LEI GERAL DE PROTEÇÃO DE DADOS – A RESPONSABILIDADE CIVIL DA EMPRESA DIANTE DO VICIO DE CONSENTIMENTO E O USO ABUSIVO DE DADOS NA RELAÇÃO DE EMPREGO

Yasmim Honorato da Silva[1]
Andrea Andrade Fernandes[2]

RESUMO

O presente artigo visa identificar se a empresa responderá civilmente diante do vício de consentimento e do uso abusivo de dados de seus empregados, bem como qual o regime dessa responsabilidade. Possui como finalidade abordar a LGPD e o uso de dados na relação de emprego; tratar sobre o consentimento e os vícios de consentimento; e discutir a responsabilidade civil da empresa diante do vício explicando os regimes de responsabilidade. Dispõe de pesquisa de natureza básica, com objetivos descritivos, por meio de uma abordagem qualitativa, metodologia dedutiva e procedimento bibliográfico. Em síntese, é possível concluir que convivem na LGPD os dois regimes de responsabilidade civil: a responsabilidade subjetiva e a responsabilidade objetiva.

Palavras-chave: LGPD. Relações de emprego. Responsabilidade civil. Vicio de consentimento. Uso abusivo de dados.

GENERAL DATA PROTECTION LAW – THE COMPANY'S CIVIL RESPONSIBILITY FACING THE CONSENT VICE AND THE ABUSIVE USE OF DATA IN THE EMPLOYMENT RELATIONSHIP

ABSTRACT

This article aims to identify whether the company will respond civilly to the

[1] Acadêmico(a) do Curso de Direito do Centro Universitário do Rio Grande do Norte. E-mail: yasmimhonorato16@gmail.com
[2] Professor(a) Orientador(a) do Curso de Direito do Centro Universitário. E-mail: andreaandrade.adv@hotmail.com

defect of consent and the abusive use of its employees' data, as well as the regime for this responsibility. Its purpose is to address the LGPD and the use of data in the employment relationship; deal with consent and consent vices; and discuss the company's civil liability in the face of defect, explaining the liability regimes. It has basic research, with descriptive objectives, through a qualitative approach, deductive methodology, and bibliographic procedure. In summary, it is possible to conclude that the two civil liability regimes coexist in the LGPD: subjective liability and objective liability.

Keywords: LGPD. Employment relationships. Civil responsibility. Consent addiction. Misuse of data.

1 INTRODUÇÃO

A Constituição Federal de 1988 já havia se dedicado a proteção da vida privada e da intimidade dos cidadãos, no entanto com o advento das novas tecnologias que se baseiam em análise massiva de dados, a partir da inteligência artificial e da robótica, houve a potencialização dos riscos de invasão da privacidade e intimidade das pessoas, despertando assim a necessidade de regulamentação no que se refere a proteção dos dados pessoais.

No Brasil foi aprovada a lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a qual foi fortemente inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia, também conhecido como General Data Protection Regulation (GDPR), regulamento (UE) nº 679/2016.

A Lei Geral de Proteção de Dados é uma lei de base principiológica, pois além de fomentar as inovações tecnológicas e a livre iniciativa, visa proteger princípios como a dignidade da pessoa humana, o valor social do trabalho, a intimidade, a privacidade, a honra e a imagem das pessoas.

Além disso, juntamente com a Lei de Acesso à Informação (Lei 12.527/2011) e o Marco Civil da Internet (Lei 12.965/2014), a LGPD estabelece normas para regulamentar o tratamento dos dados pessoais, físicos e digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, regulamentando o tratamento de dados pessoais tanto dos consumidores e clientes, quanto dos funcionários e

colaboradores que atuam nas empresas, refletindo diretamente nas relações de emprego.

O uso abusivo de dados pessoais, especialmente em ambientes digitais, deu origem a escândalos de vazamento.

Um exemplo, que tomou grande proporção, foi o caso do Facebook e da empresa Cambridge Analytica, onde a coleta de informações pessoalmente identificáveis de até 87 milhões de usuários do Facebook, foi utilizada para influenciar a opinião de eleitores em vários países com a finalidade de ajudar políticos a influenciarem no resultado de eleições.

Quanto a caracterização do uso abusivo de dados, a LGPD não fornece uma definição propriamente dita. Entretanto, ao longo do texto legal várias são as possibilidades de caracterização do uso abusivo.

Um exemplo ocorre ao ler os artigos da LGPD que estipulam hipóteses para que seja autorizado o tratamento de dados. Por meio dessa leitura é possível extrair que o uso abusivo de dados pessoais é todo e qualquer tipo de manipulação de dados do titular[3] que não se enquadre em nenhum dos requisitos necessários para o tratamento de dados, as chamadas bases legais.

Além disso, uma outra extração possível, é quanto a finalidade para que são colhidos e tratados os dados dos titulares, de modo que toda atividade realizada com os dados pessoais para outra finalidade que não a consentida e informada na coleta dos dados pode ser considerada uso abusivo de dados.

Diante disso, a posição legislativa em não caracterizar o uso abusivo de dados pode, inicialmente, ser percebida como uma lacuna, porém sob outro ângulo pode ser considerada como a forma encontrada pelo legislador para não limitar o rol de possibilidades de violação a direitos como a privacidade, a intimidade, a honra e imagem das pessoas e também fornecer liberdade ao titular de dados para ter o controle sobre seus dados.

Ademais, no que concerne as sanções administrativas, o descumprimento e a desconformidade das empresas com a lei de proteção de dados pode ensejar penalidades e responsabilidades.

Quanto a responsabilidade civil, a qual pretende-se abordar nesse artigo, essa pode ser gerada principalmente se, decorrente da base legal do consentimento, a

[3] Toda pessoa que tem seus dados coletados para que venha sofrer algum tipo de tratamento.

vontade real do titular de dados for viciada, ou seja, se essa não for observada ou não puder ser manifestada, acarretando assim em falhas no negócio jurídico.

Por conseguinte, para análise do tema, o presente artigo visa identificar se a empresa responderá civilmente diante do vício de consentimento e do uso abusivo de dados de seus empregados, bem como qual o caráter dessa responsabilidade.

Em um primeiro momento, o artigo abordará a LGPD e o uso de dados na relação de emprego, apresentando o tratamento de dados e seus requisitos, bem como os agentes responsáveis pelo tratamento.

Em sequência, se propõe a tratar sobre o consentimento e os vícios de consentimento, explicando como ocorre sua obtenção, se é passível de revogação e as consequências advindas do vício.

Por fim, versará sobre a responsabilidade da empresa diante do vício de consentimento à luz do instituto de responsabilidade civil brasileiro, explicando as responsabilidades subjetiva e objetiva.

2 DA LGPD E DO USO DE DADOS NA RELAÇÃO DE EMPREGO

A Lei Geral de Proteção de Dados, em seu artigo 1º, traz como finalidade a proteção aos direitos fundamentais referentes a liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, sem fazer nenhuma distinção quanto ao tipo de relação jurídica em que se dá o tratamento de dados pessoais, possibilitando assim o entendimento de que seus efeitos e consequências se aplicam as mais variadas espécies de relações, inclusive as relações de trabalho.

Diferentemente da GDPR, a LGPD não traz se quer um capitulo ou artigo voltado ao Direito do trabalho, no entanto sua aplicação a ele é categórica, pois a coleta; recepção; armazenamento e retenção de dados pessoais abordados pela LGPD permeiam desde as fases anteriores a celebração contratual, como coleta de informações sobre o candidato, currículo, histórico, entre outras informações, até a execução do contrato de trabalho.

Na relação de emprego, informações pessoais são inerentes à própria individualização daqueles que celebram negócios jurídicos em geral, principalmente contratos de trabalho, como se depreende do art. 2º e 3º da CLT.

Um exemplo é a necessidade de identificação profissional ocorrer através da

CTPS – Carteira de Trabalho e Previdência Social, pelo Livro de Registro de Empregados, conforme capitulo específico sobre o registro profissional da CLT.

A extensa regulamentação legal sobre o tema, bem como, a CLT considerar crime o tratamento inadequado das informações atinentes à relação de trabalho, conforme o art. 49, destaca a relevância conferida pelo legislador ao tema.

No âmbito das relações empregatícias é comum que o empregador colha determinados dados pessoais de seus empregados, e registre determinadas informações dos trabalhadores com quem mantém algum vínculo contratual.

Documentos comuns às relações de trabalho são: os de ordem médica (evidenciados através do atestado de saúde ocupacional – ASO); os exames obrigatórios (art. 168, CLT); outros dados pessoais como aqueles constantes na carteira profissional – CTPS, RG, CPF, CNH, RNE; registros expedidos pelos órgãos de classe – OAB, CREA, CRM entre outros; comprovantes de residência; título de eleitor; cartão do PIS; carteira de reservista; informações acerca de eventual aposentadoria ou benefício previdenciário; informações sobre formação profissional e educação (diplomas de graduação, histórico escolar, especialização, mestrado ou doutorado), informações sobre filhos, dependentes, cônjuges.

Há ainda outros dados pessoais coletados pelo empregador que merecem atenção e cautela - os dados automatizados, são eles: os e-mails; as mensagens trocadas em aplicativos de comunicação; as imagens dos empregados e colaboradores no local de trabalho (gravação de meio ambiente do trabalho); reconhecimento facial; testes para a apuração do consumo de substâncias entorpecentes, inclusive decorrentes de imposição legal (art. 168, § 6º, CLT); as chamadas em sistemas de teleconferência e o registro biométrico da jornada de trabalho.

Em razão do princípio da transparência, abordado pela LGPD, nenhum tratamento de dados pode se dar de forma oculta. O tratamento de dados ocultos é um tratamento ilícito.

Portanto, os dados só podem ser tratados mediante prévio aviso ao empregado. De modo que o empregador pode, por exemplo, monitorar com vídeo o ambiente de trabalho desde que haja um prévio aviso.

Apesar da nova Lei não ter regulamentado a aplicação da proteção de dados no âmbito das relações de trabalho, é fundamental compreender a importância do tratamento de dados nessas relações, bem como seu funcionamento, considerando as

necessidades decorrentes de cada empresa como forma de evitar o uso abusivo de dados.

2.1 DO TRATAMENTO DE DADOS E SEUS REQUISITOS

O tratamento de dados, conforme art. 5º, X, da LGPD, é toda operação realizada com dados pessoais, podendo-se elencar a coleta, produção, recepção, classificação, reprodução, processamento, arquivamento, armazenamento, eliminação, transferência, entre outros.

Para que ocorra o tratamento de dados a Lei determina alguns princípios, são eles: Finalidade, adequação e necessidade; princípio do Livre acesso, qualidade dos dados e transparência; Segurança, prevenção e não discriminação; e Responsabilização e prestação de contas.

Em seus artigos 7º e 11 estipula hipóteses nas quais, as empresas devem se enquadrar para que obtenham autorização quanto ao tratamento de dados pessoais[4] e sensíveis[5].

De forma sucinta, os requisitos estabelecidos como hipóteses ou bases legais para tratar dados são: o consentimento do titular; legitimo interesse; cumprimento de obrigação legal ou regulatória; tratamento pela administração pública; realização de estudos e de pesquisas; execução ou preparação contratual; exercício regular de direitos; proteção da vida e da incolumidade física; tutela de saúde do titular e proteção de crédito.

No âmbito trabalhista, o tratamento de dados começa antes mesmo da admissão do empregado, na fase denominada pré-contratual. Nessa fase, caracterizada por ser o momento em que ocorre o processo seletivo, ou seja, abertura de vagas; captação e triagem de currículos e entrevistas, até a efetiva contratação do funcionário, a empresa deverá tratar não somente dos dados que se mantem no banco de currículos, mas também dos dados presentes nos currículos daqueles candidatos não selecionados para a vaga.

Além disso, algumas precauções são fundamentais como por exemplo: solicitar

[4] Informação relacionada a pessoa natural identificada ou identificável.
[5] Dados específicos que possam levar a discriminação ao serem tratados, como por exemplo aqueles de 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.

do candidato apenas informações estritamente necessárias para avaliação e seleção; cuidar do manuseio e arquivamento dos currículos, uma vez que, mesmo com o consentimento do titular, a proteção dos dados deve continuar; informar ao candidato o tratamento oferecido as informações por ele fornecidas, bem como se há interesse em manter seu currículo no banco de dados da empresa, sendo necessária obtenção de autorização expressa; utilizar os dados, pelos candidatos fornecidos, especificamente para a candidatura da vaga anunciada, não podendo utiliza-los para outro fim, a exceção de dados estatísticos em que as informações são tratadas de forma anônima; atentar para uso e repasse das informações obtidas em entrevistas, mediante a responsabilidade na preservação das informações tidas como sensíveis e destinar corretamente as informações dos candidatos não selecionados para a vaga, seja via banco de currículos ou eliminação dos dados, devendo ser ofertada a escolha aos candidatos.

Tais precauções são essenciais para que não ocorra nenhuma forma de discriminação para com o titular de dados, e candidato à vaga, na fase de seleção.

Já na fase contratual, iniciada com a admissão do empregado ou formalização do contrato com o prestador de serviços, os dados e documentos advindos da relação entre a empresa e seus funcionários terão um fluxo maior, demandando assim maior cuidado com a definição de processos e procedimentos pelo qual passará os dados de acordo com a realidade de cada empresa.

Desse modo, é importante que as empresas realizem uma análise dos departamentos que terão acesso aos dados dos funcionários e colaboradores como por exemplo o setor de RH; a contabilidade e também setores da área financeira, bem como verificar se tais dados são transmitidos ou compartilhados com terceiros; como se dá essa transmissão e o tratamento desses dados e principalmente onde e como são armazenados.

Partindo dessa análise, também denominada de mapeamento de dados, torna-se possível prevê os riscos e identificar as necessidades de adequações à Lei, por meio de revisão de cláusulas contratuais, políticas e treinamentos específicos para a empresa.

Com relação ao tratamento de dados pessoais sensíveis do trabalhador, apesar da coleta de alguns desses dados estar fundamentada em lei, tais dados exigem maior cautela, visto que, são dados que contém informações importantes, as quais em caso de vazamento podem ocasionar consequências como a discriminação, ferindo

diretamente a intimidade de seu titular. Um exemplo é quanto as informações de saúde dos empregados, as quais podem ser fornecidas ao empregador por atestados médicos ocupacionais e planos de saúde empresariais, tais informações também podem ser consideradas dados sensíveis. Nesse caso a empresa deverá rever seu contrato com a seguradora que presta serviços, posto que o controlador poderá ser responsabilizado por incidentes de segurança decorrentes dos operadores por ela indicados.

No que se refere aos atestados médicos ocupacionais, entende-se que não há exigência de consentimento por parte do empregado, uma vez que a CLT prevê como obrigação legal do empregador. Entretanto, o repasse de informações médicas de funcionários para fornecimento de planos de saúde empresariais necessita de autorização expressa do trabalhador.

Outro caso importante, que pode gerar grandes discussões é o uso da biometria dos empregados na empresa.

Segundo o artigo 5º, II da nova Lei, dados biométricos são dados pessoais sensíveis e, portanto, requerem tratamento diferenciado por parte das empresas.

É importante destacar que biometria não se restringe apenas a impressão digital, podendo ser extraída a partir da íris, face, voz ou até mesmo deambulação[6].

O uso de dados biométricos na relação de emprego é, geralmente, para fins de registro de ponto.

A própria CLT em seu art. 74, estipula a necessidade de registro de ponto, admitindo que este se dê por meio manual, mecânico ou eletrônico.

Por ser, em muitos casos, obrigatório para o acesso a empresa, o uso de dados biométricos necessita de autorização prévia e expressa de cada funcionário, de forma que seu uso deve se restringir somente ao fim a que se destina, sendo vedada sua utilização para outra finalidade sem consentimento expresso do titular.

No que tange a contratação de menores de idade pala empresa ou ainda se o trabalhador indicar menores de idade como dependentes, conforme a lei, os responsáveis legais devem autorizar o tratamento de dados, bem como devem ser informados sobre todas as atualizações e modificações realizadas no tratamento dos dados pessoais dos menores.

Dessarte, na fase pós contratual, marcada pelo desligamento do funcionário dos quadros da empresa, essa deve informar ao titular sobre a finalização do uso de seus

[6] Ato ou efeito de deambular; passeio.

dados.

Ao final das relações de trabalho, a legislação trabalhista impõe a guarda de documentos como prova em futuras ações trabalhistas ou mesmo para concessão de informações relacionadas as contribuições sociais ou eventuais fiscalizações pelo Ministério da Economia.

Em conformidade com o artigo 11-A da CLT, "A pretensão quanto a créditos resultantes das relações de trabalho prescreve em cinco anos para os trabalhadores urbanos e rurais, até o limite de dois anos após a extinção do contrato de trabalho", permitindo assim que a empresa possua garantia legal para a guarda desses documentos por pelo menos o período correspondente ao prazo prescricional.

Ainda referente a manutenção de documentos do titular pela empresa, é mister destacar que a LGPD, em seu artigo 16, apresenta hipóteses em que é autorizada a conservação dos dados:

> Art. 16. Os dados pessoais serão eliminados após o término do 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 terceiros, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV – Uso exclusivo do controlador, vedado seu acesso por terceiros, e desde que anonimizados os dados (BRASIL, 2018).

Conforme inciso I, os dados do titular podem não ser eliminados caso haja qualquer determinação legal, seja ela federal, estadual, municipal, internacional ou regulatória, como por exemplo dados tributários. Vale salientar que, caso as boas práticas, comprovadamente seguidas no nicho de mercado, apontem para a não eliminação dos dados, o controlador poderá reter os dados pessoais do titular (MALDONADO *et al.*, 2021, p. 225).

Já o inciso IV, é possível a retenção dos dados, assim que encerrada a relação entre o controlador ou operador e o titular, desde que anonimizados, como é o caso de informações detalhadas de perfis, para uso exclusivo do controlador (GARCIA *et al.*, 2020, p. 68).

Contudo, sustenta Maldonado *et al.* (2021, p. 226) que,

> [...] sendo os dados de fato anonimizados, é possível sustentar que, como não mais estarão diretamente protegidos por esta Lei, eles podem ser divulgados ou compartilhados com terceiros, desde que todos os demais dispositivos sejam atendidos, especialmente os que tratam sobre as restrições ao uso dos dados, mesmo anonimizados.

Importante salientar que, conforme indica Garcia *et al*. (2020, p. 68), sempre que houver a retenção de dados após o fim do seu tratamento, mesmo que procedido a sua anonimização, o titular deve ser informado com a sua respectiva justificativa.

Ainda assim, no decurso do prazo de guarda, a empresa deve estar em conformidade com as diretrizes da LGPD, mantendo o tratamento e sigilo dos dados até o término desse período, sendo então obrigatório seu descarte.

Conforme Maldonado, *et al*. (2019, p. 187) salienta, o descarte dos dados deve ser irreversível nos arquivos principais, bem como suas cópias de segurança que eventualmente tenham sido geradas no decorrer do tratamento.

Algumas opções como: picotar ou incinerar documentos em papel; excluir informações na Nuvem e formatar HD´s físicos para garantir que não haverá mais acesso aos dados, são bem vindas, no entanto é preciso informar ao titular de dados, com clareza, quanto a política de descarte da empresa.

O descarte de dados ainda é alvo de grandes discussões principalmente entre os profissionais de Tecnologia de Informação, uma vez que existem divergências quanto real possibilidade de descarte.

De acordo com o Gerente de Segurança da Informação para o Brasil e Argentina na Tata Consultancy Services (TCS), Rodrigo Ferrarez, em entrevista fornecida ao site Infor Channel, em 16 de novembro de 2020,

> Na TCS utilizamos o padrão da ISO 27.001, que também dá recomendações sobre as formas de descarte seguro para todos os meios, e devemos sempre observar e seguir as políticas de classificação de dados, já que é através delas podemos entender quais os cuidados na hora de transmitir, armazenar e descartar dados e informações. A LGPD não dá uma receita de bolo de quais tecnologias ou controles específicos devem ser utilizados para proteger as informações então é preciso que cada empresa determine, dentro de seu contexto de negócio, quais serão as medidas de proteção e descarte seguro, e comunique as partes interessadas.

A ISO 27.001 é uma norma internacional de Gestão de Segurança da Informação

que visa a adoção de um compilado de requisitos, processos e controles, com a finalidade de gerir com maior qualidade e antecipação os riscos de segurança da informação nas organizações.

De modo que, não importa o meio no qual a informação circula, online ou offline, todo dado deve ser igualmente protegido inclusive no momento de descarte e é responsabilidade de quem realiza atividade de tratamento, fazê-lo.

Portanto, todas as empresas devem possuir uma política de descarte de dados, analisando quais aqueles necessários para atingir suas finalidades e quais aqueles dados não são mais atuais ou já não são úteis perante a política de proteção de dados informada ao titular, valendo-se disso, tanto para dados físicos, quanto para dados digitais, para que a empresa não seja uma "acumuladora" (MARINHO, 2020, p. 23).

Contundente a isso, é de suma importância definir hierarquias de acesso aos dados, analisando quem realmente deve ter acesso, minimizando vazamentos e utilizações inadequadas das informações.

2.2 DOS AGENTES RESPONSAVEIS PELO TRATAMENTO DE DADOS

A LGDP menciona ainda agentes responsáveis pelo tratamento de dados, sendo eles: o controlador, o operador e o encarregado.

O controlador de dados é, segundo a lei, pessoa física ou jurídica que determina o modo e a finalidade do tratamento dos dados pessoais, isto é, no âmbito da relação de emprego é possível compreender o controlador como a empresa ou empregador, responsável por definir como ocorrerá o tratamento de dados da coleta à eliminação. Sendo ele a figura mais interessada no tratamento de dados e também sobre quem recai maior responsabilidade.

Por sua vez, o operador é a pessoa física ou jurídica que realiza de fato o tratamento dos dados pessoais em nome do controlador e conforme suas orientações. Por tratar diretamente com os dados pessoais a Lei também estabelece responsabilidade sobre este.

Já o encarregado, também chamado de Data Protection Officer[7] (DPO), é indicado pelo operador e controlador para atuar na comunicação entre controlador, titular dos

[7] Encarregado da proteção de dados.

dados e a Autoridade Nacional de Proteção de Dados[8] (ANPD), garantindo ainda a proteção dos dados em posse do controlador.

Outrossim, a nova Lei estabelece que os agentes de tratamento além de garantir um acesso facilitado ao titular e de reformular suas bases de dados para facilitar o compartilhamento, devem reforçar os mecanismos de segurança e proteção dos dados, ser capazes de produzir relatórios de impacto a proteção de dados pessoais com detalhes sobre o fluxo e a transformação sofrida pelos dados, bem como, manter um registro das operações realizadas com os mesmos.

Ademais, é preciso relembrar que para o tratamento de dados pessoais é fundamental o enquadramento da empresa em uma das hipóteses legais previstas em lei.

No capítulo seguinte, será abordado com especificidade a base legal do Consentimento, visto que é o foco do presente artigo.

3 DO CONSENTIMENTO E DOS VICIOS DE CONSENTIMENTO

Em conformidade com o artigo 5º, inciso XII, consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Nesse contexto é possível considerar que há quatro requisitos para se considerar consentimento, são eles: a manifestação livre; informada e inequívoca e a necessidade de uma finalidade determinada.

Sobre a manifestação livre, o titular não é obrigado a fornecer consentimento, bem como esse consentimento não pode ser obtido de forma automática, nem mesmo de forma tácita.

Em conformidade com o artigo 18 da LGPD, os titulares poderão pedir aos agentes de tratamento a confirmação de seus dados, o acesso a eles, sua correção, anonimização, bloqueio, eliminação e portabilidade. Assim, para que o consentimento seja livre é necessário que o titular possua o controle de seus dados, tendo livre acesso as informações sobre eles e também quanto ao tratamento a que estão sendo submetidos.

Quanto a manifestação informada, no artigo 8º, caput e §1º da LGPD, é

[8] Órgão fiscalizatório e regulador da LGPD.

estipulado que o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a vontade do titular" e que, caso seja fornecido por escrito, deve "constar de clausula destacada das demais cláusulas contratuais". Dessa forma, a declaração de consentimento deverá ser informada de maneira inteligível e de fácil acesso, numa linguagem clara e simples, sem cláusulas abusivas.

No que se refere a manifestação inequívoca, o titular precisa compreender as condições do que está consentindo, não podendo haver dúvidas sobre o consentimento.

Com relação a finalidade, o consentimento não pode ser genérico, devendo ter um fim especifico e determinado.

Além disso, conforme o art. 8º, § 5º, da LGPD, podem ainda os titulares, caso não estejam de acordo com o modo que ocorre o tratamento de seus dados, revogar o consentimento de uso dado anteriormente.

No caso de o titular de dados não dispor de livre escolha ou não puder recusar nem retirar o consentimento sem prejuízo não será possível considerar que o consentimento foi dado de livre e espontânea vontade, tornando o negócio jurídico ineficaz.

Nesse sentido, para Rodolfo P. Filho e Vicente V. C. Junior (2020, p.19), a inobservância à LGPD pode ensejar a nulidade do consentimento: "eventuais disposições contratuais que gerem danos ao titular dos dados será considerada como se ali não estivesse escrita, [...], como forma de tutelar os interesses da parte hipossuficiente".

Diante disso, cabe ao controlador e ou ao agente de tratamento, o ônus de provar que o titular deu o seu consentimento de forma livre e inequívoca à operação de tratamento dos dados e que tanto o controlador quanto o operador agiram em conformidade com a LGPD.

Ademais, é importante destacar que o consentimento é apenas uma das bases legais que autorizam a empresa a tratar dados dos empregados. Entretanto, na relação de emprego, considerando a finalidade e a relação estabelecida com o titular de dados, o consentimento pode não ser a base mais adequada.

Ao analisarmos a subordinação, um dos requisitos para caracterizar a relação de emprego, torna-se visível que a vontade do empregado é limitada pelo contrato de trabalho assinado entre ele e o empregador, o qual detém a direção das funções, ou

seja, o empregado tem o dever de cumprir as determinações do empregador, claro, respeitando-se seus direitos legais.

Dessa forma é possível perceber que há uma disparidade no negócio jurídico celebrado entre o empregador e o empregado.

Assim, um dos principais problemas quanto ao uso da base legal consentimento está relacionado ao termo "consentimento livre", o que não pode ser verificado em uma relação de emprego, em que há subordinação, tendo em vista o desequilíbrio entre as partes.

Nesse contexto, a GDPR, em seu Considerando nº 43, aponta expressamente que "a fim de assegurar que o consentimento seja dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento". O órgão consultivo europeu independente, Grupo de Trabalho 29[9], considera um problema os empregadores procederem o tratamento de dados pessoais de seus empregados com base no consentimento, visto que é questionável que esse consentimento seja dado espontaneamente.

Por tanto, em razão do risco de não ser considerado valido, o uso do consentimento no âmbito das relações de trabalho não é recomendável. Entretanto, há outras hipóteses mais indicadas para o tratamento de dados pessoais provenientes da relação de emprego.

O artigo 7º, inciso V, da LGPD, prevê a realização do tratamento de dados pessoais quando necessário para a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular, a pedido deste.

Sendo o contrato de trabalho, um acordo firmado por duas partes, nesse caso entre o empregado e empregador, a LGPD prevê que o controlador trate os dados pessoais sem o consentimento do titular, uma vez que existe uma manifestação de vontade de ambas as partes. Além disso, uma outra hipótese de tratamento de dados está prevista no artigo 7º, inciso II, da LGPD, onde é permitido o tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador.

Nesse caso, um exemplo é a exigência que o empregador tem para com o Estado, de prestar obrigações derivadas da relação de emprego, que são os recolhimentos

[9] Working Party29º é o grupo de trabalho europeu independente que lidou com as questões relacionadas a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD).

fiscais e previdenciários dos seus empregados.

Por fim, no artigo 7º, inciso VI, da LGPD, há uma hipótese que confere ao empregador a possibilidade de tratar dados dos titulares sem a necessidade de consentimento, que é para o exercício regular de direitos em processo judicial, administrativo ou arbitral, tendo como exemplo mais comum, as demandas judiciais perante a Justiça do Trabalho.

Embora não seja a base legal mais adequada para tratar dados na relação de emprego, tendo em vista que há outras bases, o tratamento de dados pelo consentimento é possível.

Um exemplo, são as iniciativas adotadas pela empresa quanto confraternizações ou aniversários de seus funcionários e colaboradores.

Em muitos casos há divulgação de nomes e datas em murais ou até mesmo nas mídias sociais da empresa. Nesses casos, é comum que algum dos funcionários não se sinta à vontade, seja por motivos pessoais ou íntimos, de expor tais dados, assim a base legal do consentimento torna-se a melhor opção a ser utilizada, pois permite ao titular estar no controle de seus dados pessoais.

Outro exemplo, é o abordado na Guideline nº 259/2017[10] do Grupo de Trabalho do Artigo 29, que trata de orientações relativas ao consentimento (Guidelines on consent under Regulation 2016/679):

> Uma equipe de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.

Com base nos dois exemplos apresentados, percebe-se que a utilização do consentimento como base legal nas relações de trabalho, apesar de não ser a mais adequada, é possível, desde que a negativa deste consentimento não venha a prejudicar o titular e que seja realizado de forma livre, para não incorrer em vicio de consentimento.

Partindo do pressuposto de que a vontade é um elemento essencial para que atos e negócios jurídicos se realizem, e deve ser externada de forma livre, espontânea e

[10] Diretriz sobre consentimento nos termos do regulamento 2016/679.

clara, como diz o doutrinador Silvio de Salvo Venosa (2012, p. 46);

> A vontade é a mola propulsora dos atos e negócios jurídicos. Essa vontade deve ser manifestada de forma idônea para que o ato tenha vida normal na atividade jurídica e no universo negocial. Se essa vontade não corresponder ao desejo do agente, o negócio jurídico tornar-se-á suscetível de nulidade ou anulação.

Portanto, sempre que a vontade real do titular não for observada ou manifestada, ocorrerá vicio de consentimento, acarretando em falhas no negócio jurídico.

Em conformidade com o Código Civil brasileiro, são vícios de consentimento: erro ou ignorância; dolo; coação; estado de perigo ou lesão.

O erro ocorre quando o agente possui uma falsa percepção da realidade, enganando-se sozinho, ou seja, possui uma percepção destorcida daquilo que realmente é.

Segundo Silvio de Salvo Venosa (2012, p. 53), o erro "Trata-se de manifestação de vontade em desacordo com a realidade, porque o declarante tem uma representação errônea da realidade. Já na ignorância, o declarante nada sabe a respeito da realidade", ou seja, diferentemente do erro a ignorância é o completo desconhecimento da realidade.

Um exemplo é quando ocorre a contratação de um homônimo[11]. De modo que havendo prestação de trabalho haverá o contrato de emprego, independentemente do erro.

O artigo 138, do Código Civil, trata do erro, reforçando que quando a declaração de vontade ocorrer mediante erro substancial, escusável e real o negócio jurídico realizado é passível de anulação.

No que se refere ao dolo, previsto no artigo 145, do Código Civil, igualmente ao erro trata-se de uma falsa percepção da realidade, entretanto, a falsa percepção é introduzida por outrem.

De acordo com o doutrinador Patrick Lendl Silva (2011, p.72): "No dolo, o agente não causa o efeito sozinho. A outra parte que integra o negócio jurídico, ou um terceiro estranho a essa relação jurídica, é que dá ao declarante a falsa percepção da realidade, que, sozinho, não teve".

[11] Pessoas que possuem um nome idêntico a outra.

Um exemplo, é quando ocorre a obtenção desautorizada de documentos necessários a uma contratação.

Com relação a coação, prevista no artigo 151, CC., essa ocorre sempre que uma pessoa se utiliza de pressão psicológica ou ameaça física para que o agente realize algo contra sua vontade.

Conforme determina os doutrinadores De Plácido e Silva (2020, p 69): "Coação é toda ameaça ou pressão exercida sobre um indivíduo para forçá-lo, contra a sua vontade, a praticar um ato ou realizar um negócio".

A coação se divide em duas: absoluta e relativa. A primeira, caracterizar-se pelo emprego de força física, não ocorrendo qualquer consentimento ou manifestação de vontade por parte do agente. Já na segunda o coator se utiliza do emprego de ameaça, impondo ao agente uma condição de que, caso não faça o solicitado, corre o risco de vir a sofrer os atos ditos nas ameaças.

Um exemplo, ocorre quando o empregado é forçado a pedir demissão sob pena de divulgação de sua situação pessoal.

Sobre a nulidade do negócio jurídico cabe ressaltar que quando é usado o emprego de força física, o negócio jurídico se torna nulo. Desse modo, somente os atos realizados mediante ameaça e pressão psicológica são anuláveis.

Ademais, quanto ao estado de perigo, previsto no artigo 156, CC., o agente é levado a realizar um negócio jurídico para salvar a si próprio ou alguém de sua família, assumindo uma obrigação desproporcional e excessiva, sendo que este dano causado é conhecido pela outra parte.

Por fim, a lesão, prevista no artigo 157, CC., ocorre quando o agente é levado a realizar um negócio jurídico, seja por inexperiência ou por necessidade, sendo que tal negócio se torna extremamente oneroso em comparação com a contraprestação que receberá, sendo ele credor ou devedor.

Em sequência, o capítulo seguinte tratará sobre a responsabilidade civil da empresa diante do vício de consentimento.

4 DA RESPONSABILIDADE CIVIL DA EMPRESA NA LGPD

A responsabilidade civil pode ser designada como o ramo do direito civil que se ocupa dos danos advindos da vida social.

A responsabilidade civil que antes se dava em torno da noção de ato ilícito e em especial do elemento subjetivo culpa, compreendida como um mecanismo de sanção; com o passar dos anos e com o avanço das novas tecnologias deslocou-se de culpa para dano.

Nesse sentido, tendo como base o dano, tornou-se necessário a criação de um novo regime de responsabilização civil, calcado não mais na culpa, mas sim no risco.

Atualmente, na maior parte dos ordenamentos jurídicos, ambos os regimes convivem, competindo ao legislador ou ao juiz definir quais atividades se encontram sob a égide da responsabilidade subjetiva e quais se encontram sob a égide da responsabilidade objetiva.

Em sintonia com a história da responsabilidade civil, a Lei Geral de Proteção de Dados, em seus artigos 42 a 45 trata da responsabilidade civil patrimonial e extrapatrimonial dos agentes de tratamento de dados, considerando tanto o controlador quanto o operador responsáveis por eventuais danos patrimonial, moral, individual ou coletivo, em caso de violação à respectiva legislação.

De modo que, tanto o Controlador quanto o Operador devem adotar medidas para resguardar a segurança das informações, bem como notificar o titular em caso de um incidente de segurança. Tal exigência vale para todos os agentes da cadeia de tratamento.

Em conformidade com o inciso II, §1, do artigo 42, da LGPD, se um controlador causar dano a alguém em virtude de uma atividade de tratamento, poderá ser responsabilizado solidariamente, devendo reparar o dano.

Assim, para assegurar a indenização ao titular dos dados, o operador responde solidariamente quando descumprir as obrigações da lei ou caso não tenha seguido as instruções do controlador. E o controlador, por sua vez, envolvido em tratamento de dados também responderá solidariamente.

Caso não haja violação à LGPD ou o dano seja de culpa exclusiva de terceiros ou do titular dos dados, nenhum dos agentes será responsabilizado.

Entretanto, mais precisamente com relação ao artigo 42, é perceptível a lacuna quanto o regime de responsabilização que deveria recair sob o encarregado e eventuais terceiros que participem dos processos relacionados à proteção dos dados pessoais. Uma vez que, as disposições do artigo não esgotam as situações de coleta, tratamento e armazenamento dos dados pessoais, gerando insegurança ao seu titular.

Por sua vez, quanto o regime de responsabilização civil adotado pelo legislador para ser aplicado na LGPD, esse é alvo de grandes discussões por parte dos doutrinadores.

Parte da doutrina defende o regime objetivo e parte defende o subjetivo.

4.1 DO REGIME OBJETIVO

Grande parte da doutrina que defende o regime objetivo como sendo o regime de responsabilidade civil adotado pelo legislador na LGPD, se fundamenta no fato de que a atividade de tratamento de dados seria uma atividade de risco, e o titular dos dados, portanto, seria uma partícula suficiente em relação ao agente de tratamento, de maneira que ele teria uma hipossuficiência técnica em relação ao agente e por isso de acordo com o Código Civil estaria submetido ao regime de responsabilidade civil objetiva.

Segundo os doutrinadores Danilo Doneda e Laura Schertel Mendes "o tratamento de dados apresenta risco intrínseco aos seus titulares" (2020).

Dentre as previsões da LGPD nessa linha, citam o art. 7º, no qual há uma delimitação exaustiva das hipóteses em que o tratamento de dados pessoais poderá ser realizado; o art. 6º, III ("princípio da finalidade") e II ("princípio da adequação", cujos termos prescrevem que o tratamento não deve ser admitido quando for inadequado ou desproporcional "em relação à sua finalidade"); o art. 16, que impõe, "como regra", a necessidade de "eliminação dos dados quando seu tratamento esteja encerrado", bem como, por fim; as várias ocasiões em que a LGPD acena para a obrigação "de se levar em conta o risco presente no tratamento de dados" . Em síntese percebe-se que o argumento dos autores é pautado no fato de que a própria LGPD visa delimitar expressamente as hipóteses permitidas de tratamento, como forma de evitar sua banalização e, justamente da criação das restrições, extrai-se a caracterização da atividade como sendo de risco, a ponto de atrair a responsabilização dos agentes de tratamento, independentemente de conduta culposa.

Desse modo, considerando a responsabilidade civil do controlador objetiva, bastaria que o titular dos dados, comprovasse a conduta, ou seja, o tratamento dos dados, o nexo de causalidade e o dano, não precisando provar a culpa.

Outro argumento é que mesmo tendo a LGPD forte inspiração da legislação

europeia, é possível identificar grande semelhança da LGPD com o Código de Defesa do Consumidor, principalmente quanto a sessão de responsabilidade civil.

Além disso, por esse regime tanto o controlador quanto o operador responderiam objetivamente, ou seja, sem necessidade de provar culpa, contudo o controlador responderia diretamente, ao passo que o operador responderia apenas subsidiariamente.

Ademais, conforme a legislação de dados, nos casos, em que o operador não siga as regras estabelecidas pelo controlador é possível que o operador responda diretamente ao invés de subsidiariamente. Por isso a importância de estarem em conformidade com a nova Lei.

4.2 DO REGIME SUBJETIVO DE RESPONSABILIDADE

Por outro lado, há doutrinadores que entendem pelo regime subjetivo, argumentando que apesar da semelhança com o CDC a LGPD em momento algum emprega a expressão "independente de culpa", como consta no CDC e no CC.

Além disso, um forte argumento, aos que entendem o regime como subjetivo, é a possibilidade do agente de tratamento de dados se eximir da responsabilidade de indenizar, mediante comprovação de ter agido conforme a lei e adotado as medidas de segurança.

Em seu art. 43, a LGPD aborda hipóteses que excluem a responsabilidade dos agentes. De forma que estes só não serão responsabilizados quando provarem que não realizaram tratamento de dados pessoais no caso em questão; ou se provarem que realizaram tratamento, mas seguiram rigorosamente as regras da LGPD e regulamentos da ANPD; ou se provarem que o dano decorreu por culpa exclusiva do titular dos dados ou de terceiros.

Caso não haja violação à LGPD ou o dano seja de culpa exclusiva de terceiros ou do titular dos dados, nenhum dos agentes será responsabilizado.

Segundo as doutrinadoras Gisela Sampaio e Rose Meireles, a LGPD adota a teoria subjetiva da responsabilidade civil, devendo haver prova da conduta culposa do agente de tratamento na ocasião do dano, por sua vez fundamentada na omissão de medidas de segurança para o tratamento adequado dos dados e no descumprimento das obrigações impostas na lei.

Para as autoras, o capítulo VI, artigos 46 a 54, da LGPD - que trata dos padrões de conduta a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados - seria também fundamento para o reconhecimento da responsabilidade subjetiva.

Em complementação ao entendimento das autoras, na análise das excludentes de responsabilidade do artigo 43, da LGPD, o inciso II indicaria a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva ao estatuir que só não serão responsabilizados se, ainda que exista o dano, não houver violação da legislação de proteção de dados.

A violação da lei, para as autoras, seria elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados.

Assim, não haverá obrigação de indenizar quando o agente de tratamento de dados tiver demonstrado que observou o padrão esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa.

Em resumo, sustentam as autoras que a LGPD adota a teoria subjetiva da responsabilidade civil, com base em duas brechas deixadas pelo legislador: a primeira no artigo 42, quando o legislador faz menção a medidas de segurança e a segunda no art. 43, II, quando o legislador estabelece excludente de ilicitude referente ao cumprimento das normas da LGPD.

Por fim, é possível concluir que a LGPD adota os dois regimes distintos de responsabilidade civil: a responsabilidade subjetiva e a responsabilidade objetiva.

É o que ocorre no Código Civil, no qual convivem as cláusulas gerais de responsabilidade subjetiva e objetiva, no Código de Defesa do Consumidor, e também na legislação trabalhista onde o empregador é o responsável pelos danos causados por seus empregados de forma objetiva, dependendo apenas da demonstração do dano e da relação com a empresa que causou o dano e o empregado responde de forma subjetiva, sendo necessária demonstração de dolo ou culpa.

Todavia é importante mencionar que a não qualificação do regime de forma explicita na lei pode deixar brechas para que os julgadores decidam de acordo com seu próprio entendimento, gerando assim enorme insegurança jurídica.

5 CONSIDERAÇÕES FINAIS

Com o advento das novas tecnologias que se baseiam em análise massiva de dados, a partir da inteligência artificial e da robótica, bem como diante de escândalos de vazamento de dados, potencializou-se os riscos de invasão da privacidade e intimidade das pessoas, despertando assim a necessidade de regulamentação no que se refere a proteção dos dados pessoais.

Ao dar início a pesquisa, relembrou-se que a LGPD é uma lei recente e por consequência muitas empresas ainda não estão em conformidade com ela, entretanto essa desconformidade das empresas principalmente no âmbito das relações de trabalho pode incorrer em responsabilização pelo uso indevido de dados, muitas vezes decorrentes de vícios no consentimento fornecido pelos empregados da empresa.

Diante da relevância desse assunto, tornou-se fundamental abordar o tema LGPD: a responsabilidade civil da empresa diante do vício de consentimento e o uso abusivo de dados na relação de emprego.

Constata-se que o objetivo geral foi atendido, pois conseguiu identificar tanto que a empresa pode ser responsabilizada civilmente diante do vício de consentimento e uso abusivo de dados na relação empregatícia, quanto os regimes de responsabilização adotados pela lei.

O objetivo inicial era abordar a LGPD e o uso de dados na relação de trabalho, tal objetivo foi atendido uma vez que não apenas abordou a Lei de proteção de dados na esfera trabalhista como também possibilitou identificar que a Lei não dispõe de capitulo voltado para o direito do trabalho, fazendo com que os juristas devam adaptar a nova Lei à outras normas legais, de acordo com o caso concreto.

O segundo objetivo especifico era tratar sobre o consentimento e os vícios de consentimento, tal finalidade foi alcançada visto que se tratou sobre o que é o consentimento; como ocorre; se é passível de revogação; e quanto ao vício, o que é; como ocorre, quais os seus efeitos. Além disso, tratou-se ainda dos cuidados que a empresa deve ter com os dados de seus empregados antes, durante e após a relação de emprego. Alcançar esse objetivo possibilitou identificar que quanto as relações de trabalho, principalmente na fase contratual, a base do consentimento pode não ser a mais adequada.

O terceiro e último objetivo era discutir a responsabilidade civil da empresa diante do vício explicando as responsabilidades subjetiva e objetiva. Tal objetivo foi conquistado, uma vez que, adequando a LGPD ao Código Civil identificou-se que a

empresa deve ser responsabilizada solidariamente na esfera civil em caso de vicio, bem como, por breve explanação do pensamento de doutrinadores, foi capaz de explicar os regimes de responsabilização.

Buscando encontrar resposta para saber se a empresa, diante do vício de consentimento e do uso abusivo de dados de seus empregados, responderá civilmente e para identificar o regime de responsabilidade, o artigo dispôs de pesquisa de natureza básica, com objetivos descritivos, por meio de uma abordagem qualitativa, metodologia dedutiva e procedimento bibliográfico, tendo como foco a legislação e a doutrina.

Apesar da LGPD não esclarecer o regime de responsabilização, se subjetiva ou objetiva atrelado ao fato de deixar uma lacuna quanto a responsabilização que deveria recair sob o encarregado e eventuais terceiros, é possível concluir que convivem na LGPD os dois regimes distintos de responsabilidade civil: a responsabilidade subjetiva e a responsabilidade objetiva. Entretanto, é importante mencionar que a não qualificação do regime na lei pode deixar brechas para que os julgadores decidam de acordo com seu próprio entendimento, gerando assim enorme insegurança jurídica.

Em suma, a responsabilidade civil em matéria de dados pessoais é primordial para o equilíbrio das relações trabalhistas, sobretudo quando envolvida a tecnologia.

É fundamental que as empresas estejam adaptadas à LGPD.

Sabendo que cada empresa possui uma especificidade diferente, é importante que ocorra o engajamento de todas as áreas da empresa, principalmente os setores Jurídicos, Recursos Humanos e Tecnologia da Informação para que seja realizada uma análise inicial sobre como a LGPD irá impactar o negócio, além de levantar questões sobre como, porque e quais categorias de dados pessoais deverão ser tratados.

Faz-se necessário também que consigam comprovar tal adequação, bem como, espera- se que estejam sempre vigilantes, seja em relação aos seus fornecedores e prestadores de serviço, seja em relação aos seus próprios sistemas de segurança da informação.

Somente assim as empresas conseguirão se resguardar e mitigar os prejuízos advindos da responsabilidade prevista na LGPD.

REFERÊNCIAS

ACESSO À INFORMAÇÃO PÚBLICA: **uma introdução à lei 12.527**, de 18 de novembro de 2011. Brasília, DF: CGU, 2011b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em: 31 out. 2021.

BRASIL. **Decreto-Lei 5.452 de 1º de maio de 1943**. Consolidação das Leis do trabalho, Brasília, DF, out. 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto- lei/del5452.htm Acesso em: 30 out. 2021.

BRASIL. **Decreto nº 10.474, 26 de agosto de2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019- 2022/2020/decreto/D10474.htm Acesso em: 26 ago. 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm Acesso em: 31 out. 2021.

BRASIL. **ISO/IEC 27001**, Tecnologia da informação. Técnicas de segurança. Sistemas de gestão de segurança da informação, 2006. Disponível em: https://www.pmgacademy.com/produto/curso-online-iso-27001-foundation-isfs/?utm_campaign=GoogleAds&utm_source=ISO27001Foundation&gclid=EAIaIQobChMI nIKa182V8wIVwYORCh0hGA9zEAAYASAAEgIzSvD_BwE Acesso em: 20 set. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 26 ago. 2021.

BRASIL. **Lei nº 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 Acesso em: 17 ago. 2021.

CÓDIGO DE DEFESA DO CONSUMIDOR. **Decreto Presidencial nº 2.181**, de 20 de março de 1997, Brasília, DF, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso em: 01 nov. 2021.

FERRAREZ, Rodrigo. **Como descartar dados sensíveis e prevenir cibercrimes diante da LGPD?** Infor Channel**.** Disponível em: https://inforchannel.com.br/2020/11/16/como- descartar-dados-sensiveis-e-prevenir-cibercrimes-diante-da-lgpd/ Acesso em: 20 set. 2021.

FILHO, Rodolfo Pamplona e JUNIOR, Vicente Vasconcelos Coni. A Lei Geral de Proteção de Dados e seus impactos no Direito do Trabalho. **Revista Direito UNIFACS – Debate Virtual**, 2020. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/6744> Acesso em: 30 out. 2021.

GARCIA, Lara Rocha. **Lei geral de proteção de dados (LGPD)**: guia de implementação. 1 ed., São Paulo: Blucher, 2020. Acesso em: 31 out. 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**, Editora RT: São Paulo, 2019, p. 231. Acesso em: 2 de nov. 2021.

MALDONADO, Viviane Nóbrega *et al*. **LGPD**: lei geral de proteção de dados pessoais comentada. 3 ed., São Paulo: Thomson Reuters Brasil, 2021. Acesso em: 31 out. 2021.

MARINHO, Fernando. **Os 10 mandamentos da LGPD**: como implementar a Lei Geral de Proteção de Dados em 14 passos. 1 ed., São Paulo: Atlas, 2020. Acesso em: 31 out. 2021.

MENDES, Laura Schertel; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de direito do consumidor**, v. 120, p. 555, 2018. Acesso em: 2 nov. 2021.

SILVA, De Plácido e. **Dicionário Jurídico Conciso**. 1. ed. Rio de janeiro: Editora Forense, 2008. 749p. Acesso em: 31 out. 2021.

SILVA, Patrick Lendl**. Fatos jurídicos**: teoria e prática. Porto Alegre: Verbo Jurídico, 2011. 261 p. Acesso em: 2 nov. 2021.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679**. Bruxelas, Bélgica: Parlamento Europeu,2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 Acesso em: 22 ago. 2021.

VENOSA, Silvio Salvo. **Direito Civil**. 12 ed. São Paulo: Atlas, 2012. v.1. Acesso em: 2 nov. 2021.