

FUNDAÇÃO GETULIO VARGAS

Escola de Direito de São Paulo

Theodoro Luiz Liberati Silingovschi

CONTRATOS DE LICENÇA DE USO DE *SOFTWARE* “*ENTERPRISE RESOURCE PLANNING*” E A LEI GERAL DE PROTEÇÃO DE DADOS: A REESTRUTURAÇÃO CONTRATUAL COM BASE NA METODOLOGIA *PRIVACY BY DESIGN*

São Paulo

2024

Theodoro Luiz Liberati Silingovschi

CONTRATOS DE LICENÇA DE USO DE *SOFTWARE* “*ENTERPRISE RESOURCE PLANNING*” E A LEI GERAL DE PROTEÇÃO DE DADOS: A REESTRUTURAÇÃO CONTRATUAL COM BASE NA METODOLOGIA *PRIVACY BY DESIGN*

Versão final do trabalho de conclusão apresentado no Programa de Pós-Graduação *Stricto Sensu* na linha de Direitos dos Negócios na Fundação Getulio Vargas.

Orientadora: Profa. Dra. Mônica Steffen Guise

São Paulo

2024

Silingovschi, Theodoro Luiz Liberati.

Contratos de licença de uso de software “Enterprise Resource Planning” e a Lei Geral de Proteção de Dados : a reestruturação contratual com base na metodologia Privacy by Design / Theodoro Luiz Liberati Silingovschi. - 2024.

87 f.

Orientador: Mônica Steffen Guise Rosina.

Dissertação (mestrado profissional) - Fundação Getulio Vargas, Escola de Direito de São Paulo.

1. Proteção de dados - Legislação. 2. Lei Geral de Proteção de Dados Pessoais (LGPD). 3. Sistemas de Informação Gerencial. 4. Tecnologia da Informação. 5. Programas de computador - Licenças. I. Rosina, Mônica Steffen Guise. II. Dissertação (mestrado profissional) - Escola de Direito de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 343.45

THEODORO LUIZ LIBERATI SILINGOVSKI

CONTRATOS DE LICENÇA DE USO DE *SOFTWARE* “*ENTERPRISE RESOURCE PLANNING*” E A LEI GERAL DE PROTEÇÃO DE DADOS: A REESTRUTURAÇÃO CONTRATUAL COM BASE NA METODOLOGIA *PRIVACY BY DESIGN*

Dissertação apresentada à Escola de Direito de São Paulo da Fundação Getúlio Vargas, como requisito para obtenção do título de Mestre em Direito.

Área de concentração: Direito dos Negócios

Data de aprovação: __/__/____

Banca examinadora:

Profa. Dra. Monica Steffen Guise Rosina
(Orientadora)
FGV Direito SP

Prof. Dr. Osny da Silva Filho
FGV Direito SP

Prof. Dr. Carlos Augusto Liguori Filho
Professor Convidado

RESUMO

O presente trabalho de dissertação tem como escopo tratar dos impactos que a Lei Geral de Proteção de Dados trouxe aos sistemas ERP “*Enterprise Resource Planning*” utilizados no comércio varejista, considerando, necessariamente, a extensa quantidade de dados armazenados pelo mesmo. Buscou-se, a partir desta análise, definir os impactos mais relevantes que demandem a necessidade de alteração da estrutura do *software* ERP e também do seu respectivo contrato de licença de uso, buscando garantir conformidade com a Lei Geral de Proteção de Dados e conferir mais segurança jurídica para os integrantes da relação contratual, isto é, Licenciante e Licenciado. Após a consolidação da análise da legislação em questão e de uma profunda abordagem sistêmica do *software* em foco, passou-se a analisar o conceito metodológico empregado no *General Data Protection Regulation* (GDPR) denominado *Privacy by Design*, sua aplicabilidade no Direito Brasileiro, em específico, na Lei Geral de Proteção de Dados, e a efetividade da utilização de seus preceitos e fundamentos como norte da reestruturação do sistema e, por consequência, do modelo contratual adotado pela Licenciante. Procurou-se não apenas analisar o conceito e aplicá-lo à um contrato de licença de uso na prática, mas aprofundar o estudo para extrair modelos de boas práticas seguros e eficientes para sua reestruturação, apontando as incompatibilidades encontradas e divulgando o produto gerado deste estudo, como um modelo de boas práticas de implementação de um programa de conformidade com a legislação.

Palavras-chave: Lei Geral de Proteção de Dados; Conformidade; Sistemas ERP; Enterprise Resource Planning software; Empresa Licenciante; Empresa Licenciada; Contratos de licença de uso; Empresa Licenciante; Empresa Licenciada; Comércio varejista; *Privacy by Design*; Reestruturação contratual.

ABSTRACT

The present paper has the scope to deal with the impacts that the Brazilian General Data Protection Law brought to the Enterprise Resource Planning systems used in the retail commerce business, necessarily considering the extensive amount of data stored by it. Based on this analysis, we sought to define the most relevant impacts that require the need to change the Enterprise Resource Planning software structure and also its respective license assignment agreement, seeking to ensure compliance with the Brazilian General Data Protection Law and provide more legal certainty for the members of the contractual relationship, that is, Licensor and Licensed. After consolidating the analysis of the legislation in question and a deep systemic approach to the software in focus, the methodological concept used in the European General Data Protection Regulation (GDPR) called Privacy by Design was analyzed, its applicability in Brazilian Law, in particular, in the General Data Protection Law, and the effectiveness of the use of its precepts and foundations as a guide to the restructuring of the system and, consequently, of the contractual model adopted by the Licensor. It was sought not only to analyze the concept and apply it to a license assignment agreement in practice, but to deepen the study to extract safe and efficient models of good practices for its delivery, to aspire to the incompatibilities met and to publicize the product generated from this study as a model of good practices for implementing a compliance program with legislation.

Keywords: General Data Protection Law; Compliance; ERP systems; Enterprise Resource Planning software; License assignment agreements; Licensing Company; Licensed Company; Retail business; Privacy by Design; Contractual restructuring.

SUMÁRIO

1	INTRODUÇÃO.....	5
2	A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NOS CONTRATOS DE LICENÇA DE USO DE <i>SOFTWARES</i> “ERP”	11
2.1	Lei Geral de Proteção de Dados: Da normatização à regulação no setor privado.....	11
2.2	Contratos de licença de uso de <i>softwares Enterprise Resource Planning</i> (ERP).....	19
2.3	Contextualização da estrutura do software <i>Enterprise Resource Planning</i> (ERP).....	24
2.4	Análise dos principais impactos da Lei Geral de Proteção de Dados nos contratos de licença de uso de software ERP: Uma análise do setor varejista.....	29
3	A METODOLOGIA <i>PRIVACY BY DESIGN</i> E SUA APLICABILIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS.....	38
3.1	Definições, conceitos e princípios do <i>Privacy by Design</i>	38
3.2	A aplicabilidade da metodologia <i>Privacy by Design</i> na Lei Geral de Proteção de Dados.....	45
4	O SOFTWARE ERP E SUA CORRESPONDENTE REESTRUTURAÇÃO CONTRATUAL VISANDO CONFORMIDADE COM A LGPD COM BASE NA APLICAÇÃO DA METODOLOGIA <i>PRIVACY BY DESIGN</i>.....	50
4.1	A viabilidade da utilização do conceito metodológico <i>Privacy by Design</i> no software ERP e em seu respectivo contrato.....	50
4.2	A aplicação da metodologia <i>Privacy by design</i> na operação e nos contratos de licença de uso de software ERP no setor varejista – Proposições e medidas em busca da conformidade.....	56
5	CONCLUSÃO.....	77
	REFERÊNCIAS	82

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados entrou em vigor em setembro de 2020 tendo como objetivo principal a regulamentação da proteção de direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, através do tratamento de dados nos meios físicos e digitais.

Com disposições descritivas, a Lei Geral de Proteção de Dados atribuiu novos conceitos ao mercado, imputando direitos, obrigações, responsabilidades e sanções aos personagens interligados à disciplina da proteção de dados.

Por ter uma abrangência largamente definida sobre sua regulamentação, isto é, pura e simplesmente a atividade de tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica, de direito público ou privado, toda e qualquer empresa, independentemente de seu tamanho e seguimento, que necessariamente trate dados, sofrerá implicações e também a necessidade de adequação, até mesmo porque quase todas as empresas lidam, ao menos de forma básica, com dados pessoais.

Dentro dos procedimentos de adequação à Lei Geral de Proteção de Dados, tem-se muito claro pela maciça maioria dos profissionais da área, que os instrumentos contratuais sofrerão necessários reajustes e readaptações, muito por conta dos princípios que regem a atividade de tratamento de dados pessoais, pelos requisitos legais trazidos para se justificar o tratamento de dados pessoais e, principalmente, pela ampla gama de direitos que foram garantidos aos titulares destes dados.

A primeira problemática se desenvolve a partir deste ponto. Na prática, a atuação jurídica em empresas na elaboração e remodelação dos processos internos e instrumentos contratuais visando adequação à Lei Geral de Proteção de Dados, principalmente sobre a definição de agentes de tratamento, delimitação de obrigações destes agentes, definição de suas responsabilidades e limitações, bem como, sobre a definição de uma política cooperativa entre os *players* do negócio jurídico, vem trazendo desafios aos profissionais do direito, exigindo inovação e propostas personalizadas e dinâmicas.

Na atual era 4.0 (era digital), a maioria das empresas já está estruturalmente informatizadas, isto é, dispõem de meios telemáticos, virtuais e digitais para desenvolver o

seu negócio, seja em relação ao seu próprio produto ou como meios acessórios, na parte administrativa, contábil, de recursos humanos e comercial.

Nesta linha, com a quantidade de informações e dados de diversos setores que são acumulados pela empresa para os mais variados objetivos, desde o cumprimento de uma obrigação tributária de um órgão fiscalizatório até a melhoria em termos de eficiência de controle de estoque, surge a necessidade de facilitar o seu acesso e manuseio, o que indiscutivelmente é melhor alcançado através dos meios digitais.

Assim, o escopo de estudo do trabalho tem plena relevância prática para o profissional que atua com direito contratual e assessoria empresarial atendendo empresas de tecnologia da informação e de sistemas, uma vez que apresentará um relatório de impactos sobre as questões que principalmente se busca tutelar nos contratos, como direitos, responsabilidades e obrigações e abordará a melhor temática, à luz do conceito de *Privacy by design*, na remodelação destes instrumentos contratuais.

Este trabalho se aprofundará justamente na análise dos contratos dos sistemas acessórios, isto é, aqueles que auxiliam a empresa de algum modo organizacional, viabilizando uma correta estrutura contábil, comercial, de recursos humanos e administrativa, buscando sempre a maximização da eficiência operacional, são os conhecidos sistemas “*ERP - Enterprise Resource Planning*”, em português, Sistema integrado de planejamento de recursos empresariais.

Em outro recorte, necessário para direcionar o leitor para um ambiente que facilite o entendimento do funcionamento do sistema, e, em decorrência, do manuseio do instrumento contratual, o trabalho abordará a problemática da Lei Geral de Proteção de Dados, já posta acima, a partir de uma análise dos sistemas de ERP quando licenciadas às empresas do comércio varejista.

Com o passar do tempo, a gestão de uma empresa de qualquer setor de atuação, se mostrou mais segura, organizada e efetiva através dos meios digitais. Percebendo essa mudança na administração empresarial, surgiram várias empresas especializadas em sistemas informatizados de gestão de recursos e planejamento, são os chamados *Enterprise Resource Planning Softwares*, que passaram a ser utilizados em larga escala por empresas de médio e grande porte, principalmente do setor varejista, considerando a necessidade de controle de

estoque, de política de preços e práticas de fidelização de clientes através de promoções e demais programas de fidelidade.

Para este tipo de estabelecimento, na era digital, buscando esse meio organizacional digital para melhor performar em eficiência operacional, muitas empresas buscam sistemas ERP informatizados prontos para atenderem essa demanda, uma vez que a criação de um sistema próprio, além de ser muito custoso, também envolve a contratação de profissionais específicos e técnicos para tanto, fazendo com que a alternativa mais viável seja, de fato, a contratação de uma licença de uso de *software* já desenvolvida e oferecida por uma empresa do ramo.

Segundo a Revista Valor Investe, somente em *softwares* de ERP foram investidos R\$ 14 bilhões em 2020, um crescimento de 25% nos investimentos das empresas em relação a 2019. Isso indica uma migração acelerada dos negócios para o ambiente digital, o que tem forte implicação do ponto de vista da Lei Geral de Proteção de Dados.¹

Neste contexto, o uso de *softwares* ERP em empresas do setor comercial, vem se mostrando quase que essencial na era digital, seja pela facilidade no manuseio dos dados, até mesmo pela necessidade de adequação ou pela melhor operacionalização de seu negócio. Essa modalidade de *software* ERP parte da funcionalização básica de inserção de dados pelo usuário, que por sua vez é o Licenciado, cliente da empresa licenciante, ou seja, aquela que lhe concedeu a licença de uso do *software*.

Acontece que não só os dados deste Licenciado ficam armazenados no banco de dados correspondente ao *software* de ERP, mas também os dados ali inseridos por este em relação ao seu próprio cliente, que no caso do comércio varejista, é um consumidor que adquiriu algum produto, funcionário ou trabalhador autônomo que lhe preste algum serviço, ou um fornecedor de alguma outra empresa, organização ou cooperativa.

Desta forma, a empresa licenciante, detentora da concessão do *software* ERP, detêm em seus bancos de dados, o acesso e possibilidade de alteração destes dados. Daí decorre a necessidade de um cuidado especial com o manuseio do *software* licenciado e de sua

¹ BRAUN, Daniela. Receita de software alcançou R\$ 44 bilhões no Brasil em 2020, diz consultoria. Revista Valor Investe Empresas. 2021. Disponível em <https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/05/07/receita-de-software-alcancou-r-44-bilhoes-no-brasil-em-2020-diz-consultoria.ghtml> Acesso em: 11 dez. 2022.

correspondente, e também necessária, estruturação jurídica contratual no ato de seu licenciamento para uso, a fim de delimitar responsabilidades, obrigações, custos, suporte, etc.

Por mais que a relação contratual e a operação do varejo gere desdobramentos em termos de obrigações e responsabilidades, o que também será abordado no trabalho, é importante ressaltar que o foco quanto ao agente da operação não será apresentar proposições de conformidade ao Licenciado, mas sim ao Licenciante, isto é, o detentor da tecnologia cedida via instrumento contratual.

A partir destes contornos fáticos, o trabalho abordará a possibilidade e os benefícios de se partir da aplicação da metodologia *Privacy by Design* em referida reformulação contratual pós regulação da Lei Geral de Proteção de Dados, aliada à possibilidade/necessidade de alteração do *software* ERP regido por este contrato, foi necessário traçar alguns elementos basilares para sustentar as reflexões jurídicas subsequentes.

Verifica-se, assim, extrema relevância e importância neste estudo, principalmente para se (i) entender se há a necessidade de alteração dos instrumentos, (ii) qual é a melhor forma de se alterar o contrato de licença de software, (iii) como garantir ao empresário licenciante as melhores garantias contratuais e uma delimitação de responsabilidades respaldada na melhor prática, e (iv) analisar se o conceito metodológico *Privacy by design* importado da GDPR (General Data Protection Regulation), regulamentação da União Europeia sobre Proteção de dados, pode ser utilizado e como pode ser utilizado como molde na regulamentação contratual destas empresas.

Em segundo ponto, ainda no segundo capítulo, buscando uma análise concreta sobre as funcionalidades básicas dos *softwares* ERP nas empresas do comércio, será analisada formalmente sua estrutura informatizada a partir de alguns exemplos de empresas do comércio, necessário como recorte, passando também pelo seu correspondente sistema jurídico composto necessariamente pelo contrato, seu objeto, desdobramentos, obrigações e responsabilidades. Será exposto o ambiente concreto da utilização do software e sua contextualização fática, visando moldar bem o contexto da pesquisa.

Em um terceiro momento, serão contrapostas as análises exploratórias acerca do aprofundamento sobre a Lei Geral de Proteção de Dados e a contextualização sobre os

contratos de licença de uso de *software* ERP, buscando o apontamento de seus principais impactos, o que será exposto de forma reflexiva, também a partir de exemplos práticos na operação de licença junto à empresa de comércio varejista.

A definição de medidas de impacto, necessidade de remodelação dos sistemas ERP e sua correspondente reestruturação contratual, a partir da vigência da Lei Geral de Proteção de Dados, é de extrema relevância teórica para embasar, também sob um pretexto reflexivo após prática exploratória, a contextualização da metodologia do *privacy by design* como base destas alterações.

Visando entender a aplicação da *Privacy by design* no GDPR e na LGPD para depois embasar os seus pontos de impacto, no terceiro capítulo, o trabalho voltará à sua temática exploratória para discorrer, após profunda análise doutrinária, especificamente de artigos e trabalhos internacionais e análise do GDPR (*General Data Protection Regulation*) - legislação Europeia sobre a proteção de dados – voltados à metodologia do *Privacy by design*, seu contexto histórico, conceito, princípios, aplicação na Lei Geral de Proteção de Dados e possibilidade de ser utilizado como um norte na política empresarial visando a plena conformidade regulatória.

Em último plano, no quarto e último capítulo, de ímpar importância para responder a parte final da questão central de pesquisa, isto é, se buscando a conformidade com a LGPD, é possível reestruturar o contrato de licença de software ERP em uma operação do comércio varejista com base na metodologia *Privacy by design* e quais são os ganhos atrelados ao uso desta metodologia.

As análises exploratórias mais acima descritas serão postas em reflexão para a discussão acerca dessa possibilidade da reformulação do *software* ERP e a correspondente reestruturação contratual com base na aplicação da metodologia *privacy by design* do ponto de vista da operação de licença à uma empresa licenciada atuante em comércio varejista, observadas as suas peculiaridades.

A partir da contextualização fática do problema trazida acima, será necessário estudar a necessidade de alterações operacionais técnicas e contratuais, definir quais são os impactos gerais da entrada em vigor da Lei Geral de Proteção de Dados nos contratos de licença de uso de softwares ERP, para que seja possível buscar a questão central de pesquisa

do trabalho que é: Buscando a conformidade com a LGPD, é possível reestruturar o contrato de licença de uso de software ERP em uma operação do comércio varejista com base na metodologia *Privacy by design*? Quais são os ganhos atrelados ao uso desta metodologia? Em um primeiro momento, já no capítulo dois, será feito um necessário aprofundamento teórico acerca de aspectos relevantes sobre a regulação, princípios e fundamentos da Lei Geral de Proteção de Dados. Isso dará embasamento para que seja compreendido o impacto que a lei trouxe em todo o ordenamento jurídico, mas, em específico, na estrutura jurídica do contrato de licença e da operação do *software* ERP, o que mais adiante será abordado.

O trabalho será exposto em formato de artigo científico, sendo bem descritos os conceitos, fundamentos e impactos das estruturas em estudo, passando obrigatoriamente, pela Lei Geral de Proteção de Dados, contratos de licença de uso de *softwares* ERP e a metodologia *Privacy by design*, buscando-se, a partir deste estudo, desenvolver a melhor prática empresarial de reestruturação contratual no ato da implementação e adequação à Lei Geral de Proteção de Dados.

A questão central de pesquisa e a busca do possível produto deste trabalho, o que concretamente se buscará no capítulo quatro, será abordado através de reflexões e proposições a partir do estudo dos conceitos e princípios atribuídos pela metodologia *privacy by design*, e como os mesmos, de alguma forma, conseguem contribuir para um seguro e eficiente programa de reformulação contratual e sistêmica da operação da licença.

2 A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NOS CONTRATOS DE LICENÇA DE USO DE *SOFTWARE* “ERP”

É inegável que a entrada em vigor da Lei Geral de Proteção de Dados tenha causado uma considerável movimentação e reformulação no mercado. Grandes empresas que se associam e se relacionam com Multinacionais, por conta da entrada em vigor da *General Data Protection Regulation* - a legislação sobre proteção de dados Europeia - já vinham, desde 2016, se adequando mesmo que minimamente à regulação imposta pelo tema.

A OCDE (Organização para a Cooperação e Desenvolvimento Econômico), já em 2016, apontava a necessidade das empresas em seguir regras de privacidade: “Muitas organizações ainda tendem a abordar a privacidade apenas como uma questão de conformidade legal, e não também como um risco econômico e social, e uma questão estratégica que pode fornecer a elas uma vantagem competitiva no mercado”.²

Muito se discutiu e ainda vem sendo discutido sobre a Lei Geral de Proteção de Dados nos últimos dois anos. Embora sancionada em 14 de agosto de 2018, houveram diversos debates no Congresso Nacional para preencher a lacuna legislativa sobre o tema interligado entre a proteção de dados e a privacidade, o que, política e economicamente teve forte reflexo da legislação Europeia (GDPR) e dos agentes econômicos transnacionais.

Após muito debate, alguns ajustes legislativos e mais de dois anos depois, entrou em vigor a Lei Geral de Proteção de Dados, precisamente em 18 de setembro de 2020. Deixando de lado alguns de seus aspectos polêmicos e contexto histórico em que está inserida, é necessário para o desenvolvimento deste trabalho ao menos um estudo basilar sobre suas características e conceitos.

2.1 Lei Geral de Proteção de Dados: Da normatização à regulação no setor privado

É imprescindível que se firme o contexto do quão impactante a Lei Geral de Proteção de Dados foi em termos de estrutura jurídica, isto é, a definição de novos conceitos,

²OECD. "Managing Digital Security and Privacy Risk". *OECD Digital Economy Papers*, Paris, n. 254, França, 2016. DOI: <https://doi.org/10.1787/5j1wt49ccklt-en>

fundamentos e princípios, o que acabou gerando amplos debates sobre o seu efetivo cumprimento, responsabilizações e consequências, tanto econômicas, quanto jurídicas.

A partir da conscientização sobre o seu impacto no ordenamento jurídico e no mercado, no aspecto geral, pode-se partir para o afunilamento buscado neste trabalho, que é, em primeiro ponto, os seus reflexos em uma certa modalidade de contrato civil, a licença de software, especificamente para empresas do comércio varejista, e em um segundo momento, após um melhor entendimento sobre os seus reflexos na operação da empresa, sobre a viabilidade da aplicação de um conceito metodológico como base na estruturação da objetivada conformidade da Lei.

Pois bem. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) tem como principal objetivo a regulamentação da proteção de direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, através do tratamento de dados nos meios físicos e digitais.

Partindo deste escopo, a Lei Geral de Proteção de Dados se divide em mais de 350 dispositivos, se considerados os artigos, incisos e parágrafos. Trata-se de uma Lei de tamanho considerável que trata de diversos assuntos e temas delicados, impondo definição de agentes, responsabilidades e até mesmo sanções.

Antônio Carlos Negrão discorre que a Lei Geral de Proteção de Dados introduz no ordenamento jurídico brasileiro, um sistema de regras abrangente e transversal, que incidirá sobre praticamente todos os setores da economia, afetando principalmente o relacionamento com o cliente.³

O artigo 2º de referida lei, determina os fundamentos da disciplina de proteção de dados, tema central da mesma, relacionando 7 (sete) incisos, veja-se:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

³ NEGRÃO, Antonio Carlos. Economia Digital, Proteção de Dados e Competividade. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020. p. 30.

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.⁴

Quando se dispõe sobre fundamentos de uma disciplina, molda-se toda uma base objetiva ligada à regulamentação, fixando-se o que se espera alcançar em termos de efeitos gerais. Para se regular proteção de dados, por exemplo, deve-se trazer como fundamento principal o respeito à privacidade.

A disciplina de proteção de dados deve ter o escopo preliminar e fundamental de garantir o respeito da privacidade, isto porque antes de adentrar outras disciplinas que também são fundamentais, como por exemplo, a liberdade de expressão (art. 2º, III, Lei Geral de Proteção de Dados) ou o desenvolvimento econômico (art. 2º, V, Lei Geral de Proteção de Dados) deve-se, necessariamente, garantir o respeito e a segurança do que é privado, do que é de cada indivíduo.

Daí surge o primeiro e talvez mais importante conceito que será abordado mais adiante no capítulo sobre o conceito metodológico do *Privacy by Design – Respect for User Privacy – Keep it User-Centric*⁵ – ou seja, o respeito pela privacidade do titular de dados no centro da relação.

É necessário respeitar e garantir a privacidade do titular de dados e o Estado deve garantir ao indivíduo o direito de dispor ou não de sua privacidade e até que ponto o fazer, tal premissa encontra-se na Constituição Federal, inclusive, no art. 5º, inciso X, considerado como cláusula pétrea (Artigo 60, 4º, inciso IV, CF⁶) pela sua alta relevância. O inciso X da Constituição Federal descreve necessariamente a vida privada, cujo conceito é sinônimo do que é privado, oriundo da privacidade, tratando-a como inviolável.

Luiz Alberto David Araujo e Vidal Serrano Nunes Júnior descrevem que por privacidade, deve-se entender os níveis de relacionamento social que o indivíduo

⁴ BRAIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

⁵ CAVOUKIAN, Ann. **Privacy by Design** The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada. Published May 2010. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em: 01 fev. 2022.

⁶ BRASIL. Constituição (1988). **Constituição [da] República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

habitualmente mantém oculto ao público em geral”, isto é, “A privacidade resguarda o indivíduo da publicidade.⁷

Mas como, essencialmente, o direito à proteção de dados, sob um aspecto da Lei Geral de Proteção de Dados está relacionado à privacidade? É fácil visualizar uma ampla abordagem de meios quando se discute o direito à privacidade, mas em termos de proteção de dados e na regulamentação descritiva da Lei Geral de Proteção de Dados, a privacidade está intimamente conectada ao tratamento de dados pessoais nos meios físicos e digitais, por pessoas naturais, ou seja, ainda tratando de uma abordagem ampla.

De um aspecto geral, todo dado pessoal deve ser tratado com a devida privacidade, observada, por evidencia, a especificidade e mais segurança aos dados chamados sensíveis. Aqui há uma importante distinção entre o direito à privacidade e o direito à proteção de dados, o que, segundo Rafael Mafei Rabelo Queiroz:

Ao contrário do direito à privacidade, o direito à proteção de dados não faz, em princípio, um filtro substantivo sobre a qualidade do dado para decidir se ele está ou não em seu escopo: se é dado pessoal, interessa ao direito da proteção de dados pessoais, ainda que não seja sensível à privacidade do titular.⁸

Apesar desta constatação, é salutar que mesmo sobre o dado pessoal que necessariamente não seja sensível à privacidade do titular, haja uma tutela fundamentada pelo respeito à privacidade. A propósito, a Lei Geral de Proteção de Dados é explícita em seu art. 7º, parágrafo 3º, ao determinar que mesmo dados de acesso público, sendo dados pessoais, devem considerar a finalidade, a boa-fé e o interesse público que motivaram sua disponibilização, que como regra não passa, por óbvio, por qualquer finalidade comercial.⁹

Conclui-se, à vista das exposições acima, que ao mesmo tempo em que o direito à proteção de dados não se limita a ser um aspecto do direito à privacidade, o segundo necessariamente tutela o fundamental aspecto do primeiro. Destas assertivas, decorre a importância da noção de *Privacy by Design*, determinando que a segurança e o sigilo de dados

⁷ ARAUJO, Luiz Alberto David; NUNES JUNIOR, Vidal Serrano. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2005, p. 139-140.

⁸ QUEIROZ, Rafael Mafei Rabelo. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. Lei Geral de Proteção de Dados Pessoais, São Paulo. **Revista do Advogado AASP**, n. 144, p. 19, nov., 2019.

⁹ *Ibid.*, p. 19.

devem ser elementos centrais na concepção, desenvolvimento, aplicação e avaliação de produtos e serviços.¹⁰

Além dos fundamentos da Lei Geral de Proteção de Dados, o seu primeiro capítulo também apresenta os conceitos que estão abrangidos em 19 (dezenove) incisos no art. 5º, onde são colocados de forma descritiva alguns importantes aspectos para se compreender a lei e os seus desdobramentos.

No mesmo capítulo, também estão descritos os princípios da legislação, que são divididos nos 10 (dez) incisos do art. 6º, além da disposição sobre a observância da boa-fé, um dos princípios fundamentais do direito privado brasileiro, que fora importado e já disposto no caput.

Para um melhor entendimento quando da discussão sobre os impactos da Lei Geral de Proteção de Dados nos contratos e, em específico, nos contratos de licença de software *ERP*, é essencial à disposição sobre alguns conceitos postos no art. 5º, como dado pessoal, titular, controlador, operador e tratamento, veja-se:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

(...)

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

(...)

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;¹¹

¹⁰ MEDON, Filipe. Resenha à obra Lei Geral de Proteção de Gados Pessoais e suas repercussões no direito brasileiro, de Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (coord.). São Paulo: Thomson Reuters Brasil, 2019. **Revista Brasileira de Direito Civil RBDCivil**, Belo Horizonte, v. 23, p. 195-203. jan./mar. 2020. DOI: 10.33242/rbdc.2020.01.009.

¹¹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

Sintetizando todos estes conceitos em um contrato por um cliente, como exemplo da importância de tais definições, temos a seguinte disposição operacional: O titular, possuidor de dados pessoais, contrata com uma empresa que é um agente de tratamento. Para executar a operação do contrato, a empresa, que poderá figurar como operadora ou controladora dos dados deste titular, necessitará de uma base legal de tratamento destes dados, ao passo que, a execução da operação do contrato necessitará, na maioria das vezes, passar pelo tratamento desses dados. Em síntese, de um panorama geral de um contrato, é essa a relação primária que é atingida pela Lei Geral de Proteção de Dados.

Isto é, antes da entrada em vigor de referida lei, não havia a necessidade desta base legal para o tratamento de dados e para a execução da operação do contrato, e daí a primeira mudança que causou as primeiras discussões no âmbito empresarial, principalmente do enquadramento da operação nas hipóteses de base legal de tratamento.

No âmbito dos contratos de licença de software de *ERP* a relação da operação é um pouco mais complexa, já que tratamos de um sistema que tem como condão armazenar e organizar – como ação de tratamento – não só os dados de uma empresa, mas também do cliente desta empresa, mas isso será mais aprofundado nos próximos tópicos.

Além das definições e conceitos, no âmbito do tratamento de dados pessoais, a Lei Geral de Proteção de Dados delimita que os agentes de tratamento, ao tratarem dados, deverão observar uma série de princípios, estes que estão descritos no art. 6º.

Cada atividade de tratamento de dados realizado por uma empresa em sua operação, deverá observar as disposições acima expostas e não poderão ferir o seu conteúdo. Mas não é só, além da observância dos princípios com base nos fundamentos propostos, o tratamento de dados só poderá ser realizado em algumas hipóteses, estas que são expostas já no capítulo II da Lei Geral de Proteção de Dados, a partir do art. 7º.

O mencionado dispositivo dispõe que o tratamento de dados pessoais só poderá ocorrer em algumas hipóteses, sendo elencadas as 10 (dez) delas em seus respectivos incisos, sendo os relevantes para o trabalho, os incisos II - para o cumprimento de obrigação legal ou regulatória pelo controlador; e V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

A questão do consentimento não tem muita relevância para o escopo do trabalho, considerando a realidade fática bilateral entre Licenciante-Contratado e Licenciada-Contratante, sendo evidente, ainda, que a sociedade moderna evoluiu para um nível de relação em que formalizamos contratos com o simples toque de um botão no *smartphone*, e daí a dificuldade de se garantir uma forma de consentimento livre e inequívoco sem que isso esbarre em uma cláusula de *take-it-or-leave-it choice*, aquela em que o usuário ou aceita todos os termos daquele produto e/ou serviço ou simplesmente não pode ter acesso ao mesmo.

Daí decorrem as grandes discussões que já tiveram palco no âmbito legislativo e que agora estão em cena na seara da regulação específica, havendo claramente uma necessidade de adequação para cada setor econômico e empresarial.

Desta considerável gama de imposições legislativas, algumas empresas viram a necessidade de alteração do modo como executam suas operações, isso demonstra o tanto que a Lei Geral de Proteção de Dados impactou o setor empresarial. Não foi diferente com as licenciadas de *softwares* “ERP”, ao passo que os impactos também foram significativos, o que será melhor abordado nos tópicos próximos.

Partimos de um ambiente um tanto quanto desregulado, até mesmo porque anteriormente o Marco Civil da Internet (Lei nº 12.965/2014) e o Código de Defesa do Consumidor (Lei nº 8.078/1990) traziam algumas disposições de forma não específica sobre o tema, para uma vasta regulação jurídica que não faz distinção setorial, econômica ou de níveis empresariais.

Percorrendo itens principais da Lei Geral de Proteção de Dados, depois de discorrer sobre os fundamentos, princípios e conceitos, importante analisar alguns institutos faltantes para um pano de fundo coerente com a abordagem que será feita mais adiante.

A forma como está estabelecido o art. 18, que trata dos direitos dos titulares, deixa clarividente que os dados são do titular e encontram-se na posse – apenas enquanto perdurar o tratamento – pelo agente operador ou controlador. Isto é, os direitos ali descritos, passam por todas as garantias que o titular pode ou não fazer com os seus dados, o que, por evidência, deverá de alguma forma ser garantido pelo agente de tratamento. Daí decorre uma relevante observação em termos de conformidade com a Lei Geral de Proteção de Dados, ou seja, a

empresa passará a ter a obrigação de garantir todos esses direitos ao titular, mudando a sua operação, inclusive, se necessário.

Mais adiante, ainda em temas relevantes para o desenrolar deste trabalho, tratamos dos artigos 37 e seguintes, onde se descreve mais detalhadamente a figura do operador e do controlador, principalmente quanto à obrigação de manter registro das operações de tratamento de dados pessoais que realizarem.¹²

Já em termos de responsabilidade e ressarcimento de danos, o artigo 42 dispõe: *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.*¹³

Já em caso de desrespeito às normas e imposições da Lei Geral de Proteção de Dados, os agentes de tratamento poderão, em razão das infrações cometidas, se sujeitarem a sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), que variam entre multa de 2% (dois por cento) do faturamento da pessoa jurídica de direito privado até R\$ 50.000.000,00 (Cinquenta milhões de reais) por infração.

A ANPD pode ainda sancionar a empresa aplicando multa diária, publicização da infração após apuração e confirmação de sua ocorrência, eliminar os dados a que se referem a infração e suspender o exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, o que pode acabar por inviabilizando a sustentabilidade do negócio.

Por mais que a ANPD possa sancionar as empresas, a partir de uma regulação específica por este órgão, o que vem ocorrendo também por consultas públicas e emissão de resoluções pontuais, o que se observa é que microempresas, empresas de pequeno porte e empresas que tem tratamento mínimo de dados, dificilmente serão foco de autuações e fiscalizações mais abrangentes e incisivas.

¹² BRASIL. Art. 37 - Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

¹³ *Ibid.*

Para o objeto deste trabalho, o que se deve ter em mente é que o estudo abordará a empresa licenciante do software, detentora de considerável quantidade dados, e não da licenciada, comércio varejista com atuação mais local.

Não obstante a ANPD ter sido criada para zelar pela proteção dos dados pessoais, nos termos da Lei Geral de Proteção de Dados (art. 55-J), além de outras diversas incumbências, outros órgãos fiscalizadores e instituições como Ministério Público ou PROCON, podem e já estão utilizando referidos ditames legais para aplicar multas, sanções, fundamentar ações, dentre outros.

É inegável, portanto, que a gama de disposições legais trazidas pela Lei Geral de Proteção de Dados, além de preencherem uma lacuna legislativa e garantirem mais direitos ao titular de dados, também trouxe enormes incumbências às empresas em termos de adequação, seja do ponto de vista jurídico ou técnico. Nos contratos de licença de software *ERP*, estas incumbências tem relevância ímpar, o que veremos a seguir.

2.2 Contratos de licença de *softwares Enterprise Resource Planning (ERP)*

A Lei do *Software* (Lei nº 9.609/1998) dispõe sobre as características de um programa de computador, a proteção de seus direitos autorais, seu registro e traz outras providencias sobre garantias do usuário, a forma de transferência da tecnologia e também penalidades pelo seu mau uso.

É certo que a Lei do *Software* foi criada em um ambiente quase que inaugural em termos de programas de computador, uma vez que em 1998, o setor de informática iniciava os seus passos rumo ao contexto tecnológico que hoje nos encontramos.

Não obstante, referida lei atende consideravelmente, em conjunto com outras importantes disposições legais, todas as amarras necessárias para se tutelar referido bem jurídico.

A Lei do Software dispõe em seu art. 1º que:

Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos

periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.¹⁴

O art. 9º da lei em questão, dispõe que o uso de programa de computador no país será objeto de contrato de licença.¹⁵ Ou seja, a imposição legislativa deixa claro que a transferência da tecnologia contida no *software* se opera através do contrato de licença de uso.

Referidos instrumentos podem ser firmados em caráter perpétuo, ocasião em que a concessão da licença é feita através de uma compra definitiva, ou em caráter provisório, ocasião em que a concessão da licença se opera por períodos, mediante o pagamento de uma mensalidade, semestralidade ou anuidade.

Na abordagem delimitada no presente trabalho, teremos como enfoque os contratos de licença de uso de *software ERP* em sua modalidade provisória, isto é, aqueles que necessitam de pagamentos periódicos para a continuação da concessão de seu uso.

Não nos interessa, pelo menos para a discussão a ser feita neste trabalho, a licença de uso de *software* em caráter perpétuo, isto é, aquele que a transferência da inteligência da tecnologia é feita de uma só vez, não havendo mais vínculo com o licenciante. Isso porque, nesses casos, a transferência da inteligência da tecnologia não acompanha uma prestação de serviço inerente ou uma manutenção temporal deste sistema, ou seja, o licenciante não terá a custódia, e assim, não tratará os dados colacionados neste *software* cuja licença foi cedida em caráter perpétuo.

Portanto, o que está ligado à discussão sobre o impacto da Lei Geral de Proteção de Dados nos contratos de licença de *software* não é a sua natureza em si, mas sim o seu caráter intrínseco de manutenção, desenvolvimento contínuo e, por fim, o suporte técnico, sendo que esses pontos resvalam diretamente em singulares pontos da Lei. Mais adiante serão abordadas essas importantes características do modelo de contrato de licença provisória.

A concepção atual do que se utiliza de um contrato de licença de *ERP* acabou sofrendo alterações constantes com o passar dos anos, principalmente com o advento de novas tecnologias e regulações. Conforme sobredito, referida modalidade de contrato também

¹⁴ BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Lei do Software. **Diário Oficial [da] República Federativa do Brasil**. Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

¹⁵ *Ibid.*

acompanha, na grande maioria das vezes, a necessidade de suporte técnico também incluído neste contrato de licença.

Apesar de se tratar de uma prestação de serviços técnicos especificamente voltada à manutenção ou melhorias no *software*, também se designa a manter o produto em perfeito estado, garantindo a sua melhor performance e a inócorrência de defeitos e *bugs*. O suporte também está intimamente ligado ao treinamento para manuseio e alimentação do *software*, além de buscar garantias para que nenhum dado seja perdido e que a sua arquitetura esteja em constante evolução.

Também incluído junto ao contrato de licença do *ERP*, normalmente se disponibiliza um produto incluso que trabalha na escrituração das informações e dados armazenados no sistema, aperfeiçoando-as e salvando as mesmas em formatos utilizados para serem enviados aos órgãos reguladores, principalmente em relação a informações contábeis, informações financeiras e de recolhimentos fiscais sobre funcionários, isto é, dados sobre recolhimentos e retenções de impostos, contribuições e taxas. Mas, frise-se, não são todos os sistemas *ERP* disponíveis no mercado que operam com a capacidade de escrituração aos órgãos fiscais.

Temos, portanto, um contrato que em sua origem tem o objetivo de licenciar uma tecnologia sob um custo mensal, nos termos do que a Lei de Software delimita, mas em outros planos e até para uma melhor execução deste contrato, acompanha um serviço de manutenção, escrituração, performance e também de suporte técnico, ou seja, uma inerente prestação de serviços.

Verifica-se, que os contratos atuais fugiram à regra do que fora disposto em 1998 na Lei do Software, e isso não poderia ser diferente, afinal, a evolução informática trouxe impactos em todos os setores da economia. Daí um ponto importante pra se discutir sobre essa espécie de contrato, por exemplo sob a ótica da aplicação da Lei Geral de Proteção de Dados e as suas implicações.

É certo que, se discutido o contrato *ERP* na concepção da Lei do Software, isto é, aquele contrato que simplesmente o licencia, ou seja, transfere a tecnologia para o adquirente, o impacto da Lei Geral de Proteção de Dados teria uma proporção reduzida e fácil de ser analisada, uma vez que não haveria um fluxo constante de informações e dados entre

licenciante e licenciado, ao passo que na licença final, os dados se transfeririam ao licenciado e não mais retornariam.

Todavia, ao ser avaliada a concepção moderna do mesmo, que implica em uma inclusa e direta prestação de serviços, temos um aprofundamento do impacto de aludida Lei no desenrolar da execução desta modalidade contratual, principalmente pela constante troca de informações e possibilidade/necessidade de acessos em bases de dados mantidas pela outra parte.

Portanto, como recorte deste trabalho, importante delimitar sobre a estrutura do contrato de software ERP o qual será utilizado como um modelo de partida da análise dos impactos e proposições a partir da metodologia *Privacy by design*.

Como estrutura padrão, partir-se-á de uma concepção moderna de contrato de licença de software, conforme já dito acima. Sua estrutura contempla a definição das partes contratantes, no caso em específico, licenciante e licenciada; O objeto do contrato, qual seja, a transferência da tecnologia de gestão empresarial integrada; As definições sobre a reserva e extensão de direitos sobre essa transferência de tecnologia; Os requisitos de *hardware* e de *software* necessários para a correta instalação e fiel desenvolvimento da tecnologia com o licenciado; Definições de capacitação e treinamento a serem ministrados pela equipe do Licenciante à Licenciada, visando uma perfeita operacionalização do *software*; Definição de obrigações inerentes ao Contratante-Licenciado e à Contratada-Licenciante; Os valores envolvidos na licença do *software*, no treinamento e instalação; O termo de acordo e de serviço designando-se horários e formato de atendimento em suporte técnico; As disposições envoltas ao *backup* da empresa Licenciada; Disposições sobre responsabilidade civil sobre o sistema em si, tratamento de dados, confidencialidade e propriedade intelectual; Formato de rescisão, renovação e rescisão, além de demais cláusulas gerais e eleição de foro.

Para estudo de preceitos de aplicabilidade da Lei Geral de Proteção de Dados e reestruturação, seria essa a estrutura do contrato de licença de *software* ERP tido como modelo e ponto de partida a ser abordado neste trabalho.

Daí o cerne da necessidade de se aprofundar sobre o estudo desta modalidade contratual, uma vez que o uso de *softwares ERP* em empresas do setor comercial, principalmente, vem se mostrando essencial na era digital, seja pela facilidade no manuseio

dos dados, pela pura necessidade de adequação, ou, até mesmo, pela melhor operacionalização de negócio.

Esses *softwares ERP* partem da funcionalização básica de inserção de dados que são postos pelo usuário, que por sua vez é o cliente da empresa que lhe concedeu a licença de uso do *software*. Acontece que não só os dados deste cliente ficam armazenados no banco de dados correspondente ao *software ERP*, mas também os dados ali inseridos por este cliente em relação ao seu próprio cliente, que no caso do comércio varejista, é um consumidor que adquiriu algum produto.

Desta forma, a empresa licenciante, proprietária da inteligência do *software*, no contexto moderno do contrato de licença, isto é, aquele que acompanha a inerente prestação de serviços, acaba atraindo os dados desse cliente e também aqueles postos no seu banco de dados, que são de terceiros. Aqui o cerne da necessidade de discussão e reestruturação do contrato de licença de *software ERP* pós Lei Geral de Proteção de Dados.

Mas não apenas o armazenamento e acesso são possíveis ao Licenciante através do banco de dados, há também a possibilidade de classificação, alteração, compartilhamento e transferência desses dados, opções de tratamento de relevante impacto descritas no art. 5º, inciso X, da Lei Geral de Proteção de Dados, conforme visto no tópico I.

Daí decorre a necessidade de um cuidado especial com o manuseio do *software* licenciado e de sua correspondente, e também necessária, estruturação jurídica contratual no ato de seu licenciamento para uso, a fim de delimitar responsabilidades, obrigações, custos, suporte, etc.

Voltando ao contexto do substrato jurídico propriamente dito do contrato de licença, uma outra característica comum é a sua não-exclusividade. As empresas licenciantes, aquelas que detêm a tecnologia contida no *software* para ser transferida mediante o contrato de licença, trabalham com diversas cessões simultâneas, garantindo uma maximização econômica, objeto, por evidência, da relação empresarial. Por conta disso, os contratos de licença não possuem o caráter de exclusividade, ao passo que poderão ser utilizados por outros licenciados, na mesma versão do *software*, inclusive.

Ligado à essa maximização econômica de cessões simultâneas da licença do *software*, atrela-se, por óbvio, uma grande quantidade de contratos, de clientes, portanto, e na

linha do que foi esboçado até o presente momento neste trabalho, atrela-se, também, uma grande quantidade de dados.

O presente subcapítulo buscou pincelar a natureza jurídica dos contratos de licença de *software* ERP, e suas concepções estruturais, o que garantirá uma melhor abordagem sobre a constituição técnica do *software* e, mais adiante, sobre os específicos impactos da Lei Geral de Proteção de Dados.

2.3 Contextualização da estrutura do *software Enterprise Resource Planning* (ERP)

Também necessário, para traçar um pano de fundo sobre a discussão dos impactos da Lei Geral de Proteção de Dados, não apenas a natureza e nuances jurídicas do contrato de licença do *software*, é necessário também, entender a contextualização de estrutura operacional do próprio sistema.

Pois bem, o contexto socioeconômico da modalidade de sistema ERP, tem forte influência de dois pontos: a Globalização e a Tecnologia da Informação. A globalização, como um fenômeno de conexão social, econômica e cultural, viabilizou, a partir dos avanços de ferramentas tecnológicas, a possibilidade da internacionalização das empresas, ao passo que, atualmente, as empresas não tem barreiras territoriais e a sua atuação se contempla por todo o globo terrestre. A tecnologia da informação, como uma ferramenta que proporciona inovação em soluções de modo célere, objetivo e funcional, vem, no contexto dos avanços tecnológicos e do fenômeno da globalização, impulsionar as empresas para facilitar a ultrapassagem dessas barreiras territoriais.

Neste sentido, Ernesto Haberkorn explica:

Nesta corrente entre globalização e tecnologia da informação, “o elo dos sistemas de Gestão Empresarial (ERP) é de fundamental importância. Tais sistemas tiveram de se adaptar à nova realidade. Impulsionados pelos avanços do Hardware e das ferramentas de Software disponíveis, evoluíram. Os usuários passaram a exigir mais. Os sistemas não tem mais limites. Automatizam tudo”.¹⁶

Pensando em seu conceito, necessário colacionar o entendimento de Lucio Colangelo Filho:

¹⁶ HABERKORN, Ernesto. **Teoria do ERP – Enterprise Resource Planning**. 2. ed. São Paulo: Makron Books, 1999, p. 5.

Não há uma definição precisa e inquestionável do que seja um “sistema ERP”. Para nossos propósitos, vamos considera-lo um *software* aplicativo que permite às empresas: - automatizar e integrar parcela substancial de seus processos de negócios, abrangendo finanças, controles, logística (suprimentos, fabricação e vendas) e recursos humanos; - compartilhar dados e uniformizar processos de negócios; - produzir e utilizar informações em tempo real. A noção-chave dessa definição é integração.¹⁷

A discussão sobre integração no sistema é absolutamente necessária, uma vez que se trata da sua característica mais importante. Só é um *software* ERP aquele que for integrado, da sua tradução para o português - Sistema integrado de planejamento de recursos empresariais – uma vez que o gerenciamento e aplicação de forma individual em cada setor da empresa, não traduz à otimização que a integração proporciona.

Como exemplo dessa assertiva, pode-se explicar que um determinado setor da empresa, como por exemplo, o estoque, se não for integrado com o setor de compras, justamente para informar de forma automatizada e imediata que há falta de determinado produto e que ele precisa ser comprado, não teremos o resultado otimizado e objetivo que se pretende.

Partindo-se da premissa da licença para uma empresa do setor varejista, se discute uma estrutura básica de aplicabilidade do *software* ERP que contempla o chamado *Back office*, conceito diretamente ligado à “parte de trás do escritório” na tradução literal, ou comumente reconhecido como a retaguarda do escritório, no auxílio e desenvolvimento dos processos rotineiros, de suporte e de organização.

Lucio Colangelo Filho, explica as funções ligadas ao *Back Office*, explicando também que suas funcionalidades não tem limites:

A maior parte dos sistemas ERP oferecidos comercialmente cobre ao menos parcialmente as três áreas básicas das funções de suporte das organizações, também chamadas de back-office: Finanças, Operações/Logística e Recursos Humanos. A cada dia é mais difícil definir quais são os limites funcionais de um sistema ERP, uma vez que os fornecedores estão continuamente expandindo as funcionalidades de seus produtos, seja por meio de desenvolvimentos adicionais ou por fusão ou aquisição de fornecedores de *software* complementar e integração dos produtos.¹⁸

No contexto trazido pela citação acima, é que revestimos a atual situação dos sistemas ERP. Atualmente, a integração entre os setores da empresa é bem avançada.

¹⁷ COLANGELO FILHO, Lucio. **Implantação de sistemas ERP (Enterprise Resource Planning):** Um enfoque de longo prazo. São Paulo: Atlas, 2001, p. 17.

¹⁸ *Ibid.*, p. 19.

Atualmente, com as inovações tecnológicas e aumento da capacidade de processamento dos computadores, os sistemas já tem possibilidades de desenvolvimento e integrações muito mais avançadas.

Portanto, partindo-se da conjuntura associada a empresas do ramo varejistas quando postas como licenciadas, na época atual, a integração ocorre em muitas outras áreas da empresa, além de que as áreas de aplicação do sistema ERP são muito mais abrangentes do que a mera organização, suporte e administrativo atinentes ao *Back Office*.

Quanto maior a integração entre os setores da empresa, por óbvio, maior é o fluxo de dados que tramitam por estes setores, o que, conforme será abordado mais adiante, incide em uma maior necessidade de regulação interna do ponto de vista da Lei Geral de Proteção de Dados.

Para o estudo em questão neste trabalho, é importante partir da estrutura moderna do sistema ERP, principalmente sobre aquela que é atualmente utilizada por empresas especialistas em licença de *software* para empresas do setor varejista, concepção, esta, já abordada no tópico anterior.

Ainda em explicação ao recorte deste trabalho, é necessário demonstrar bem qual o ponto que se busca a abordagem do Software ERP. Atualmente, com o desenvolvimento maciço da internet, é possível encontrar esse tipo de *software* disponível em uma versão gratuita online, ou até mesmo em diferentes versões ou extensões que necessariamente sofrerão um impacto diferente em termos de Lei Geral de Proteção de Dados.

Portanto, o tipo de software que será utilizado como premissa para uma regularização em termos de conformidade, será especificado e aprofundado neste tópico, ou seja, uma estrutura específica ligada ao comércio varejista, que necessariamente contemple suporte como uma prestação de serviços inerente com o respectivo pagamento mensal.

Assim sendo, o que se deve ter em mente, até para um melhor dimensionamento do próximo tópico, é que a empresa licenciante do *software* ERP sempre terá acesso ao banco de dados do comércio varejista, ora empresa licenciada. Para efeitos deste trabalho, é importante que se tenha isso em mente, justamente porque, em sendo esse acesso aos dados automático e constante, a gama de obrigações e medidas necessárias para a abordagem de melhores práticas e fiel cumprimento da Lei Geral de Proteção de Dados, é necessariamente maior.

A estrutura do Software ERP “*Enterprise Resource Planning*”, tem início nas rotinas genéricas, aquelas ligadas no dia a dia do sistema refletindo a estrutura da organização. Neste sentido, a descritiva de Ernesto Haberkorn, em sua obra, Teoria do ERP – Enterprise Resource Planning:

Rotinas Genéricas.

Capacidade de processar várias empresas e filiais. Faz consolidações das filiais e das empresas. Os arquivos podem ser alocados em vários servidores de dados. As regras de negócios podem ser alocadas em vários servidores de aplicação. O software é apresentado em diversos idiomas. Trabalha com dicionário de dados ativo: Permite incluir novos campos; Excluir campos; Excluí-lo das telas e relatórios; Excluí-lo do browse do cadastramento; Alterar seu tamanho; Alterar sua máscara de edição; Inserção de zero à esquerda em campo alfa; Alterar sua validação; Utilização de funções gerais; Utilização de funções próprias (usuário); Uso de ".and." e ".or." Acesso a arquivos ou tabelas relacionados; Acesso a outros campos digitados na mesma tela. Uso de fórmulas definidas pelo usuário. Inicialização baseada em registro anterior (carry on). Inicializador Padrão na inclusão de registros. Inicialização baseada em outros campos digitados (gatilhos). Alterar a ordem de apresentação dos campos. Acessar diretamente o registro via várias sequências. Visualizar todos os seus dados. Criar arquivos próprios. Alteração on-line do banco de dados. (...).¹⁹

As rotinas genéricas são o primeiro passo da execução do *software* ERP, sendo as primeiras execuções disponíveis no sistema. Essas execuções podem ser pré-programadas para atuarem automaticamente ou também serem alimentadas de forma manual, dependendo da necessidade de cada operação e/ou projeto da empresa.

Em termos de fluxo, inventário de dados, possibilidade e armazenamento e tipos/espécies de dados disponíveis a serem preenchidos para armazenamento e tratamento, no contexto do que será tratado a partir das rotinas genéricas, é possível indicar os mais importantes e sensíveis abaixo:

Financeiro

Controla os títulos a pagar, classificando-os por natureza (duplicatas, folha, impostos etc). Controla os títulos a receber. Controla saldos bancários. Este controle é feito por agência/conta. Facilidade para reconciliação com extrato. Recepção via modem dos movimentos da conta. Considera a disponibilidade dos cheques depositados. Considera a disponibilidade dos recebimentos. Controla fluxo de caixa: Apresenta em tela o saldo diário projetado. Considera vencimento real. Fornece analítico em nível de título. Considera títulos provisórios. Considera pedidos de compras. Considera pedidos de vendas. Considera solicitações de compras. Considera previsões de vendas.

¹⁹ HABERKORN, Ernesto. **Teoria do ERP – Enterprise Resource Planning**. 2. ed. São Paulo: Makron Books, 1999, p. 145-167.

Considera rendimento das aplicações. Imprime fluxo em forma de coluna separado por natureza. Faz simulação financeira. Apresenta gráfico no fluxo. Faz controle orçamentário. Controle em nível de natureza. Permite até dez níveis de totais, definidos pelo usuário. Permite quebras invertidas (ex: bbbbbbbaaaaa). Permite criação de índices próprios. Emite comparativo entre orçado e realizado. O comparativo trata até 12 meses. (...) Faz consolidação de várias empresas. Tem facilidade para se cadastrar o endereço de cobrança, considera retenção bancária na atualização do saldo bancário. Fornece motivo de não pagamento de um título. Mantém histórico do processo de cobrança de um título. Considera IR retido na fonte. Considera ISS retido na fonte.

Lojas e Comércio Varejista

Disponibiliza tela front-end para o caixa. Emite a nota ao cliente. Aceita código de barra para os produtos. Emite estatística por produto. Emite estatística por vendedor. Controla o preço de venda real em relação a uma tabela. Calcula comissão de vendas. Fornece o custo dos produtos vendidos. Tem tela de sugestão de vendas para o cliente. Controla o estoque do depósito. Controla o estoque do balcão. Controla o saldo bancário/caixa. Controla sangrias. Controla cheques pré-datados. Controla as despesas da loja. Interliga-se com PDV. Armazena dados de endereço dos clientes. Emite etiquetas de mala direta.²⁰

Da extensa gama de ações possíveis através da utilização do *software* ERP, para os fins deste trabalho, isto é, para levantar e estudar as rotinas mais impactadas pela Lei Geral de Proteção de Dados a ponto de revelarem a necessidade de uma estruturação contratual, a abordagem passará necessariamente por grupos de dados que se encontram nas especificações acima, sendo eles: Convênios; Clientes; Vendedores; Fornecedores; Produtos; Cadastros; Cobrança; Contas a Pagar; Orçamentos; Venda em PDV (Ponto de venda/Caixa); Estoque; Escrituração; Financeiro; Credenciais bancárias; TEF.

Dentro desta subdivisão de grupos de dados, o sistema ERP contempla um elaborado índice de classificação passando por uma grande quantidade de diferentes tipos de dados. Esses dados poderão ter um conteúdo mais sensível ou não, o que, precisamente, necessitará de um nível maior de segurança e de regulação em termos de privacidade e proteção de dados.

A integração desses âmbitos estruturais da empresa e das rotinas genéricas proporcionadas pelo *software*, visam também a fidelização de clientes e aumento de vendas, além de um controle e a administrativo e financeiro com painéis de indicadores e transmissão automática de dados e informações.

Todo esse esquema estrutural é bem específico e singular aos softwares ERP utilizados no varejo, passando a serem praticamente indispensáveis em larga escala de vendas,

²⁰ HABERKORN, Ernesto. **Teoria do ERP – Enterprise Resource Planning**. 2. ed. São Paulo: Makron Books, 1999, p. 145-167.

clientes e depósito. Atualmente, a título de curiosidade, um dos softwares ERP mais comercializados e utilizados no Brasil é o TOTVS VAREJO, da empresa de capital aberto TOTVS S.A.

Necessária essa distinção, uma vez que para cada nicho de mercado, existe um tipo de software ERP que pode ser desenvolvido de forma própria, abordando as necessidades e peculiaridades daquele ramo específico. Neste ponto, uma empresa que oferece a licença do software ERP incluindo-se toda a estrutura e trabalho de treinamentos, instalação, acompanhamento da execução, suporte técnico, eventuais melhorias e alterações específicas, se diferencia singularmente de qualquer software *White Label* ou Software de prateleira, ou seja, respectivamente, aqueles que podem ser customizados para cada tipo de negócio, ou aqueles encontrados online e já estão prontos para a execução em qualquer ramo de negócio.

A partir do tópico seguinte, e principalmente no capítulo 4 deste trabalho, alguns subitens dessa classificação serão utilizados como exemplo para os impactos da Lei Geral de Proteção de Dados no *software* ERP e, conseqüentemente, no seu contrato de licença, ao passo que o resultado desta sucinta análise será propositalmente avaliado a partir da leitura metodológica do *Privacy by Design*.

2.4 Análise dos principais impactos da Lei Geral de Proteção de Dados nos contratos de licença de uso de *software* ERP: Uma análise do setor varejista

A partir de uma breve contextualização sobre a Lei Geral de Proteção de Dados, sobre os contratos de licença de software ERP e da estrutura do próprio sistema, é necessário fazer a junção desses temas para solidificar e embasar a busca do quesito central deste trabalho.

É evidente, que para atrelar os dois temas e discutir sobre os impactos e conseqüências que um tem sobre o outro, isto é, que a Lei Geral de Proteção de Dados tem sobre os contratos de licença de uso de *software* ERP, necessário, ao menos, traçar o seu ambiente de análise.

Mas antes disso, em um passo atrás, valioso apontar os impactos que a Lei Geral de Proteção de Dados trouxe para o âmbito empresarial em um contexto geral. Segundo Andreia

Saad e Antonio Hiunes, “projetos básicos de estruturação para o cumprimento com a LGPD, tanto sob o aspecto de TI quanto sob o aspecto jurídico, podem custar entre R\$ 25.000,00 (Vinte e cinco mil reais) e R\$ 3.000.000,00 (Três milhões de reais) a depender da dimensão da empresa, isto, sem contar os custos de execução e manutenção, que são perenes.”²¹

Afora o aspecto de Tecnologia da informação, que não deixa de ser fundamental para a conformidade com a LGPD, que não será tema deste capítulo ou até mesmo deste trabalho, o aspecto jurídico tem grandes desafios, ao passo que uma lei como a LGPD, de pouco mais de 60 artigos, conforme já demonstrado no primeiro tópico deste trabalho, impõe extensos direitos, obrigações, responsabilidades e sanções.

É evidente que sem uma amostragem ou um caso prático desenvolvido, não é possível se ter uma dimensão concreta de impactos que atingem uma ou outra empresa que atua no setor objeto de estudo deste trabalho, daí a razão dos recortes feitos nos tópicos anteriores.

Mas além dos necessários recortes, com a abrangência mais genérica da forma como se buscou o estudo deste trabalho, justamente por não haver uma amostragem ou um estudo de caso específico, o objetivo não seria indicar algo específico, como uma cláusula ou um termo de tratamento, que resolverá todos os problemas que a LGPD traz a este tipo de empresa, pelo contrário, as exposições buscarão serem mais genéricas com a busca de abordar a maior quantidade de situações que se possam envolver neste tipo de operação.

Se enquadrado em um contexto consumerista, conforme abordado no tópico sobre a natureza jurídica do ERP, ampliam-se de um aspecto processual e procedimental os direitos e necessidade de criação de ferramentas de conformidade e de segurança das empresas fornecedoras que tratam dados de seus clientes de alguma forma.

De forma geral e bem simplória, quando uma lei entra em vigor, as pessoas e empresas devem cumpri-la. Mas o ponto chave, e que terá uma face importante neste tópico, seria a criação do termo jurídico, no âmbito da leitura da LGPD, da palavra tratamento.

²¹ SAAD, Andrea; HIUNES, Antonio. Ela, a LGPD, vista pelas empresas: uma proposta de visão prática e otimista. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020, p.19.

Após o advento da LGPD, a palavra tratamento, inserida no contexto do art. 5º, inciso X, passou a ter o significado mais relevante para o setor empresarial. Parafraseando de forma singela referido dispositivo, tratamento é toda operação realizada com dados pessoais. Em seguida, o texto legal colaciona uma série de ações a serem feitas pelo agente, dentre elas, as mais relevantes, como coleta, armazenamento, modificação e transferência.

Automaticamente após a promulgação de referida legislação, qualquer operação empresarial que tratasse dados pessoais, no sentido do art. 5º inciso X, passaria a sofrer impacto de algum modo.

Destaca-se que a ação de tratamento deveria respeitar princípios criados e insculpidos no art. 6º, aqueles já mencionados no primeiro tópico deste trabalho. Em sequência, no art. 7º temos as hipóteses em que um dado pessoal poderá ser tratado, realçando duas hipóteses que nortearam os impactos a serem apresentados neste tópico, ressaltando a importante hipótese de cumprimento de exigência de obrigação legal ou regulatória (Art. 7º, II, LGPD) e para a execução de contrato ou de procedimentos relacionados ao contrato de que seja parte o titular, a seu pedido (art. 7º, V, da LGPD).

Além disso, é preciso garantir os direitos do titular, aqueles expostos no artigo 9º e 18º da LGPD, que também trazem imposições e necessidade de fixação de garantias e demais obrigações, cuja suas extensões dependerá da qualidade de operador ou controlador.

Buscando perfilar mais ainda as conclusões de impacto geral da LGPD, é necessário ter em mente, conforme já abordado acima e no tópico 2.1, que as imposições, obrigações e responsabilidades e extensão de sanções são diferentes para operadores e controladores de dados, razão pela qual é fundamental levar em conta qual é o enquadramento de agente de tratamento da empresa que se busca a conformidade.

Neste ponto, buscando o estreitamento da análise de impacto da Lei no contexto empresarial, é crucial que se faça tal análise a partir de um determinado ambiente, isso porque o *software* ERP, dada a sua proporção e escalabilidade no contexto empresarial, pode ser utilizado para diversos tipos de operação, daí, visando afunilar o conteúdo da análise, é saudável que seja delineado o contexto em que está inserido.

Por mais que essa modalidade de *software* tenha larga aplicabilidade empresarial, conforme discutido nos subcapítulos anteriores, o objeto deste trabalho o abordará a partir da aplicação em uma operação de varejo, como em um supermercado, por exemplo.

Igualmente, quando a discussão se trava a partir de uma análise de principais impactos, conforme o tópico predispõe, é certo que não serão abarcadas todas as possibilidades, mas somente aquelas que são mais relevantes à luz da experiência do pesquisador e no que comumente vem sendo mais discutido no ambiente profissional, isto é, em um programa de conformidade jurídica de uma empresa que licencia *software ERP* ao setor varejista.

Isto posto, um dos pontos categóricos para dar início à análise de impactos que a Lei Geral de Proteção de Dados tem nesta modalidade de *software*, é definição dos agentes contratuais, no caso do contrato em estudo, do Licenciante e Licenciado.

É importante explicar que a análise é do contrato de licença de *software ERP*, vislumbrando a relação contratual entre o Licenciante e o Licenciado, ao passo que o impacto da LGPD incorre em ambas as empresas, de forma separada, mas também de forma solidária na relação bilateral do fluxo de dados que ali são tratados.

É daí a concepção trazida por alguns doutrinadores de uma possível correção regulada entre empresas que contratam entre si e que efetuam o tratamento de dados nos enquadramentos de encarregado e operador. É manifesto que ambas contratarão e buscarão de forma bilateral, estabelecer uma relação segura, ao passo que o tratamento irregular feito pelo operador pode impactar diretamente o controlador, daí a noção de responsabilidade solidária contida no art. 42, parágrafo 1º, incisos I e II da LGPD, já comentada no tópico 2.1.

Também há disposições sobre a autorregulação regulada, encontrada de forma concreta no art. 46 e seguintes da LGPD, onde são expostas a necessidade de adoção pela empresa, de medidas de segurança e critérios a serem observados para boas práticas.

Conforme será visto no capítulo 4, a aplicação do *Privacy by design* como método de conformidade do contrato de licença de *software ERP* com a Lei Geral de Proteção de Dados, pode ser visto como uma autorregulação regulada, uma vez que busca a aplicação de medidas técnicas e de segurança criteriosas, que em alguns aspectos são mais abrangentes que a própria percepção dispositiva da mencionada Lei, e isso acaba ocorrendo a partir de uma

mudança de cultura empresarial, buscando algo além da simples conformidade técnica e jurídica.

O Licenciante é o detentor da inteligência da tecnologia do *software* que está sendo cedida através do instrumento particular de licença, ao passo que o Licenciado, é aquele agente que pagará mensalmente, semestralmente ou, anualmente, excluída a análise do formato da licença vitalícia já exposto em tópico posterior, pela utilização de uma das cessões daquele *software*.

Em uma operação de comércio varejista, o Licenciado utiliza do *software ERP* para gerir todo o seu ambiente de negócios. A partir das rotinas genéricas expostas no tópico acima, o Licenciado poderá alimentar o sistema com as informações e dados retidos na empresa, passando a aloca-los em seus determinados fluxos e inventários, nos termos também dos exemplos já trazidos.

De forma prática, em uma relação de licença como a do exemplo em questão, em respeito às disposições descritivas do art. 5º da LGPD, a primeira problemática cinge no enquadramento do agente titular, ou seja, na relação entre licenciante e licenciado do contrato de licença, quem é o controlador e quem é o operador? A resposta para essa pergunta impacta diretamente a relação da parte com órgãos reguladores, fiscalizadores e até mesmo com o Poder Judiciário, do ponto de vista do direito de titulares buscado de forma individual.

Essa relação será abarcada para efeitos práticos e de exemplificação para nortear o estudo proposto neste trabalho, mas não se trata de uma verdade absoluta envolvendo essa relação, até mesmo por haver casos mais específicos entre licenciante e licenciado que fugirão à regra deste paradigma.

A resposta é pragmática, mas tímida. Na relação em questão, devido aos fluxos de tratamento de cada parte, a depender da operação e da rotina a ser aplicada ao *software*, ambos poderão ser operadores e controladores. Daí, no contexto da virtude que este trabalho busca, uma das primeiras singularidades que esta relação contratual propõe. Para explicar este contexto, também é necessário um exemplo:

A empresa licenciante garante a instalação do software ERP na licenciada, em conjunto com um treinamento para o manuseio do mesmo; Inicia-se o trabalho da licenciada de compor o acervo de dados e informações nas abas ligadas ao sistema, no formato exposto

no tópico 2.3; Detalhe que esses dados podem ser tanto dos clientes da licenciada – como, por exemplo, dados pessoais de um cadastro de clientes da mesma – ou da própria licenciada – como, por exemplo, informações inseridas em relação à folha de pagamento de seus próprios funcionários; Por mais que não se finde a inserção de dados e informações, uma vez que no exemplo do comércio varejista há diversas inserções por dia (vendas ao cliente, por exemplo), em um determinado momento (devidamente programado pelo Licenciado) ocorrerá o *backup* dessas informações para um banco de dados cujo acesso é garantido à Licenciante, uma vez que essa dispõe da tecnologia de classificação e armazenamento desses dados em caso de algum problema de *hardware* (na máquina da licenciada) ou até mesmo em uma campanha que se necessite uma classificação robusta de dados (como por exemplo uma promoção de determinado tipo de produto); Esses dados e informações ficam armazenados em um banco de dados cujo acesso é garantido ao Licenciante, isso pois, ocorre, até com certa frequência, pequenos erros e *bugs* que necessitam retificações, classificações e, eventualmente, transferência, para a nuvem, por exemplo; Ao mesmo tempo, esses dados também ficam à disposição de acesso da própria Licenciada, que é a detentora dessas informações e está à todo momento o alimentando e garantindo que esses dados sejam positivamente revertidos para o fluxo da operação, que é efetivamente vender ao consumidor varejista.

Veja-se, à vista disso, que a relação contratual tem um fluxo bilateral de dados e informações, onde os acessos e determinação de medidas das rotinas do *software* ERP ficam disponíveis para a Licenciante e Licenciada, ou seja, elas tramitam entre as partes de forma constante.

Do aspecto do enquadramento em operador e controlador de dados, considerando que o operador realiza o tratamento de dados pessoais em nome do controlador, enquanto que a esse compete as decisões referentes ao tratamento de dados pessoais, é possível concluir, que à depender da rotina a ser aplicada, caberá a decisão ao Licenciante, como controlador, por força da questão de conhecimento técnico, o que inclusive está atrelado ao conhecimento da tecnologia que é cedida através da licença, enquanto também poderá recair ao Licenciado, também como controlador, em razão da tomada de decisão que lhe compete do ponto de vista da forma e manejo de suas próprias inserções de dados e informações.

Outrossim, há rotinas a serem aplicadas, onde a Licenciante pode ser uma mera operadora, simplesmente classificando e armazenando os dados à mando e ordem da Licenciada, como também, esta, por sua vez, se posicionar como operadora quando

meramente aplica uma rotina pré-disposta e direcionada pela Licenciante visando a boa funcionalidade do fluxo de dados no *software* ERP.

Detalhe não menos importante, que neste emaranhado de dados e informações, conforme já mencionado acima, há dados dos clientes da Licenciada, mas também há dados da própria Licenciada.

Nota-se a dificuldade em se regular contratualmente esta relação no que tange a implicações de incidentes, responsabilidades com o titular de dados, obrigações inerentes à órgãos reguladores como PROCON, SENACOM, Ministério Público, Ministério Público do Trabalho, Autoridade Nacional de Proteção de Dados e a própria regulação indiretamente empreendida através do Poder Judiciário. Daí, um dos primeiros exemplos do extenso impacto que a Lei Geral de Proteção de Dados transcende nesta modalidade de relação contratual.

Outro exemplo de impacto singularmente ligado à esta modalidade de relação contratual, seria a dificuldade de se buscar um investimento em segurança da informação e tecnologia da informação, uma vez que, a empresa Licenciante, por óbvio, efetuará tal investimento em sua própria infraestrutura, buscando convalescer os seus próprios problemas e falhas operacionais.

Neste caso, de certo, haveria uma melhora na segurança da informação nos fluxos e rotinas que partem da Licenciante, todavia, tal investimento dificilmente abarcaria eventuais falhas e problemas de rotinas e fluxos de dados que partem da Licenciada, caso a mesma não tenha um nível de investimento em segurança e tecnologia da informação à altura de sua coobrigada.

Por último, da série de exemplos de impactos trazidos pela LGPD de forma muito própria aos contratos de licença de *software* ERP, seria a hipótese de autorização elencada à Licenciante para tratar dados pessoais dos clientes da Licenciada.

Em uma operação normal do setor varejista, o cliente vai ao mercado, compra um produto, paga por ele e vai embora. Pode ser que o cliente não forneça nenhum dado pessoal nesta compra, sem aprofundamento de dados técnicos voltados à Id de PIX ou do TEF do cartão de crédito, mas pode ser que aquele cliente tem um cadastro em um clube de

relacionamento daquele mercado, onde ele fornece o seu CPF para ativar certas promoções e descontos.

Ressalte-se, que atualmente, a extensa maioria dos supermercados trabalham com programas de relacionamento, garantindo pequenos descontos ao cliente, tudo em busca de fidelização e também, como uma política de aceleração de venda de determinado produto, por exemplo.

Voltando à rotina do estabelecimento, insta detalhar que quando ocorre o cadastro no clube de relacionamento, o cliente teve de fornecer uma série de dados pessoais, seu CPF, endereço, nome completo, idade, enfim. De outra sorte, toda vez que o cliente coloca o seu CPF na compra, ativando os descontos, o sistema ERP tende a arquivar e classificar o histórico de compra deste cliente.

Os desdobramentos disso são diversos, aplicada uma rotina no sistema, é possível verificar, por exemplo, os produtos que o cliente mais compra, a média de gastos mensais dele, preferência por marcas, o seu nível financeiro, etc. Todas essas informações são utilizadas pelo sistema para fornecer promoções e descontos ao próprio cliente, através de campanhas de *marketing*, por exemplo, visando fidelização do cliente e gastos constantes naquele mercado licenciado.

Por outro lado, o contrato de licença de *software* ERP, pelo lado do Licenciante, deve se cercar de medidas de proteção e de boa-práticas, visando o não comprometimento técnico e jurídico por parte do mesmo, em caso de não cumprimento estrito da legislação pela Licenciada, e vice-versa, no sentido da Licenciada se cercar de disposições e conteúdo que lhe garanta isenções em caso de um tratamento irregular nos dados de clientes fornecidos pela Licenciada ao Licenciante.

De se notar, mais uma vez, um particular impacto nos contratos de licença de *software* ERP, a partir das aplicações legais que a LGPD impôs, além, evidentemente, das regulações administrativas de outros órgãos e institutos.

Na prática, o formato de reestruturação para a aplicação da metodologia pode ocorrer de duas formas: Pela inserção de uma cláusula de proteção de dados no contrato de licença ou na criação de um termo de tratamento de dados a ser incluído como anexo deste contrato. Os dois formatos deverão, imprescindivelmente, observar toda a operação, podendo ocorrer,

inclusive, eventuais modificações em outras cláusulas que vão de encontro à melhor prática para o respectivo tratamento.

É evidente que tais formas de reestruturação, obviamente deverão seguir a operação do *software* na prática, ou seja, pode ser que um determinado software tenha rotinas e modos de operação que não são possíveis de se aplicar um termo de tratamento ou uma simples cláusula, sendo o caso de um relatório de impacto de proteção de dados para a minimização de eventuais desconformidades e vazamentos.

Traçados estes exemplos, que necessariamente foram buscados e trazidos de forma exemplificada, para demonstrar impactos singulares e específicos nesta modalidade de relação contratual, a seguir, será abordada a metodologia do *privacy by design*, vislumbrada como uma proposta de boas práticas para um adequado e seguro programa de conformidade com a LGPD.

3 A METODOLOGIA *PRIVACY BY DESIGN* E SUA APLICABILIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS

De fundamental importância para o deslinde proposto neste trabalho, é a discussão acerca do *privacy by design* e sua presença na Lei Geral de Proteção de Dados, conforme previsto alhures.

Em primeiro, importa ressaltar que há discussão sobre o conceito por detrás deste tema, além de extensões de sua definição, o que se mostrou mais manifesta após a sua contundente aparição no GDPR.

A análise sobre a sua aplicação direta ou indireta na Lei Geral de Proteção de Dados, havendo controvérsia também, por exemplo, sobre a sua presença desmembrada, traz algumas dúvidas sobre a sua utilização como uma metodologia norteadora em uma reestruturação contratual que já se mostrou necessária após o aprofundamento fático e teórico do capítulo 2.

A busca da utilização de uma metodologia como suporte em uma reestruturação contratual motivada por alteração legislativa, ou seja, através de regulação legislativa, deve, em primeiro momento, dialogar com supostas similitudes compostas na lei, que facilitarão o trabalho da implementação e do cumprimento da regulação.

É este o papel deste capítulo, além de, por óbvio, estabelecer uma convicção envolta do tema do *privacy by design* que garanta uma melhor assimilação de conteúdo no capítulo 4, quando finalmente será colocada em prática a proposta da reestruturação contratual e, se necessário, da orientação operacional do próprio *software ERP* colocado à licença.

3.1 Definições, conceitos e princípios do *Privacy by Design*

Previamente a iniciar o estudo conceitual e principiológico acerca do tema *Privacy by Design*, este que já apareceu por tantas vezes no conteúdo, sem necessariamente ser discutido, é salutar discutir o conceito de privacidade, e Woodrow Hartzog traz uma definição sobre:

Privacidade é um conceito amorfo e indescritível, o que surpreende pelo seu papel central na lei e na vida cotidiana. É um daqueles conceitos que todos nós intuitivamente reconhecemos e almejamos. No entanto, quando pressionados a articular o que é privacidade, ficamos perplexos. Nenhuma definição pegou, embora o fracasso não seja por falta de tentativa. Quase todas as tentativas de definir privacidade acabam sendo muito específicas para serem aplicadas em geral ou muito gerais para serem úteis ²².

Não necessariamente uma definição e conceito sobre privacidade, precisamente porque a citação delimita que se trata de um conceito amorfo e indescritível, Woodrow instiga a refletir sobre uma questão a qual atribuímos tanta importância, que fundamentalmente sabemos do que se trata, mas temos dificuldade em atribuir um conceito que lhe vista de forma completa.

O próprio título do capítulo 3 ou o início do tópico 3.1 deste trabalho, dá um breve adiantamento de como será o emprego do *Privacy by design* no contexto ora estudado. A ideia de considerar o *Privacy by design* como um conceito ou uma metodologia, não é novidade no âmbito doutrinário.

Alguns autores suportam a tese de que o *Privacy by design* nada mais é do que uma metodologia que visa incorporar princípios à uma operação, buscando a proteção à privacidade e aos dados pessoais dos atores envolvidos.

Pelo dicionário, metodologia são regras ou normas estabelecidas para o desenvolvimento de uma pesquisa, é um ramo da lógica que estuda os métodos em diferentes ciências.

Camilla do Vale Jimene delimita que:

O termo *privacy by design* refere-se à metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano. Assim, a proteção da privacidade seria o ponto de partida para o desenvolvimento de qualquer projeto, sendo incorporada à própria arquitetura técnica dos produtos ou serviços.²³

²² HARTZOG, Woodrow. **Privacy's Blueprint: The Battle to Control the Design of New Technologies**. Cambridge, Massachusetts, Harvard University Press, 2018, p. 10.

²³ JIMENE, Camilla do Vale. Reflexões sobre *privacy by design* e *privacy by default*: da idealização à positivação. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. 1ed. São Paulo: Revista dos Tribunais, 2018. p. 165-180.

Carlos Affonso Pereira de Souza também faz menção ao *Privacy by design* como metodologia, indicando que os seus objetivos são atingidos a partir da aplicação de sete princípios fundamentais, que serão mais adiante abordados.²⁴

Por mais que as palavras tenham próxima percepção, há quem delimite que o *Privacy by design* é um conceito, e não uma metodologia. Este trabalho suportará a ideia de que o *Privacy by design* é uma metodologia, que utiliza do emprego de métodos para se chegar à um objetivo. Assim sendo, a abordagem ao *Privacy by design* será de metodologia, ou seja, de aplicação de métodos, a partir de seus sete princípios, para se buscar uma melhor prática de respeito e proteção à privacidade e à dados pessoais.

Aprofundando o tema, o termo *Privacy by design*, que atualmente reveste o artigo 25 do *General Data Protection Regulation* (GDPR) e que posteriormente foi importado e inserido na Lei Geral de Proteção de Dados Brasileira, o que será visto no tópico seguinte, originalmente foi criado em 1990 pela então Comissária de Informação e Privacidade do Canadá, Profa. Ann Cavoukian.

Segundo Daniela Ježová, *privacy by design*, sob a *General Data Protection Regulation* significa que os processadores de dados devem considerar a privacidade já nos estágios iniciais ao projetar, desenvolver um produto, serviços que envolvam o processamento de dados pessoais. O GDPR introduziu os novos requisitos neste conceito.²⁵

Na concepção de Ann Cavoukian, criadora da *Privacy by Design* é a filosofia e metodologia de incorporação da privacidade nas especificações de design de tecnologias da informação, práticas de negócios e infraestruturas de rede como uma funcionalidade principal. E continua dizendo que *Privacy by Design* significa construir privacidade desde o início, diretamente nas especificações de projeto e arquitetura de novos sistemas e processos.²⁶

²⁴ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Editora Revista dos Tribunais. 2020. p. 424.

²⁵ JEŽOVÁ, Daniela. **Principle of Privacy by Design and Privacy by Default**. Regional Law Review, Beograd, 2020, p. 4. Disponível em: <https://ssrn.com/abstract=3755514>. Acesso em: 2 ago. 2022

²⁶ CAVOUKIAN, Ann. **Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers**. Ontario, CA: Information and Privacy Commissioner of Ontario, Canada, 2011, p. 3. Disponível em: <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf>. Acesso em: 20 set. 2022

Ann Cavoukian ainda delimita que o objetivo desse conceito, o que se atinge através da aplicação dos seus sete princípios, é garantir privacidade e obter controle pessoal sobre as informações de alguém e, para as empresas, obter uma vantagem competitiva sustentável.²⁷

É possível verificar no campo “*Key Issues*”, traduzido para assuntos chave do conteúdo de formação do GDPR, um conceito atribuído ao termo *Privacy by design*, o qual propõe: O termo “Privacidade por Design” significa nada mais do que “proteção de dados por meio do design de tecnologia”. Por detrás disso está o pensamento de que a proteção de dados nos procedimentos de processamento de dados é melhor adotada quando já está integrada na tecnologia desde sua criação.

A partir deste amplo, mas incisivo conceito, passamos a discutir a sua definição. Em tradução literal, o termo significa privacidade por design, essa última palavra que pode ser adaptada à definição de projeto. Privacidade pelo projeto, portanto, indica que a concepção de respeito à privacidade está inserida desde o seu início, que por sua vez, composto na discussão de proteção de dados, remonta ao respeito pela centralidade da privacidade.

Em remate, Daniela Ježová dispõe que *Privacy by design* significa que, caso um sistema inclua escolhas para o consumidor sobre a quantidade de dados pessoais que serão compartilhados com outros, as configurações padrão devem ser as mais amigáveis à privacidade.²⁸

Mesmo sendo trazidos vários conceitos, por mais extensos e abrangentes que sejam, o termo *Privacy by design* não será definido em uma frase de começo, meio e fim. O termo é muito mais abrangente e colheu, após a inserção no GDPR, o tratamento de metodologia, conforme acima já delineado.

Essa metodologia é retratada pela criadora do *Privacy by Design*, Profa. Ann Cavoukian, que em maio de 2010 publicou um artigo denominado *Privacy by Design The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*.

²⁷ CAVOUKIAN, Ann. **Privacy by Design**. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010, p. 1. Disponível em: <chrome-extension://efaidnbmninnibpcapjpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em 2 set. 2022.

²⁸ JEŽOVÁ, Daniela. **Principle of Privacy by Design and Privacy by Default**. Regional Law Review, Beograd, 2020, p. 3. Disponível em: <https://ssrn.com/abstract=3755514>. Acesso em: 2 ago. 2022

Aludido artigo tinha o propósito de fornecer aos leitores informações adicionais, esclarecimentos e orientações sobre a aplicação dos 7 (sete) princípios fundamentais do *Privacy by design*.²⁹

Aqui cabe um relevante ponto para a continuidade deste capítulo. Quando de seu desenvolvimento inicial, o *Privacy by design* tinha seus elementos voltados para profissionais técnicos da área da Tecnologia da Informação, ou seja, o tema não tem criação propriamente jurídica.

A metodologia traz conceitos que auxiliam o desenvolvedor a efetivamente criar ferramentas e desenvolver a operação do *software* com o devido respeito às questões técnicas que, por sua vez, também impactam nos direitos desses usuários. A sua aplicação em um contexto dito jurídico, só entrou em cena após sua menção e caracterização no GDPR.

Portanto, os 7 (sete) princípios fundamentais de *Privacy by design* são: (1) *Proactive not Reactive; Preventative not Remedial* (Proativo não Reativo; Preventivo não corretivo); (2) *Privacy as the Default Setting* (Privacidade como configuração padrão); (3) *Privacy Embedded into Design* (Privacidade incorporada ao design); (4) *Full Functionality – Positive-Sum, not Zero-Sum* (Funcionalidade completa - Soma Positiva, não Soma Zero); (5) *End-to-End Security – Full Lifecycle Protection* (Segurança de ponta a ponta – proteção completa do ciclo de vida); (6) *Visibility and Transparency – Keep it Open* (Visibilidade e Transparência – Mantenha-o Aberto); (7) *Respect for User Privacy – Keep it User-Centric* (Respeito pela privacidade do usuário – Mantenha-o centrado no usuário).³⁰

É facilmente perceptível que o conceito abarcado na metodologia do *Privacy by Design*, conforme atribuído por Ann Cavoukian, é muito mais amplo e confere uma gama muito maior de definições, fundamentos, regras e conceitos do que a singela ideia de considerar o direito de privacidade desde o início de um projeto ou desenvolvimento de um sistema.

²⁹ CAVOUKIAN, Ann. **Privacy by Design**. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010, p. 1. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em 2 set. 2022.

³⁰ *Ibid.*, p.1-5.

Para a discussão pretendida neste trabalho, traça-se aqui um divisor de águas em relação às definições e atribuições que foram esboçadas acima. Quando se visa a incorporação de um projeto para adequação à nova regulação imposta, ainda mais um regramento vasto, que traz consideráveis definições, conceitos, obrigações, responsabilidades e penalidades, conforme visto no capítulo 2 deste trabalho, é necessário adotar a melhor prática possível como norte.

Com efeito, a aplicação da metodologia da *Privacy by design*, em um determinado sistema, produto, ou, já aproveitando a inserção proposta deste trabalho, para a estrutura do *software* ERP e seu respectivo contrato de licença de uso, deverá observar e cumprir todas as diretrizes expostas nos 7 (sete) artigos acima mencionados.

A partir daqui, visando traçar as mais importantes informações e reflexões possíveis, serão aprofundados um a um os princípios fundamentais da metodologia *Privacy by design*, o que embasará as propostas de reestruturação e de melhores práticas que serão feitas no capítulo 4.

(1) *Proactive not Reactive; Preventative not Remedial* (Proativo não Reativo; Preventivo não corretivo) - A proatividade é a regra deste princípio. As empresas devem antecipar eventuais problemas e falhas na segurança e na estrutura de privacidade, visando minimizar ou extinguir potenciais vulnerabilidades.

(2) *Privacy as the Default Setting* (Privacidade como configuração padrão) – Importante princípio que acabou se tornando um novo conceito, também largamente utilizado atualmente, o *Privacy by default*. A ideia aqui é que uma operação, relação, produto ou serviço, que colete dados, deve ter estabelecidas configurações padrão de coleta mínima e restrita, visando garantir maior privacidade do usuário.

(3) *Privacy Embedded into Design* (Privacidade incorporada ao design) – Busca a mesma concepção de definição de privacidade incorporada no design, na estrutura do produto ou do serviço, tratando-o como um requisito e não um bônus.

(4) *Full Functionality – Positive-Sum, not Zero-Sum* (Funcionalidade completa - Soma Positiva, não Soma Zero) – Busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva, afastando a ideia de serem necessários *trade-offs* para que se proteja

conjuntamente a segurança e a privacidade, buscando essa dupla proteção.³¹ Busca afastar a falsa dicotomia de que é necessário abrir mão da privacidade pra se ter segurança, ou vice-versa.

(5) *End-to-End Security – Full Lifecycle Protection* (Segurança de ponta a ponta – proteção completa do ciclo de vida) – A segurança e a proteção devem estar compostas em todo o ciclo da vida dos dados na operação da empresa.

(6) *Visibility and Transparency – Keep it Open* (Visibilidade e Transparência – Mantenha-o aberto) – Busca garantir à todas as partes interessadas, que seja qual for a prática de negócios ou tecnologia envolvida, a empresa está operando de acordo com as promessas e objetivos declarados, garantindo a sujeição à verificação independente.

(7) *Respect for User Privacy – Keep it User-Centric* (Respeito pela privacidade do usuário – Mantenha-o centrado no usuário) – O respeito à privacidade do usuário deve ser o centro e o foco da operação. Esse princípio traduz o respeito que as corporações devem ter com os titulares dos dados pessoais. É um princípio que visa afastar a coisificação do indivíduo.³²

Sobre a metodologia *privacy by design*, Jonas Valente traz algumas técnicas para uma melhor assimilação dos princípios:

- a) Minimizar – os dados coletados devem ser reduzidos ao mínimo possível;
- b) Esconder – os dados e sua inter-relação não devem ser publicizados;
- c) Separar – o processamento dos dados deve se dar em compartimentos separados, sempre que possível;
- d) Agregar – os dados devem ser processados com alto nível de agregação e com o mínimo de detalhes;
- e) Informar (transparência) – os sujeitos dos dados devem ser sempre informados dos processamentos de suas informações;
- f) Controlar – os sujeitos dos dados devem ter controle sobre a coleta e o processamento de seus dados;
- g) Fiscalizar e aplicar as leis – as políticas de privacidade devem estar em conexão com as exigências legais e devem poder ser fiscalizadas;
- h) Demonstrar – controladores de dados devem poder demonstrar o respeito às políticas de privacidade e aos requisitos legais.³³

³¹ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2020. p. 425.

³² LARA, Larissa Leandro. A Importância do Plano Emergencial de Incidente de Vazamentos de Dados Diante de um cenário extremamente incerto. In: TEIXEIRA, Tarcisio (coord.). **Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados**. Salvador: JusPodivm, 2021. p. 160.

³³ VALENTE, Jonas. **Promovendo a privacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies**. Privacidade em perspectivas. Rio de Janeiro: Lumen Juris, 2018. p. 119.

Uma vez estudados todos os princípios e feita uma reflexão conceitual da metodologia *Privacy by design*, passar-se-á, no tópico a seguir, a dialogar referido tema com as próprias disposições da Lei Geral de Proteção de Dados.

A metodologia *privacy by design*, através dos sete princípios acima elencados e explicados, serão enquadrados com disposições legais trazidas na Lei Geral de Proteção de Dados, sendo importante essa ligação para auxiliar no seu aprofundamento, além de discutir e analisar pequenas diferenciações em seu conteúdo.

3.2 A aplicabilidade da metodologia *Privacy by Design* na Lei Geral de Proteção de Dados

Quando se discute aplicabilidade, se discute a possibilidade de presença com qualidade de algo em algum lugar, para este caso, a presença do conteúdo da metodologia *Privacy by design* na letra da Lei Geral de Proteção de Dados dá subsídios ao deslinde da reestruturação proposta neste trabalho.

O fato de alguns pontos desta metodologia estarem intrinsecamente nos artigos de referida disposição legal, não necessariamente implica dizer que se adequando de forma singela à lei, haveria a adequação com base íntegra nas disposições que a metodologia propõe, tampouco o inverso disso pode ser considerado verdadeiro.

Daí uma das diferenciações que se discute neste trabalho, em específico, neste capítulo. Há a necessidade de diferenciar e referenciar os pontos e atributos em que a Lei Geral de Proteção de Dados se pautou no GDPR (Regulamento Geral de Proteção de Dados da União Europeia), e por consequência, na *Privacy by design*, e os pontos em que a metodologia atinge horizontes mais distantes, buscando uma base sólida de princípios norteadores, proposta buscada como fonte central de um programa de conformidade legal para os contratos de licença de uso de *software* ERP.

Há quem defenda que a metodologia *Privacy by design* foi introduzida na Lei Geral de Proteção de Dados, através do artigo 46, parágrafo segundo, abaixo transcrito:

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

alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

(...)

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

Sobre o assunto, Daniel Arbix comenta:

Tanto a Lei 13.709/2018 (Lei Geral de Proteção de Dados) quanto o Regulamento Geral de Proteção de Dados (General Data Protection Regulation) europeu têm como aspecto fundamental o princípio de que a privacidade deve ser protegida desde a concepção de um produto ou serviço, e que esta preferência deve ser mantida da mesma forma por todos os ciclos de desenvolvimento e inovação e ao longo das interações entre controladores e operadores e titulares de dados pessoais, como na obtenção de consentimento, na determinação de mecanismos de controle de dados e na delimitação das finalidades e do escopo de processamento.³⁴

No mesmo sentido, Carlos Affonso Pereira de Souza indica que a Lei Geral de Proteção de Dados recepciona esta ideia da metodologia *Privacy by design*, ou seja, a noção de que produtos e serviços precisam tomar a segurança e o sigilo de dados como um elemento a ser levado em conta em todas as suas fases de concepção, desenvolvimento aplicação e avaliação.³⁵

E complementa, delimitando que a positivação do conceito na LGPD não foi tão explícita como a que ocorreu na legislação europeia, mas é possível extrair a *ratio* criada na década de 1990 do mencionado art. 46, parágrafo segundo, indica, ainda, que se percebe nele a inspiração da metodologia criada.³⁶

De fato, o art. 46, parágrafo segundo, assim com outros dispositivos da Lei Geral de Proteção de Dados, contemplam, em parte, o conteúdo da metodologia *Privacy by design*, mas conforme acima já proposto, simplesmente observando as medidas do art. 46 desde a sua concepção, ou seja, simplesmente observando a normativa de referida disposição, não necessariamente está sendo aplicada a metodologia *Privacy by design*, daí um necessário recorte que baseia a proposta deste trabalho.

³⁴ ARBIX, Daniel. A importância da privacidade por Design e por Default (*Privacy by design and Default*). In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020, p.56.

³⁵ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2020. p. 423.

³⁶ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2020. p. 424.

A ideia é de que simplesmente aplicando a letra da lei na concepção de seu produto ou serviço, não implica dizer que fora aplicada a metodologia em questão, justamente por sua concepção traduzida nos sete princípios já discutidos no capítulo anterior.

É arrojado dizer, portanto, que houve a aplicação, talvez, da definição resumida de *Privacy by design* proposta pelo GDPR e em sequência, na LGPD, mas não o seu amplo conceito metodológico abarcado pelos 7 (sete) princípios fundamentais criados pela Professora Ann Cavoukian.

Fato é, que não somente no art. 46, parágrafo segundo, da LGPD, podemos verificar concepções e conceitos da mencionada metodologia. Buscando aprofundar este debate, é salutar trazer à discussão outros pontos em que a LGPD aplicou de forma intrínseca alguns dos princípios trazidos pela metodologia *Privacy by design*.

De forma intrínseca, pois, em sua grande maioria, o conceito e definição de alguns dos sete princípios da metodologia *Privacy by design* são mais comumente encontrados também junto às definições dos princípios criados pela Lei Geral de Proteção de Dados, aqueles elencados nos dez incisos do art. 6º.

O primeiro princípio da metodologia *Privacy by design*, proativo não reativo; preventivo não corretivo, pode ser encontrada, por exemplo, em dois princípios elencados no art. 6º da LGPD, os incisos VII e VIII, princípios da segurança e da prevenção, respectivamente.

A ideia de se ter a segurança e a prevenção como antecipação ao problema e não visando simplesmente sanar o problema após ocorrido, é justamente a postura buscada pela metodologia *Privacy by design* em seu primeiro princípio norteador.

Em relação ao segundo princípio – privacidade como configuração padrão - Bruno Bioni observa que o conceito de *Privacy by default*, já comentado no capítulo passado, pode ser extraído do princípio da necessidade, ao lado do da responsabilização e prestação de contas da LGPD (Art. 6º, incisos III e X).³⁷

O quarto princípio da *Privacy by design* – funcionalidade total, que busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva – está de certa forma

³⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 200.

inserido no contexto que se buscou pelo texto da LGPD, uma vez que cria um panorama legal em que diferentes princípios e regras devem ser observados simultaneamente.³⁸

Carlos Affonso Pereira de Souza sustenta que o quinto princípio, segurança de ponta a ponta, faz referência ao ciclo total de vida dos dados, sendo também um dos princípios norteadores da proteção de dados pessoais. A LGPD traz essa ideia não apenas no princípio da necessidade (Art. 6º, inciso III), mas também no direito à eliminação dos dados disposta no artigo 18, inciso IV.³⁹

O sexto princípio - Visibilidade e Transparência – Mantenha-o aberto – Busca garantir à todas as partes interessadas, que seja qual for a prática de negócios ou tecnologia envolvida, a empresa está operando de acordo com as promessas e objetivos declarados, garantindo a sujeição à verificação independente. Os conceitos e disposições deste princípio podem ser encontrados no artigo 6º da LGPD, primordialmente nos princípios da finalidade, adequação, livre acesso e transparência, elencados nos incisos I, II, IV e VI, respectivamente.

Por último, o sétimo princípio, respeito pela privacidade do usuário, se associa com a ideia do princípio da transparência, presente no inciso VI do art. 6º da LGPD, além de também se relacionar com os direitos do titular, elencados no art. 9º.

Estes são alguns dos exemplos onde é possível se assimilar os princípios do *Privacy by design* com as disposições e conceitos trazidos na Lei Geral de Proteção de Dados. Não obstante, é possível verificar a ideia conceitual mais à fundo no artigo 46, parágrafo segundo, da LGPD, conforme largamente defendido por importantes Autores.

A ideia da aplicação das medidas de segurança desde a concepção, desde a criação do produto ou do serviço até a sua execução, evidentemente é a base central do contexto da metodologia *Privacy by design*. Todavia, apesar de o artigo 46 da LGPD dispor sobre medidas de segurança, técnica e administrativa a serem observadas pelo agente de tratamento, visando a proteção de dados, deve-se ter em mente que não há uma identificação clara e objetiva de quais seriam essas medidas de segurança, técnica e administrativa.

³⁸ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2020. p. 425.

³⁹ *Ibid.*

Sobre o assunto, Ronaldo Lemos e Sérgio Branco delimitam que caberá, assim, à Autoridade Nacional de Proteção de Dados identificar quais são os padrões mínimos a serem observado por todos a quem a norma se destina. Isso permitirá, ao menos em tese, a atualização periódica desses padrões, deixando-os em conformidade com o estado da arte e alinhados às demandas mais recentes de proteção de dados pessoais dos indivíduos⁴⁰.

De igual importância mencionar que referidos padrões e medidas de segurança poderão ter extensões diferentes para cada tipo de empresa, a depender da atividade de atuação, quantidade de dados em tratamento, nível de transnacionalidade, enfim, há diferentes níveis de medidas que poderão ser implementados pelas empresas.

Por exemplo, é claro que empresas que transacionam dados, ou seja, que tem uma atuação internacional, devem ter uma regulamentação mais complexa do que empresas de médio porte, que só atuam no âmbito nacional.

De outra banda, a quantidade de dados tratados e finalidade de seu tratamento também é um aspecto importante a ser considerado para se pensar em um segundo nível de regulação, que pelo que se espera da Lei Geral de Proteção de Dados, será buscado pela Autoridade Nacional de Proteção de Dados, que já tem previsões para se tornar uma Agência Nacional reguladora.

Ronaldo Lemos e Sérgio Branco finalizam explicando que ainda é cedo pra saber qual o verdadeiro impacto da *Privacy by design* no cotidiano das operações relativas à proteção de dados, apesar de reconhecerem que, ainda assim, a LGPD deu um passo muito importante e definitivo para atender de modo mais adequado a demanda por segurança de dados no tempo presente.⁴¹

Para o contexto deste trabalho, isto é, para a aplicabilidade da metodologia *Privacy by design* face à reestruturação dos contratos de licença de *software Enterprise Resource Planning*, busca-se a conformidade além da própria LGPD, mas de conceitos, definições e medidas mais abrangentes, conforme visto acima e melhor explorado a partir do próximo e último capítulo.

⁴⁰ LEMOS, Ronaldo. BRANCO, Sérgio. *Privacy by design: Conceito, fundamentos e aplicabilidade na LGPD*. In: MENDES, Laura Schertel. DONEDA, Danilo. SARLET, Ingo Wolfgang. JUNIOR, Otavio Luiz Rodrigues. **Tratado de Proteção de Dados Pessoais**: Rio de Janeiro: Forense, 2021, p. 457.

⁴¹ *Ibid.*, p. 457.

4 O SOFTWARE ERP E SUA CORRESPONDENTE REESTRUTURAÇÃO CONTRATUAL VISANDO CONFORMIDADE COM A LGPD COM BASE NA APLICAÇÃO DA METODOLOGIA *PRIVACY BY DESIGN*

Nos capítulos acima, já foi considerado que a Lei Geral de Proteção de Dados trouxe disposições que obrigam a busca da conformidade por algumas empresas, em específico, às empresas licenciadas e licenciadoras na operação da licença do *software* ERP.

Foi também abordado, que a metodologia *privacy by design* se aplica de forma direta e esparsa, a partir de forte influência do GDPR, no ordenamento jurídico composto pela LGPD, muito embora, conforme visto no tópico acima, adequar-se simplesmente à LGPD não significa necessariamente estar em consonância com todas as diretrizes e princípios da metodologia *privacy by design*.

Todavia, há certas diferenças entre a aplicação do contexto de *privacy by design* composto na Lei Geral de Proteção de Dados e a própria metodologia *privacy by design*, através dos sete princípios aplicados um a um no projeto de reestruturação visando a conformidade.

Uma vez aprofundados referidos temas, em específico nos contratos de licença de *software*, este capítulo terá o papel de assimilar os conteúdos abordados e buscar responder à pergunta central deste trabalho: Buscando a conformidade com a LGPD, é possível reestruturar o contrato de licença de *software* ERP em uma operação do comércio varejista com base na metodologia *Privacy by design*? Quais são os ganhos atrelados ao uso desta metodologia?

4.1 A viabilidade da utilização do conceito metodológico *Privacy by Design* no software ERP e em seu respectivo contrato

A primeira questão a ser debatida, já levantada acima, seria delimitar se simplesmente buscando a aplicação dos sete princípios do *Privacy by design* no software ERP, a empresa, independentemente de seu ramo de atuação, estaria em plena conformidade com a Lei Geral de Proteção de Dados.

Já num contexto conclusivo, após uma sucinta análise da metodologia e dos impactos da LGPD e sua descritiva normativa nas empresas, o que fora feito nos capítulos anteriores, é ousado delimitar, desde já, que a resposta para essa questão é não. Ao se aplicar pura e simplesmente todos os princípios da metodologia *Privacy by design* em um projeto/operação empresarial que trata dados, a empresa não estará em conformidade com a ampla cadeia de obrigações, direitos e responsabilidades que a Lei Geral de Proteção de Dados trouxe à tona.

Em resposta mais aprofundada ao recorte temático deste trabalho, é possível responder que aplicando os sete princípios do *Privacy by design*, uma empresa licenciante de *software* ERP para o setor varejista, também não estaria em plena conformidade com a Lei Geral de Proteção de Dados.

Todavia, para uma empresa licenciante de *software* ERP do setor varejista, na linha da operação que foi retratada nos capítulos anteriores, a aplicação da metodologia *Privacy by design* pode ser utilizada como os primeiros passos visando estabelecendo um norte na reestruturação contratual da licença de uso deste *software*, visando a conformidade com a Lei Geral de Proteção de Dados.

A aplicação da metodologia *Privacy by design* desde o início do projeto de reestruturação visando conformidade com a Lei Geral de Proteção de Dados, tende a estabelecer uma estrutura sólida, com base principiológica, que busca o resultado dotado de boas práticas e mudança de paradigma empresarial.

Outrossim, a aplicação da metodologia *Privacy by design* desde o início do projeto de reestruturação visando conformidade com a Lei Geral de Proteção de Dados tende a ser um instrumento facilitador para se buscar e aplicar as diretrizes regulatórias trazidas em referida lei, uma vez que a partir da larga abrangência dos sete princípios a serem aplicados, de forma mais fácil e com mais robustez é possível atingir a conformidade com a regulação composta na lei.

A maioria das empresas busca a conformidade, simplesmente para cumprir a lei, visando não sofrerem sanções administrativas e fiscalizatórias, além de se resguardar de eventuais problemas jurídicos, contingências e perdas financeiras.

No que concerne à responsabilidade corporativa, deve-se tutelar a viabilidade econômico-financeira das organizações, de modo a reduzir as externalidades negativas de

seus negócios e de suas operações e aumentar as positivas, levando em consideração os diversos capitais, a partir da perspectiva do curto, médio e longo prazos.⁴²

Segundo Elismar Álvares, Celso Giacometti e Eduardo Gusso, a boa governança está calcada em princípios que inspiram e norteiam o funcionamento das empresas e outras organizações e lhe propiciam maior credibilidade e criação de valor.⁴³

Essa mudança de paradigma de cultura empresarial, visa não só cumprir literalmente a Lei e afastar eventuais sanções, mas, de fato, priorizar a privacidade do cidadão, através das melhores práticas da operação de tratamento de dados do sistema ou projeto.

Referida mudança de paradigma, atualmente rende frutos às empresas, que já a utilizam como marketing, visando a valorização da marca no mercado, além de mais reconhecimento por clientes e consumidores. Aliás, a prática de privacidade e proteção de dados já vem sendo observada como um dos compromissos compostos na agenda ESG “*Environmental, Social and Governance*”, traduzido do inglês, ASG – Ambiental, Social e Governança.

Neste sentido é a proposição deste trabalho. A proposta de reestruturação contratual de licença de uso de *software* ERP que se almeja, não é aquela em que meramente se cumprem artigos da lei, como o GDPR ou a LGPD, mas sim aquela que muda um paradigma corporativo, aquela que muda toda uma cultura empresarial, que vem crescendo constantemente desde o início dos avanços tecnológicos e ainda não havia se estabilizado para avistar esse direito que é a privacidade, e para a busca desse objetivo, a metodologia *privacy by design* se mostrou fundamental.

Portanto, além de ser completamente viável, é amplamente recomendável, que se considere, no projeto de conformidade com a LGPD de uma empresa licenciante de *software* ERP para o setor varejista, a utilização como norte da metodologia *privacy by design*, desde o início da reestruturação do *software* e do respectivo contrato que reflete a operação, com a ressalva, conforme acima já abordado, de que também há a necessidade de traçar um caminho conjunto com a específica regulação da LGPD para se buscar a conformidade efetiva.

⁴² DA ROCHA, Claudia. Boas Práticas e Governança Corporativa na ótica da Lei Geral de Proteção de Dados. In: TEIXEIRA, Tarcisio (coord). **Empresas e Implementação da LGPD** – Lei Geral de Proteção de Dados. Salvador: JusPodivm, 2021. p. 87.

⁴³ ÁLVARES, Elismar; GIOACOMETTI, Celso; GUSSO, Eduardo. **Governança corporativa: um modelo brasileiro**. Rio de Janeiro: Elsevier, 2008, p. 43.

No projeto de conformidade com a LGPD, há a necessidade de se atentar não apenas para o *Privacy by design*, conforme já previsto, mas por conta da percepção de que os seus sete princípios se amoldam à operação de forma mais abstrata, mais principiológica, uma vez que a normativa legal da LGPD traz obrigações e implicações mais objetivas e concretas, essas que necessitam de uma direta aplicação, daí, talvez, a diferenciação da necessidade de não se utilizar apenas a metodologia *Privacy by design*.

Ann Cavoukian defende que o conceito *privacy by design* antecipa a ideia de que o futuro da proteção de dados depende idealmente de uma mudança organizacional, transformando o modo de operação padrão de entidades que lidam com produtos ou serviços ancorados no tratamento de dados ou que possam impactar a privacidade de seus usuários e de terceiros.⁴⁴

Assim, a proteção de dados não será apenas assegurada pelo cumprimento de parâmetros regulatórios, mas sim por meio de um repensar por parte do agente de tratamento de dados sobre como a sua atividade pode impactar o usuário e terceiros.⁴⁵

Em outras palavras, a proposta de reestruturação e o empenho pelas boas práticas da operação, não buscará apenas o cumprimento de eventual disposição legal aplicado pela Lei Geral de Proteção de Dados importado da legislação Europeia sobre o tema, mas sim, propor, com fundamento no conceito metodológico acima apontado, o alcance desta mudança de concepção operacional.

Uma vez já abordada a temática sobre a viabilidade e conveniência para a utilização da metodologia *privacy by design* na reestruturação do contrato de licença de uso de *software* ERP, necessário discutir sobre a programação e desenvolvimento do próprio *software*, segunda proposta deste subcapítulo.

A problemática se desenvolve também a partir deste ponto. Para adequar-se à Lei Geral de Proteção de Dados não basta que os instrumentos contratuais estejam em conformidade com a recente legislação, é preciso, mais do que tudo, que o contrato reflita a operação da empresa na prática, isto é, os processos internos da empresa devem também observar a padronização trazida nos respectivos instrumentos de contratação.

⁴⁴ CAVOUKIAN, Ann. Publicação da *Information and Privacy Commissioner of Ontario*. Publicado em agosto de 2009. Revisado em janeiro de 2011. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso 2 dez. 2022.

⁴⁵ *Ibid.*

É certo, conforme já explicado neste trabalho, que o contrato de licença deve refletir a operação composta no *software ERP* que é licenciado. Assim sendo, em nada adianta efetuar a reestruturação do contrato, se a própria operação não refletir identicamente as disposições técnicas e legais ali compostas, e vice-versa.

Aliás, um dos objetivos de autoridades de regulação, através das auditorias internas, é justamente investigar se toda a composição de políticas, contratos e de termos de tratamento apresentados no ato da fiscalização, correspondem à operação constituída de tratamento de dados.

Em outras palavras, a composição jurídica do contrato deve refletir a prática da operação no dia a dia de tratamento de dados na empresa. Daí a necessidade de se ter em mente que não basta, por óbvio, escrever a política de privacidade mais robusta possível, montar a cláusula contratual que mais lhe garanta benefícios em uma relação bilateral de tratamento de dados, e referidas disposições não refletirem, na prática, as reais operações de tratamento da empresa.

A propósito, o primeiro grande desafio do programa de conformidade é entender o contexto da operação que trata dados, esmiuçar as obrigações, responsabilidades e delimitação de agentes de tratamento nela envolvidas, por fim, montar a política de privacidade, contrato e termo de tratamento de dados, entre outros documentos relevantes, que garanta fidelidade ao contexto operacional, além de ser um objetivo realizável e plausível de ser alcançado pela empresa.

Importante delinear sobre este contexto de objetivo apto, ou seja, algo que seja possível de ser realizado, justamente porque, nos termos de correção e autorregulação regulada, conforme já explícito neste trabalho, há diferentes níveis de empresa, logo, há diferentes níveis de investimento técnico, tecnológico e jurídico, nas mais variáveis categorias de programa de conformidade possíveis.

Sobre o assunto, Tarcisio Teixeira e André Pedroso Kasemirski delimitam:

Quando se pensa especificamente no *compliance* de dados pessoais, há de se reconhecer a insuficiência da regulação clássica fornecida pelo Estado, pois não detém o conhecimento técnico necessários dos setores econômicos, bem como sob risco de tornar eventuais regras e parâmetros obsoletos em razão da evolução tecnológica.

Nesse sentido, se mostra como alternativa a autorregulação regulada, consistindo como aquela em que as empresas de forma individualizada ou ainda agrupadas em setores, conforme art. 50 da LGPD, elaborem suas regras e processos, de acordo com o risco e atividade econômica que desenvolvem, e levam até chancela estatal para homologação ou ratificação, o que promove maior segurança jurídica e legitimidade aos procedimentos desenvolvidos.⁴⁶

Uma vez concluído que é necessária a reestruturação do contrato de licença à luz da Lei Geral de Proteção de Dados, sob o aspecto do *software* ERP, também se mostram necessárias alterações programáticas do sistema para que o mesmo passe a abarcar os fundamentos e princípios postos na Lei, além de garantir os direitos dos titulares que lá também estão expostos.

Portanto, aliado à reestruturação do contrato, a busca da conformidade também passará por uma reestruturação do *software*, que daí deverá contemplar toda a atividade de tratamento do agente, seja operador ou controlador, no formato das proposições do subcapítulo 2.4.

Considerando a necessidade de atentar-se à tão comentada disposição do art. 46, parágrafo 2º, da Lei Geral de Proteção de Dados, principalmente acerca da observância de medidas de segurança, técnicas e jurídicas desde a concepção do produto ou serviço, o *software* deverá sofrer uma remodelação em sua arquitetura de coleta, armazenamento e classificação de dados, sendo inseridas todas as disposições da Lei.

Conforme acima já exposto, a metodologia *Privacy by design*, teria forte aplicabilidade na infraestrutura técnica do *software*, auxiliando o programador na edição e atualização das ferramentas e rotinas genérica disponíveis ao licenciante e ao licenciado, a partir da aplicação de seus sete princípios, visando a adoção de melhores práticas de segurança, técnica, administrativa e jurídica.

Mas nem sempre referida metodologia poderá ser aplicada ao *software*. Haverão casos em que a estrutura e o desenvolvimento da operação do *software* estarão tão robustos e avançados que será praticamente impossível reescrevê-lo com observância dos 7 princípios já abarcados, principalmente a ideia de privacidade desde a concepção. Quando não está a se

⁴⁶ TEIXEIRA, Tarcisio; KASEMIRSKI, André Pedroso; Compliance (Conformidade) de dados pessoais para microempresas: Autorregulação regulada e requisitos para efetividade. *In*: TEIXEIRA, Tarcisio (coord). **Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados**. Salvador: JusPodivm, 2021. p. 30.

desenvolver o *software* do início, para que observe os parâmetros da metodologia *privacy by design* os desafios são maiores em termos de readaptações, reinscrições e retificações.

Tratam-se de alguns impedimentos operacionais, na busca das proposições a serem apresentadas neste trabalho, que foram encontradas no decorrer da pesquisa. Basta imaginar como exemplo uma empresa Licenciante já ativa no mercado há mais de 10 (dez) anos, que conta com mais de 1.000 (mil) clientes em aberto. Cada um desses clientes-Licenciados é um comércio varejista que já está com o *software* ERP consolidado e em pleno funcionamento há alguns anos. Com o advento da LGPD, mesmo com o interesse e necessidade de alteração da estrutura operacional do *software*, mostra-se técnica e financeiramente impossível que a empresa refaça o seu *software* já pronto e aperfeiçoado à luz da metodologia *privacy by design*.

Conclui-se, portanto, que não se pode buscar a conformidade com a atual Lei Geral de Proteção de Dados no contexto de uma operação de licença de *software* ERP, sem alterar a ferramenta jurídica do contrato e a própria estrutura informatizada do *software* ERP licenciado, o que também nem sempre será viável técnica ou operacionalmente à empresa licenciante.

Em ambos os procedimentos, a metodologia *privacy by design* teria forte contribuição não só para a busca da conformidade com a legislação e regulação, mas para a mudança de um paradigma cultural empresarial, obtendo-se a privacidade dos titulares e indivíduos envolvidos e agregando valor à empresa Licenciante e também aos clientes Licenciados que operam de seu *software*, muito embora existem impeditivos técnicos e também financeiros para que isso se desenvolva de tal forma.

4.2 A aplicação da metodologia *Privacy by design* na operação e nos contratos de licença de uso de *software* ERP no setor varejista – Proposições e medidas em busca da conformidade

É árduo o trabalho de atribuir proposições e medidas para qualquer tipo de conformidade legal. No caso dos contratos de licença de *software* ERP, seguindo a metodologia *Privacy by design*, com o objetivo de ser o núcleo deste trabalho, este subcapítulo buscará abordar de forma prática e exemplificativa, sob a ótica do setor varejista, o caminho da conformidade com a Lei Geral de Proteção de Dados.

Em primeiro ponto, resta claro que a partir das disposições nos capítulos anteriores, que a aplicação da metodologia *Privacy by design* será abordada partindo do *software* para o contrato de licença. Ou seja, não há possibilidade de você aplicar a metodologia para conformidade com a Lei Geral de Proteção de Dados apenas no *software* ou no contrato de licença, isso pois, um deverá refletir o outro.

Não se alcança a conformidade jurídica, ou seja, não se cumpre a legislação regulatória sobre o tema apenas alterando disposições contratuais sem uma efetiva alteração na operação que é revestida por aquele contrato. Em caso contrário também não se atinge a almejada conformidade, apenas alterando a operação do *software* para fielmente cumprir a legislação sem, contudo, delimitar contratualmente sobre essa alteração, uma vez que, conforme visto no capítulo dois, as formas de regulação abrangem uma necessária fidelidade da documentação interna da empresa.

Portanto, tanto a operação e desenvolvimento do *software* na prática quanto sua correspondente estrutura contratual, deverão estar em plena sintonia, e ambas, caso assim seja verificado, deverão sofrer a reestruturação proposta neste trabalho.

Feita essa consideração, uma importante reflexão também é necessária para dar início ao presente subcapítulo. Pensando em reestruturação e na necessidade de isso passar pela operação, ou seja, pelo *software*, encontramos o primeiro grande obstáculo, qual seja, a inviabilidade técnica de se aplicar o *Privacy by design* em um *software* já escrito e finalmente desenvolvido, o que já foi tema pincelado no tópico passado.

Em uma reflexão feita a partir do próprio nome da metodologia, não há como desenvolver uma metodologia que exige inserções, reinserções e proposições desde a sua concepção, em um *software* que já se encontra finalizado. Reescrever, a partir do desenvolvimento técnico, algumas linhas do *software* para a readequação a partir dos princípios da metodologia *Privacy by design*, evidentemente seria o cenário ideal para a busca da conformidade legal, todavia, nem sempre será possível alcançar este resultado do ponto de vista da viabilidade técnica.

Este trabalho não passará pela discussão de viabilidade técnica na possibilidade de reinscrição das linhas do *software*, uma vez que fugiria completamente o tema e escopo jurídico-contratual que se busca no mesmo.

Traçando um pano de fundo para o aprofundamento quanto aos princípios da metodologia em estudo, para os casos em que não houve viabilidade técnica de reinscrever o *software* em adequação às diretrizes trazidas pela metodologia *Privacy by design*, a proposição sugerida seria a criação de um relatório de impacto identificando os pontos onde o *software* já escrito não atende os princípios de referida metodologia, criando-se no dispositivo contratual os pontos de mitigação de eventual não conformidade.

Feita essa consideração, é salutar que toda e qualquer proposição, até mesmo pela proposta do trabalho, será necessariamente pautada a partir dos 7 (sete) princípios da metodologia *Privacy by design*, sendo apresentada em formato de termos e políticas. Neste sentido, o formato de aplicação da metodologia passa pela necessidade da implementação de um programa de conformidade de dados, o que dará a estrutura necessária para a busca da conformidade com a Lei Geral de Proteção de Dados.

A busca da conformidade com a Lei Geral de Proteção de Dados, vem sendo o objetivo das empresas brasileiras, ao menos para aquelas que se preocupam em seguir diretrizes legais e/ou agregar algum tipo de valor à operação e ao nome da empresa. Essa conformidade está escorada em vários projetos que podem ser aplicados na empresa, o que está intimamente ligado à ideia da criação das diretrizes de atendimento aos artigos 46⁴⁷ e 50⁴⁸ da Lei Geral de Proteção de Dados.

Conforme já visto, não apenas grandes empresas estão buscando a conformidade, a partir da ideia da autorregulação regulada, já vista acima, pequenas e médias empresas, visando manter contratação com entes públicos ou até mesmo se relacionarem com empresas maiores, também estão buscando adaptações em prol da conformidade.

⁴⁷ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

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

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

⁴⁸ Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

É certo, todavia, que a extensão das responsabilidades, regulações, fiscalizações e penalidades à essas pequenas e médias empresas, vem se mostrando praticamente nulo no ambiente da Autoridade Nacional de Proteção de Dados – ANPD, e também em demais órgãos como o Ministério Público e o PROCON. Isso se tornou ainda mais presente quando a ANPD divulgou a aprovação do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.⁴⁹

Dito isso, em direção de embasar as melhores proposições e medidas para a conformidade com a Lei Geral de Proteção de Dados através da aplicação do *Privacy by design*, é necessário traçar os seus respectivos conceitos gerais, em seguida, o devido aprofundamento nos aspectos técnicos e jurídicos, à luz da metodologia *Privacy by design*.

Nessa linha, nos termos do que já fora proposto no capítulo 2, no item 2.4, a criação de um programa de conformidade com a Lei Geral de Proteção de Dados, pode ser considerado, conforme proposto no art. 50 da mencionada lei, como proposições de autorregulação regulada, isto é, a partir do conhecimento do meio empresarial em questão - para o caso vertente da licença ao comércio varejista – e a adoção de uma metodologia que busca a melhor versão em termos de privacidade e tratamento de dados, conforme é a *Privacy by design*, a própria empresa cria uma política de privacidade que abrange essencialmente todas as medidas necessárias para a correta e fiel aplicação da lei, mas não só isso, da adoção da melhor prática operacional.

De outra banda, mas também de singular importância a ser fixada como base, antes de adentrar às proposições e medidas, uma a uma, partindo dos princípios da *Privacy by design*, o que já foi abarcado em tópico sobre a natureza do contrato de licença do *software* ERP, seria a sua inerente característica de prestação de serviços atrelada à licença do *software* e sua constante transmissão de dados. Isso foi bastante discutido nos tópicos anteriores, sendo um dos pontos singulares das diferenças deste tipo de contrato, o que também necessita um olhar atento do aspecto da conformidade.

Alinhado ao desenvolvimento do software ERP e toda a estrutura para a sua concessão ao licenciado, necessariamente passa-se pela prestação de serviços no sentido de

⁴⁹ BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Diário Oficial [da] República Federativa do Brasil, Brasília, 28 de janeiro de 2022.

instalação, realização de *backup* e portabilidade de dados, treinamento e, eventualmente, correções de bugs informatizados ou também correções de erros e problemas de *hardware*, o que também é feito *in loco*.

A prestação de serviços, da forma descrita acima, também garante o acesso local aos dados da licenciada, feita pelos colaboradores da licenciante, o que tem como objetivo a correta entrega do *software* e suas diretrizes, esse acesso local, além de toda a estrutura informatizada que delimita a operação, também deve ter uma atenta regulamentação interna pela empresa, o que se dará também a partir das medidas e proposições que a seguir serão expostas.

Ultrapassadas essas premissas introdutórias, passa-se às proposições e medidas a serem adotadas à luz dos sete princípios da metodologia *Privacy by design*, visando trilhar o caminho da conformidade.

A ideia de conformidade, neste ponto, induz à uma reflexão que não se confunde com a reestruturação do contrato licença. Para que a estrutura operacional da empresa tenha condições de receber sua correspondente reestruturação contratual, conforme já aprofundado, é necessário que a operação da empresa esteja em acordo com questões técnicas mínimas no que tange aos requisitos trazidos pela LGPD, e no caso da proposição deste trabalho, com a metodologia *Privacy by design*, para daí em diante instrumentalizar a operação de uma forma segura, descritiva e com os devidos liames obrigacionais e de responsabilização.

Portanto, em dois passos anteriores à dita reestruturação contratual, está a necessidade de verificar se há viabilidade técnica na aplicação da metodologia *Privacy by design*. Em um passo anterior à dita reestruturação contratual, está o alinhamento da operação com instrumentos internos que refletem a operação, estes que serão mais adiante aprofundados. Realizados esses passos preliminares, a empresa Licenciante do *software* ERP terá plenas condições técnicas para o importante passo do contrato.

Percebe-se, portanto, que não se trata de uma mera reestruturação contratual, e para que aqui fique claro, o termo reestruturação contratual, no contexto deste trabalho, está intimamente ligado à alteração das disposições do contrato de licença de software ERP entre Licenciante e Licenciado, buscando constar a fixação de ações, obrigações e responsabilidades no tratamento de dados daquela operação, mas antes disso, a necessidade

prévia de adequar a operação do *software* e instrumentalizar essa adequação em formato de políticas que lhe garantam a correlata e futura alteração contratual.

Veja que não se trata da inclusão de uma cláusula, de um anexo ou de um aditivo que contemple disposições sobre a Lei Geral de Proteção de Dados. É preciso ter um substrato técnico interno da empresa para definir melhores padrões em contrato. O termo reestruturação contratual, que vem sendo constantemente utilizado neste trabalho, toma outro contexto a partir das disposições deste capítulo.

A criação de instrumentos, no formato de políticas divididas por assuntos e setores auxilia no englobamento de todas as necessidades de um *software* ERP licenciado à uma empresa do setor varejista, também como uma proposição para melhor assimilar os princípios da metodologia *Privacy by design*, passamos pelas seguintes políticas:

Política de privacidade – Tem o papel de demonstrar as garantias no que tange à privacidade, confidencialidade e o correto tratamento dos dados pessoais dos visitantes dos usuários de aplicativos e sistemas envolvidos ao *software* ERP. Trata-se do documento mais importante a ser redigido pela empresa durante o projeto de conformidade, nele, deverão estar devidamente elencados como os direitos dos titulares (Art. 18 da LGPD) estão sendo respeitados, além de também observar os 10 (dez) princípios do art. 6º da LGPD. Mas como elemento central, a política de privacidade se pauta e se envolve na base legal e nos requisitos com que uma empresa poderia tratar dados de titulares (Art. 7º da LGPD). A política de privacidade se relaciona diretamente com o termo ou cláusula de tratamento de dados da empresa, por essa razão, há a necessidade de revisitá-la e atualizá-la sempre que houver qualquer alteração na operação.

Política de segurança da informação – Busca estabelecer diretrizes que permitam aos colaboradores e clientes da empresa licenciante de *software* ERP, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do titular de dados. Este documento normalmente se relaciona mais com a parte técnica da organização, isto é, elementos aqui postos servirão de norte na remodelação do desenvolvimento do próprio *software*.

Política de governança de dados – Seu objetivo é, basicamente, alocar papéis e responsabilidades aos indivíduos do projeto, sobre os objetivos dos dados que circulam na

empresa, além de assegurar que as informações necessárias à operação da empresa licenciante de *software* ERP, os dados coletados e inseridas por colaboradores ou processos automatizados cumpram os requisitos de integridade, conformidade, autenticidade e disponibilidade, assegurando a qualidade, a transparência, a proteção aos dados e garantindo consistência e confiabilidade durante todo o ciclo de tratamento das informações. Segundo o decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, governança de dados é o exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos.⁵⁰

Política de controle de acesso – Tem o papel de gerir as autorizações e permissões atribuídas a pessoas para acessar certos recursos, como sistemas, localidades, informações, equipamentos, dados, objetos, documentos e a qualquer outro acesso que se exigir controle dentro do *software* ERP. O objetivo desta política de gestão é proteger organizações e pessoas contra danos (intencionais ou não), que possam ser causados por acessos indevidos a recursos que não deveriam ser acessados. Um relevante detalhe, é que na política de controle de acesso da empresa licenciante não deverão haver possibilidade de acessos por usuários da empresa licenciada, todavia, por conta da prestação de serviços inerente ao contrato de licença, conforme já debatido no capítulo 2, haverá a necessidade de acesso por usuários da licenciante no sistema interno da licenciada, o que também deverá ser observado no contrato vigente entre as partes. Também alinhado ao controle de acesso, na linha da nuance de prestação de serviços do contrato de licença, o que já foi discutido mais acima, é necessário que referida política se adeque também aos acessos locais e físicos feitos pelos colaboradores da licenciante no sistema da licenciada.

Política de *Backup e Restore* – Referida política trata da regulamentação dos dados pessoais informações eletrônicas da empresa licenciante do *software* ERP e de seus Clientes, com o objetivo de estabelecer diretrizes para o processo de cópia, armazenamento e restauração dos dados sob sua guarda, visando garantir a segurança, integridade e disponibilidade. Referida política tem um compromisso direto com a necessidade de se garantir a plena validade e integridade dos dados sob a posse da empresa licenciante.

⁵⁰ BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] República Federativa do Brasil**, Brasília, 9 de outubro de 2019; 198º da Independência e 131º da República.

Política de Descarte – Seus objetivos são estabelecer limites temporais para a retenção de dados pessoais e garantir que eles sejam respeitados, assegurar que os compromissos da empresa licenciante do *software* ERP sejam integralmente cumpridos, principalmente, à luz da LGPD, garantir o descarte seguro dos dados tratados na empresa, assegurar que os registros e documentos sejam retidos pelo período legal/contratual declarado, de acordo com as regras/orientações de regulação e mitigar riscos e/ou violações em relação à dados pessoais.

Inventário de dados contendo o seu Ciclo de vida – Tem o papel de determinar, organizar e classificar onde estão e quais são todos os dados pessoais que são tratados pela empresa licenciante do *software* ERP, estabelecendo para cada um de seu tipo e espécie, um ciclo de vida dentro da empresa que observe ao mínimo um dos requisitos e hipóteses estabelecidos pelo artigo 7º da Lei Geral de Proteção de Dados.

Por fim, o relatório de impacto à proteção de dados, documento já mencionado no início deste subcapítulo, é a 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. (Art. 5º, inciso XVII, da LGPD)⁵¹

Necessário lembrar que o RIPD, conforme comumente chamado, tem em alguns casos, a obrigatoriedade de ser criado e apresentado, consoante especificações contidas nos artigos 10, parágrafo 3º⁵² e 38⁵³ da Lei Geral de Proteção de Dados.

Aprofundada a sistemática das políticas propostas, visando seguir a metodologia do *Privacy by design*, necessário revisitar um a um os seus princípios, visando estabelecer

⁵¹ BRASIL. Art. 5º, inciso XVII - Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

⁵² Art. 10. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

⁵³ Art. 38. 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.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, 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.

propostas práticas a serem adotadas pela empresa licenciante de *software* ERP ao licenciado do setor varejista.

Conforme já visto, a abordagem da metodologia *Privacy by Design* é caracterizada por medidas proativas em vez de reativas, ou seja, ele visa antecipar e evitar eventos invasivos de privacidade antes que eles aconteçam. Trata-se da disposição do princípio nº 1 da metodologia.

Quando uma política de privacidade que reflete a operação empresarial e o contrato de licença tem característica proativa e não reativa, é possível mediar junto ao licenciado, no caso, o comércio varejista, formas de prevenir o descumprimento da legislação e também reestruturar eventual operação que, a partir da aplicação do programa, se desvinculou da regularidade, a partir daí é o deslinde para a discussão sobre o segundo princípio.

Em relação ao segundo princípio da metodologia *Privacy by Design* - Privacidade como configuração padrão, evidente que a proposição principal é, à luz do que fora discutido nos tópicos acima, em especial sobre a necessidade de readequar a estrutura do *software* ERP à luz da LGPD, garantir que os requisitos básicos de coleta do sistema estejam alinhados com o padrão máximo de privacidade, ou seja, requisição mínima de dados para sua funcionabilidade.

É necessário que, quando tecnicamente viável, se parta da reestruturação do *software* na busca da conformidade com a LGPD, uma vez que isso garantirá uma melhor validação dos fluxos e dos objetivos que podem ser alcançados pelo *software* a partir dos desenvolvimentos voltados à adaptação da estrutura em torno dos sete princípios da *Privacy by design*, em específico, do segundo princípio, que ora se discute.

Não se garantiria uma fiel padronização, neste sentido, se a empresa iniciasse as alterações no contrato de licença para depois transferir as necessidades descritas na operação ao *software*. Nem sempre é possível fidelizar, na operação do *software*, o que foi garantido em contrato, daí parte também a necessidade de se fixar um objetivo almejável e alcançável pela empresa licenciante, o que também variará a depender do seu porte e da quantidade de dados tratados.

Antes da Lei Geral de Proteção de Dados, ainda se discutindo o segundo princípio, quando se iniciaram as criações de *software* ERP, não havia uma preocupação com a questão

de níveis de coleta de dados, este sistema sofre alterações e modificações com o passar dos anos, e daí advém a discussão sobre a necessidade de reestruturação de *software* à luz deste princípio, ou seja, alterar a estrutura de coleta de dados do sistema, garantindo o padrão mínimo de coleta para a sua execução.

Em relação ao comércio varejista, por exemplo, antes da Lei Geral de Proteção de Dados, o *software* ERP tinha classificações que não respeitavam princípios básicos da Constituição Federal, como por exemplo a igualdade e a própria privacidade, vez que a assimilação dos dados era arquitetada para gerar mais vendas e receita ao estabelecimento licenciado, e *software* ERP que tinham essa funcionabilidade, obviamente, tinham até mais prestígio no mercado.

Existem alguns casos, por exemplo, de que o comércio varejista tem convênios com empresas que tem grande quantidade de funcionários, e para a vinculação deste convênio, dentro de uma política não ideal de tratamento, o banco de dados completo desses funcionários seriam indevidamente colacionados no *software* ERP como clientes em potencial, onde suas classificações medem poder aquisitivo (com base no salário), quantidade de clientes colaterais (com base nos familiares), perfil do consumidor para divulgação de promoções e vendas (solteiro ou casado, por exemplo), enfim, são diversas as possibilidades de uso irregular desses dados, quando não se há uma política estabelecida para cada operação, e em consequência, para cada tratamento e sua finalidade.

A resposta para essas condutas está também no segundo princípio da metodologia, garantindo um nível padrão de coleta e de execução da operação do sistema, padrão que deve ser nivelado pelo extremo respeito à privacidade.

Também não é necessária a reestruturação de toda a arquitetura do *software*, porém, há a necessidade de criar mecanismos com padrão de coleta mínima, de informação sobre essa coleta e também sobre o uso destes dados, enfim, toda a divulgação sobre requisitos e limites de tratamento de dados que devem ser minuciosamente expostas em uma política de privacidade.

Seguindo as orientações da criadora da metodologia *Privacy by design*, Ann Cavoukian, o que viabilizaria uma política de privacidade robusta em relação ao seu sistema de tratamento de dados, seriam as orientações abaixo transcritas:

Especificação de finalidade – as finalidades para as quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao indivíduo (titular dos dados) no momento ou antes do momento em que as informações são coletadas. Os propósitos especificados devem ser claros, limitados e relevantes para as circunstâncias da operação.

Limitação de coleta – a coleta de dados pessoais deve ser justa, legal e limitada ao que é necessário e para os fins especificados.

Minimização de dados – a coleta de dados de identificação pessoal deve ser mantida de forma mínima. O desenho de programas, tecnologias de informação e comunicação e sistemas devem começar com interações e transações não identificáveis, como padrão. Sempre que possível, a identificação, o acesso e a vinculação de informações pessoais devem ser minimizadas.

Limitação de uso, retenção e divulgação - o uso, retenção e divulgação de dados pessoais limitar-se-á às finalidades relevantes identificadas para o indivíduo, para as quais ele ou ela tenha consentido, exceto quando exigido por lei. Os dados pessoais devem ser retidos apenas pelo tempo necessário para cumprir os propósitos declarados e, em seguida, destruídos com segurança. Onde a necessidade ou uso de dados pessoais não for clara, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado: as configurações padrão devem ser as que mais protegem a privacidade.⁵⁴

Essas diretrizes são excepcionalmente importantes para uma operação de licença de *software* ERP para um comércio varejista, principalmente pela grande quantidade de dados pessoais e da extensão de informações destes indivíduos por conta da operação da licenciada, isto é, a compra de produtos em referido estabelecimento.

O princípio da privacidade como configuração padrão, portanto, abrange não só a operação da coleta e do tratamento de dados pessoais, mas também a readequação de seu uso, retenção e divulgação. No cenário ideal em discussão, Henrique Dantas delimita que na aplicação deste princípio, os aplicativos/programas coletariam somente o necessário para a sua execução, e permitiriam que o usuário ativasse eventual coleta extra de dados, caso tenha este interesse.⁵⁵

A ideia de coleta mínima também é uma proposição relevante para o *software* ERP. A configuração padrão visando o mínimo possível de coleta de dados pessoais para tratamento, aqueles necessariamente exigidos e necessários para a operação da gestão

⁵⁴ Tradução livre do autor: CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 3. Disponível em: <chrome-extension://efaidnbmninnibpcapjcgilefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 20 ago. 2022.

⁵⁵ DANTAS, Henrique. *LGPD: O que é Privacy by Design e Privacy by Default*. 2019. Disponível em <https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv>. Acesso em: 10 dez. 2022.

integrada do comércio e da respectiva venda à varejo, também deve ser vista como prioridade pelo Licenciante.

Neste sentido, o *software* ERP, do ponto de vista do licenciante e visando não se exceder em relação ao tratamento de dados e sua finalidade, deve, além de não efetivar as práticas maliciosas, impedir que a configuração do sistema possa ser utilizada pelo licenciado de uma forma que não ocorra o respeito à privacidade nos moldes propostos pela política da empresa.

Percebe-se que é uma junção de fatores, onde a configuração padrão pela privacidade tem extensa aplicabilidade e consegue refletir em toda a operação não somente do licenciante do *software*, mas também do licenciado.

Daí em diante, pode se discutir, ainda na cadeia da operação da venda, o contato de uma empresa de meio de soluções em pagamento que teve acesso a isso, a partir de um *software* também vinculado ao ERP, que lhe proporciona também a coleta e o tratamento. Há uma cadeia ramificada na relação que toca outros agentes, abrange outros setores da operação de venda, e pode, também de forma pejorativa à política de privacidade, causar problemas regulatórios ou até mesmo judiciais aos envolvidos.

O terceiro princípio, privacidade incorporada ao *design*, apresenta proposições de ordem estrutural no manejo da operação. O Licenciante do *software* ERP deve ter em mente que toda a estrutura de sua tecnologia e de sua operação deve já ter a privacidade devidamente inserida em todos os seus contextos.

Não somente inserida, mas a incorporação deve se dar de forma holística, visando garantir contextos adicionais e mais amplos do que a operação comum, de forma integrativa, buscando garantir os interesses de todos os envolvidos, principalmente do titular de dados, e também criativo, visando a inaplicabilidade de alternativas à privacidade, o que as vezes exige a reinvenção das escolhas na operação.⁵⁶

⁵⁶ Tradução livre do autor: CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 3. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 23 ago. 2022.

O objetivo na aplicação deste princípio é que a privacidade seja um componente essencial da funcionalidade principal que está sendo entregue, que é a própria operação. Neste sentido, a privacidade deve ser integrada ao sistema, não permitindo escolhas e alternativas quanto a diminuição de sua funcionalidade.

Do ponto de vista do *software* ERP, toda a arquitetura da operação, não somente desde a coleta de dados, mas desde o início da funcionabilidade do sistema, deve estar assimilada à política de privacidade, de governança de dados e de segurança da informação da empresa licenciante, garantindo ao licenciado únicas alternativas e caminhos que levem ao respeito à privacidade.

Em decorrência disso, o cliente final, consumidor do estabelecimento varejista licenciado, não será afetado por eventual mudança na composição da estrutura do *software* que possa resultar em diminuição de padrões de segurança e de privacidade.

A padronização do *software* neste sentido, não deve ser entendida como um engessamento comercial, ou que dificulte a escalabilidade da licença para demais usuários e licenciados. Não se pode esquecer, que por mais que seja um *software* específico, feito para a gestão daquela determinada operação varejista, eventuais mudanças ou desvios na operação, visando flexibilizar os tratamentos de coleta, classificação, armazenamento, compartilhamento e descarte de dados, não devem ser aceitas.

Daí a necessidade de se ter uma visão criativa na operação, sendo sempre necessário no contrato de licença, deixar bem claro que a relação e o fluxo de dados são bilaterais e demandam também um mútuo respeito às normas de segurança e de privacidade, sob pena, inclusive, da responsabilização objetiva e solidária destes agentes de tratamento.

Assim, a estrutura, design e eventuais aplicabilidades do *software* ERP podem sofrer alterações à cada caso, visando facilitar o aspecto comercial da licença, todavia, a estrutura de privacidade nas operações de tratamento de dados deve permanecer integrativa e íntegra.

Aspectos importantes como a transnacionalidade da dados, ou seja, o compartilhamento com banco de dados fora da jurisdição brasileira, mesmo que visem apenas o armazenamento em nuvem, também devem constar no contrato e na operação de licença.

Isso, pois, atualmente, toda a estrutura do *software* ERP acabam estando disponíveis *online*, isto é, o empresário licenciado, detentor da licença, acessa um computador ligado à internet de qualquer lugar, não necessariamente somente de sua loja, e tem acesso ao andamento de todo o sistema de gestão integrada de sua empresa. Essa ferramenta só é disponível graças à hospedagem em nuvem, onde os dados ficam armazenados. Ressalte-se, que se trata de uma contratação específica de produto, ao passo que essa forma de hospedagem normalmente segue empresas do exterior, que possuem uma estrutura mais robusta em termos de segurança e privacidade.

Neste sentido, na operação da licença, a empresa licenciante deve se ater à referida disposição, inclusive por haver passagem específica sobre tal assunto no artigo 33 e seguintes da Lei Geral de Proteção de Dados, contida na seção II que trata da responsabilidade.

Sempre que possível, avaliações detalhadas de impacto e risco na privacidade devem ser realizadas e publicadas, inclusive para os licenciados e seus clientes finais, documentando claramente os riscos de privacidade e todas as medidas tomadas para mitigar esses riscos, incluindo a consideração de alternativas e a seleção de métricas que foram tomadas.⁵⁷

Em último esboço, os impactos da privacidade na tecnologia e na operação da licença do *software* ERP devem ser comprovadamente minimizados, não podendo aceitar alteração de configuração ou alteração de objetivos no tratamento.⁵⁸

O princípio da soma positiva e não soma zero, passa a ideia de que não devemos, dentro do escopo da operação do *software* ERP, abrir mão de um objetivo em prol do outro, ou seja, não devemos priorizar, por exemplo, a estrutura comercial ou os interesses do tratamento em prejuízo à privacidade ou à segurança informacional e vice-versa.

⁵⁷ Tradução livre do autor: CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 3. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em 2 set. 2022. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em: 24 ago. 2022.

⁵⁸ Tradução livre do autor: CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 3. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 24 ago. 2022.

O objetivo da privacidade como do escopo da operação do *software* ERP não deve ser vestida de modo a competir com outros interesses legítimos, como o design ou as capacidades técnicas do sistema. E mais, ao incorporar a privacidade em uma determinada tecnologia, processo ou sistema, isso deve ser feito de forma que a funcionalidade total não seja prejudicada e, na medida do possível, que todos os requisitos sejam otimizados.⁵⁹

Como exemplo, inserido no contexto da licença de *software* ERP, o licenciante não deverá deixar de garantir plataformas para que o licenciado estruture uma promoção que visa a expansão de vendas em seu comércio varejista, a partir da estrutura e do banco de dados do *software*, por que isso poderia ser visto como uma prática que fere a privacidade dos titulares.

É possível visar um objetivo comum que comporte todas as áreas e práticas, e isso passa necessariamente pelo envolvimento de todos os setores da empresa. Acomodar privacidade, expansão comercial, segurança da informação, arquitetura e *design* de *software*, ferramentas de praticidade ao licenciado, dentre outros, é plenamente alcançável através da busca do princípio da soma positiva e não da soma zero. As estruturas do *software* ERP devem se complementar, se integrar e não se anular ou se desvalorizar.

Acerca do quinto princípio, a segurança da informação é ponto chave na arquitetura de uma licença de *software*. Isso, pois, na cadeia da operação, temos a infraestrutura do licenciante, empresa que regularmente lida com a tecnologia e temos a infraestrutura do licenciado, que muitas vezes, pensando em um mercado ou conveniência de médio porte, não tem o correspondente investimento apropriado.

O princípio da segurança de ponta a ponta – proteção completa do ciclo de vida – deve ser um dos principais objetivos quando se trata de empresas ligadas à tecnologia e que mantêm a estrutura praticamente integral no âmbito digital. O motivo disso, de forma exemplificada, é que a empresa licenciante acaba armazenando e classificando dados de todas as suas licenciadas, conforme já discutido no tópico 2.4.

Sobre o princípio, Ann Cavoukian acrescenta:

⁵⁹ Tradução livre do autor: CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 4. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 24 ago. 2022.

A privacidade deve ser continuamente protegida em todo o domínio e ao longo do ciclo de vida dos dados em questão. Não deve haver lacunas na proteção ou na responsabilidade. O princípio da segurança tem especial relevância aqui porque, em sua essência, sem forte segurança, não pode haver privacidade.⁶⁰

De tal modo, uma empresa licenciante que armazena dados de duzentas empresas licenciadas, por exemplo, o armazenamento é equivalente a todos os dados que todas essas empresas tem em sua posse. Daí a grande necessidade de se ter um robusto sistema que garanta a plena segurança, de ponta a ponta, dentro do contexto operacional da empresa licenciante.

Para a operação de licença de *software* ERP, o quinto princípio tem uma definição ímpar, uma vez que a empresa licenciante, do ponto de vista comercial e buscando escalar a quantidade de licenciados, não pode exigir uma infraestrutura muito robusta dos mesmos. Isso faz com que haja um disparate considerável entre a infraestrutura do licenciante e do licenciado.

Uma consequência disso, seria que, do ponto de vista da segurança, o que necessita de investimento em infraestrutura técnica e tecnológica, há um problema no ciclo de tratamento de dados no momento em que ele atinge a esfera do licenciado. A operação e a base de dados têm o melhor cuidado quando seu ciclo se mantém no licenciante, todavia, conforme já explicado no tópico sobre a estrutura do *software* ERP, esse ciclo é constante e tem um fluxo bilateral quase que automático na operação de tratamento de dados.

Aqui, há de ser observado um ponto em especial para o licenciante, em termos de delimitação de responsabilidades e de eventuais incidentes como vazamento de dados, quando o problema partir do licenciado. Essa observação pode ser prevista na política de segurança da informação e, principalmente, no contrato de licença de *software*.

Não obstante não exigir da empresa licenciada o melhor investimento e prática do ponto de vista da segurança da informação, referido princípio nos alerta para, ao menos, disponibilizar ao licenciado quais seriam as melhores práticas técnicas a serem adotadas, o que também deverá ser registrado no instrumento contratual.

⁶⁰ Tradução livre do autor: CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 4. Disponível em: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf](https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf). Acesso em: 24 ago. 2022.

Referidos pontos, por mais que possam parecer simples aos olhos do jurídico encarregado do instrumento de licença, tem ímpar relevância em termos das boas práticas descritas no artigo 50 e seguintes da Lei Geral de Proteção de Dados.

Visando garantir do início ao fim o gerenciamento seguro do ciclo de vida dos dados, um outro ponto relevante, muito defendido pela *Privacy by design*, seria a destruição dos dados retidos após a finalização do processo de tratamento, o que pode singularmente ser alcançado, de forma segura e legítima, através de robustas políticas quanto ao inventário, ciclo de vida e de descarte de dados.

O sexto princípio da metodologia *Privacy by design, Visibility and Transparency – Keep it Open* (Visibilidade e Transparência – Mantenha-o Aberto), trata de buscar garantias às partes interessadas, de que qual seja a prática de negócios ou tecnologia envolvida, a empresa está operando de acordo com as promessas e objetivos declarados, garantindo, inclusive, a verificação independente.

Referidas promessas, declaração de objetivos e garantias, devem ser necessariamente elencadas na Política de privacidade da empresa. Conforme visto mais acima, tal política deve especificar tipos de dados coletados, base legal de tratamento, limites e objetivos da utilização e do tratamento desses dados, responsáveis internos por tais práticas e, por fim, referida política deve ter suas bases bem expostas no contrato de licença de *software* ERP. Mantendo uma política de privacidade robusta, que atenda as diretrizes do *Privacy by design*, e que seja pública, ou seja, que seja devida e claramente informada aos titulares e contratantes licenciados, há o atendimento à referido princípio.

Não é demais lembrar que referido princípio pode ser lido nas entrelinhas do também princípio composto no art. 6º, inciso VI, conforme já abordado, o princípio da transparência, nos termos da redação da Lei Geral de Proteção de Dados, visa garantir aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.⁶¹

Mas mais do que isso, o sexto princípio do *Privacy by design*, passa ainda por três pontos chave que são bem explicados pela própria criadora, Ann Cavoukian:

⁶¹ BRASIL. Art. 5º, inciso XVII - Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

Responsabilização – A coleta de dados pessoais implica em um dever de zelar pela sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado, e atribuído a um indivíduo especificado. Ao transferir informações pessoais para terceiros, a proteção de privacidade equivalente através de meios contratuais ou outros meios devem ser assegurados.

Abertura – Abertura e transparência são fundamentais para a prestação de contas. Informações sobre as políticas e as práticas relativas ao gerenciamento de informações pessoais devem ser prontamente disponibilizadas para indivíduos.

Conformidade – Mecanismos de reclamação e reparação devem ser estabelecidos e as informações comunicadas sobre eles para indivíduos, incluindo como acessar o próximo nível de apelação. Etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade.⁶²

Percebe-se, que nos três pontos acima especificados, há a necessidade de menção da correspondente política aplicada pela empresa, e no caso das licenciantes de *software* ERP isso não é diferente. Deve ainda, haver cuidados específicos com o manuseio do dado quando ele está em tratamento e posse do licenciante e quando está no tratamento e posse do licenciado, conforme amplamente já debatido neste tópico. Isso porque, no mais das vezes, a estrutura de proteção de dados criada pela licenciantes não tem nenhum tipo de adesão ou de equiparação por parte da licenciada, e daí a importância dos três pilares acima detalhados.

Sobre o sexto princípio, especificamente quanto aos três pontos em questão, Camilla do Vale Jimene lembra que “o objetivo central é garantir responsabilidade e confiança, na medida em que quanto mais transparente a operação, mais fácil será a identificação dos responsáveis no caso da ocorrência de incidentes de segurança da informação e, conseqüentemente maior será a confiança do usuário”.⁶³

O sétimo e último princípio desenvolvido na metodologia *Privacy by design, Respect for User Privacy – Keep it User-Centric* (Respeito pela privacidade do usuário – Mantenha o usuário no centro), preza pela simples ideia de manter o foco da operação no respeito à

⁶² Tradução livre do autor: CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 5. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 28 ago. 2022.

⁶³ JIMENE, Camilla do Vale. Reflexões sobre *privacy by design* e *privacy by default*: da indenização à positivação. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (coord). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: RT, 2018. p. 181.

privacidade do titular de dados e do usuário do *software* ERP, isto é, desenvolver a aplicação a partir do núcleo da privacidade em torno do titular de dados, do usuário do *software*.

Nas palavras de Ann Cavoukian, os melhores resultados em termos de *Privacy by Design* geralmente aqueles que são conscientemente projetados em torno dos interesses e necessidades de usuários individuais, que têm o maior interesse investido na gestão de seus próprios dados.⁶⁴

Aqui cabem apartes e distinções iniciais, conforme já debatidas antes, na linha da definição de atores e agentes na relação de operação de licença de *software* ERP, temos o cliente da licenciante, ou seja, o licenciado, e temos os clientes finais do licenciado, que são os consumidores do estabelecimento comercial varejista.

É importante o Licenciante ter em mente, na linha do que preza o sétimo princípio, que não devem haver distinções de segurança, privacidade ou da própria estrutura do *software* em relação ao Licenciado ou ao titular final de dados. O respeito aos dados pessoais, por exemplo, do funcionário do Licenciado, deve ser o mesmo atribuído ao consumidor deste mesmo licenciado.

Sobre aludido princípio, Carlos Affonso Pereira de Souza delimita que o respeito à privacidade do usuário exige que os interesses do usuário sejam colocados em primeiro lugar, oferecendo medidas como padrões de privacidade fortes, avisos apropriados e opções fáceis de serem utilizadas pelo usuário (*user-friendly* – Ser amigo do usuário).⁶⁵

Na linha do contrato de licença, algumas práticas do Licenciante podem ser postas em política de privacidade e efetivamente executadas, visando arquitetar a estrutura do *software* para servir à privacidade do usuário e ao titular de dados, não somente os pessoais. Tal ferramenta facilita a assimilação de informações para uma melhor classificação e contextualização das informações relevantes para a gestão da empresa Licenciada.

⁶⁴ Tradução livre do autor: CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Ontario, Canada: Creation of a Global Privacy Standard, 2010. p. 5. Disponível em: <chrome-extension://efaidnbnmnibpcjpcglclefindmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 28 set. 2022..

⁶⁵ DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2020. p. 426.

Já para o Licenciado, visando garantir, ao cliente final, as bases legais de tratamento e de acesso aos dados pessoais para uma melhor precisão sobre o seu conteúdo, e o livre conhecimento de limitações e objetivos deste tratamento, podem ser garantidas nas próprias campanhas promocionais ou como uma política norteadora em todos os procedimentos de venda da empresa.

Na bilateralidade existente no contrato entre Licenciante e Licenciado, e ainda, nas cláusulas de definição de tratamento compartilhado de dados, quanto mais bem formatada for a estrutura de respeito à privacidade do *software* ERP, mais restritas serão as ações e ferramentas disponíveis ao Licenciado em termos de tratamento de dados, o que lhe engessa no sentido do cumprimento dessas disposições também para o seu cliente final.

Um outro ponto importante para a operação do contrato entre Licenciante e Licenciado, seria uma ferramenta de acesso e validação pessoal dos dados, o que objetiva melhor acurácia e entendimento sobre a base legal de tratamento por parte do titular de dados. É claro que essa proposição exige investimento em infraestrutura tecnológica, como um aplicativo, por exemplo, mas se trata de uma relação de ganho mútuo entre os agentes de tratamento (licenciante e licenciado) e o titular de dados.

A proposta de uma ferramenta de livre acesso já é realidade para as empresas licenciadas de *software* ERP. Em aplicações de comércio varejistas com venda e *delivery* de mercadorias, é possível consultar dados cadastrais, políticas de compra e venda, além de histórico de gastos e produtos mais selecionados pelo usuário. Importante consignar que tais ferramentas devem ser informativas e de fácil manuseio e acesso ao titular de dados.

Todo esse conjunto de informações e ferramentas, também tem o poder de prever, coibir, e eventualmente, documentar como prova, eventuais abusos e tratamento indevido de dados pessoais que possam ferir ou estar ferindo os direitos e a privacidade do titular ou de outro agente de tratamento.

Esgotado neste capítulo, o relatório e proposições pensadas e sugeridas a partir de cada um dos princípios da metodologia *privacy by design*, em busca do preparo da conformidade para um pleno atentamento à regulação da Lei Geral de Proteção de Dados em relações empresariais da operação de licença de *software* ERP.

Foi possível verificar que a base principiológica e necessariamente fundamentalista dos conceitos abordados facilitam a implementação e a busca de uma cultura de respeito à proteção de dados e à privacidade, o que atualmente vem sendo visto como um sinal de elevada estrutura empresarial, de respeito às normas e de segurança na relação empresarial com terceiros.

5 CONCLUSÃO

Considerando o custoso desafio proposto na introdução deste trabalho, que foi buscar, necessariamente através de um trabalho de mestrado profissional, atribuir questões reflexivas e proposições que contribuíssem de alguma forma com o ambiente profissional técnico e jurídico das empresas licenciadas de *software* ERP, a presente conclusão será um reflexo de toda a matéria asseverativa apresentada no decorrer dos capítulos e subcapítulos.

Seguindo a proposta didática contida na introdução, passou-se pela análise descritiva e reflexiva sobre a regulação legislativa da Lei Geral de Proteção de Dados, sobre os contratos de licença de *software Enterprise Resource Planning* (ERP) e sua estrutura técnica e jurídica para se analisar e pontuar alguns dos impactos na operação junto ao setor de comércio do varejo.

Em primeiro, verificou-se que a regulação legislativa em torno da LGPD trouxe fortes e consideráveis impactos em todos os setores empresariais. Em específico, nos contratos de licença de *software* ERP, pela sua natureza bilateral, com tratamento e fluxo de dados constante entre os agentes envolvidos, e, ainda, pela sua inerente relação de prestação de serviços atrelada a questões de *hardware* e de treinamento, por exemplo, houveram profundos e significativos impactos. Seus impactos são tamanhos, na medida em que é necessário que seja repensada toda a estrutura, arquitetura e ferramentas do *software* ERP, e a partir disso, refletir a operação no contrato de licença, de um modo que garanta segurança jurídica, correta identificação das modalidades e tratamento e definição de obrigações e responsabilidades entre os *players* do negócio jurídico em questão.

Do aspecto profissional, o trabalho de conformidade com a LGPD é árduo, custoso e, conforme sustentado, demanda envolvimento de toda a empresa. No ponto de vista dos contratos de licença de *software* ERP, esse trabalho, ousado dizer, é mais custoso e mais árduo, justamente pelas singulares características do mesmo.

Não se pôde deixar de lado, do ponto de vista da busca empresarial da eficiência econômica, que as empresas licenciadas tratam uma vasta gama de dados, justamente pelas inserções em grande escala feita pelas licenciadas e pela sua grande quantidade de clientes, que são características inerentes do setor varejista. É certo ainda, que a ANPD e demais

órgãos fiscalizadores e reguladores vêm aplicando de forma diferente o contexto de penalidades e multas, observando-se uma incidência quase nula em pequenas e médias empresas, diferente dos grandes conglomerados de e-commerce, empresas de tecnologia e/ou instituições financeiras.

Em alvitre seguinte, aprofundou-se a temática da metodologia *Privacy by design*, sua origem, definições, princípios e os desdobramentos em aplicação ao GDPR (*General Data Protection Regulation*), sua aplicabilidade e perpetuação também na Lei Geral de Proteção de Dados, para que, em último plano, fossem analisadas propostas, medidas e ponderações a serem utilizadas na operação de licença de software ERP sob a ótica do Licenciante com reflexos ao Licenciado.

Referida metodologia tem uma base principiológica vasta, todavia, depreendeu-se, que a aplicação singular da metodologia *Privacy by design* nos contratos de licença de software ERP, não seria suficiente para a plena conformidade com a Lei Geral de Proteção de Dados. Isso, porque, por mais que se relacionem os fundamentos e os princípios, isto é, a base norteadora, o que foi plenamente demonstrado nos tópicos 3.2 e 4.2, há uma diferença de aplicabilidade prática, ao passo que a LGPD tem sua regulação feita de forma mais concreta e direcionada ao país em que foi regida, diferente da metodologia *Privacy by design*, que tem uma aplicabilidade mais abstrata, mais genérica.

Por esses motivos, em resposta à algumas das questões formuladas no início deste trabalho, concluiu-se que aplicando referida metodologia não lhe garantiria uma plena conformidade com a LGPD. De maneira prática, a LGPD exige mais do que a mera aplicação das bases principiológicas, exige o fiel atendimento à regulação, de forma concreta, com antecipação em produção de provas, com antecipação de problemas e com autorregulação, com o fiel diálogo com outros agentes de tratamento, sempre em respeito à privacidade.

Ainda destas considerações, mas na mesma linha de ideias, concluiu-se também que a metodologia *Privacy by design* está fortemente presente na normativa da LGPD, muito também, pelos reflexos do GDPR, sendo apontados, em específico no tópico 3.2, as suas similitudes e onde se complementam de alguma forma.

Outra importante conclusão, que também teve impacto no tópico central do trabalho, foi a necessidade, a partir da regulação da LGPD, de se reestruturar e remodelar o próprio

software ERP, isto é, adequá-lo às necessidades técnicas, de segurança e, principalmente, de atribuir base legal e principiológica às suas rotinas genéricas. Essa questão se apresentou de forma asseverativa no decorrer das pesquisas e teve um deslinde importante no nuclear e último tópico deste trabalho.

Também foi possível concluir, a partir da análise do *software* em estudo e de seu inerente contrato, que a metodologia *Privacy by design* tem mais a auxiliar na necessária reestruturação do *software*, de um ponto de vista de tecnologia e segurança da informação, do que necessariamente na reestruturação jurídico-contratual. O estudo da metodologia, do formato contratual e do próprio *software*, traz essa sensação, talvez porque não há na metodologia, um atendimento a regras e obrigações, mas uma preparação, uma proposição do que seria uma boa prática, do que seria necessariamente o respeito à privacidade do titular de dados.

Daí, também, outro fundamento que levou à uma das conclusões mais importantes deste trabalho, que inclusive responde à questão central de pesquisa, de que não basta a aplicação da metodologia *Privacy by design*, há, também, a necessidade de se atentar singularmente à normativa regulatória da LGPD.

Além disso, mas de igual fundamento, tais reflexos levaram à uma outra proposição registrada no tópico 4.2. Em um programa de conformidade de uma empresa licenciante de *software* ERP ao setor varejista, há a necessidade, quando tecnicamente viável, de se partir da alteração programática do *software*, para depois visar a alteração/reestruturação do seu inerente contrato, fixando-se, para os casos tecnicamente inviáveis, a necessidade de um controle e apontamentos específicos no Relatório de Impacto à Proteção de Dados.

Na mesma linha de ideias, também a depender do programa de conformidade, é possível que se estabeleça níveis de segurança, técnicos e jurídicos, mais fortes com determinado cliente/licenciado, do que com outros. Isso, porque, conforme observado, a operação da licença age em nível bilateral, com um fluxo constante de troca e acesso de dados, portanto, a operação tende a estar mais segura quando a posse desses dados remonta ao Licenciante, empresa do ramo da tecnologia que já tem uma estrutura informatizada apta. Já do lado do Licenciado, sempre serão observados níveis de investimento e de estrutura diferentes, e na maioria das vezes, incompatíveis com os níveis de segurança exigidos pela

LGPD. Daí o desafio do Licenciante, em acomodar muito bem a sua operação, garantindo contratualmente sua segurança em caso de incidentes envolvendo o licenciado.

Um outro ponto que se mostrou fundamental após as reflexões levantadas, foi o cuidado de se estabelecer os agentes de tratamento de acordo com a operação de tratamento de dados correlata, fixando-se instrumentos de isenção da responsabilização por parte do Licenciante em relação à um Licenciado que não nivelou a sua segurança informatizada ou não adequou seus artifícios jurídicos de igual modo.

Concluiu-se, que para a efetiva adequação à Lei Geral de Proteção de Dados não basta que os instrumentos contratuais estejam em conformidade com a recente legislação, é preciso, mais do que tudo, que o contrato reflita a operação da empresa na prática, isto é, que os processos internos da empresa também observem a padronização exigida pela Lei Geral de Proteção de Dados. Daí, também, a importância de se entender a operação, aperfeiçoá-la do ponto de vista da conformidade, para depois se buscar a regularização contratual, em primeiro momento olhando para dentro da empresa e em seguida, olhando para os licenciados contratantes.

Não obstante haver uma gama de políticas para cada setor e nicho atrelado à reestruturação contratual no sentido da adequação à LGPD, os fundamentos e objetivos de cada política deverão estar estruturalmente compostos no contrato de licença de *software* ERP, o que garantirá a transparência e a plena ciência da operação e do tratamento que vigorará entre as partes licenciante e licenciada.

O contexto de reestruturação contratual da empresa Licenciante de *software* ERP também teve forte alteração no decorrer do estudo e da montagem do trabalho. Concluiu-se que não se trata de uma mera inclusão de cláusula e/ou criação de termo de tratamento, a reestruturação passa também pela prévia estruturação da operação do *software* e de instrumentos internos que reflitam essa operação, mas que, ao final, necessariamente promovam a alteração contratual entre Licenciante e Licenciado.

Observou-se, também, que nos casos onde há inviabilidade técnica ou financeira para a reestruturação da operação do *software* com base na metodologia *Privacy by design*, a reestruturação pode pautar-se somente em uma correta integração do Relatório de Impacto de Proteção de Dados.

Por fim, a rigorosa aplicabilidade dos conceitos por detrás de cada um dos sete princípios da metodologia em estudo gerou proposições a serem observadas no dia a dia da operação não apenas do contrato de licença, mas da estrutura e ferramentas informatizadas que o *software* ERP oferece ao licenciado e também para os consumidores finais, também como titulares de dados, o que se observou a fundo no tópico 4.2.

Com as propostas trazidas no capítulo quatro, o que necessariamente se partiu dos conceitos e princípios da metodologia *Privacy by design*, se pretendeu apresentar algumas proposições e reflexões a serem executadas pelas empresas licenciadas de *software* ERP destinadas ao setor varejista, na facilidade da busca do cumprimento da Lei Geral de Proteção de Dados no que tange às obrigações, mas mais do que isso, na aplicação de ferramentas que prezem pelos direitos do titular de dados sem lesar a estrutura comercial, de arquitetura, funcionabilidade e de execução do sistema junto ao seu usuário.

O que foi pretendido e alcançado com os levantamentos, reflexões, e ao final, proposições e conclusões feitas neste trabalho de mestrado profissional, foi, de um certo modo, definir os desafios e problemas, e ao final, auxiliar e colaborar com o profissional técnico e jurídico atuante na seara da licença de *software* ERP ao comércio varejista, no programa de conformidade de dados da empresa licenciante.

Buscou-se demonstrar ao profissional técnico e jurídico atuante na seara da licença de *software* ERP no comércio varejista, que não há necessidade de se pautar única e exclusivamente na normativa da LGPD e na regulação de outras agências e entidades, mas também se ativar através de autorregulação e correção, com base em outras ferramentas como a metodologia do *Privacy by design*, que se mostrou útil e contributiva ao enfoque e objetivo final, que é a conformidade com a LGPD.

REFERÊNCIAS

ÁLVARES, Elismar; GIOACOMETTI, Celso; GUSSO, Eduardo. **Governança corporativa: um modelo brasileiro**. Rio de Janeiro: Elsevier, 2008.

ARAÚJO, Luiz Alberto David; NUNES JUNIOR, Vidal Serrano. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2005.

ARBIX, Daniel. A importância da privacidade por Design e por Default (Privacy by Design and Default). *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020, p.56.

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

BLUM, Renato Opice (org.). **Proteção de Dados: desafios e soluções na adequação à Lei. 2. ed.** Rio de Janeiro: Forense, 2021.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega. **Lei Geral de Proteção de Dados – Comentada**. São Paulo: Revista dos Tribunais, 2019.

BRASIL. Art. 5º, inciso XVII - Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

BRASIL. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. **Diário Oficial [da] República Federativa do Brasil**, Brasília, 28 de janeiro de 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção de Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

BRASIL. Constituição (1988). **Constituição [da] República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] República Federativa do Brasil**, Brasília, 9 de outubro de 2019; 198º da Independência e 131º da República.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial [da] República Federativa do Brasil**. Brasília, 10 de janeiro de 2002; 181º da Independência e 114º da República.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (Lei Geral de Proteção De Dados). **Diário Oficial [da] República Federativa do Brasil**, Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. **Diário Oficial [da] República Federativa do Brasil**. Brasília, 11 de setembro de 1990; 169º da Independência e 102º da República.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Lei do *Software*. **Diário Oficial [da] República Federativa do Brasil**. Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

BRAUN, Daniela. Receita de *software* alcançou R\$ 44 bilhões no Brasil em 2020, diz consultoria. **Revista Valor Investe**, 07 de maio de 2021. Disponível em: <https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/05/07/receita-de-software-alcançou-r-44-bilhoes-no-brasil-em-2020-diz-consultoria.ghtml>. Acesso em: 20 ago. 2022.

CAIÇARA JUNIOR, Cícero. **Sistemas Integrados de Gestão – ERP: Uma abordagem gerencial**. 4. ed. Curitiba: Ibpx, 2011.

CAVOUKIAN, Ann. **Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers**. Ontario, CA: Information and Privacy Commissioner of Ontario, Canada, 2011. Disponível em: <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf>. Acesso em: 20 set. 2022.

CAVOUKIAN, Ann. **Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices**. Ontario, Canada: Creation of a Global Privacy Standard, 2010. Disponível em: <chrome-extension://efaidnbmninnkcepbajpglecfndmkaj/https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em 2 set. 2022. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em: 20 ago. 2022.

CAVOUKIAN, Ann. **Publicação da Information and Privacy Comissioner of Ontario**. Publicado em agosto de 2009. Revisado em janeiro de 2011. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso 2 dez. 2022.

COLANGELO FILHO, Lucio. **Implantação de sistemas ERP (Enterprise Resource Planning): Um enfoque de longo prazo**. São Paulo: Atlas, 2001.

DA ROCHA, Claudia. Boas Práticas e Governança Corporativa na ótica da Lei Geral de Proteção de Dados. In: TEIXEIRA, Tarcisio (coord). **Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados**. Salvador: JusPodivm, 2021. p. 87.

DANTAS, Henrique. **LGPD: O que é Privacy by Design e Privacy by Default**. 2019. Disponível em: <https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv>. Acesso em: 10 dez. 2022.

DE SOUZA, Carlos Affonso Pereira. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2020.

DECISION RESOURCES. **How Important is Data Security When Choosing an ERP System?** Pittsburgh, PA: Sept. 22, 2021. Disponível em: <https://www.decision.com/how-important-is-data-security-when-choosing-an-erp-system/#:~:text=An%20ERP%20solution%20provides%20a,and%20processes%20for%20security%20advancement>. Acesso em: 2 ago. 2022.

DINIZ, Maria Helena. **Código Civil anotado**. 14. ed. São Paulo: Saraiva, 2009.

DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020.

EUROPE UNION. Official Journal of the European Union: Key Issues. **General Data Protection Regulation**. Regulation (EU) 2016/679 of the European Parliament and of the Council. Brussels, 27 April 2016. Disponível em: <https://gdpr-info.eu/issues/privacy-by-design/#:~:text=GDPR%20Privacy%20by%20Design&text=The%20term%20%E2%80%9CPrivacy%20by%20Design,in%20the%20technology%20when%20created>. Acesso em: 10 ago. 2022.

FORGIONI, Paula A. **Contratos Empresariais: teoria geral e aplicação**. 4. ed. São Paulo: Revista dos Tribunais, 2019.

GALLINDO, Sergio Paulo Gomes. Economia intensiva em dados, virtudes da LEI GERAL DE PROTEÇÃO DE DADOS e primeiros desafios quanto à efetividade. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020.

GIANNAKAKIS, Ioannis. **Privacy by Design and By Default**. LAP Lambert Academic Publishing. Republic of Moldova, 19 September 2019.

HABERKORN, Ernesto. **Teoria do ERP – Enterprise Resource Planning**. 2. ed. São Paulo: Makron Books, 1999.

HARTZOG, Woodrow. **Privacy's Blueprint: The Battle to Control the Design of New Technologies**. Cambridge, Massachusetts, Harvard University Press, 2018.

JEŽOVÁ, Daniela. **Principle of Privacy by Design and Privacy by Default**. Regional Law Review, Beograd, 2020. Disponível em: <https://ssrn.com/abstract=3755514>. Acesso em: 2 ago. 2022.

JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. 1ed. São Paulo: Revista dos Tribunais, 2018. p. 165-180.

JIMENE, Camilla do Vale. Reflexões sobre privacy by design e *privacy by default*: da indenização à positivação. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato

(coord). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia.** São Paulo: RT, 2018.

KALLONIATIS, Christos; LAMBRINOUDAKIS, Costas; MUS AHL, Mathias; KANATAS, Athanasios; GRITZALIS, Stefanos. **Incorporating privacy by design in Body Sensor Networks for Medical Applications: A Privacy and Data Protection Framework.** Greece: University of Piraeus, 2020.

KREBS, David. Privacy by Design: Nice-to-Have or a Necessary Principle of Data Protection Law? **JIPITEC**, v. 4, p.1-20, 2013. Disponível em: <https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf>. Acesso em: 2 set. 2022.

LANGENWALTER, Gary A. **Enterprise Resource Planning and Beyond: Integrating Your Entire Organization.** Boca Raton, Florida: St. Lucie Press, 2000.

MALDONADO, Viviane; BLUM, Renato. **Comentários ao Gdpr: Regulamento Geral de Proteção de Dados da União Europeia.** São Paulo: Revista dos Tribunais, 2021. Disponível em: <https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1339455450/6-reflexoes-sobre-privacy-by-design-e-privacy-by-default-da-idealizacao-a-positivacao-comentarios-ao-gdpr-regulamento-geral-de-protecao-de-dados-da-uniao-europeia>. Acesso em: 20 dez. 2022.

MARTIN, Kelly D. *et al.* Data Privacy in Retail. **Journal of Retailing**, v. 96, n. 4, p. 474-489, 2020. Disponível em: <https://doi.org/10.1016/j.jretai.2020.08.003>. Acesso em: 20 set. 2022.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz. **Tratado de Proteção de dados Pessoais**, Rio de Janeiro: Forense, 2021.

MILLER, Meredith R. Party Sophistication and Value Pluralism in Contract. In: **Touro Law Review**, v. 29, n. 3, p. 659-679, 2013. Disponível em: <https://core.ac.uk/reader/231071310>. Acesso em: 3 ago 2022.

NEGRÃO, Antonio Carlos. Economia Digital, Proteção de Dados e Competividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados.** São Paulo: Thomson Reuters Brasil, 2020.

O'LEARY, Daniel Edmund. **Enterprise Resource Planning Systems: Systems, Life cycle, electronic commerce, and risk.** Cambridge, United Kingdom: Cambridge University Press, 2000.

O'NEIL, Cathy. **Algoritmos de destruição em massa: Como o big data aumenta a desigualdade e ameaça a democracia.** Santo André: Rua do Sabao, 2020.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Managing Digital Security and Privacy Risk.** OECD Publishing. 2016. Disponível em: <https://www.oecd-ilibrary.org/docserver/5j1wt49ccklt-en.pdf?expires=1643806719&id=id&acname=guest&checksum=3AE19A682AF60E76F4E60F6F4710FBE3>. Acesso em: 01 fev. 2022.

PEREZ HERNANDEZ, Yoliliztli. Consentimiento sexual: un análisis con perspectiva de género. **Rev. Mex. Sociol**, Ciudad de México, v. 78, n. 4, p. 741-767, 2016. Disponível em: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032016000400741. Acesso em: 2 ago. 2022.

QUEIROZ, Rafael Mafei Rabelo. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado AASP**, São Paulo, ano 39, n. 144, p.15-21, nov., 2019.

RUBINSTEIN, Ira. Regulating Privacy by Design. **Berkeley Technology Law Journal**, v. 26, p. 1409-1456, 2012. Disponível em: <https://ssrn.com/abstract=1837862>. Acesso em: 5 set. 2022.

RUBINSTEIN, Ira; GOOD, Nathan. **Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents**. **Berkeley Technology Law Journal**, v. 1333, 2013. Disponível em: <https://ssrn.com/abstract=2128146>. Acesso em: 20 set. 2022.

SAAD, Andrea; HIUNES, Antonio. Ela, a LGPD, vista pelas empresas: uma proposta de visão prática e otimista. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020.

SALAMA, Bruno Meyerhof. O que é pesquisa em direito e economia?. **Revista Direito UNIFACS**, n. 160, p. 1-17, 2013. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/2793>. Acesso em: 2 set. 2022.

SERPA, Pedro Ricardo e. **Arranjos Negociais I - Fragmentação do Direito dos Contratos (e) Os Novos Princípios Contratuais**. São Paulo: Programa de Pós-Graduação Stricto Sensu da Fundação Getulio Vargas, 2021. (Aula)

SHTUB, Avraham. **Enterprise Resource planning (ERP): The Dynamics of operations management**. Norwell, Massachusetts: Kluwer Academic Publishers, 1999.

SPIEKERMANN, Sarah. The Challenges of Privacy by Design **Communications of ACM**, v. 55, n. 7, p. 1-3, 2012. Disponível em: <https://ssrn.com/abstract=3600803>. Acesso em: 20 set. 2022.

TEIXEIRA, Tarcisio. **Empresas e a Implementação da Lei Geral de Proteção de Dados**. Salvador: JusPodivm, 2021.

TEIXEIRA, Tarcisio; KASEMIRSKI, André Pedroso; Compliance (Conformidade) de dados pessoais para microempresas: Autorregulação regulada e requisitos para efetividade. *In*: TEIXEIRA, Tarcisio (coord.). **Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados**. Salvador: JusPodivm, 2021.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019. Resenha de: MEDON, Filipe. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 23, p. 195-203, jan./mar. 2020. DOI:10.33242/rbdc.2020.01.009.

TEPEDINO, TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

VALENTE, Jonas. **Promovendo a privacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies**. Privacidade em perspectivas. Rio de Janeiro: Lumen Juris, 2018.

VIEIRA, Adriana Carvalho Pinto; SANTOS, Jamilton Pereira dos. **Análise Jurídica dos Contratos da Área de Direito de Propriedade Intelectual: Fundação Civil, Comercial ou Consumerista a Respeito da Responsabilidade?** In: CONGRESSO NACIONAL DE MILHO E SORGO, 24., 2002, Florianópolis, SC. Anais [...]. Florianópolis: ABMS, 2002. Disponível em <https://ainfo.cnptia.embrapa.br/digital/bitstream/item/33713/1/Analise-juridica.pdf>. Acesso em: 5 set. 2022.

WALDMAN, Ari Ezra. Data Protection by Design? A Critique of Article 25 of the GDPR **Cornell International Law Journal**, v. 53, 2021, Northeastern University School of Law Research Paper No. 411-2021. Disponível em: <https://ssrn.com/abstract=3773143>. Acesso em: 20 ago. 2022.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, v. IV n. 5, dezembro de 1890.

ZANETTI, Cristiano de Sousa. A Fragmentação da Liberdade Contratual. **GEN Jurídico**, São Paulo, jun., 2007. Disponível em: <https://genjuridico.wordpress.com/artigos/artigo-a-fragmentacao-da-liberdade-contratual/>. Acesso em: 20 set. 2022.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: Public Affairs, 2019.