os professores que fizeram parte da minha formação e a minha orientadora, professora Daniella Barcellos. Todos os seus ensinamentos foram extremamente importantes para que eu pudesse me tornar uma profissional completa e qualificada, sem contar o incentivo para continuar no meio acadêmico.

Resumo

A presente monografia tem por objetivo delinear a necessidade da elaboração de um marco regulatório no Brasil em relação ao armazenamento de dados, diante o grande fluxo de informações e dados com desenvolvimento e avanço tecnológico. Dessa forma, o presente trabalho busca analisar em um primeiro momento os marcos regulatórios existentes a respeito da proteção de dados e direito à privacidade até a constituição da Lei n.º 13.709/2018 ("Lei Geral de Proteção de Dados"). E, considerando que a Lei Geral de Proteção de Dados é aplicável a qualquer ramo do direito desde haja dados a serem regulamentos, a pesquisa busca correlacionar os dispositivos da LGPD no ambiente de trabalho, visto que as empresas terão que criar rotinas e novos hábitos para cumprirem a legislação, especialmente dentro das relações de trabalho em que há alto fluxo e compartilhamento de informações e dados. Busca-se, ainda, analisar quais seriam os impactos previstos em Lei em eventual descumprimento ou vazamento de dados de empregos no campo da responsabilidade civil. Outrossim, por se tratar de legislação recente, como a jurisprudência e doutrina entendem a natureza jurídica da responsabilidade.

Palavras-chave: LGPD; Proteção de Dados; Relações de emprego; Direito do Trabalho; Responsabilidade Civil.

Sumário

1. INTRODUÇÃO

O processo de globalização, nos moldes em que se apresenta na atualidade, tem como uma das características mais evidentes a valorização da tecnologia e a sua interferência cada vez mais direta no cotidiano. Isso porque, ao desempenhar suas funções, os indivíduos contam cada vez mais com o fenômeno da "inteligência artificial". Reflexo disso foram os últimos anos marcados pelas inúmeras notícias sobre vazamentos de dados pessoais por ausência de mecanismos de proteção por parte das Empresas.

Diante o crescimento desacerbado do auxílio da tecnologia em uma sociedade dinâmica, tem-se que os direitos estão em constante transformação para tutelar as novas estruturas. E no mercado de trabalho não poderia ser diferente! Considerando este cenário cada vez mais tecnológico em que uma informação pessoal é a mais nova criptomoeda, bem como ao fato de que das Empresas ao explorarem com grandes bancos de dados em prol do crescimento econômico exponencial, por consequência, criou-se uma necessidade de lei específica, em razão as lacunas deixadas pelas leis anteriores, a fim de se evitar riscos de vazamentos de dados cada vez maiores.

Ante todo o contexto e a necessidade de tratar dados de forma mais consciente, foi introduzida a Lei 13.709/18 – Lei de Proteção de Dados ("LGPD") no ordenamento brasileiro, em nítida influência da tendência do mundo, criada com intuito de regulamentar questões relacionadas ao tratamento de dados que são disponibilizados nos meios digitais, além de ter como base a boa-fé e com respeito à privacidade e às liberdades individuais, o que está elencado na garantia das liberdades e direitos fundamentais da pessoa humana na nossa Constituição Federal de 1988.

Não obstante a interdisciplinaridade do tema, eis que tal legislação é aplicável quando houver tratamento de dados pessoais, a LGPD também terá enfoque no direito do trabalho, já que os funcionários lidam com armazenamento e coleta de dados, seja interna – da própria Empresa - seja de clientes externos. Mostra-se necessário, portanto, que o direito do trabalho caminhe junto com

estes acontecimentos, de modo que o reflexo do desenvolvimento tecnológico e as sensibilidades que trazem consigo possam ser tuteladas pelos operadores de dados.

Levando em consideração a pretensão do legislador em garantir o direito à privacidade pelos controladores de dados, tem-se como recorte do trabalho a necessidade de uma nova estrutura de medidas preventivas e proativas correlacionada ao direito do trabalho para que os agentes privados (Empresas) e funcionários possam atender à legislação vigente nova forma de armazenar e tratar dados, sob pena de serem responsabilizados por meio de sanções e danos decorrentes.

Deste modo, com uma legislação tão recente que entrou em vigor a partir do ano de 2020 e a necessidade não só de sua aplicação na esfera judicial, mas também pelas empresas que lidam com dados de seus empregados e clientes, sob pena de sanções, o objetivo geral desta pesquisa é analisar o papel do empregador e a necessidade de reestruturação a fim de atender à Lei, sendo passível de responsabilização dos agentes privados.

Para atingir o objetivo, em um primeiro momento se contextualizará a necessidade da criação da norma com base em princípios e garantias fundamentais. A partir desta base, em seguida, se estabelecerá a relação entre a LGDP e a sua importância nas relações de trabalho, bem como a adoção de medidas pelas Empresa para anteder as medidas advindas pela Lei nº 13.709/2020, sob pena de responsabilização. E, por fim, conjuntamente com as ponderações anteriores, far-se-á uma análise e reflexões sobre a adoção de práticas e possíveis consequências com base em julgados anteriores a vigência da norma.

2.A LEI GERAL DE PROTEÇÃO DE DADOS (“LGDP”)

Antes de adentrar ao cerne da questão, imperioso destacar o contexto e fundamentação para a criação da Lei de Proteção de Dados. Conforme exposto acima, a forma em que se armazena os dados pessoais tem sido um assunto recorrente em escala global, tendo a Sociedade passado a se preocupar com esse tipo de questão a partir das notícias a respeito de vazamento e compartilhamento de dados por empresas sem consentimento dos seus titulares. Os maiores exemplos disso, aos quais repercutiram no âmbito internacional e geraram as reflexões para a criação de novas leis ao redor do mundo para regulamentar o tratamento de dados, foram os escândalos envolvendo as empresas: *Microsoft*[1], *Facebook* [2]e até mesmo a Uber[3].

Contudo, apesar do assunto de tratamento de dados e os seus desdobramentos, principalmente no âmbito jurídico, serem atuais, vale destacar que a discussão a respeito da privacidade e proteção de dados não é recente. Isso porque, a Declaração da ONU dos Direitos Humanos e a Declaração dos Direitos do Homem são consideradas as primeiras declarações de âmbito internacional que fazem menção a privacidade e o direito à proteção, ainda que de forma superficial.[4]

Em relação ao ordenamento brasileiro, a discussão sobre o direito à privacidade não é de hoje. Conforme se apreende do artigo 5º, X, da Constituição da República Federativa do Brasil de 1988, há previsão de que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas.

Não obstante, o Código Civil de 2002 por meio de seus artigos assegurou que vida privada da pessoa natural é inviolável. Conforme se aprende dos dois institutos normativos do

---

[1]https://www.cnnbrasil.com.br/business/vazamento-expoe-milhoes-de-dados-de-empresas-e-agencias-governamentais-dos-eua/
[2]https://g1.globo.com/economia/tecnologia/noticia/2021/04/07/facebook-atribui-vazamento-de-dados-de-530-milhoes-de-dados-a-raspagem.ghtml
[3]https://g1.globo.com/economia/tecnologia/noticia/uber-avisa-brasileiros-que-tiveram-dados-roubados-em-ataque-que-vazou-informacoes-de-57-milhoes-no-mundo.ghtml
[4]https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/181610/2020_araujo_bruna_lgpd_aplicada.pdf?sequence=1&isAllowed=y

ordenamento brasileiro, infere-se a grande importância aos direitos da personalidade e sua proteção, de modo que preza por resguardar a esfera íntima dos indivíduos que correlaciona com a noção de privacidade.

Apesar das tentativas de tutelar este direito à privacidade, de modo que seja aplicada na prática, ao decorrer do tempo restou bastante claro as lacunas deixadas por ausência de lei específica, na medida em que o desenvolvimento tecnológico exponencial passou a interferir nessa esfera da vida privada a partir da coleta e armazenamento de dados. Em outras palavras, nenhum marco regulatório acompanhava a evolução informacional.

Isso porque, (BONFIM, 2020, p. 47) esclarece que "os dados, cada vez mais, são processados e valorados economicamente, sendo considerados o principal insumo da sociedade contemporânea e equiparados ao petróleo de outros tempos". Dessa forma, tendo em vista que a sociedade é dinâmica, na mesma medida em que os direitos estão em constante transformação para tutelar novas modalidades, surge-se a Lei 13.709/2018 ("LGPD") como forma de proteger os dados disponibilizados no Brasil de pessoas naturais.

Muito embora a LGPD seja de aplicação geral, isto é, onde se tem dados há aplicação da referida Lei, verifica-se que no campo das relações trabalho há uma incidência significativa, vez que se tem um alto fluxo de dados pessoas, seja pelo empregado, seja do próprio empregador e seus clientes. O que reforça a necessidade de as empresas repensarem e adaptarem os seus procedimentos internos, cujo objetivo é implementar forma de obter dados e tratá-los com transparência e confiabilidade.

A partir disso, neste trabalho presente trabalho busca, portanto, analisar todo o histórico que levou a Lei Geral de Proteção de Dados Pessoais, dispositivo recentemente introduzido no ordenamento brasileiro com vistas de regulamentar o tratamento de dados pessoais no país.

Em relação ao tratamento de dados, SARLTET; MARIONONI; MITIDEIRO[5], destacam que o direito à proteção de dados pessoais:

> "Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana".

O maior enfoque do trabalho será dado à implementação dos termos estabelecidos em uma Lei tão recente que atendam os seus dispositivos e ferramentas que as empresas devem ter e mente para conferir o seu funcionamento e suas dificuldades, tendo em vista que as empresas têm sido obrigadas a montar projetos de implementação tão rápidos.

Não obstante, a responsabilização dos agentes privados e o procedimento para aplica das sanções previstas, nos termos estabelecidos pela Lei.

Todavia, Monteiro (2019) deixa evidenciado que existem poucos trabalhos acadêmicos que analisem especificamente os mecanismos de proteção de dados dispostos na LGPD. Nesse sentido, há indagações que, a partir da entrada em vigor da LGPD, seria entender qual a intenção imposta pela legislação com a vigência e aplicação da proteção de dados nas relações de emprego, bem com as boas práticas que entes privados devem adotar para proteção dos dados de seus empregados.

Diante da zona cinzenta da LGPD devido a sua inovação e entrada em vigor tão recente – sendo inexistentes ainda regulamentos específicos para que as Empresas sigam, bem como a escassez de jurisprudência – é possível a partir dos princípios estabelecidos no artigo 6º, refletir em um primeiro momento para "traçar diretrizes gerais capazes de orientar as organizações sobre as tapas que serão necessárias para implementar os dispositivos da LGP" (ROXO, 2020, p. 300).

---

[5] SARLET, Ingo Wolfgang. MARINONI, Luiz Guilherme. MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Saraiva, 2018.; 2018, p.497)

Ante o exposto, neste período de adaptação e escassez de informações concretas diante a sua entrada em vigor recente, verifica-se que a LGPD impõe às empresas uma revisão de procedimentos adotados, bem como a implementação de novos mecanismos, de modo que seja possível deixar transparente o devido cumprimento das novas regras vigente.

2.1. Panorama histórico

Segundo Voíla Bonfim, temos passado por uma Quarta Revolução Industrial em que há fluxo intenso de informações, sendo os dados, cada vez mais, são processados e valorados economicamente, sendo considerados o principal insumo da sociedade contemporânea e equiparados ao petróleo de outros tempos. Por isso mesmo, afirma-se que a economia é dirigida por dados ("data *driven economy*").[6]

Embora essa massificação de dados disponibilizados já perdura por um tempo, é certo que o Brasil até recentemente estava com uma lacuna legislativa para disciplinar a matéria de tratamento de dados pessoais, o que resultava em uma fragilidade de exposição.

Contudo, salienta-se que, muito embora a legislação brasileira demorou para disciplinar o tratamento de dados – para garantir a transparência e consentimento - não se pode esquecer que já existiam institutos que previam e regulamentavam, tais como a Constituição Federal, princípios e leis infraconstitucionais. Na realidade, o que se verifica é que, até então, era "escasso" na legislação unir todos os elementos que regulamentam a privacidade e intimidade dos indivíduos, bem como atualizar para que todos os desdobramentos desencadeados por estar dentro de um contexto em que a sociedade é regida pelos avanços tecnológicos.

Conforme mencionado acima, a garantia acerca do direito à privacidade não é uma nova discussão, a Constituição já previa em seu artigo 5º, X, da Constituição Federal que regula o direito à vida privada e intimidade das pessoas, nos seguintes termos: *"X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização*

[6] VOILA BONFIM – Manual do Compliance Trabalhista (2021, p. 723)

pelo dano material ou moral decorrente de sua violação". [7] Há, ainda, previsão do inciso XII que assegura a inviolabilidade do sigilo em relação a correspondências

Por sua vez, o Código Civil de 2002, se trata de marco regulatório o qual se atenta direito à privacidade e proteção no tocante a inviolabilidade da vida privada da pessoa natural e os mecanismos jurídicos competentes para garantir esse direito. Em seu artigo 20 e 21 não deixa dúvidas quanto à inviolabilidade da vida privada da pessoa natural, além de prever, a pedido do interessado, atitudes judiciais para observância dessa

De acordo com ARAUJO e LIMA (2020, p.2), o Marco Civil pela Lei de nº 12.9652014 é considerada a primeira legislação a falar e regulamentar de forma expressa os dados pessoais, na medida em que a lei dispunha dispositivos sobre neutralidade da rede, retenção de dados e funções sociais da internet, como liberdade de expressão, transmissão de conhecimento[8] e responsabilidade civil. Em que pese a referida lei, suas ressaltaram a indispensabilidade de uma lei específica para a proteção de dados pessoais no Brasil.

Chama-se atenção em relação ao Código de Defesa do Consumidor - Lei 8.078/1990 - que buscou mitigar os impactos e vulnerabilidades do consumidor. Vê-se que este instituto normativo evolui, ainda mais, na busca pela defesa de informações e tem uma seção específica sobre cadastros e banco de dados. No texto, a legislação defende o direito de o consumidor acessar os dados que uma empresa tem sobre ele e solicitar sua correção, caso alguma informação esteja incorreta. A redação dos artigos 11 e 43 da Lei nº 8.078/90, assim dispõe:

> "Artigo 11 Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento
> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes."

---

[7] (BRASIL, 1988, art. 5, X) Link de acesso: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

[8] https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/181610/2020_araujo_bruna_lgpd_aplicada.pdf?sequence=1&isAllowed=y

Em que pesem os institutos normativos ora mencionados, ainda sim, foi necessário a criação de lei específica para que os indivíduos pudessem ter um manto protetor que abarcasse todas as perpetuações em consonância com a tendência mundial. Segundo SOMBRA[9] (2019), os dados pessoais, com o avanço tecnológico, ganharam um valor para as empresas ganhou, sendo necessário criar um regramento próprio como forma de garantir a privacidade aos seus titulares:

> "dois dos principais campos afetados por esse processo de desenvolvimento tecnológico foram a privacidade e a proteção de dados pessoais. Em virtude da capacidade proeminente de gerar benefícios diretos e indiretos de todas as espécies, a privacidade e a proteção de dados pessoais foram colocadas no epicentro do bem-estar social e do modelo econômico em gestação. Com uma nova força motriz de geração de riqueza - os dados pessoais -, a privacidade se viu diante de uma encruzilhada: tornar-se um obstáculo rígido ao fluxo transnacional de informações ou adaptar-se à nova realidade econômica para viabilizar ganhos sociais mais difundidos".

Como se sabe, o "estopim" sobre esse tema se deu, em especial, a partir dos escândalos noticiados a respeito do vazamento de dados em multinacionais que instigaram a preocupação e insegurança. Contudo, não se podem passar despercebidas outras situações de vazamento de dados por empresas no âmbito nacional.

A título de exemplo, entre meados de 2017 a 2018, uma das maiores empresas de comércio eletrônico no Brasil, a Netshoes[10], teve um vazamento de aproximadamente 2 milhões de dados de clientes do site, ocasião na qual lhe foi imputada multa de R$500 mil reais.

Outra situação relevante que confirmou a necessidade do cumprimento dos dispositivos da LGPD foi a empresa C&A[11], uma das maiores lojas do varejo nacional, também passou por uma situação de vazamento de dados dos seus clientes, sendo alvo de inquérito do Ministério Público.

---

[9] SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados. São Paulo: Thomson Reuters Brasil, 2019, p. 28.

[10] https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml

[11] https://valor.globo.com/empresas/noticia/2018/08/31/c-a-e-alvo-de-hackers-no-brasil-com-vazamento-de-dados-de-clientes.ghtml

O Banco Inter[12], um dos primeiros bancos a oferecer contas digitais no país, também registrou um vazamento de dados a 19 mil correntistas, sendo-lhe imputado uma multa de R$1,5 milhões de reais por deixar clientes vulneráveis.

Em novembro de 2020, cerca de 290 mil clientes da concessionária de energia Enel em Osasco, na Grande São Paulo, tiveram informações sensíveis vazadas após falha de segurança. Além de dados cadastrais, vazaram índices de leitura, nível de consumo e histórico de pagamentos[13].

Ademais, foi noticiado em 2022 que o Banco Central registrou três vazamentos de dados em que incidentes de segurança expuseram por volta de meio milhão de chaves de PIX. Com isso, diversos dados pessoais, tais como, nome completo, CPF, instituição, número de agência e conta, foram vazados.[14]

Assim, apesar de todos os esforços dos legisladores durante todos esses anos para garantir a segurança e privacidade, diante os avanços tecnológico e transformações na Sociedade, o ordenamento brasileiro se viu em uma situação de carência de lei específica sobre o tema que, como bem pontuado acima, reunisse todos as especificidades sobre o tratamento de dados. Dessa forma, ante a necessidade de atender o desenvolvimento e a forma de compartilhamento de dados, culminou na criação da Lei 13.709/2018, a Lei de Proteção de Dados.

Vale destacar, ainda, que grande parte das notícias mencionadas foram após a promulgação da Lei 13.709/2018, o que apenas corrobora ao entendimento de que é necessário implementação e cumprimento aos dispositivos da LGPD. Dessa forma, organizações que realizam o tratamento de dados pessoais no território brasileiro ou oferecem produtos ou serviços a

---

[12] https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/
[13] https://www.procon.sp.gov.br/vazamento-de-dados-da-enel/
[14] https://www.cnnbrasil.com.br/business/meio-milhao-de-chaves-pix-ja-foi-alvo-de-vazamento-saiba-como-identificar-exposicao/#:~:text=Entre%20setembro%20do%20ano%20passado,desde%20o%20final%20de%202020.

indivíduos localizados no Brasil devem buscar entender o impacto da LGPD em suas atividades e como se adequar às suas regras.[15]

É possível notar, portanto, que os países, buscam cada vez, proteger e tutelar o tratamento de dados, tendo em vista tantos casos de vazamento em grandes empresas. Esse panorama é uma tendência mundial que após muito debate, o Brasil se viu obrigado a disciplinar a matéria em prol da sociedade.

2.2. Jurisprudência comparada

Como pontuado acima, a LGPD trata-se de um instituto normativo que é reflexo da globalização e a valorização da tecnologia, utilizando-a cada vez mais para executar tarefas do cotidiano, especialmente nas relações de emprego em que se lida tanto com dados dos empregados, como a coleta de dados de clientes do empregador.

Essa tendência do Século XXI e a Quarta Revolução Industrial tem sido um ponto em que os países têm analisado para verificar a necessidade de tutelar os desdobramentos desta alta interferência de dados e tecnologia. De certa forma, pode-se verificar que o Brasil criou norma jurídica sobre um assunto que já vem sendo bastante discutido e até mesmo tutela por outros países.

A título de exemplo, a Europa já vem disciplinando a matéria desde a década de 1970. Isto porque, o Conselho Europeu regulamentou o tratamento de dados por meio da Resolução nº 22 de 1973 e 29 de 1974, as quais versam sobre fundamentos para a proteção de dados e banco que coletam informações a respeito dos indivíduos.

Este direito foi inicialmente reconhecido pelo Tribunal Constitucional Alemão na década de 1980 a partir do julgamento do caso da “Lei do Censo Alemã”. Na época a referida lei foi declara inconstitucional, pois, para a realização do chamado censo demográfico, a coleta de

---

[15] Guia de prática sobre a LGPD, Julho de 2019 Acesso: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf

informações necessárias seria excessiva.[16] Outro caso alemão emblemático sobre a proteção de dados ocorreu na década de 1990, SADEN (2012) conta que uma empresa, com objetivo de reduzir o quadro de empregados sem aval do Conselho da Empresa se utilizou da base de dados do sistema de administração pessoal. A partir das informações extraídas, a empresa tomou a decisão de extinguir a conexão de ônibus oferecida aos seus funcionários até determinada área residencial. Tal medida impactou diretamente o quadro de funcionários, pois foi constatado pelos dados coletados que aquela linha de ônibus era utilizada principalmente por jovens mães e, a partir, da sua extinção, as empregadas se viram obrigadas a pedir demissão, uma vez que não teriam mais a condição de conciliar o trabalho e as obrigações familiares. No caso mencionado não houve propositura de qualquer tipo de ação judicial, porém demonstra a importância da proteção de dados e os impactos de se mau uso.

Não obstante, outro marco para a proteção de dados foi no ano de 1995. De acordo com Voila Bonfim, a União Europeia ciou a partir da Diretiva nº 46 o "Regulamento Geral da Proteção de Dados". Inclusive no ano de 2018, diante várias notícias de vazamento de dados, a União Europeia se viu obrigada a revisitar suas regras e posicionamento sobre o tratamento de dados pelas empresas. Tal ocasionou na criação do "GDPR", o qual instituiu que empresas deveria mudar a forma de coletar dados.

GASPAR (p. 199) também cita como um dos exemplos mais recentes, o escândalo de 2018 a respeito do *Cambridge Analytica* notificado pelo New York Times, ao qual foi mencionado que durante a época das eleições nos Estados Unidos, dados sensíveis de mais de 50 milhões de usuários foram vazados e utilizados favoravelmente ao candidato Donald Trump. [17]Tal notícia também repercutiu no fundador do *Facebook*, Mark Zuckerberg.

Com isso, uma lei específica brasileira que tutela a proteção de dados nada mais é que o reflexo de uma tendência global dentro de uma Sociedade com alto fluxo de dados. Ressalta-se

---

[16] LIMA SILVA, PINHEIRO, BOMFIM; Manual de Compliance Trabalhista, Teoria e Prática, 2ª Edição, 2021, capítulo 11, página 728.
[17] GASPAR, Gabriel. A LGPD e o Tratamento de Dados Sensíveis; Reflexos da LGPD o Direito e no Processo do Trabalho, 2020. P. 199.

que, ainda que cada país deva olhar para as particularidades e lacunas de seu próprio país, vez que temos sistemas jurídicos diferentes (*common law e civil law)*, é certo que no Direito Brasileiro - a partir de debates – restou demonstrada a necessidade e seriedade a respeito do assunto.

2.3. Procedimento de implementação da LGPD e Agência Nacional de Proteção de Dados (ANPD)

FILHO (2020) esclarece que "Percebe-se, portanto que a lei geral de proteção aos dados pessoais abarca desde direitos fundamentais como a proteção à intimidade e a vida privada até ao seu entendimento de um direito autônomo. Desta forma, enfrenta questões inéditas frente a mudança de paradigmas nas relações sociais e na economia, decorrentes da era da velocidade digital."

Em 2022 foi aprovada a Emenda Constitucional 115ª, de 10 de fevereiro de 2022 que alterou a Constituição Federal de 1988 para incluir em seu rol de direitos e garantias fundamentais a proteção de dados pessoais, bem como fixar a competência privativa da União para legislar sobre a proteção e tratamento de dados pessoais. Esta Emenda Constitucional foi originada pela Proposta de Emenda à Constituição (PEC) 17/2019, a qual foi aprovada pelo Senado Federal em 20 de outubro de 2021. Conforme se apreende do texto constitucional, foi incluído o inciso LXXIX no artigo 5º da Constituição Federal de 1988 de que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais[18].

Nos termos da Proposta de Emenda à Constitucional nº 17, 2019

> A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.
>
> O avanço da tecnologia, por um lado, oportuniza racionalização de negoc1os e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por

[18] https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm

> outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados.[19]

Chama-se atenção, ainda, que o Relator da Proposta de Emenda à Constituição, o Senador Eduardo Gomes, utilizou como base para justificar a pretensão a partir de uma comparação de outros países sobre a regulamentação de tratamento de dados, confirmando que se trata de tendência mundial a preocupação na forma de armazenar e regular o compartilhamento de dados.

> Na América do Sul, países vizinhos como Chile e Argentina, entre outros, já contam com I eis próprias de proteção de dados.
> (...)
> Foi o caso de Portugal: sua Constituição, adotada em 1976, assegura o direito e a garantia pessoal de utilização da informática, estabelecendo, também, normas específicas de acesso e tratamento de dados pessoais. Algo similar se vê na Estônia, Polônia e, mais recentemente, no Chile, que, em 5 de junho de 2018, editou a Ley no 27.096, constitucionalizando a proteção de dados pessoais.[20]

2.4. Princípios da Lei de Proteção de Dados

Apesar do marco regulatória da LGPD ser recente e, por isso, sua aplicação na prática - ainda que urgente, - é bastante superficial. E como forma de dar luz ao que o legislativo pretende por meio da Lei, em seu artigo 6º já há uma delimitação do que se espera daqueles que operam com dados, nos termos:

> I — Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II — Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III — Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

---

[19] https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1647518557279&disposition=inline
[20] https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1647518557279&disposition=inline

> IV — Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V — Qualidade de dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI — Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII — Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII — Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX — Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X — Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Tem-se que a LGPD é uma legislação multidisciplinar que conversa com todos os ramos do direito, isto porque, onde há dados há necessidade de diretrizes de armazenação para garantir a segurança e privacidade das pessoas naturais. Dessa forma, sua aplicação em qualquer tipo de relação é quase que imediata, diante da urgência das Empresas se organizarem e criarem estruturas para receber os impactos previstos na referida Lei, cujo objetivo é a garantia do tratamento dos dados pessoais de forma segura e ética.

Caio Mario (2018, p. 326) traz elucidações sobre a responsabilização de agentes, no sentido que “se fixa no fato de que, se alguém põe em funcionamento uma qualquer atividade, responde pelos eventos danosos que esta atividade gera para os indivíduos, independentemente de determinar se em cada caso, isoladamente, o dano é devido à imprudência, à negligência, a um erro de conduta”.

Infere-se, portanto, que a Lei é uma nova oportunidade, diante os avanços tecnológicos, de repensar os nossos modelos, na medida em que as Empresas se aproveitaram do fenômeno da

"inteligência artificial", pois até então se tratava de território quase ausente de regulamentação usufruído de forma desacerbada como meio de exploração econômica. Carece, portanto, relações de transparência e confiança com as pessoas, sejam elas empregados, parceiro ou clientes.

Dessa forma, tem-se que os princípios regem a LGPD são de extrema relevância para disciplinar a matéria. A título de exemplo, o princípio da finalidade determina que o tratamento de dados pessoais precisa necessariamente ter propósitos legítimos, específicos, explícitos e com consentimento do título para a utilização das informações.

O princípio da transparência, que é de extrema relevância e a base para implementação da LGPD, é garantir aos seus titulares o direto de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.[21] Outrossim, há que se destacar a última parte do VI, do artigo 6º, uma vez que se deve ponderar o que, de fato, é necessário divulgar, principalmente quando se tratam de dados sigilosos a respeito da própria atividade empresarial, de modo a não ferir os interesses comercial, nos exatos termos do referido inciso.

Por sua vez, os princípios da adequação e da necessidade estão diretamente ligados ao princípio da finalidade, haja vista que enquanto este o utiliza como base para limitar as atividades relacionadas a manipulação ou, então, a alteração de dados, aquele utiliza-se do princípio como um paradigma para definir quais atividades são ou não adequadas.

A finalidade, portanto, norteará toda a cadeia das atividades envolvendo dados pessoais, do consentimento do titular ao término do tratamento, servindo, inclusive, como referência objetiva para eventuais excessos e abusos por parte dos agentes. Segundo a cartilha Guia sobre a LGPD[22] de 2019 do escritório de advocacia Mattos Filho, o tratamento de dados pessoais

---

[21] Guia para a Lei Geral de Proteção de Dados, Julho 2019 Acesso: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf

[22] Guia para a Lei Geral de Proteção de Dados, Julho 2019 Acesso: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf

deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias.

O princípio do livre acesso, previsto no inciso IV do art. 6º, se materializa nas prerrogativas dos titulares de dados, previstas no artigo 9º, que estabelece que o titular tem o direito ao acesso facilitado e inteligível às informações referentes ao tratamento de seus dados. Dessa forma, o grande objetivo deste princípio é garantir a consulta eficiente e facilitada aos titulares a partir de três pilares: a forma, duração do tratamento e integralidade dos dados pessoais[23].

Outrossim, o princípio da não discriminação, previsto no inciso IX do art. 6º da referida Lei, assegura que o tratamento de dados seja uma obrigação ética, o que vedando finalidades discriminatórias ilícitas ou abusivas, o que possui respaldo na própria Constituição Federal ao qual a punição de discriminações atentatórias dos direitos e liberdades fundamentais.

Ao encontro, o artigo 42 da Lei prevê as consequências pelo vazamento de dados:

> Artigo 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

---

[23] Guia para a Lei Geral de Proteção de Dados, Julho 2019 Acesso: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf

> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso (BRASIL, 2018).

Não obstante, os princípios da segurança, prevenção e da responsabilização e prestação de contas possuem buscam evitar possíveis danos, responsabilizando-se pela implementação de medidas eficazes que atendam aos requisitos, o que melhor serão destrinchados ao longo do trabalho.

Especificamente sobre o princípio da responsabilização, há, também a prestação de contas que é essencial para ambientes corporativos, uma vez que prevê a obrigação em detalhar a adoção de medidas eficazes para observância e cumprimento dos dispositivos da LGDP.

Outrossim, merece atenção o princípio da qualidade dos dados, tendo em vista que o princípio consubstanciado no artigo 6º, V, da Lei 13.709/2018 garante aos seus titulares que seus dados sejam exatos, claros relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Ou seja, a legislação busca a proteção desses dados, de modo que não sejam danificados ou, então, no pior cenário, sejam perdidos.

Dessa forma, a Lei de Proteção de Dados buscar trazer uma conscientização sobre a coleta de dados, como forma efetiva de garantir o princípio constitucional a privacidade. Congruente ao pensamento de FILHO (2020):

> "(...) a finalidade da LGPD é garantir privacidade e transparência no tratamento dos dados das pessoas físicas, principalmente dos consumidores, empregados e prestadores de serviço, gerando para todas as pessoas jurídicas tanto de direito púbico como privado,

> independentemente do porte e atividade empresarial exercida, o dever de atender os novos comados legislativos e se adequar para cumprir a vasta gama de direitos dos titulares dos dados pessoais"

Com efeito, a LGPD, por meio do seu artigo 6º traz um rol mínimo de princípios para guiar tanto os titulares dos dados pessoais, assim como, os operadores e controladores de dados.

3. A INTERFACE DA LGPD NAS RELAÇÕES DE EMPREGO

O compartilhamento de dados, tendo em vista o avanço na tecnologia e a privacidade, é um tema relevante, sendo que suma importância a adoção das diretrizes da LGPD em empresas. Isso porque, o artigo 1º da LGPD estabelece a finalidade da Lei ao mencionar que o direito fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. [24]

Dessa forma, nota-se que os efeitos da Lei de Proteção de Dados são aplicáveis em diversos âmbitos e tipos de relações desde que se tenha uma pessoa natural envolvida. FRAZÃO, TEPEDINO e OLIVA destacam[25] a transversalidade da aplicação da LGPD:

> "Nesse contexto, observa-se que o *compliance* de dados não se limita apenas ao relacionamento com consumidores, mas acaba por repercutir em várias esferas da atividade empresarial, a demandar adaptação também de setores que, inicialmente, não estariam diretamente relacionados com a LGPD. O *compliance* de dados assume caráter transversal, a tornar necessário rever os padrões de conduta estabelecidos para cumprimento de outras normas. Remeta-se, mais uma vez, à relação de trabalho: as regras de conformidade adotadas nesse setor deverão ser atualizadas para contemplar também os preceitos da LGDP, evitando- se, por exemplo, a coleta de dados desnecessários ou cujo emprego possa ser considerado discriminatório."

---

[24] BRASIL, Lei nº 13.809/2018, de 14 de agosto de 2018. Artigo 1º. Acesso: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[25] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de Dados Pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord). Op Cit.p.695

Nesse sentido, FILHO (2020) esclarece que a lei geral de proteção aos dados pessoais abarca desde direitos fundamentais como a proteção à intimidade e a vida privada até ao seu entendimento de um direito autônomo. Desta forma, enfrenta questões inéditas frente a mudança de paradigmas nas relações sociais e na economia, decorrentes da era da velocidade digital.

Não obstante, PIERONI (2021 p. 35) complementa que o propósito da LGPD com enfoque no Direito do Trabalho esclarecendo que a nossa Carta Magna de 1988 traça linhas gerais para garantir aos trabalhadores urbanos e rurais a proteção em face da automação (CF, artigo 7º, XXVII). Em outras palavras, o legislador pretende garantir a proteção, no que diz respeito "uso de ferramentas ou técnicas computadorizadas, de modo a aperfeiçoar os processos produtivos, logo, os dados tratados no âmbito das relações de emprego". E por isso, a necessidade de lei específica.

Sob esse ângulo (BONFIM, 2020, p. 49) esclarece que há enfoque no Direito de Trabalho para aplicação da LGPD, uma vez que há elevado fluxo de dados nas relações de emprego em grandes proporções, o que "o empregador, desde a fase pré-contratual (processos seletivos e admissão), passando pela fase contratual e chegando até a fase pós-contratual, tem acesso e se torna responsável pelo armazenamento e pela guarda de dados pessoais dos trabalhadores".

Nesse aspecto, ao encontro da fala acima, prescreve o art. 3º da LGPD:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019); III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (BRASIL, 2018)

Nesta seara, ainda que a LGPD não seja um tema trabalhista, está intrinsecamente ligado. Afinal, onde se há Empresas se há relações de emprego e coleta de dados de seus funcionários. Sendo assim, importante se atentar obrigações impostas pela referida Lei e "adequar as rotinas trabalhistas às exigências de proteção de dados" (BONFIM, 2020, p. 50), pena de serem responsabilizados pelo vazamento de informações pessoais.

Isso porque, o fluxo de dados de pessoas naturais é inesgotável, sejam eles de empregados, prestadores de serviços, fornecedores ou clientes. [26] Até porque, sequer seria possível iniciar uma relação de trabalho ou de prestação de serviços sem a devida coleta e armazenamento de dados. [27]

Nas palavras de MIZIARA (2020), a LGPD exigirá dos empregadores enormes esforços para adequar suas rotinas trabalhistas às exigências legais, providência que desde já se recomenda, sob pena de serem responsabilizadas e arcar com danos decorrentes.

3.1. Os conceitos centrais da LGPD nas relações de emprego

Em relação a interface da LGPD e as relações de emprego, Ana Francisca Sanden destaca que:

> "As relações empregatícias são um importante palco para a realização de objetivos diversos, como a inclusão de determinados grupos no mercado de trabalho, o cumprimento de padrões no atendimento ao consumidor, a gestão da saúde ocupacional dos empregados e o pagamento de benefícios previdenciários a empregados ou a seus familiares. Normalmente, o empregador funciona como estação de trânsito das informações necessárias para a realização desses misteres. E, em ambiente marcado pelo uso das tecnologias da informação e da comunicação, todas essas informações, mesmo que fragmentárias, formam uma base de dados multifuncional que, por meio das operações de processamento, propiciam a

[26] Revista do Tribunal Regional do Trabalho da 10ª Região, v. 24. Nº 2, 2020; SANTOS, Alcassa Flávia, A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Exposição de Dados Sensíveis nas Relações de Trabalho
[27] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista, Teoria e Prática, 2 Edição, 2021, p. 726.

> exploração de acordo com as expectativas e as políticas empresariais e trazem o risco de fragilizar a posição do empregado e de prejudicá-lo."[28]

Com isso, diante o panorama que a Sociedade se encontra e os arcabouços normativos de proteção jurídica aos dados, cria-se a necessidade de as empresas implementarem um programa de proteção de dados que atendam a lei, minimizando eventuais sanções e, o mais importante, o vazamento de dados. Assim, a LGPD nada mais é do que a aplicação de uma lei por parte dos controladores e operadores de dados, sendo uma forma das empresas atuarem de forma ética e preserve a sua imagem e de seus empregados perante a Sociedade. [29]

Conforme se apreende da Lei 13.709/2018, o artigo 5º, I, prevê "informação relacionada a pessoa natural identificada ou identificável". Com isso, o dado a ser protegido é aplicável a pessoas físicas sendo considerados como dados pessoais, o nome estado civil, escolaridade, endereço, filiação, dentre outros[30]. Já o inciso II do referido artigo dispõe em sua redação o que é considerado como dados pessoal sensível qual seja, qualquer informação da pessoa natural sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.[31]

Verifica-se, portanto, que o artigo 5º da LGPD destaca diversas hipóteses exemplificativas sobre informações a respeito de pessoas naturais, as quais devem ser tuteladas a fim de garantir a proteção e privacidade, principalmente aqueles considerados como dados sensíveis. Há que se ressaltar que muito embora os referidos incisos disponham expressamente os tipos de informações que são categorizadas como dados pessoais, é certo que não se trata de rol taxativo, inclusive, sendo possível que a Autoridade Nacional de Dados, dentro de suas

---

[28] SANEN, Ana Francisca M. de Souza. A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. Tese de Doutorado apresentada à Faculdade de Direito da Universidade de São Paulo. 2012.
[29] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 299)
[30] LIMA SILVA; PINHEIRO; BONFIM, Manual do Compliance Trabalhista: Teoria e Prática; 2021, 2ª Edição, p.732
[31] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

competências previstas pelo artigo 55-J da LGPD, aborde outras hipóteses caracterizadoras. Tal competência é estabelecido por meio do inciso XX “deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos”.

Segundo os dispositivos previstos na LGPD dentro de uma cadeia para tratamento de dados pessoais há enfoque em dois agentes principais que são definidos conforme as funções que desempenham. De início, importante destacar que o instrumento normativo entende que o verbo “tratar” dados é considerado como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”, sendo que sua redação traduz em um proteção ampla de dados.

Em relação aos sujeitos dos tratamentos de dados pessoas, a legislação traz como agentes os titulares de dados pessoais, controlado, operador e encarregado. A figura do encarregado será explorada em tópico abaixo. No que diz respeito ao titular de dados, vê-se que a legislação é clara ao destacar que tal é apenas aplicada a pessoas naturais, porém PINHEIRO e BONFIM (2021) trazem a seguinte reflexão:

> “Merece reflexão de microempreendedor individual (MEI), do empregador doméstico e do empregador pessoa física, como os profissionais liberais. Isso porque todos esses se constituem em pessoas naturais, normalmente com hipossuficiência econômica em relação as empresas.”

O inciso VI do art. 5° da Lei n.º 13.709/18 dispõe que o controlador se trata de “a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Não obstante, o inciso VII resguarda que o operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Nessa toada, tem-se como as principais obrigações do controlador: (i) atender a determinadas requisições dos titulares dos dados pessoais por ele tratados, conforme previsão do art. 18 da LGPD; (ii) fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para as decisões tomadas unicamente com

base em tratamento automatizado de dados pessoais (art. 20 da LGPD); (iii) elaborar, mediante determinação da autoridade nacional de proteção de dados, relatório de impacto à proteção de dados pessoais referente a suas operações de tratamento de dados (art. 38 da LGPD); (iv) verificar a observância pelo operador das instruções que lhe forneceu e das demais normas sobre tratamento de dados (art. 39 da LGPD); (v) instituir um encarregado pelo tratamento de dados (art. 41 da LGPD); (vi) comunicar à autoridade nacional e aos titulares de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48 da LGPD).

Observa-se que cada um desses agentes tem obrigações próprias. Assim, enquanto a obrigação principal dos operadores, como acima apontado, é realizar o tratamento de dados segundo as instruções fornecidas pelo controlador, é ao controlador a quem competem as decisões referentes ao tratamento de dados pessoais e a LGPD ainda destina especificamente ao controlador uma série de outras obrigações relevantes.

Por sua vez a figura do operador poderá existir ou não a depender da contratação de uma pessoa natural ou jurídica pelo empregador para e seu nome realizar o tratamento de dados, sendo neste caso os empregados. Contudo é plenamente possível que o empregador acumule a função de controlador e operador.

3.2. *Compliance* Trabalhista

LIIMA SILVA, PINHEIRO e BONFIM (2021, p. 728), trazem como exemplo prático da LGPD nas relações de trabalho a situação sobre a entrega de atestados médicos que possuam o diagnóstico de alguma doença ou, até mesmo, o CID (Código de Identificação da Doença). É certo que o empregado tem direito de que aquela informação sobre o seu estado de saúde não seja compartilhada entre os demais, até mesmo para evitar qualquer tipo de tratamento de cunho discriminatório. Por outro lado, é de extrema importância que a Empresa saiba guardar aquela documentação para fins previdenciários.

O exemplo prático acima demonstra que a instituição e transição para que as empresas atendam aos dispositivos da LGPD é um projeto, sendo necessário que as empresas estejam

preparadas para que seus procedimentos sejam seguros, passando confiança aos seus empregados, prestadores de serviços e clientes. Com isso, o projeto para a aplicação da LGPD pelas empresas, principalmente em relação aos seus empregados devem ser baseadas nos seguintes pilares: (i) mapeamento; (ii) bases legais; (iii) análise de risco; (iv) governança; (v) documentos e (vi) conscientização[32].

Segundo ROXO (2020, p. 300), para o início de um programa de implementação da LGPD cabe a mobilização das pessoas que serão envolvidas: interno, externo ou a contratação de novos profissionais para viabilizar a implementação das novas medidas; sendo uma figura importante nesse início o Encarregado. Conforme destacado acima, dentro dos sujeitos de tratamento de dados pessoais, existe o Encarregado em que se trata de pessoa indicada pelo controlador e operador para atuar por meio de canal de comunicação. Ou seja, a figura do Encarregado, na mais é do que manter a proximidade e canal entre os controladores – dentro do contexto desta monografia – os empregadores – os titulares dos dados – os empregados – e a Autoridade Nacional de Proteção de Dados. A LGPD, por meio do artigo 41, estabelece que cabe ao controlador indicar um encarregado pelo tratamento de dados pessoais.

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º 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.

Veja-se que para a indicação de um Encarregado não obriga que seja um empregado da empresa, inclusive, é possível que seja um prestador de serviços para desempenhar essa função,

---

[32] Soler, Fernanda G. Proteção de dados: reflexões práticas e rápidas sobre a LGPD. Disponível em: Minha Biblioteca, Editora Saraiva, 2022.

desde que a identidade e informações desta pessoa designada seja divulgada de forma pública, clara e objetiva, preferencialmente no site do controlador, conforme previsto no § 1º do artigo 41. Importante mencionar que eventual terceirização desta função pode vir a aumentar a exposição de riscos, o que demonstra a necessidade de zelar para quem se está terceirizando atividade sensível.[33]Sendo empresas do mesmo grupo econômico, não se faz necessário mais de um Encarregado para promover a comunicação entre as empresas, empregados e a ANPD, nos termos do artigo 37, II, da GDPR e artigo 8º da CLT.

Não obstante, é certo que o rol de atividades do Encarregado apresentado pelo artigo 41 é meramente exemplificativo, uma vez que o parágrafo 3º da referida Lei prevê a possibilidade de que a autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

VIEIRA (2019) destaca que nessa fase inicial é interessante estabelecer um Comitê de Privacidade e Proteção de Dados[34], cujo objetivo é ter executivos das principais áreas envolvidas no programa quais seja, áreas relacionadas a tecnologia e segurança da informação, *compliance*, jurídico, ao qual poderá ser montado tanto por profissionais da própria empresa, como também a contratação de um escritório externo para realizar esse tipo de demanda. Ressalta-se a importância de que os Recurso Humanos faça parte do Comitê, haja vista que são estes profissionais que lidam com dados desde o momento pré-contratual, durante a relação de trabalho e pós-contratação. Escolhidos os profissionais, é necessário que estes estejam todos na mesma página em relação ao treinamento e cursos direcionados aos negócios da empresa, de modo a entender os potenciais riscos envolvendo a privacidade da empresa. Não obstante, é este Comitê que estará responsável por discutir, conduzir e ministrar treinamentos, workshops e entrevistas com empregados. [35]

---

[33] LIMA SILVA; PINHEIRO; BONFIM, Manual do Compliance Trabalhista: Teoria e Prática; 2021, 2ª Edição, p.737
[34] VIEIRA, Claudinei. Capítulo 1 – Fase 1: Preparação, in MALDONADA, Viviane Nóbrega (coord). LGPD: Lei de Proteção de Dados pessoais: manual de implementação. São Paulo. Thomson Reuters Brasil, 2019
[35] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 302)

Após a instauração, VIEIRA (2019) entende que o próximo passo é a realização de workshops e entrevistas iniciais sobre o tema com intuito de levantar questões sobre a privacidade dentro da empresa, lei geral de proteção de dados, como vem ocorrendo para fomentar discussões e sugestões acerca do projeto de implementação da LGPD para que seja alinhado o programa com base nas especificidades da empresa. Destaca-se, ainda, que é necessário o comprometimento e envolvimento de cada setor e respectivo gestor, sendo importante que participem (i) workshops; (ii) entrevistas e reuniões para colher informações sobre os dados tratados; (iii) adquirir conhecimento a respeito da privacidade da empresa; (iv) informar e conscientizar os pontos principais sobre a LGPD[36], de modo que a partir disso, se tenha uma documentação a respeito de todo o procedimento para a implementação da LGPD e como a referida lei irá conversas com as normas da Constituição Federal, Consolidação das Leis Trabalhistas, as normas coletivas, dentre outros marcos regulatórios que as empresas também precisam cumprir.

A avaliação inicial é de extrema importância, uma vez que a maior parte das pessoas não possuem consciência da relevância de questões como a privacidade e dados pessoais[37], e com o elevado fluxo de dados nas relações de emprego, a LGPD impacta grande proporção dentro das relações, pois a referida lei deve ser aplicada desde a fase pré-contratual, a fase contratual e até mesmo a fase pós-contratual. [38]Há compartilhamento e armazenamento de informações durante todo o ciclo do empregado na empresa.

Passando-se da fase inicial, há a fase de mapeamento de dados, que segundo ROXO (2020, p. 304) nada mais é do que um inventário de dados, como forma de mapear todas as informações que são tratadas pela empresa. Nessa fase, há que se ter os seguintes pontos alinhados (i) setor responsável; (ii) quem é o titular e de onde é a fonte e forma coletada desses dados; (iii) quais são os dados pessoais e dados sensíveis; (iv) de que forma é armazenado esses dados; (v) qual a localização de coleta; (vi) quais departamentos têm acesso; (vii) há transferência de dados de forma externa ou internacional; (viii) quais são as medidas de segurança adotadas; e (ix) por

---

[36] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 303)
[37] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 303)
[38] LIMA SILVA; PINHEIRO; BONFIM, Manual do Compliance Trabalhista: Teoria e Prática; 2021, 2ª Edição, p.726

quanto tempo elas ficam armazenadas. Ao passar por esse processo, deve-se levar em conta todos os dados oriundos de uma eventual relação, desde a fase pré-contratual, contratual e pós-contratual. Isso porque, até a relação pós-contratual é disciplinada pela LGPD, na medida em que os artigos 15 e 16 estabelecem que:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.
>
> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Inclusive, o artigo 16 estabelece diversas hipóteses em que os dados armazenados podem ser conservados desde que seja por imposição legal; utilização para fins de pesquisa desde que anonimizados; transferências a terceiros, como por exemplo, quando é o caso de um empregado que será direcionado para outra Sede da empresa ou até no âmbito da Justiça do Trabalho, quando autoridades requerem informações, ou até mesmo para uso do controlador, desde que utilizada a técnica da anonimização de dados pessoais, conforme previsão no inciso IV, do artigo 16.

Com isso, por meio do mapeamento de dados o ROXO (2020, p. 305) traz o conceito de “levantamento e diagnóstico inicial” em que se é possível verificar a forma atual em que o tratamento de dados vem sendo realizado e, por consequência, avaliar o cenário da privacidade dentro do ambiente da empresa e eventuais riscos e falhas. Após todo esse estudo a respeito da estruturação da empresa para a implementação da LGPD, parte-se para o desenvolvimento do plano

de ação em que o Comitê Executivo de Privacidade e Proteção dos Dados Pessoais deverão acompanhar para que, como tempo e seus desdobramentos, possam ser revistados e aperfeiçoados.

O plano de ação envolve as bases legais que serão utilizadas para tratar os dados da empresa, políticas de privacidade que serão implementadas. É nesse momento em que se deve aprofundar o mapeamento mencionado acima e, portanto, nessa fase, a empresa não mais está verificando como o tratamento tem sido realizado na prática, e sim - a partir daquilo que foi diagnosticado -, como é possível alterar/ajustar de modo que se atenda a LGPD. Com isso, é importante que esteja definido pelo Comitê: (i) a base legal para tratamento de dados; (ii) como serão garantidos os direitos dos titulares; (iii) a duração de tempo em que será mantido esses dados dentro das previsões estabelecidas pela LGPD (vide artigos 15 e 16 da Lei 13709/2018); (iv) quais serão as medidas de segurança; (v) como será o descarte; (vi) os requisitos e critérios a serem utilizados na hipótese de transferência. Nota-se, portanto, que na fase de mapeamento a questão era "como ocorre" e, neste momento, a dúvida é "como será".

Verificados todos esses pontos, é imprescindível a elaboração de relatório para documentar todos os passos, avanços e aperfeiçoamentos do projeto de implementação da LGPD, conforme estabelecido pelo artigo XVIII do artigo 5º relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco[39]. A documentação e elaboração de relatório também possibilita que o Comitê tenha esse controle e facilite caso seja solicitado pelo órgão fiscalizador, ANDP, em eventual fiscalização, o que resguarda a imagem da Empresa. Outrossim, o próprio artigo 38 da LGPD contém previsão de que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.[40]

---

[39] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

[40] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Ainda, há mais um passo para seguir com o plano de ação, ROXO (2020, p. 307) destaca que:

> "Após essa etapa, passa-se ao inventário dos dados: fase em que são confirmadas as informações colhidas no mapeamento, são introduzidas novas informações e conclusões sobre os riscos identificados e as bases legais que serão introduzidas para o tratamento de dados pessoais".

Em outras palavras, a fase antecedente a implementação dos mecanismos e práticas da LGPD na mais é do que a correlação entre o mapeamento de dados – o que na prática estava ocorrendo – e as bases legais para as mudanças – o que será necessário para cumprir as diretrizes da LGPD. E, a partir dessa correlação, constata-se a possibilidade ou não de executar para a criação e boas práticas e governança. No que diz respeito a governança, conforme será explorado no capítulo abaixo, a Lei Geral de Proteção de Dados instituiu por meio do seu artigo 50 a possibilidade de criação de práticas de boa governança a fim de garantir o estrito cumprimento a Lei 13.40/2018. Dentro das relações de emprego, as formas mais recorrentes de tratamento de dados pessoais legítimas: (a) cumprimento de obrigação legal ou regulatória; (b) execução de contrato ou de procedimentos preliminares relacionados ao contrato; (c) exercício regular de direitos em processo judicial, administrativo ou arbitral. [41]

A título de exemplo, LIMA SILVA, PINHEIRO e BONFIM (2021, p. 729) demonstram a forma que a LGPD deverá impactar os empregados:

> "Todos os empregados devem ser informados e alguns treinados para o armazenamento, descarte e demais formas de tratamento de dados pessoais e sensíveis, inclusive os que aparentemente não lidam com dados, como a faxineira, o contínuo ou o garçom, pois podem ter acesso fortuito pregador (controlador) a adoção das medidas de precaução e proteção aos dados de todos os trabalhadores"

Assim, é necessário a implementação de um projeto para a implementação da LGPD de uma empresa, pois não se trata de aplicação superficiais de dispositivos, é necessário

[41] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista, Teoria e Prática, 2 Edição, 2021, p. 742-743

aprofundamento nas questões e embasamentos para a criação de um marco regulatório específico para dispor sobre o tratamento de dados pessoais. ROXO (2020, p. 324) destaca que se trata da conscientização da sociedade sobre o valor dos dados pessoais e sua inclusão na esfera da privacidade da pessoa natural, a integridade que será implementada para possibilitar da empresa nesse novo cenários. Em outras palavras, é uma mudança de cultura dentro do ambiente corporativo que afeta desde o empregador – aqueles que ocupam o cargo de chefia – o RH, os próprios empregados que lidam com alto fluxo de informações, eventuais colaboradores e até clientes.

4. RESPONSABILIDADE CIVIL NA LGPD

As relações de trabalho vêm sofrendo impactos diante uma Sociedade com alto desenvolvimento tecnológico e fluxo de informações compartilhadas. Por conseguinte, no mundo corporativo, tais mudanças podem ser observadas por meio do monitoramento de e-mails, uso da internet no local de trabalho, câmeras para fins de controle de conduta, dentre outras medidas que vem sendo instauradas dentro de um contexto atual da onda neoliberal. E, desde então, vem sendo discutido no âmbito judicial a possibilidade de indenizar, quando restar comprovado o exercício arbitrário do empregador ou, então, nas palavras de ZAVANELLA e MAISTRO JUNIOR (2021), o desvirtuamento das legítimas finalidades, por violação aos princípios e regras constitucionais e legais sendo os exemplos mais marcantes, a dignidade humana, intimidade e até mesmo a livre-iniciativa.[42]

Com isso, caso não cumpridas as diretrizes estabelecidas pela LGPD, há uma Seção da referida Lei denominada “Da Responsabilidade e do Ressarcimento de Danos” disciplinando a responsabilidade dos agentes de tratamento de dados e eventuais danos e multas impostas a estes em caso de má conduta de processamento de dados e eventuais danos que os titulares possam sofrer, implicando na violação ao direito à intimidade ou à privacidade quanto ao tratamento de dados pessoais.

[42] Reflexos da LGPD no Direito e no Processo do Trabalho (p. 233)

Não obstante, também foi criado o órgão fiscalizador, a Autoridade Nacional de Proteção de Dados ("ANPD") a partir da Lei nº 3.853/2019[43], a qual é responsável por fiscalizar, implementar e incentivar o cumprimento das diretrizes da LGPD.

4.1. As boas práticas para empresas atenderem a LGPD

Conforme destacado acima, atender aos dispositivos da LGPD não foi proposto apenas para se evitar sanções por meio do órgão regulamentar (ANPD), mas principalmente para que as empresas possam atuar de forma mais ética. ROXO (2020, p. 299) destaca que além de correr o risco de empresas serem multadas, em razão do acesso aos dados pessoais bloqueados, a depender do tipo de vazamento de dados, a violação pode gerar danos devastadores à imagem da empresa interferindo diretamente em seu desenvolvimento econômico. [44]

Para cumprimento aos dispositivos da LGPD e evitar eventuais penalidades, a Lei de Proteção de Dados é clara por meio do seu artigo 50 estabelecer que 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.[45]

Com isso, conforme mencionado acima, as empresas devem implementar um verdadeiro *compliance* de dados no âmbito trabalhista para anteder aos princípios norteadores da Lei de Proteção de Dados. Por meio do § 1º do artigo 50, quando da implementação de regras de

---

[43] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

[44] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 299)

[45] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

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.[46]

O § 2º do artigo 50 do marco regulatório prevê que a adoção de boas práticas pelas empresas deve levar em consideração os princípios da transparência e segurança, além de estabelecer parâmetros para a criação dessas regras e implementação de boas práticas:

> § 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

[46] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Segundo BONFIM (2021, p. 726):

> "Mesmo que a legislação brasileira não tenha regulamentado a aplicação da proteção de dados no âmbito das relações de trabalho, é essencial investigar as causas legitimadoras do tratamento de dados nas relações de trabalho, bem como a forma de operacionalizá-las, considerando-se as necessidades decorrentes da dinâmica dos negócios"[47]

O Tribunal Regional do Trabalho da 10ª Região[48], como formas de adotar boas práticas pelas empresas em prol de garantira a transparência e segurança aos funcionários, destaca o artigo da Revista Síntese que elenca uma série de medidas para que empresas adotem para refletir nas relações de emprego. A título de exemplo, na fase pré-contratual em que já se exige o tratamento e armazenamento correto de dados, é necessário o treinamento e conscientização do uso devido dos dados pessoais, junto ao departamento de Recurso Humanos das empresas.

Além disso, com a entrada em vigor da LGPD, também é necessário adequar as práticas e documentos de governança das empresas. Com isso, revisar ou elaborar (i) Políticas de Segurança sob à ótica dos três pilares: confidencialidade, integridade e disponibilidade, (ii) cláusulas atinentes à Privacidade nos contratos com empregados de conformidade com a LGPD; (iii) aditivos dos contratos em vigor para adequar a LGPD; (iv) cláusula nos contratos de prestadores de serviços; (v) fichas e formulários de entrevistas de acordo com o Princípio da minimização de dados (adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados).

Não obstante, (i) adotar políticas de privacidade de uso de dados dos empregados e terceiros e (ii) elaborar termos de autorização de envio de dados a terceiros para finalidade específica. Também elaborar um Código de Ética e Conduta para gerenciar dados dos candidatos

---

[47] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista, Teoria e Prática, 2 Edição, 2021, p. 726.
[48] https://revista.trt10.jus.br/index.php/revista10/article/view/419/347

às vagas da empresa e dos Contratos de empregados ativos (Delimitar claramente os papéis que cada parte exercerá no tratamento dos dados pessoais, o que impacta diretamente na definição de suas responsabilidades, de acordo com a lei).

Os fundamentos e princípios da LGPD devem ser norteadores para a criação de políticas e procedimentos internos, de modo que os seus titulares (empregados, prestadores de serviços e até mesmo clientes) possam ter livre acesso, transparência e qualidade de dados.[49] Cumpre destacar que um dos fundamentos da LGPD é a autodeterminação informativa, que segundo Ana Maria Neves Paiva Navarro:

> Pode-se falar, dessa forma no direito à autodeterminação informativa como um direito oponível em face do Estado, para a preservação de ações lesivas, por parte deste (direito de defesa), coo também para exigir ações positivas. Com efeito, "los derechos a atos estatales e creación de normas", consoante a Robert Alexy"[50]

Dessa forma, o ponto chave deste fundamento é garantir ao titular acesso aos dados e o direito de ter controle sobre eles. Uma boa prática que a empresa pode estabelecer a fim de garantir e zelar pela efetividade deste fundamento é implementar mecanismo para que eventuais dados sempre estejam disponíveis para serem corrigidos, quando necessário.

ROXO (p. 312-313) exemplifica a implementação de medidas de segurança a partir da fiscalização da comunicação feito por meio telemáticos, tais como: e-mails, mensagens no Teams e no WhatsApp, entre outros. Neste particular, nas palavras de Tatiana Bhering Roxo, há uma colisão de direitos fundamentais: dignidade da pessoa humana/intimidade e privacidade versus exercício do poder empregatício, que está fundamentado no direito de propriedade, da livre-iniciativa e na assunção dos negócios e riscos do empreendimento pelo empregador.[51] Contudo,

---

[49] ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados. (2020, p. 310)

[50] O direito fundamental à autodeterminação informativa; Link: http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c

[51] ROXO, Tatiana Bhering. Serradas Bom de Souza. O poder de controle empresarial: suas potencialidade e limitações na ordem jurídica: o caso das correspondências eletrônicas. São Paulo. 2013

desde que avisada de forma clara, é possível a sua implementação em uma Política de Privacidade e Proteção dos Dados, uma vez que visa a preservação da segurança.

Outro exemplo a respeito da implementação da LGPD, são os procedimentos preliminares a um potencial contrato [52] durante o ciclo do emprego (fase pré/pós contratual). Isso porque, a empresa deverá ter mecanismos que legitimam o acesso as informações daquele candidato. Dessa forma, deve-se zelar que as informações disponibilizadas sejam tão somente essenciais e necessárias para a função e, com isso, deve-se também evitar formulação de informações consideradas sensíveis, tais como (i) gênero; (ii) estado civil; (iii) existência de filhos/ (iv) pretensão de matrimônio; (v) religião; (vi) doenças prévias; (vii) patrimônio genético; (viii) antecedentes criminais e (ix) investigação de vida financeira. Por sua vez, durante o período contratual há diversos mecanismos que deverão ser adotados, conforme mencionados acima, porém, especificamente sobre informações do empregado, a empresa deve ter atenção em relação a dados tratados sobre jornada, valor de salário, descontos, faltas e suas justificativas, doenças, acidentes, situações particulares que envolvem família e até mesmo inclusão de dependentes. [53]

Em relação a terceirizados e parceiros, também é possível a revisão de contrato para que sejam reavaliadas as regras estabelecidas em relação a transferência de dados pessoais para que conste expressamente a sua finalidade para que o controlador de dados garanta a proteção e observância ao princípio da LGPD.

Com isso, a partir de parâmetros mínimos estabelecidos pelo § 2º do artigo 50 da LGPD é possível criar diversas práticas com objetivo de mudar a cultura da Empresa e a dinâmica das relações de trabalho. E, com essas mudanças de boas práticas para governança de informações dos empregados, ambos os lados – titulares dos dados pessoais e controladores – se sentem seguros dentro da dinâmica das relações de emprego.

Isso porque, a adoção dessas práticas mitiga o risco de vazamento de dados, o que diminui a chance de eventuais fiscalizações por órgão regulador ou, então, reclamações

[52] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista, Teoria e Prática, 2 Edição, 2021, p. 742.
[53] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista, Teoria e Prática, 2 Edição, 2021, p. 743.

trabalhistas. Por sua vez, a governança de dados dos empregados não os deixa em uma situação de vulnerabilidade, considerando os princípios da transparência e segurança.

O inciso II, do artigo 50 prevê, ainda, que há possibilidade de as empresas serem requeridas a demonstrarem 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.[54] Sendo o mesmo caso do artigo 38 da referida Lei de que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial[55]. O parágrafo único do artigo, ainda estabelece as diretrizes mínimas sobre o relatório com as medidas adotada de que a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.[56]

O que se verifica deste inciso, nada mais é do que a aplicação dos princípios da responsabilização e da prestação de contas traduzidos pela demonstração de medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados dos empregos. Em outras palavras, não basta empresas criarem boas práticas para mitigar os riscos de exposição dos seus empregados, é necessário demonstrar, quando solicitado, perante autoridade nacional a devida prestação de contas, comprovando que as práticas estabelecidas são efetivas para diminuir o vazamento de dados dos seus empregados e clientes.

---

[54] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

[55] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

[56] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

No mais, ainda sobre a criação de boas práticas, o § 3º do referido artigo dispõe que as regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional[57], sendo possível perceber os princípios da finalidade e adequação, norteadores da Lei de Proteção de Dados, uma vez que o tratamento e armazenamento de dados (i) deve ser realizado para propósitos legítimos e explícitos, bem como (ii) compatível com as finalidades informadas ao titular dos dados pessoais.

Dessa forma, é imprescindível que os empregados saibam, de forma clara, qual é o objetivo em ter os seus dados pessoais e ter a segurança de que serão avisados, caso a finalidade do armazenamento daquelas informações mudem o seu propósito. Importante destacar, ainda, que dentro da Seção II da Lei 13.709/2018, o artigo 51 determina que a autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

Tendo em vista os dispositivos legais acima destrinchados sobre a implementação de boas práticas e governanças por parte das empresas sob a ótica nas relações de emprego, é certo que por se tratar de legislação recente, a adoção de tais medidas é um projeto, ou seja, está sujeito a pontos de desenvolvimentos a longo prazo e aperfeiçoamentos a partir das implementações dos mecanismos pelas empresas. Afinal, a própria legislação também é suscetível de alterações a partir da sua aplicabilidade pelas empresas e entendimento jurisprudencial.

4.2. Responsabilidade civil em caso de vazamento de dados pessoais

A partir da LGPD e a criação de órgão administrativo fiscalizador, a ANDP, em caso de inadimplemento as obrigações legais previstas no marco regulatório de proteção de dados há previsão no artigo 42 da Lei 13.709/2018 a respeito da responsabilidade civil patrimonial e extrapatrimonial dos agentes de tratamento de dados, sejam eles controlares ou operadores.

---

[57] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a reparálo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso (BRASIL, 2018).

Conforme se depreende da redação do artigo, nota-se a importância do papel do controlador, enquanto figura que decide a forma que se dará o tratamento de dados. Tanto é que há previsão para que responda por eventuais danos. Entretanto, a figura do operador também

Sob este aspecto, o artigo 55-j da Lei 13.709/2018 elenca rol com as diversas competências da ANDP, dentre elas, (i) zelar pela proteção dos dados pessoais; (ii) zelar pela observância dos segredos comercial e industrial; (iii) elaborar diretrizes para a Política do órgão fiscalizador; (iv) fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento a Lei; (v) apreciar petições de titular contra controlador, passado o prazo estipulado em regulamentação e não solucionada, quando da apresentação de reclamação ao controlador; (vi) incentivar o conhecimento das normas e políticas públicas sobre a LGPD e medidas de segurança; (vii) incentivar estudos sobre práticas nacionais e internacionais; (viii) elaborar relatórios anuais; (ix) editar regulamentos e procedimentos, dentre outras.

Enquanto no seu papel fiscalizador, a ANDP possui competência para aplicar sanções administrativas aos agentes de tratamento de dados em caso de violações, consubstanciado pelo inciso iv, do artigo 55-J. Dessa forma, empresas que lidam com alto fluxo de dados, principalmente de seus empregados e clientes, podem vir a ser imputadas por eventuais descumprimentos à Lei de Proteção de Dados.

Nos termos do artigo 52 da LGPD há diversas sanções por descumprimento, a título de exemplo:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
> 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;

Dessa forma, diante do poder fiscalizador atribuído a ANDP, verifica-se que o eventual descumprimento dos dispositivos da LGPD pode gerar sanções disciplinares, sejam elas apenas advertências ou até mesmo a imposição de sanções de natureza pecuniária que podem variar de valor a depender da receita da pessoa jurídica, uma vez que o cálculo da multa é de 2% em relação ao faturamento da empregadora sendo limitado ao valor de R$ 50 milhões por infração. Ademais, o dispositivo também prevê a possibilidade de concomitância e multa diária, sempre levando em consideração a gravidade e extensão da violação, conforme alterações trazidas pela Lei de nº 14.010, de 10 de junho de 2020 em relação aos artigos 52, 53 e 54 da LGPD. [58]

[58] BRASIL. Lei nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidente da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019- 2022/2020/lei/L14010.htm#view

E não é só. As disposições no referido artigo não substituem a aplicação de sanções administrativas, civis ou penais definidas em legislação específica. [59] Tanto é assim que as violações podem vir a ser objeto em reclamações trabalhistas, denúncias ao Ministério Público do Trabalho, além das fiscalizações pela ANDP.

Enquanto na figura do controlador de dados, a LGPD prevê diversas obrigações em que os titulares dos dados podem exigir, uma vez que aquele toma as decisões acerca do tratamento de dados pessoas, cabendo a ele zelar pela conservação e atender as diretrizes e exigências da Lei, pena de aplicação de sanções. Com isso, (i) provar o consentimento foi obtido nos termos da Lei; (ii) confirmar a existência ou providências o acesso a dados pessoais a partir da requisição do titular, levando em consideração os princípios do artigo 6º que preveem a facilidade e simplicidade ao acesso; (iii) informar ao titular caso haja qualquer tipo de alteração na finalidade da coleta de dados; (iv) mediante solicitação da ANPD, elaborar relatório de impacto à proteção de dados.

No campo da responsabilidade civil, a Lei de Proteção de Dados não indica expressamente o tipo de natureza jurídica sobre a responsabilidade quais sejam, objetiva ou subjetiva. Inclusive, trata-se de discussão relevante, pois, não há entendimento pacificado a respeito. TEPEDINO[60] traz a reflexão de que, apesar das semelhanças entre a LGPD e o Código de Defesa do Consumidor, neste há pelo menos dois artigos que expressamente indicam a natureza, sendo objetiva. Por outro lado, não há qualquer norma análoga na LGPD, pois não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva.[61]

Muito embora seja omissa em relação a natureza jurídica da responsabilidade civil, conforme a reflexão de Caio Mário da Silva Pereira:

---

[59] BRASIL, Lei 13.079/2018, de 14 de agosto de 2018, artigo 52, § 2º; Acesso: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[60] Tepedino, Gustavo, et al. *Fundamentos do Direito Civil: Responsabilidade Civil. v.4*. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022

[61] BRASIL, Lei 13.079/2018, de 14 de agosto de 2018, artigo 52, § 2º; Acesso: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[61] Tepedino, Gustavo, et al. *Fundamentos do Direito Civil: Responsabilidade Civil. v.4*. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022

> "A multiplicação das oportunidades e das causas de danos evidenciaram que a responsabilidade subjetiva mostrou-se inadequada para cobrir todos os casos de reparação. Esta, com efeito, dentro na doutrina da culpa, resulta da vulneração de norma preexistente, e comprovação de nexo causal entre o dano e a antijuridicidade da conduta do agente. Verificou-se, como já ficou esclarecido, que nem sempre o lesado consegue provar estes elementos. Especialmente a desigualdade econômica, a capacidade organizacional da empresa, as cautelas do juiz na aferição dos meios de prova trazidos ao processo nem sempre logram convencer da existência da culpa, e em consequência a vítima remanesce não indenizada, posto se admita que foi efetivamente lesada." (2018, p. 319)

Nesse contexto, a partir do entendimento de Caio Mário, entende-se que a natureza jurídica da responsabilidade civil seria objetiva, na medida em que o nível de complexidade envolve a Lei de Proteção de Dados, dinâmica das relações de emprego e a sua dificuldade de comprovação, não parece razoável entender pelo elemento da culpa.

Isso porque, quando se tem o elemento culpa, cabe, ainda, à vítima, provar o vínculo de causalidade entre a atividade do agente e o dano causado (MARIO, Caio; 2018, p. 342) e dinâmica envolvendo o tratamento de dados. Sendo que dentro do âmbito da LGPD, sua dinâmica e especificidades sobre o tratamento de dados, não parece razoável impor a vítima, ou seja, os empregados ou até mesmos clientes, comprovarem a responsabilidade civil e dano causado. Na realidade, causa até particular estranheza, eis que o advento da legislação veio para proteção de pessoas naturais, não sem aplicável os seus dispositivos a pessoa jurídicas.

Por outro lado, VOILA (2021, p. 256) destaca que há forte tendência doutrinária em se adotar apenas a responsabilidade subjetiva, com culpa presumida e, via de consequência, em afastar o entendimento de responsabilidade objetiva do empregador, por aplicação do artigo 42 e incisos II e II do artigo 43 da LGPD, que expressamente isenta de responsabilidade aquele não violou a lei. Até porque, não é toda a exposição de dados que implica em situações vexatórias ou abalo à saúde psíquica do titular. Neste particular, destaca-se que durante o trâmite legislativo, o único

dispositivo da LGPD que mencionava a responsabilidade objetiva foi retirado da redação da lei[62]. Ou seja, há forte indicativo sobre o que os legisladores pretendem da interpretação da LGPD.

Também se verifica forte indício de preferência pela interpretação de responsabilidade civil subjetivo, uma vez que: a versão inicial do Projeto de Lei n.º 5276 trazia, no Capítulo sobre "Transferências internacionais de dados", uma regra geral expressa de responsabilidade solidária e objetiva desses agentes pelos danos causados em virtude do tratamento de dados (art. 35). Além disso, na Seção sobre "Responsabilidade e Ressarcimento de danos", havia uma abordagem ampla sobre os sujeitos obrigados a reparar o dano ("todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais causar a outrem dano") (art. 42), e outra regra igualmente ampla prevendo a solidariedade entre todos os agentes da cadeia de tratamento, sem qualquer distinção entre controlador e operador ("[n]os casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesma obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos causados")[63].

Não obstante, a reparação de dano decorrente de responsabilidade objetiva estar regulada de forma genérica pelo Código Civil, a qual detém mesma hierarquia que a Lei de Proteção de Dados. Considerando que lei posterior pode revogar anterior desde que de mesma hierarquia ou a especial revogar a geral, o que se verifica no caso em tela. Nas palavras de Vóila Bonfim (2021, p. 757):

> "Entretanto, mesmo antes do Código Civil (parágrafo único do art. 927) a jurisprudência já vinha alargando o conceito de "culpa", cujo requisito é necessário para o dever de indenizar. A culpa presumida nasce de premissa do dever de que todos temos de não prejudicar ninguém e praticar atos com segurança. Ainda que não se confunda com a culpa presumida, a atividade de risco é mero desdobramento dessa tese, pois a pessoa que explora economicamente a atividade de risco é mero desdobramento dessa tese, pois a pessoa que explora economicamente a atividade de risco deve ser responsabilizada pelos prejuízos materiais e morais daí decorrentes"

---

[62] Tepedino, Gustavo, et al. Fundamentos do Direito Civil: Responsabilidade Civil. v.4. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022.
[63] Tepedino, Gustavo, et al. Fundamentos do Direito Civil: Responsabilidade Civil. v.4. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022.

Com isso, há, em tese, a possibilidade de aplicação da responsabilidade objetiva, uma vez que a lei especial, LGPD, não trouxe a culpa como elemento necessário para configuração de responsabilidade civil. Nos Tribunais, os dois posicionamentos, de um lado, a necessidade de comprovação da prática de ato ilícito para demonstrar o dano causa e, por outro lado, a mera demonstração de violação a legislação de proteção de dados, tem sido bastante debatida. [64]

A reparação do dano moral adquire na LGPD contornos específicos, que corroboram a crítica à utilização da técnica *in re ipsa*. Isso porque, segundo TEPEDINO, afirma-se, com frequência, que o dano moral não precisa ser provado, sendo antes *in re ipsa*. Por isso, em numerosas hipóteses, a prova do dano moral tem cedido lugar à sua presunção, notadamente quando se trata de reparar danos à imagem.

De acordo com TEPEDINO (2022), utilizar-se da presunção do dano moral, ao argumento de que se trata *in re ipsa*, parte do conceito subjetivo de dano moral. Neste particular, a prova sobre a indenização por dano moral não é necessária, uma vez que não seria razoável exigir em juízo a prova da repercussão sentimental do evento danoso sobre a vítima, não só porque a dor e o sofrimento são fatos inteiramente subjetivos[65]. E, diante a sua subjetividade, comprová-los é difícil, pois não há formas de demostra ou mensurar o sofrimento alheio. Defendendo, portanto, a concepção objetiva, sob sua ótica, deve exigir-se não a prova da dor ou do sofrimento da vítima, mas, antes, a prova da lesão sofrida, como se exige a prova da lesão ao patrimônio no caso do dano patrimonial. É evidente que, em se tratando de dano moral, nem sempre a lesão deixará traços materiais, mas essa mesma dificuldade ocorre no campo patrimonial, quando a faceta do dano patrimonial que se quer reparar é a dos lucros cessantes (e nem por isso o lesado está liberado de fazer a prova do dano – ainda que não se exija "certeza absoluta", ao menos o lesado deve demonstrar a "probabilidade objetiva" que tinha de auferir o lucro frustrado).[66]

---

[64] https://www.conjur.com.br/2021-set-16/marcelo-carvalho-lgpd-dano-moral-presumido
[65] Tepedino, Gustavo, et al. Fundamentos do Direito Civil: Responsabilidade Civil. v.4. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022.
[66] Tepedino, Gustavo, et al. Fundamentos do Direito Civil: Responsabilidade Civil. v.4. Disponível em: Minha Biblioteca, (3rd edição). Grupo GEN, 2022.

MEIRELIS (2021, p. 272), por outro lado, traz a seguinte reflexão a respeito da natureza jurídica da responsabilidade civil, considerando que há previsão expressa na LGPD de que a violação do direito do titular no âmbito das relações de consumo será tratada de acordo com a legislação pertinente (artigo 45), ou seja, a responsabilidade do controlador e do operador dentro do contexto da relação de consumo se sujeitariam a regramento próprio, sendo o Código do Direito do Consumidor

Por amostragem, no Tribunal de Justiça de São Paulo, em consonância com a exposição de Vóila Bonfim, há julgados no sentido de que é necessária a comprovação do dano para se ter a reparação extrapatrimonial.

> Apelação. Responsabilidade civil. Prestação de serviços. Energia elétrica. Vazamento de dados do sistema da prestadora do serviço. Ação de reparação por danos morais. Sentença de improcedência. Invasão de sistema da concessionária**. Responsabilidade objetiva da empresa no tratamento de dados (art. 42 da LGPD**). Falha na prestação de serviços (art. 14 do CDC). Dados que não se relacionam à intimidade e não envolve dado pessoal sensível (art. 5º, II, da LGPD). **Dados básicos informados com frequência em diversas situações, muitos constantes em simples folha de cheque. Ausente utilização dos dados vazados e efetivo dano. Impossibilidade de indenizar expectativa de dano.** Sentença mantida. Honorários majorados. RECURSO DESPROVIDO.(TJ-SP - AC: 10244816120208260405 SP 1024481-61.2020.8.26.0405, Relator: L. G. Costa Wagner, Data de Julgamento: 23/08/2021, 34ª Câmara de Direito Privado, Data de Publicação: 29/08/2021)

> APELAÇÃO CÍVEL – Interposição contra sentença que julgou improcedentes os pedidos formulados, nos autos da ação de obrigação de fazer c.c. danos morais. **Vazamento de informações pessoais dos consumidores**, no caso, do consumidor autor do banco de dados da empresa ré**. Falha configurada, todavia, que no caso, não caracterizadora de danos morais.** Ausência de demonstração robusta e convincente, no caso, de que os dados do consumidor tenham sido indevidamente utilizados ou causado algum dano. Honorários advocatícios majorados em grau recursal, nos termos do artigo 85, § 11, do Código de Processo Civil/2015. Sentença mantida. (TJ-SP - AC: 10045763620218260405 SP 1004576-36.2021.8.26.0405, Relator: Mario A. Silveira, Data de Julgamento: 23/08/2021, 33ª Câmara de Direito Privado, Data de Publicação: 24/08/2021)

> Ação de obrigação de fazer c.c. indenizatória moral. Fornecimento de energia elétrica. **Vazamento de dados pessoais. Incidência do CDC, nos termos do artigo 43 da LGPD. Excludente de responsabilidade.** Culpa exclusiva de terceiro (hacker). Inteligência do artigo 14, § 3º, CDC. Inúmeras ligações, propagandas via e-mail, mensagens indesejadas**. Mero aborrecimento. Fato corriqueiro. Dano moral inexistente. Sentença de improcedência. Apelo improvido.** (TJ-SP - AC: 10004070620218260405 SP 1000407-06.2021.8.26.0405, Relator: Soares Levada, Data de Julgamento: 16/08/2021, 34ª Câmara de Direito Privado, Data de Publicação: 19/08/2021)

> APELAÇÃO – Ação de obrigação de fazer c.c. indenização por danos morais – Contrato de prestação de serviços – Energia elétrica - Pretensão fundada em ocorrência de vazamento de dados pessoais da autora – Fato admitido em defesa apresentada – Falha de segurança – Responsabilidade Objetiva configurada - Situação retratada nos autos que, contudo, não basta para configurar dano de natureza imaterial – **Pretensão indenizatória calcada em presunção/expectativa de danos - Ausência de comprovação de efetiva ocorrência de prejuízos - Indenização indevida – Sentença de improcedência mantida** - Recurso desprovido. (TJ-SP - AC: 10003975920218260405 SP 1000397-59.2021.8.26.0405, Relator: Irineu Fava, Data de Julgamento: 28/07/2021, 17ª Câmara de Direito Privado, Data de Publicação: 02/08/2021)

Por outro lado, o entendimento não é pacífico, uma vez que também há julgados que entenderam pela responsabilidade objetiva e, por consequência, restou configurado o dano moral:

> COMPRA E VENDA DE BEM MÓVEL - AÇÃO DE INDENIZAÇÃO - VAZAMENTO DE DADOS DO CONSUMIDOR NO WEBSITE DA RÉ - VULNERABILIDADE DO SISTEMA - **RESPONSABILIDADE OBJETIVA** DA FORNECEDORA - DANOS MORAIS CONFIGURADOS - RECURSO PROVIDO PARA JULGAR A AÇÃO PARCIALMENTE PROCEDENTE. **A Lei Geral de Proteção de Dados dispõe que o operador de dados pessoais deve responder por eventual dano decorrente de falha de segurança, sem prejuízo da aplicabilidade das disposições consumeristas**".(TJ-SP - AC: 10031222320208260157 SP 1003122-23.2020.8.26.0157, Relator: Renato Sartorelli, Data de Julgamento: 22/06/2021, 26ª Câmara de Direito Privado, Data de Publicação: 22/06/2021)

Sobre este caso em particular, o relator partiu da premissa que "*a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) dispõe que o operador de dados pessoais deve responder*

por eventual dano decorrente de falha de segurança, sem prejuízo da aplicabilidade das disposições consumeristas, verbis :"Art. 44. O tratamento de dados pessoais será irregular".

> APELAÇÃO CÍVEL. AÇÃO CIVIL PÚBLICA. DISPONIBILIZAÇÃO INDEVIDA DE BANCO DE DADOS DE CONSUMIDORES NA REDE MUNDIAL DE COMPUTADORES. SENTENÇA DE PROCEDÊNCIA. LEGITIMIDADE ATIVA DO MINISTÉRIO PÚBLICO PARA DEFESA DOS DIREITOS DIFUSOS E INDIVIDUAIS HOMOGÊNIOS. APLICABILIDADE DO CÓDIGO DE DEFESA DO CONSUMIDOR. LEGITIMIDADE PASSIVA DE TODOS OS FORNECEDORES DE SERVIÇOS E PRODUTOS QUE INTEGRAM A CADEIA DE CONSUMO PARA RESPONDER PELOS DANOS CAUSADOS PELA FALHA NA PRESTAÇÃO DOS SERVIÇOS. RESPONSABILIDADE OBJETIVA. TEORIA DO RISCO DO EMPREENDIMENTO. INEXISTÊNCIA DE CERCEAMENTO DE DEFESA. AS RECORRENTES SEQUER ESPECIFICARAM QUAIS AS PROVAS CUJA PRODUÇÃO TERIA SIDO INDEVIDAMENTE TOLHIDA PELO MAGISTRADO OU EXPUSERAM QUAIS FATOS PODERIAM SER PROVADOS ATRAVÉS DELAS, NÃO PODENDO ASSIM SER PRESUMIDO O ALEGADO PREJUÍZO. SENTENÇA QUE NÃO APRESENTA QUALQUER VÍCIO, AO CONTRÁRIO, O JULGADOR EXPÔS CLARAMENTE AS RAZÕES DO SEU CONVENCIMENTO, REFUTANDO OS ARGUMENTOS DAS APELANTES, RAZÃO PELA QUAL INEXISTE QUALQUER VÍCIO DE FUNDAMENTAÇÃO. LITISCONSÓRICO PASSIVO NECESSÁRIO, TAL HIPÓTESE SOMENTE OCORRERIA SE A PRESENÇA DE TODOS OS LITISCONSORTES FOSSE IMPRESCINDÍVEL PARA O EXAME DO MÉRITO DA CAUSA, O QUE NÃO É O CASO. DIVULGAÇÃO INDEVIDA DE DADOS. **OFENSA A DIREITOS PERSONALÍSSIMOS DOS CONSUMIDORES E EM ESPECIAL DAQUELES INTEGRANTES DO BANCO DE DADOS MANTIDO OU UTILIZADO PELAS RÉS. DIREITO À INTIMIDADE E AO SIGILO DE DADOS VIOLADO. DANO MORAL COLETIVO. DANO MORAL IN RE IPSA. DESNECESSIDADE DA DEMONSTRAÇÃO DE PREJUÍZOS CONCRETOS OU DE EFETIVO ABALO MORAL. PRECEDENTES DA CORTE SUPERIOR. VALOR INDENIZATÓRIO QUE SE MOSTRA RAZOÁVEL E CONDIZENTE COM A RELEVÂNCIA DO TEMA E COM O CARÁTER REPRESSOR DA INDENIZAÇÃO. EVENTUAL COMPROVAÇÃO DO PREJUÍZO INDIVIDUAL QUE DEVE SE REALIZAR EM FASE DE LIQUIDAÇÃO DE SENTENÇA, CONFORME PREVISTO NO ARTIGO 97 DO CÓDIGO DE DEFESA DO CONSUMIDOR. COISA JULGADA IN UTILIBUS. RECURSO DESPROVIDO**. (TJ-RJ - APL: 04184567120138190001, Relator: Des(a). FABIO DUTRA, Data de Julgamento: 23/02/2021, PRIMEIRA CÂMARA CÍVEL, Data de Publicação: 10/03/2021)

De acordo com os julgadores, a empresa foi negligente com a forma de tratamento e armazenamento de dados "*diante da dimensão dos danos acarretados, a indenização estabelecida em R$500.000,00 (quinhentos mil reais), pelo dano moral coletivo e R$1.000.00 (mil reais) por danos materiais e morais causados aos consumidores, individualmente considerados, observa a capacidade econômica das sociedades empresariais envolvidas e a gravidade da conduta ilícita praticada. Ressalte-se que a indenização tem de possuir capacidade de, efetivamente, desestimular a repetição de casos semelhantes e de compelir os fornecedores a investirem na prevenção dos danos, por meio de tecnologia e sistemas preventivos que assegurem os direitos dos consumidores".*

Sob o aspecto da LGPD, a decisão destacou, ainda*, "Acresça-se que a necessidade de serem criadas salvaguardas para a divulgação de dados pessoais, não passou despercebida pela sociedade e pelos legisladores, tendo a Lei nº 13.709/18, conhecida como Lei Geral de Proteçâo de Dados Pessoais (LGPD), sancionada em agosto de 2018, com a redação dada pela Lei 13.853/19, tem como objetivo justamente regulamentar o tratamento de dados pessoais de clientes e usuários por parte de empresas públicas e privadas. Apenas à guisa de informação a referida legislação, ao tratar das sanções administrativas, prevê a possibilidade de multa de até R$50.000.000,00 (cinquenta milhões de reais) por infração cometida".*

No âmbito da Justiça do Trabalho e das relações de emprego, a título de exemplo sobre o reconhecimento da indenização por dano moral exposição de dados pessoais sensível de empregos, tem-se que já foi reconhecida a responsabilidade de uma Empresa em relação ao vazamento de dados sensíveis ligados à saúde de um ex-empregado, violando a sua intimidade e privacidade, por meio do julgado de nº 0010398-61.2019.5.03.002467:

> "**DANOS MORAIS**
>
> O juízo de origem condenou a reclamada ao pagamento de indenização por danos morais, nos seguintes termos:

---

[67] Tribunal Regional do Trabalho da 3ª Região Acesso: https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/nj-copasa-devera-indenizar-trabalhador-por-exposicao-de-dados-pessoais-na-rede-interna-de-informacao-da-empresa

*Do **dano moral***

Pleiteia o reclamante indenização por danos morais sob o argumento de que foi vítima de constrangimentos e humilhações na empresa. Relata que em 2015 passou por problemas pessoais os quais ocasionaram o quadro de depressão, além de acidentes ocorridos fora do local de trabalho, resultando em afastamento do trabalho, sem que recebesse qualquer suporte por parte da empresa. Aduz que após o retorno ao trabalho, a empresa (sic) foi compelido a conduzir veículo da empresa, não obstante restrição médica neste sentido. Após os fatos narrados alega que há no sistema empresa (sic) o relatório de todos os relatórios e exames médicos atinentes ao autor, sendo que tais informações, privadas do autor, encontravam-se em livre acesso a qualquer empregado. Aduz que ocorreu invasão da privacidade em decorrência de publicidade de dados sigilosos do autor.

A prova oral favorece o autor.

A reclamada em depoimento pessoal confessou a fragilidade do sistema, fl. 516: "*...que qualquer um pegar no sistema as informações sobre atestados e laudos médicos, desde que tenha acesso ao sistema através de senha individual; que todos os empregados possuem tal acesso*.".

A par disso, a testemunha ouvida declarou, fl. 516: "*...que os atestados médicos ficam em pastas de acesso público; que procurando sua própria pasta acabou se deparando com o relatório médico, onde constaria que o reclamante tinha pensamentos suicidas e era usuário de cocaína; que o depoente comunicou ao reclamante da existência do documento no sistema; que o reclamante mandou um e-mail questionando a exposição do documento, que posteriormente veio a ser retirado do sistema...*".

A indenização por danos morais pressupõe inequívoca comprovação de lesão à imagem, honra, intimidade ou vida privada do empregado (artigo 5º, X, da Constituição Federal).

A conduta da ré, por si só já revela o **dano** sofrido pelo autor, de vez que **dados sigilosos, de cunho pessoal, estiveram expostos, ainda que por um período (já que conforme alegado pela testemunha ouvida a reclamada após a verificação do ocorrido corrigiu o equívoco), certamente causou dano moral ao autor, mormente porquanto qualquer empregado da ré poderia ter ciência dos problemas de saúde e demais fatos ocorridos com autor durante o contrato de trabalho.**

Assim, tenho configurado o **dano** sofrido pelo autor, como ofensa de natureza leve para efeitos do §1º do art. 223-G da CLT, e condeno a reclamada ao pagamento de indenização no valor de três salários do autor.

Contra tal decisão ambas as partes se insurgem.

(...)

Inicialmente, deve ser ressaltado que **a previsão contida no inciso X do artigo 5º da Constituição da República de proteção à intimidade, vida privada, honra e imagem das pessoas, volta-se à efetivação de um dos direitos fundamentais de maior relevância inscrito nesse mesmo texto normativo, que é o da dignidade da pessoa humana.**

No Direito Positivo Brasileiro, o **dano** decorre de um ato ilícito que provoca, contra quem o praticou, a obrigação de repará-lo, estando a obrigação de reparar o **dano moral** prevista no citado artigo 5º, X, da CR. O princípio geral da responsabilidade civil está fundado no artigo 186 do Código Civil, que prescreve que aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito, ou causar prejuízo a outrem, fica obrigado a reparar o **dano**.

Assim, a obrigação de indenizar encontra-se condicionada à comprovação do **dano** sofrido, do dolo ou culpa do empregador e do nexo causal entre eles, sendo esses requisitos essenciais para se atribuir a responsabilidade civil.

Saliento, ainda, que o **dano moral** se caracteriza pela lesão sofrida por pessoa, física ou jurídica, em certos aspectos da sua personalidade, em razão de investidas injustas de outrem, atingindo-a na esfera íntima da moralidade, da honra, do afeto, da psique, da liberdade entre outros, causando-lhe constrangimentos.

A testemunha obreira, sr. Carlos Alexandre Falcão, afirmou:

"**que procurando sua própria pasta acabou se deparando com o relatório médico, onde constaria que o reclamante tinha pensamentos suicidas e era usuário de cocaína; que o depoente comunicou ao reclamante da existência do documento no sistema; que o reclamante mandou um e-mail questionando a exposição do documento, que posteriormente veio a ser retirado do sistema**."

Na espécie, **na esteira do entendimento adotado pelo MM. Juízo de origem, restaram suficientemente demonstrados os danos morais em virtude da exposição indevida da intimidade do obreiro.**

O acervo probatório dos autos informa que **dados sigilosos, de cunho pessoal, estiveram expostos a qualquer empregado da reclamada, permitindo que terceiros tivesse conhecimento do histórico médico, dos problemas de saúde, além de outros dados atinentes à esfera privada do reclamante.**

Ante todo o exposto, não vislumbro elementos capazes de afastar o direito do reclamante à indenização por **dano moral**(art. 186 e 927 do Código Civil). O valor fixado para a indenização, no importe de 3 salários do autor, atende à finalidade de atenuar as consequências da lesão jurídica e reveste-se de razoabilidade, ficando mantido."

(TRT da 3.ª Região; PJe: 0010398-61.2019.5.03.0024 (ROT); Disponibilização: 13/02/2020; Órgão Julgador: Segunda Turma; Redator: Convocada Maria Cristina Diniz Caixeta)

Veja-se que devido ao descuido e ausência do correto armazenamento de dados, o ex-empregado foi exposto para outro empregado, tendo dados sensíveis a sua saúde vazados dentro da sede da sua ex-empregadora, em razão de sistema interno fragilizado. Com isso, a Justiça do Trabalho manteve a decisão do juízo de primeira instância condenando a empresa ao pagamento de indenização por danos morais, eis que cabia a ela, como operadora e controladora de dados, zelar pela proteção dos dados do ex-empregado.

Da aplicabilidade da LGPD no caso concreto, constata-se que a empresa violou o artigo 5º, inciso II da Lei 13.709/2018, a qual dispõe que considera dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural[68]. Assim como o artigo 7, § 4º da referida Lei que destacada que é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir69.

É preciso, portanto, entender como é fundamental um projeto para implementação das diretrizes da LGPD a fim de possibilitar a real aplicação dos direitos previstos na referida Lei, de modo que os titulares se sintam seguros de compartilhá-los. O nível de exposição apresentado na decisão acima prejudica que pode vir a sofrer discriminação por. Neste aspecto Caitlin Mulholland 70(2018, p. 164) traz a seguinte correlação entre a discriminação e a utilização de dados pessoais:

> "Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de

[68] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm
[69] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm
[70] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, set./dez. 2018. p. 164

> ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas. Ou seja, há a possibilidade de tratamentos discriminatórios de dados, desde que não se caracterizem pela ilicitude ou abusividade, o que será determinado segundo critérios definidos tanto pelas regras expressas de direito civil e penal, quanto por princípios como o da boa-fé objetiva."

Com efeito, o artigo 50 da Lei 13.709/2018 é importante para que empresas controladoras e operadoras de dados, dentro de suas competências, formulem regras de boas práticas e de governança para mitigar os riscos de vazamento de dados e outros aspectos relacionados ao tratamento de dados pessoais.

Há que se destacar, ainda, que não é apenas o controlador que detém a responsabilidade civil sobre eventuais vazamentos de dados, mas também aqueles que operam com os dados. Em outras palavras, o operador também responde solidariamente pelos danos causados quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido instruções lícitas do controlador, hipótese em que o operador equipara-se a controlador, a teor do art. 42, § 1º, I, a LGPD.[71]

O Tribunal Regional do Trabalho de São Paulo[72] também já decidiu por manter a justa causa de um empregado que transferiu uma planilha contendo dados pessoais de outros empregados e clientes para e-mail pessoal configurou uma forma de vazamento de dados, o que foi considerada como falta grave, passível de aplicação do artigo 482, da CLT[73].

> "Assim, verifica-se que o reclamante, conscientemente, contrariou norma interna da empresa ao enviar os dados sigilosos ao seu e-mail pessoal, não se sustentando a genérica alegação de desconhecimento

---

[71] CASSAR, VIOLA BONFIM – Manual de Compliance Trabalhista , Teoria e Prática, 2 Edição, 2021, p. 736.

[72] https://ww2.trt2.jus.br/noticias/noticias/noticia/mantida-justa-causa-de-trabalhador-que-repassou-dados-sigilosos-da-empresa-para-seu-e-mail-pessoal

[73] http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

quanto ao Código de Ética da empresa. Sobre a alegação de que não há comprovação de repasse das informações a terceiros e sobre eventual vistoria do computador utilizado pelo obreiro, por relevantes, destaco os seguintes fundamentos da r. decisão de origem:

> *"Embora o reclamante tenha afirmado que ofertou seu equipamento para a reclamada vistoriar e, assim, verificar que não houve transmissão dos dados a terceiros (o que é provado por sua carta escrita de próprio punho juntada aos autos), a dispensa por justa causa não se deu em razão de envio de dados a terceiros, e sim a própria transmissão para si de tais dados. Não há qualquer prova de dolo por parte do trabalhador ou de que havia intenção de transmitir tais dados a terceiros.* ***Todavia, entendo que o próprio extravio dos dados para si mesmo já é suficiente para a implementação da dispensa por justa causa****. **Conforme confirmado em audiência, em tais tabelas havia números de CNPJ, de CPF, números de cartões da segunda reclamada, valores que foram carregados no cartão e, além disso, locais da lotação de empregados da reclamada.***
>
> ***Logo, trata-se de dados pessoais de pessoas naturais e que, de forma alguma, podem ser extraviados para meios que escapam do controle da empresa, sob pena, inclusive, de eventual responsabilização da empresa pelas pessoas físicas e jurídicas afetadas. A extração de dados tem se tornado um grande commodity da economia. Tamanha a sua importância econômica e, também, tamanha a possibilidade danosa da publicação de dados, que foi criada a Lei Geral de Proteção de Dados (Lei nº 13.709****) e disciplinada a responsabilidade civil daqueles que controlam ou operam tais dados.* ***Demonstrado em audiência que havia conhecimento de que os dados eram sigilosos, e tendo havido a transferência de tais dados para a sua conta pessoal, ainda que não haja dolo por parte do empregado ou qualquer transmissão dos dados a terceiros, entendo que se trata de falta disciplinar grave que enseja a dispensa por justa causa."*** *(sic, fl. 1063)".*

Por todo o exposto, entendo que o ato gravoso cometido pelo empregado revestiu-se de gravidade o suficiente para a rescisão imediata do contrato por justa causa de modo que, nego provimento ao recurso." (TRT da 2ª Região; PJe: 1000612-09.2020.5.02.0043 (ROT); Publicação: 22/10/2021; Órgão Julgador: Primeira Turma; Relator: Convocado Daniel de Paula Guimarães)

Neste caso em particular, o empregado havia assinado o Termo de Confidencialidade e adesão à política de segurança da informação da Empresa, não tendo seguido as instruções disponibilizadas pelo controlador (empregadora), portanto, a 1ª Turma do Tribunal Regional do Trabalho de São Paulo entendeu que, ainda que não houvesse comprovação de repasse das informações a terceiros, a transferência de dados, por si só, implica em violação aos dispositivos da LGPD, especialmente quando o empregado estava ciente sobre as diretrizes da controladora

(empresa), tendo deixado de atender a política corporativa de segurança de informação, além de cláusula de confidencialidade expressamente prevista no contrato de trabalho.

Com isso, vê-se que a responsabilidade civil de agentes controladores de dados, sejam eles controladores ou operadores, é possível nas esferas cíveis e trabalhistas, muito embora seja uma legislação recente. Por isso, são necessárias as boas práticas e a implementação de mecanismos alinhados com os dispositivos da LGPD, a fim de reduzir os riscos de punições pela ANPD e por parte do Judiciário em eventual responsabilidade civil.

5. LGPD NA JUSTIÇA DO TRABALHO

Há que se mencionar, ainda, a discussão acerca da aplicação da LGPD no âmbito da Justiça do Trabalho. Isso porque, apesar da Lei de Proteção de Dados ser aplicada em qualquer esfera ou nicho do Direito em que há necessidade de tratamento de dados, principalmente diante o alto fluxo de disponibilização de informações durante as relações de emprego, cumpre destacar que para a resolução de lides, os processos trabalhistas e investigações conduzidas pelos Tribunais Regionais do Trabalho, Procuradorias Regionais do Trabalho e demais órgãos fiscalizadores, há necessidade de disponibilização de documentos.

Com isso, de um lado, temos a legislação, cujo objetivo é observância à proteção e privacidade de dados dos empregados, prestadores de serviços ou clientes, de modo que não haja exposição sem o consentimento. Por outro, temos a Justiça do Trabalho e o Ministério Público do Trabalho e demais órgãos fiscalizadores, aos quais, em prol da resolução de reclamações trabalhistas individuais, ações civis públicas ou até investigações conduzidas, muitas vezes, requerem a exposição de diversos documentos, o que é previsto na exceção de sigilo pelos artigos 8º, § 2º, LC 75/93 [74]c/c art. 7º, II, Lei n. 13.709/2018[75].

[74] http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp75.htm

[75] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Tendo em vista que há duas normas que, se analisadas na literalidade, apontam para uma contradição. Isso porque, ao mesmo tempo que as empresas são obrigadas a atender os dispositivos da LGPD, pena de aplicação de sanções em valores - inclusive vultuosos -, também se faz necessário a cooperação durante processos trabalhistas e investigações, sendo a disponibilização desses documentos, muitas vezes, necessários para a garantia a ampla defesa e contraditório, sendo direitos constitucionais.

Dentro de uma Sociedade altamente digitalizada, os dados se tornaram um "bem de consumo", na medida em que a sua exposição, sejam de empregados, prestadores de serviços ou até mesmo de clientes, são potencialmente lucrativos, em especial dentro do mercado de trabalho, haja vista que as empresas buscam, cada vez mais, por profissionais extremamente qualificados em prol do desenvolvimento econômico. Como isso, urge sanar a dúvida: a disponibilização de dados perante a Justiça do Trabalho e eventuais investigações conduzidas pelo Ministério Público do Trabalho podem ser consideradas com uma dificuldade de efetividade da LGPD?

Nota-se, que combinar a proteção e compartilhamento de dados de os empregados no âmbito da Justiça do Trabalho e órgãos auxiliares é um desafio para as empresas, eis que estão preocupadas com o cumprimento das diretrizes da LGPD, que prezam pela proteção e privacidade de dados pessoais, pena de aplicação de sanções quando comprovado o vício de consentimento. Some-se ao fato de que, por se tratar de lei recente, gera uma insegurança a sua aplicação no âmbito corporativo, pois não há parâmetro a seguir, tampouco se tem um modelo "pronto", sendo certo que para a implementação das medidas não basta só criar mecanismos de forma tão rápida, pois se faz necessário uma mudança de mentalidade e cultura da empresa.

Lado outro, conforme pontuado pela notícia "Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados[76]", o acesso à informação também não pode ser prejudicado por conta de Lei de Proteção de Dados. Isso porque, a legislação foi criada para atender pessoas físicas, não sendo razoável a inaplicabilidade em demandas no âmbito da Justiça do

---

[76] https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/#:~:text=Autoridades%20ouvidas%20pela%20Comiss%C3%A3o%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(LGPD).

Trabalho que buscam tão somente o deslinde sobre situações decorrentes das relações de emprego e demais matérias vinculadas.

É importante destacar, ainda, que a Justiça do Trabalho não está preocupada em se utilizar da exceção prevista em Lei para adquirir informações para fins lucrativos, muito embora as informações tenham tornado um "bem de consumo", conforme mencionado acima. Tampouco, há solicitação de informações para que sejam utilizadas de forma indevida ou abusiva. Pelo contrário, o objetivo da Justiça do Trabalho é tão somente o desfecho acerca de controvérsias e, por isso, faz-se necessário a eventual disponibilização de dados na esfera judicial (reclamações trabalhistas) e extrajudicial - investigações conduzidas pelo Ministério Público do Trabalho.

Uma vez que a LGPD veio como forma de suprir uma lacuna normativa que atendesse a modernidade e refletisse os atuais fluxos das relações, a qual visa garantir a transparência na forma de tratamento de dados, não parece razoável impedir o acesso a informações por parte de agentes públicos. Afinal, está Lei busca responder à pergunta: aonde os seus dados são utilizados?

A título de exemplo, há matéria publicada no JOTA[77], em foi relatado que desde o advento da LGPD, o número de processos trabalhistas cresceu, sejam eles individuais ou coletivos. Por amostragem, sindicatos solicitam às empresas informações dos contratos dos empregados e até mesmo para verificar se as empresas estão introduzindo os dispositivos na LGPD.

Com isso, à luz dos princípios de proporcionalidade e razoabilidade, é possível conciliar a aplicação da LGPD e a disponibilização de informações perante a Justiça do Trabalho, muito embora neste momento inicial cause certo desconforto e insegurança em empresas, uma vez que se trata de legislação recente e o direito ao acesso à informação por parte de agentes públicos é um ponto pouco explorado.

---

[77] https://www.jota.info/coberturas-especiais/protecao-de-dados/a-lgpd-e-a-lai-estavam-no-mesmo-patamar-mas-a-ec-115-muda-a-divulgacao-de-dados-diz-desembargadora-13062022

6. CONCLUSÃO

No contexto de uma sociedade que é permeada por alto fluxo de dados e informações, o processamento e cuidado na forma que se tratam os dados expostos no dia a dia tornou-se uma prioridade para que as empresas, a fim de que alinhem estratégias para implementar mecanismos a fim de garantir a privacidade destes dados e informações e evitar eventuais vazamento.

Por meio do trabalho, foi explorado que a preocupação com dados é uma tendência global diante as inúmeras notícias de vazamento de informações, sendo um assunto de repercussão internacional. Especificamente no Brasil, também foi possível verificar várias notícias de dados sigilosos vazados em âmbito nacional, o que apenas corroborou para o entendimento de que era necessário um marco regulatório específico para disciplinara respeito de dados e a sua dinâmica de proteção, muito embora o ordenamento jurídico brasileiro já dispusesse de institutos legais para regulamentar e garantir a privacidade.

É de se notar que a LGPD possui um amplo escopo, sendo sua aplicabilidade em qualquer ramo do Direito desde que se tenha dados para regulamentar. Por conseguinte, dentro das relações interpessoais, especialmente de trabalho há um número inesgotável de compartilhamento de dados, o que se faz urgente a aplicação da LGPD em ambientes corporativos, a fim de zelar pelos empregados e quaisquer outros tipos de relação em que há compartilhamento de dados dentro da Sede de empresas.

Há que ressaltar, ainda, que, ao longo do trabalho foi explorado que a nova Lei requer um estudo aprofundado para sua implementação sendo que sua efetividade nos ambientes de trabalho depende de vários fatores, quais sejam a criação e revisão de políticas e contratos, mecanismos para minimizar o vazamento de dados, documentos que sejam adequados a redação desta Lei, manuais, treinamentos e, principalmente a conscientização daqueles que lidam com os dados. O que verificou é a necessidade por parte das Empresas de implementar um projeto para a sua implementação, tendo a própria LGPD deixado dispositivos com parâmetros mínimos para que empresas criem boas-práticas.

Isso porque, por se tratar de legislação recente, é certo que em um primeiro momento serão necessárias as empresas criarem mecanismos iniciais para atender a legislação, pena de cometer infração, aos quais sofrerão aperfeiçoamentos a depender de seus desdobramentos ao longo prazo. Ou seja, as empresas terão que revisitar os procedimentos.

Com o trabalho, também se constatou que foi criado um órgão fiscalizador, a ANPD, a qual detêm capacidade de sancionar organizações que se comprometeram a seguir diretrizes para o estrito cumprimento à Lei. Não obstante, as sanções estabelecidas na LGPD não excluem a possibilidade de reconhecimento da responsabilidade civil dos controladores e operadores de dados (as empresas empregadoras). Inclusive, a discussão a respeito da natureza jurídica do dano, uma vez que a LGPD é omissa a respeito da responsabilidade ser objetiva ou subjetiva. Sendo explorado, ainda, qual seria a natureza jurídica aplicável ao caso da LGPD.

Conforme se apreende da questão da responsabilidade civil, foram elaboradas tanto o estudo de jurisprudência na esfera cível como na trabalhista. Enquanto, aquele vem, em um primeiro momento, entendendo que há possibilidade de ensejar indenização por dano moral sob o aspecto subjetivo, ou seja, cabendo a vítima comprovar o efetivo dano. Por outro lado, também foi explorado que há decisões, em uma linha minoritária, que entendem pela aplicação da responsabilidade civil objetiva. É importante sempre ressalvar que a LGPD e seus desdobramentos são recentes, de modo que é possível que a construção jurisprudencial seja diferente a depender do desenvolvimento e aperfeiçoamento das boas práticas e mecanismos das empresas controladoras de dados.

Por sua vez, foi pontuado, ainda, que a necessidade de proteção de dados de empregados, prestadores e demais tipos de relações que envolvem a exposição de dados, para não colocá-los em uma posição de vulnerabilidade e manter a privacidade, é certo que a necessidade de boas práticas e efetividade em mecanismos para atender a LGPD não podem perder de vista a atuação da Justiça do Trabalho, quando se faz necessário a colaboração de informações para o deslinde de uma investigação ou até mesmo em lide.

Vê-se, portanto, que há uma dicotomia quando se fala em aplicação da LGPD em ambientes corporativos e na Justiça do Trabalho, pois, afinal, a Lei vigente veio apenas para garantir o direito fundamental à privacidade dos empregos e qualquer vulnerável titular, sendo necessário buscar a ponderação e proporcionalidade quando da aplicação da Lei.

Portanto, considerando que a LGPD prevê condições e há toda uma movimentação para que as empresas criem projetos para sua implementação e adaptem suas rotinas, devido a sua recente aplicação, restam especificidades a serem resolvidas. Ao longo prazo e com os desdobramentos do marco regulatório, é possível que os ambientes corporativos e a Justiça do Trabalho caminhem juntos à luz da razoabilidade, ponderação e proporcionalidade, para que seja possível conciliar o tratamento adequado de dados pessoas e, conjuntamente, haja colaboração em ações trabalhistas e investigações.

7. REFERÊNCIAS

1. BRASIL. Constituição Federal da República Federativa do Brasil: Senado Federal, 1998 http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

2. BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

3. MONTEIRO, Y. S. A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018. 2019 Link: https://repositorio.uniceub.br/jspui/bitstream/prefix/13383/1/21486829.pdf

4. FILHO, R. P. A, Lei de proteção de dados pessoais e seus impactos no direito do trabalho, 2020

5. MIZIARA, R. LGPD: razões de sua existência e impactos nas relações de emprego, 2020

6. MIZIARA, R; MOLLICONE, B.; PESSOA, A. Reflexos da LGPD no Direito do Trabalho e no Processo do Trabalho – Revistas dos Tribunais,

7. LGPD: A responsabilidade civil dos empregados enquanto envolvidos em operações de tratamentos de dados Link: https://www.migalhas.com.br/depeso/336154/lgpd--a-responsabilidade-civil-dos-empregados-enquanto-envolvidos-em-operacoes-de-tratamento-de-dados

8. O impacto da Lei Geral de Proteção de Dados nas relações de trabalho. Link: https://www.migalhas.com.br/depeso/342275/o-impacto-da-lei-geral-de-protecao-de-dados-nas-relacoes-de-trabalho

9. Os impactos da LGPD nas relações de emprego. Link: https://www.migalhas.com.br/depeso/348538/os-impactos-da-lgpd-nas-relacoes-de-trabalho

10. O impacto da LGPD nas relações de trabalho Link: https://www.conjur.com.br/2020-set-17/lgpd-impactos-trabalhistas

11. ROXO, Tatiana Bhering. Serradas Bom de Souza. O poder de controle empresarial: suas potencialidade e limitações na ordem jurídica: o caso das correspondências eletrônicas. São Paulo. 2013

12. ROBINSO, L. C. - A responsabilidade civil do controlar no âmbito da Lei Geral de Proteção de Dados. Link: https://pantheon.ufrj.br/bitstream/11422/12753/1/LCRobinson.pdf

13. Impactos da LGDP nas relações de trabalho Link: https://www.conjur.com.br/2021-fev-11/pratica-trabalhista-impactos-lgpd-relacoes-trabalho

14. Efeitos da LGPD nas Relações do Trabalho. Link: https://www.lgpdbrasil.com.br/efeito-da-lgpd-nas-relacoes-do-trabalho/

15. VIEIRA, Claudinei. Capítulo 1 – Fase 1: Preparação, in MALDONADA, Viviane Nóbrega (coord). LGPD: Lei de Proteção de Dados pessoais: manual de implementação. São Paulo. Thomson Reuters Brasil, 2019

16. ROXO, Tatiana Bhering. Reflexos da LGPD no Direito e no Processo do Trabalho. Como implementar na prática um programa de proteção de dados.

17. A LGPD e as relações de trabalho: o que é necessário fazer: Link: https://www.nextlawacademy.com.br/blog/a-lgpd-e-as-relacoes-de-trabalho-o-que-e-necessario-fazer

18. A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Exposição de dados sensíveis nas relações de trabalho Link: https://revista.trt10.jus.br/index.php/revista10/article/view/419/347

19. BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidente da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019- 2022/2019/lei/l13853.htm

20. Tribunal Regional do Trabalho da 2ª Região; Notícia: Mantida a Justa Causa de Trabalhador que Repassou Dados Sigilosos Da Empresa Para o Seu E-mail Pessoal; Publicada em 9 de novembro de 2021, Link: https://ww2.trt2.jus.br/noticias/noticias/noticia/mantida-justa-causa-de-trabalhador-que-repassou-dados-sigilosos-da-empresa-para-seu-e-mail-pessoal

21. NAVARRO, Ana Maria Nves de Paiva. O direito fundamental à autodeterminação informativa; Link: http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c

22. http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

23. LGPD e dano moral presumido: reflexões sobre jurisprudência em formação; publicação 16 de setembro de 2021, Link: https://www.conjur.com.br/2021-set-16/marcelo-carvalho-lgpd-dano-moral-presumido

24. Revista do Tribunal Regional do Trabalho da 10ª Região, v. 24. Nº 2, 2020; SANTOS, Alcassa Flávia, A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Exposição de Dados Sensíveis nas Relações de Trabalho; Link: https://revista.trt10.jus.br/index.php/revista10/article/view/419/347

25. G1 DF; Notícia Netshoes terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes, publicado em 5 de fevereiro de 2019, Link: https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml

26. BOUÇAS, Cibelle, Revista Valor – São Paulo; Notícia: C&A é alvo de hackers no Brasil, com vazamento de dados de clientes, publicado em 31 de agosto de 2018, Link: https://valor.globo.com/empresas/noticia/2018/08/31/c-a-e-alvo-de-hackers-no-brasil-com-vazamento-de-dados-de-clientes.ghtml

27. VEJA ABRIL, Notícia: Banco Inter vai pagar R$1,5 milhão por vazamento de dados de clientes, publicado em 19 de dezembro de 2018, Link: https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/

28. PROCON-SP Assessoria de Comunicação, Notícia: Vazamento de dados da ENEL, publicado em 18 de fevereiro de 2021; Link: https://www.procon.sp.gov.br/vazamento-de-dados-da-enel/

29. NASSIF, Tamara; Notícia: Meio milhão de chaves Pix já foi alvo de vazamento; saiba como identificar a exposição; publicado em 19 de março de 2022; Link: https://www.cnnbrasil.com.br/business/meio-milhao-de-chaves-pix-ja-foi-alvo-de-vazamento-saiba-como-identificar-exposicao/#:~:text=Entre%20setembro%20do%20ano%20passado,desde%20o%20final%20de%202020.

30. ARAÚJO, de Sá, Bruna e LIMA, Lara Sena, Luciana; Lei Geral de Proteção de Dados Aplicada pelos Tribunais Trabalhistas: A coleta de dados pelo poder judiciário e a colisão de princípios, Rev. TST, São Paulo vol. 86 nº4, outubro/dezembro de 2020, Link: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/181610/2020_araujo_bruna_lgpd_aplicada.pdf?sequence=1&isAllowed=y