REVISTA
AMOR MUNDI

LEI GERAL DE PROTEÇÃO DOS DADOS PESSOAIS: ANÁLISE ACERCA DA PROTEÇÃO DE DADOS DO CONSUMIDOR À LUZ DA LEI N. 13709/2018

GENERAL LAW ON THE PROTECTION OF PERSONAL INFORMATIONS: ANALYSIS ON THE PROTECTION OF CONSUMER IN THE LIGHT OF LAW N. 13709/2018

Laryssa Carolyne Oliveira Pinto

Universidade Federal de Roraima, Boa Vista, RR, Brasil. E-mail: laryakarolyni@gmail.com

Douglas Verbicaro Soares

Universidade Federal de Roraima, Boa Vista, RR, Brasil. E-mail: douglas_verbicaro@yahoo.com.br

DOI: https://doi.org/10.46550/amormundi.v2i6.111

Recebido em: 30.07.2021

Aceito em: 19.08.2021

Resumo: Esta pesquisa traz como tema a Lei Geral de Proteção de Dados Pessoais e uma análise acerca de sua abrangência na proteção de dados do consumidor no ambiente de consumo virtual. Nas últimas duas décadas houve um crescente avanço na utilização da internet para se realizar compras e contratar serviços. Consequentemente, tornou-se um desafio para os juristas a possibilidade de acompanhamento das atualizações acerca da nova relação de consumo. Tal fato se tornou ainda mais difícil quando surgiu o novo modo de contratar. Dessa forma, houve a necessidade de se criar mecanismos para que o consumidor pudesse navegar de forma segura nos sites de compras virtuais. Por conseguinte, surgiram normais legais para o uso de dados pessoais na internet (p. exemplo a lei n. 12.965/2014, que dispunha sobre o Marco Civil da Internet). Contudo, essas normativas careciam de uma política que visasse à regulamentação da guarda e manutenção de dados pessoais do indivíduo nos bancos de dados e cadastro de consumo. Dentro dessa realidade surgiu a Lei Geral de Proteção de Dados, vindo a regulamentar o tratamento de dados pessoais no ambiente virtual. Assim, esta pesquisa traz como destaque a análise da LGPD através de uma pesquisa bibliográfica, abordando os principais aspectos da lei referentes à proteção de dados do consumidor e relacionando as principais mudanças no campo da política de segurança da informação como solução para maior segurança e transparência no tratamento de dados.

Palavras-chave: Tecnologia. Consumidor. Comércio eletrônico. Lei n. 13.709/2018.

Abstract: *This research brings as its theme the General Law for the Protection of Personal Data and an analysis about its scope in the protection of consumer data in the virtual consumption environment. In the last two decades, there has been a growing advance in the use of the internet to make purchases and hire services. Consequently, the possibility of following up on updates about the new consumer relationship became a challenge for jurists. This fact became even more difficult when the new way of hiring appeared. Thus, there was a need to create mechanisms so that consumers could safely browse online shopping sites. Consequently, legal norms for the use of personal data on the internet emerged (for example, law n. 12.965/2014, which provided for the Marco Civil da Internet). However, these regulations lacked a policy aimed at regulating the custody and maintenance of individual personal data in databases and consumer records. Within this reality, the General*

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

Data Protection Law came to regulate the processing of personal data in the virtual environment. Thus, this research highlights the analysis of the LGPD, addressing the main aspects of the law relating to consumer data protection and listing the main changes in the field of information security policy as a solution for greater security and transparency in data processing.

***Keywords**: Technology. Consumer. E-commerce. Law no. 13.709/2018.*

1 Introdução

O consumo virtual, nas últimas duas décadas, passou a ganhar espaço com o surgimento do computador e, sobretudo, da internet. Via de consequência, muitos juristas viram a necessidade de se regulamentar o mais novo modo de contratar no campo das relações de consumo. Assim, surgiu a nova figura contratual, denominada de contrato eletrônico, que nada mais é do que a o modelo tradicional de contrato visto de uma forma revolucionária quando inserido no mundo virtual.

Com isso, o Ordenamento Jurídico brasileiro foi, ao longo dos anos, adequando-se à nova forma de contratar, sempre tomando por base o já existente Regulamento Europeu que rege sobremaneira o assunto de forma bem detalhada.

Assim, decretos e leis - a exemplo do Decreto do Marco Civil da Internet e da Lei do Cadastro Positivo – foram moldando e detalhando algumas temáticas que envolviam diretamente o comércio eletrônico, mas sempre de modo esparso.

Não por menos, a discussão foi levantada no âmbito do Congresso Nacional sob a justificativa de que o ordenamento jurídico brasileiro carecia até então de uma normativa específica para disciplinar a proteção de dados do consumidor nas relações de consumo virtuais.

Tal discussão ensejou no PLC n. 53/2018, que mais tarde se tornou a Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709/2018 – vindo a disciplinar e complementar as normativas já existentes acerca da proteção de dados e dos direitos do consumidor face ao E-commerce.

2 Análise acerca da proteção de dados do consumidor à luz da lei n. 13709/2018

A Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709/2018 – promulgada em 14 de agosto de 2018, ainda no governo Temer, que teve origem no PLC n. 53/2018, tornou-se um importante marco legal na história do ordenamento jurídico brasileiro, ao reforçar ainda mais o cumprimento das garantias e direitos fundamentais, previstos na CF/88, que tem como um de seus pilares a proteção dos Direitos Humanos (PINHEIRO, 2020, p. 15).

A referida lei, apesar de sua promulgação ter sido no segundo semestre de 2018, apresentou um dos mais longos períodos de *vacatio legis* que, em seu texto original, seria de 18 (dezoito) meses (BRASIL, 2018).

Contudo, após levantamentos e discussões entre o Congresso Nacional e a Casa Civil, lançou-se a MP n. 869, de 27 de dezembro de 2018 (BRASIL, 2018), que foi posteriormente convertida na Lei n. 13.853, de 08 de julho de 2019 (BRASIL, 2019), estendendo, assim, o período de adaptação para 24 (vinte e quatro) meses.

Assim, a vigência da LGPD se iniciou no dia 18 de setembro de 2020, devido à aprovação

pelo Senado da MP 959/2020 (PLV 34/2020) no final de agosto (BRASIL, 2020). O texto original da medida previa o adiamento da vigência da Lei n. 13.709/2018 para o fim do período de calamidade pública, conforme estabelecido no art. 4º do PLV (SENADO, 2020).

Entretanto, em atendimento à questão de ordem e a solicitações de lideranças partidárias, o presidente do Senado à época, Davi Alcolumbre, declarou a prejudicialidade desse dispositivo, que passou a ser considerado "não escrito" no projeto, transformado na Lei n. 14.058, de 2020. Alcolumbre lembrou, ainda, que em maio do mesmo ano, o Senado aprovou destaque do PDT (Partido Democrático Trabalhista) e do MDB (Movimento Democrático Brasileiro) que mantinha a vigência da LGPD para agosto de 2020 (SENADO, 2020).

A Lei n. 13.709/2018 é um marco legal que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil, garantindo, assim, maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados (SENADO, 2020).

Importante ressaltar, aqui, que o marco regulatório foi moldado a partir da revisão e atualização de legislações esparsas já existentes a respeito da temática a fim de se adaptar à nova realidade social.

Não obstante, apesar da Lei protecionista se fundamentar em uma vasta legislação esparsa – ex. Lei do Cadastro Positivo e Lei do Comércio Eletrônico e outras –, não é possível identificar no novo conjunto normativo uma mera continuidade com a ordem anterior.

O que se nota, na realidade, é uma nova sistemática e abordagem jurídica para o problema de regulamentação do uso da informação pessoal e das garantias dos direitos do seu titular, que não poderia, de modo algum, ser implementada com base nos diplomas legais anteriores já existentes (COTS; OLIVEIRA, 2019, p. 07).

Portanto, a LGPD propõe a objetivação de regras para o tratamento dos dados pessoais. Para tanto, a referida lei traz em seu bojo conceitos fundamentais, princípios de proteção de dados pessoais, um rol taxativo de hipóteses nas quais pode ser dar o tratamento de dados pessoais, além de outros aspectos legais que se fazem necessários para elucidação e interpretação acerca da aplicação do tema (COTS; OLIVEIRA, 2019, p. 08).

Salienta-se a importância que a Lei n. 13.709/2018 tem na proteção de dados do consumidor no *e-commerce*, pois muitos aspectos que seu texto legal traz são aplicáveis no âmbito da relação de consumo que se dá no ambiente virtual, conforme será visto a seguir.

2.1 Conceitos legais

A lei protecionista traz, em seu art. 5º, os principais conceitos para fins de interpretação e aplicação no âmbito da realidade do comércio brasileiro. As definições legais, nas palavras de Oliveira, servem para tornar mais objetivo ou claro os termos da lei [...] (COTS; OLIVEIRA, 2019, p. 73).

Salienta-se que neste tópico não serão explicados todos os conceitos legais, uma vez que a própria lei já traz a definição de cada termo. Assim, serão abordados de forma mais aprofundada apenas aquelas definições que detém relação direta de aplicabilidade no âmbito da relação de consumo virtual.

Desta forma, o primeiro conceito diz respeito a dado pessoal. De acordo com a referida lei,

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

dado pessoal é a informação relacionada à pessoa natural identificada ou identificável (BRASIL, 2018).

Bioni salienta que a Lei n. 13.709/2018 adotou, para a definição de dados pessoais, o critério expansionista (BIONI, 2020, p. 59-60), ou seja, não relaciona apenas como pessoais os dados que, imediatamente, identifiquem uma pessoal natural (critério reducionista) – como o nome, CPF (Cadastro de Pessoais Físicas), imagem etc. –, mas também abarcou os dados que tornam a pessoa identificável de forma não imediata ou direta (COTS; OLIVEIRA, 2019, p. 74).

Para melhor entender como funciona o critério expansionista, Oliveira, em sua obra, traz um exemplo hipotético, voltada para a relação de consumo virtual, conforme será visto abaixo.

Há 01 (um) ano, determinada pessoa realizou a compra de um produto em um *site.* Por força do Marco Civil da Internet, o *site* armazenou o endereço IP da conexão do consumidor. Atualmente, o mesmo computador, sem se "logar" no *site* fez a pesquisa de produtos e teve seu endereço IP novamente capturado pelos *cookies* instalados na página. Neste caso, o *site* consegue identificar o consumidor pelo IP, pois já possuía o mesmo em seu banco de dados, atrelando-o a pessoa natural do comprador (COTS; OLIVEIRA, 2019, p. 74).

Vale ressaltar que o Decreto n. 8.771/2016, que regulamenta o MCI, já dispunha em seu bojo o conceito de dado pessoal, previsto no art. 14, inc. I, do referido diploma legal (BRASIL, 2016).

O segundo conceito que a Lei n. 13709/2018 aborda e que se entende ser de fundamental importância para a compreensão do englobamento do referido diploma legal na proteção de dados do consumidor é a definição de dado anonimizado.

Por definição legal, um dado anonimizado é a antítese de dado pessoal. Assim, a lei protecionista define como sendo aquele dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Tornar um dado pessoal em um dado anônimo requer um processo. O referido processo é denominado por anonimização (BIONI, 2020, p. 62).

Esse processo pode se valer de diferentes técnicas que visam a eliminar elementos identificadores de uma base de dados. As técnicas são as seguintes: Supressão; Generalização; Randomização e Pseudoanonimização.

Não cabe, aqui, detalhar cada técnica, uma vez que não se trata do objetivo central deste trabalho. Entretanto, vale à pena abordar as duas primeiras, trazendo exemplos hipotéticos, a fim de se ilustrar a sua dinâmica e consolidar o entendimento acerca das implicações normativas de uma eventual dicotomia entre dados anônimos e dados pessoais, conforme seguem abaixo (BIONI, 2020, p. 62):

1) Supressão do CPF: por ser um identificar capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único. Diante disto, a sua disponibilização, ainda que parcial não seria prudente;

2) Generalização do nome completo: constaria apenas o prenome, desde que fosse observado que os nomes na base de dados não são comuns. O objetivo é evitar que um nome possa ser atribuído a um indivíduo em específico;

3) Generalização da localização geográfica: em vez de fornecer o número completo do

CEP, seriam publicados apenas os primeiros dígitos. Desta forma, haveria uma localização menos detalhada, com vistas a romper o vínculo de identificação desta informação com um sujeito.

Seguindo, a próxima definição que a Lei n. 13.709/2018 aborda é o conceito de banco de dados. De acordo com a lei protecionista, banco de dados é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Neste sentido, o CDC já dispunha acerca da formação de banco de dados e cadastro de consumidores, em seu art. 43 e seguintes (BRASIL, 1990).

Contudo, apesar da lei protecionista abordar o conceito de banco de dados, a lei consumerista traz dois conceitos que, de acordo com a doutrina, devem ser tratados distintamente, para fins de interpretação do aplicador do Direito.

Assim, nas palavras de Benjamim, os dados de um cadastro de consumo são coletados por quem mantém uma relação comercial com o consumidor, sendo a sua utilização voltada aos interesses do próprio arquivista-fornecedor, ao passo que as informações dos bancos de dados seriam resultantes de uma coleta aleatória realizada por terceiros que, por sua vez, não mantém relação comercial com o consumidor (BENJAMIN, 2011, p, 444).

Por conseguinte, a lei protecionista define titular como sendo a pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento.

Pela definição legal acima exposta, torna-se claro que o titular de dados pessoais só pode ser uma pessoa física. Neste sentido, cabe tecer algumas considerações acerca da pessoa física, a fim de se melhor entender e até mesmo antecipar um dos temas que será abordado a seguir: o consentimento.

Pois bem, Coelho ensina que toda pessoa natural (física) ostenta o atributo da personalidade, estando, assim, apta a praticar qualquer ato jurídico que deseja, salvo disposição expressa em contrário (COELHO, 2012, p. 368).

Do conceito acima, extrai-se o termo ato jurídico ou ato jurídico em sentido estrito que, nas palavras de Gonçalves, é o efeito da manifestação da vontade predeterminada na lei (GONÇALVES, 2012, p. 453). Ato jurídico é espécie do gênero ato lícito. Assim, ato lícito pode ser ainda: a) o negócio jurídico e b) o ato-fato jurídico (GONÇALVES, 2012, p. 452).

O Negócio jurídico, de acordo com o referido autor, deriva de uma ação humana que visa diretamente alcançar a um fim prático permitido em lei, dentre a multiplicidade de efeitos possíveis. Por este motivo, é necessária uma vontade qualificada, sem vícios (GONÇALVES, 2012, p. 453).

Dentre as espécies de negócio jurídico está o consentimento. Por definição legal, o referido ato consiste em uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Oliveira ensina que o consentimento é um negócio jurídico que possui forma prescrita por lei, qual seja: por escrito ou por outro meio que demonstre a manifestação de vontade do titular (COTS; OLIVEIRA, 2020, p. 92).

O autor explica que o referido ato possui nítida natureza contratual, pois, de um lado, há a manifestação de vontade de uma parte em tratar os dados pessoais para determinada finalidade e, de outro lado, há alguém que anui com tal tratamento (COTS; OLIVEIRA, 2019, p. 91).

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

Por conseguinte, a Lei n. 13.709/2018 traz, ainda, o conceito de agentes de tratamento, que consiste nas figuras do controlador e do operador, como também define o que seja tratamento de dados pessoais[1]. Além disso, o referido diploma legal traz outros conceitos que não cabe tecer aqui em virtude de não guardarem relação direta com a temática abordada.

Feita a análise das principais definições que a LGPD traz, passa-se à análise de seus fundamentos, objetivos e princípios para que se possa melhor compreender a sua finalidade.

2.2 Objetivo, Fundamentos e Princípios da lei n. 13.709/2018

Antes de se adentrar no tripé de sustentação da lei protecionista, necessário se faz diferenciar o que seja cada termo, a fim de enriquecer o presente trabalho e até mesmo esclarecer em que campo cada um está alocado.

Pois bem, os objetivos de uma norma, conforme ensina Oliveira, são direções mais precisas, intenções mais delimitadas que visam a um fim específico (COTS; OLIVEIRA, 2019, p. 48). Já o fundamento, nas palavras do autor, é a base de toda lei, o suporte sobre qual se sustenta alguma coisa (COTS; OLIVEIRA, 2019, p. 46).

Por fim, os princípios, seriam as estruturas ou colunas sobre as quais cresce uma ciência [...] (COTS; OLIVEIRA, 2019, p. 46). Neste sentido, os princípios seriam aquilo que se pode chamar de "norte" para a interpretação de qualquer arcabouço normativo, funcionando, assim, como a espinha dorsal de qualquer diploma legal.

2.2.1 Objetivo

O objetivo da Lei Geral de Proteção de Dados, nas palavras de Oliveira, é o de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (COTS; OLIVEIRA, 2019, p. 48).

O autor destaca, ainda, que o verbo "proteger" indica sobre a forma como o legislador viu o titular dos dados, ou seja, em posição desnivelada em relação aos responsáveis pelo tratamento de dados, ficando evidente a sua vulnerabilidade (COTS; OLIVEIRA, 2019, p. 48).

Neste sentido, resta claro que ao destacar o termo acima, a fim de assegurar a proteção do titular de dados, a lei teve a intenção de equilibrar a relação jurídica existente entre as partes, a fim de que direitos já existentes sejam observados pelos responsáveis pelo tratamento (COTS; OLIVEIRA, 2019, p. 49).

Ressalta-se, ainda, a recorrente vulnerabilidade do titular de dados, pois, diferentemente do que ocorre nas relações de consumo, nas quais a vulnerabilidade pode até ser quase nula, como no caso de consumidores com maior conhecimento técnico ou poder econômico superior ao do fornecedor, no que se refere ao tratamento de dados, é cediço que tal ato pode acontecer, inclusive, sem o conhecimento do titular (COTS; OLIVEIRA, 2019, p. 49).

Neste caso, uma pessoa natural se torna alvo fácil e logo se põe em posição de vulnerabilidade, pois os dados, por ser a grande maioria intangível, não permitem ao titular certeza jurídica de seu tratamento (COTS; OLIVEIRA, 2019, p. 49). Por este motivo, a lei protecionista criou mecanismos de informações e segurança para o tratamento de dados, conforme será visto a

1 Os referidos conceitos estão elencados respectivamente nos incisos VI, VII e X, do art. 5º, da Lei n. 13.709/2018.

seguir.

2.2.2 Fundamentos

A Lei n. 13.709/2018 menciona, em seu art. 2º, sete fundamentos. Entretanto, a fim de restringir a análise do tema, serão abordados apenas aqueles que detêm relação direta com a proteção de dados do consumidor.

O primeiro fundamento é o da livre iniciativa.

É possível vislumbrar o referido fundamento nos ditames constitucionais, *in verbis*:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui se em Estado Democrático de Direito e tem como fundamentos:
>
> [...] IV - os valores sociais do trabalho e da livre iniciativa;

Bastos afirma que o referido fundamento tem conotação precipuamente econômica, equivalendo aos direitos que todos têm de lançarem-se ao mercado da produção de bens e serviços por sua conta e risco, nisso, incluindo as atividades de gestão e empresa (BASTOS, 1995).

Não obstante, o diploma constitucional, nas palavras de Silva, apresenta o conceito ligado a ideia de função social (SILVA, 1998).

Assim, é base da República o direito de empreender, com objetivos econômicos, em liberdade que só pode ser mitigada quando houver conflito com outro fundamento, como, por exemplo, o valor social do trabalho, ou, ainda, princípio constitucional, a fim de se preservar a harmonia sistematizada na CF/88 (COTS; OLIVEIRA, 2019, p. 59).

Além disso, os fundamentos da livre concorrência e da defesa do consumidor também estão previstos na Lei Maior (BRASIL, 1988):

> Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos, existência digna, conforme os ditames da justiça social, observados os seguintes princípios:
>
> [...]
>
> IV - Livre concorrência;
>
> V - Defesa do consumidor;

Neste sentido, a doutrina ressalta que a livre concorrência se destaca por ser o elemento fundamental para o democrático desenvolvimento da estrutura econômica. Via de consequência é ela a pedra de toque das liberdades públicas no setor econômico. Concorrência é disputa em condições de igualdade de cada espaço [...]. Consiste, no setor econômico, na disputa entre todas as empresas para conseguir maior e melhor espaço no mercado [...] (BASTOS; MARTINS, 1990, p. 25).

Dessa forma, pode-se afirmar que aos particulares é assegurada a livre iniciativa e a livre-concorrência, a primeira sendo um fundamento da República, e a segunda como princípio da ordem econômica, sendo que ambas devem observar o princípio da legalidade, previsto na Lei Maior, assim como a função social da propriedade (COTS; OLIVEIRA, 2019, p. 60).

Por último, fala-se em defesa do consumidor. Além da CF/88, a lei consumerista não apenas prevê como também regulamenta a proteção aos direitos do consumidor, bem como

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

também aos seus dados pessoais (BRASIL, 1990).

O CDC prevê, ainda, a formação de banco de dados de dados e cadastro de consumidores, já anteriormente comentados. Contudo, há de se tecer algumas considerações acerca dessa ferramenta tão utilizada pelos fornecedores, relacionando-a, sobremodo, à proteção de dados do consumidor.

Pois bem, a Lei n. 13.709/2018 traz expressamente a definição de tratamento de dados como sendo "toda operação realizada como 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" (BRASIL, 2018).

Extrai-se da definição legal acima que o rol descrito se trata de um rol exemplificativo, não exaustivo, uma vez que o legislador optou por utilizar a expressão "toda operação", acrescido da conjunção "como" para conceituar o que seja tratamento de dados. Ainda, trata-se de hipóteses não cumulativas, ou seja, basta que se uma única atividade do rol seja realizada para restar caracterizado o tratamento (COTS; OLIVEIRA, 2019, p. 75).

Neste sentido, uma das ações que o conceito acima traz é o armazenamento de dados. Armazenar dados pessoais sem utilizá-los já considerado tratamento de dados (COTS; OLIVEIRA, 2019, p. 75). E é justamente desse tipo de ação que se originam os bandos de dados e, ainda, o cadastro de consumidores, que serão explanados a seguir.

Bioni, em sua obra, destaca um tópico acerca da mineração de dados e explica que é de total relevância saber diferenciar o que sejam dados e informação, uma vez que os dois conceitos não se confundem, ainda que sejam recorrentemente utilizados em sua sinonímia quando são abordados dentro da referida temática (BIONI, 2020, p. 31).

Neste sentido, a doutrina explica que dados são simplesmente fatos brutos, ao passo que informações são resultado de dados brutos para revelar o seu significado (ROB, 2011, p. 04).

Para ilustrar a formação de banco de dados, Bioni destaca uma Multinacional que coleta e acumula os fatos (dados) das vendas e saídas de seus produtos. Tal ação, por si só, não apresenta significado algum, somente quando organizados, para o fim de identificar quais produtos foram mais vendidos, retira-se, portanto, uma informação útil (BIONI, 2020, p. 32).

Assim, conforme exposto no exemplo acima, depreende-se que a dinâmica de um bando de dados consiste na entrada, passando pelo processamento, e finalizando na saída de uma informação (BIONI, 2020, p. 32).

Contudo, explica o autor, que a referida dinâmica possibilita uma montanha de fatos (dados) sobre os usuários da internet que, por sua vez, é gerenciada para lhes direcionar mensagens publicitárias personalizadas. Tal fato denomina-se publicidade comportamental, já anteriormente comentada aqui neste trabalho (BIONI, 2020, p. 33).

Importante relacionar a estrutura de um banco de dados com a proteção de dados no consumidor no ambiente virtual, uma vez que as decisões acerca da formação de um banco de dados vão desde a concepção de um bem de consumo ao direcionamento da mensagem publicitária (BIONI, 2020, p. 34).

Possibilita-se a identificação do perfil potencial do consumidor, bem como de seus hábitos e outras informações necessárias à tomada de decisões táticas e estratégicas. Tal fato acima é

conhecido por mineração de dados ou "*data mining*" (BIONI, 2020, p. 34).

Entretanto, a referida prática apresenta seus riscos, notadamente, no que se refere à segurança na manutenção dos dados ali armazenados, conforme será visto a seguir.

O CDC prevê em seu texto a criação de banco de dados e cadastro de consumo. Depreende-se do diploma legal que, a princípio, as duas figuras seriam equivalentes.

Contudo, a doutrina passou a tratá-los como espécies do gênero arquivo de consumo. Benjamim, que foi coautor do anteprojeto dessa parte específica do CDC, destaca que há características que diferenciam os dois institutos acima (BIONI, 2020, p. 39).

O autor revela que a primeira se relaciona a um aspecto objetivo, ou seja, o modo pelo qual os dados são coletados. Daí deriva-se a segunda característica, de aspecto subjetivo, que indica quem titulariza tais arquivos de consumo (BENJAMIN, 2011, p. 445).

Assim, de acordo com a doutrina, os dados de um cadastro de consumo são coletados por quem mantém uma relação comercial com o consumidor, sendo que a sua utilização é precipuamente destinada aos interesses do próprio arquivista-fornecedor (EFING, 2002, p. 34).

Por outro lado, as informações dos bancos de dados resultam de uma coleta aleatória que é realizada por terceiros que, por sua vez, não mantêm relação comercial com o consumidor como, por exemplo, a base de dados dos órgãos de proteção de crédito (BENJAMIN, 2011, p. 445).

O terceiro elemento, de acordo com a doutrina, trata-se da transmissibilidade. O mantenedor de um bando de dados necessariamente divide suas informações com terceiros. Cita-se o exemplo já mencionado dos órgãos de proteção de crédito. Tal fato denomina-se de transmissibilidade extrínseca. Não obstante, os dados de um cadastro de consumo são restritos apenas ao arquivista, não sendo compartilhado a terceiros. Esta última é definida como transmissibilidade intrínseca (BENJAMIN, 2011, p. 445).

A quarta característica que diferencia os referidos institutos trata-se de um elementar temporal. Pelo fato de o cadastro de consumo manter necessariamente a relação comercial com o consumidor para que torne viável o tratamento de seus dados, a partir do momento em que o cliente desfaz a relação de consumo, os seus dados consequentemente são excluídos (EFING, 2002, p. 31).

Por outro lado, no que se refere ao banco de dados, acontece exatamente o inverso. Apesar do consumidor não manter mais a relação comercial com o fornecedor, seus dados ainda assim são mantidos na base de arquivos, a fim de que possam ser consultados por terceiros (BENJAMIN, 2011, p. 444).

Por fim, a quinta e última característica é referente à (in)existência de autorização do consumidor. Um exemplo torna a ser citado, que é o banco de dados dos órgãos de proteção de crédito que, para serem tratados, prescindem do consentimento do seu titular. Já no cadastro de consumo há a obrigatoriedade da autorização do consumidor que, geralmente, é coletada quando da transação comercial entre o arquivista-fornecedor e o consumidor (BENJAMIN, 2011, p. 444-445).

Contudo, Bioni ressalta que todo o esforço acima de distinguir banco de dados e cadastro de consumo é mitigado quando a referida taxonomia é incluída na sociedade da informação, uma vez que o fluxo de informações é constante, desconstruindo, assim, os elementos diferenciadores

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

acima listados (BIONI, 2020, p. 40).

Portanto, ainda que a atividade de coleta e armazenamento de dados, de consumidores em computadores conectados à internet seja uma atividade benéfica, vale lembrar que está também apresenta seus riscos.

A materialização desse risco foi objeto de notícia veiculada em 10.12.2013, em que uma falha de segurança no aplicativo do Banco do Brasil para dispositivos móveis expôs, na noite de 09.12.2013, por alguns minutos, certos dados de contas bancárias de clientes do BB (Banco do Brasil) que usam o aplicativo (G1, 2013).

Consequentemente, traz-se à tona o direito à segurança, previsto no código consumerista. Tal direito gera expectativa ao consumidor de que seus dados, quando informados ao fornecedor, serão por ele armazenados adequadamente com mecanismos de segurança de informação atualmente disponíveis no mercado (BLUM, 2018, p. 76).

Entretanto, o que se tem visto recorrentemente é que o referido direito nem sempre é respeitado pelo fornecedor, que acaba violando não apenas a segurança de seu cliente, como também todo o arcabouço legal aí existente.

Foi dentro dessa realidade social que a LGPD surgiu, não apenas para proteger o consumidor, como também para garantir a integridade, transparência e segurança no tratamento de seus dados.

Mister se faz expor a preocupação em relação a existência de outros dados pessoais, notadamente aqueles sobre os hábitos do consumidor, que vão muito além de informações creditícias, constantes de arquivos, cadastros, fichas ou banco de registro de dados (BLUM, 2018, p. 97).

Considerando a assertiva acima, serão abordados a seguir os princípios que fundamentam a LGPD, sendo de elevada importância que se comente sobre cada um dos referidos princípios e suas aplicações práticas no âmbito da relação de consumo virtual.

2.2.3 Princípios

A lei protecionista prevê, em seu art. 6º, os seguintes princípios: a) Boa fé; b) Finalidade; c) Adequação; d) Necessidade; e) Livre acesso; f) Qualidade dos dados; g) Transparência; h) Segurança; i) Prevenção; j) Não discriminação; e; k) Responsabilização e prestação de contas.

Os princípios mencionados serão analisados sistematicamente, mas antes será explanado o conceito de princípio para que se possa esclarecer e, ainda, destacar a obrigatoriedade que o referido instituto tem na lei protecionista.

Nos ensinamentos de Canotilho (CANOTILHO, 1991, p. 545):

> Princípios são normas que exigem a realização de algo, da melhor forma possível, de acordo com as possibilidades fácticas e jurídicas. Os princípios não proíbem, permitem ou exigem algo [...], impõem a optimização de um direito ou de um bem jurídico, tendo em conta a "reserva do possível", fáctica ou jurídica.

Assim, os princípios da LGPD têm por objetivo justamente o descrito acima pelo renomado jurista, qual seja, a de impor a otimização de um direito/bem jurídico existente, neste caso, assegurar a integridade e segurança no tratamento de dados do consumidor.

Os princípios que serão abordados a seguir, não são sobressalentes uns aos outros,

funcionando, assim, de maneira harmoniosa, uma vez que não há que se falar aqui em preponderância de princípios, já que todos cumprem a mesma finalidade: a de orientar, de forma sistematizada, a interpretação da Lei n. 13.709/2018.

a) Princípio da boa-fé

A doutrina ensina que a boa-fé vem desde a Roma antiga, entrelaçada na vida social e, via de consequência, nas legislações, pois o que antes era visto apenas como regra moral, passou a ser uma prática tão recomendável que não poderia permanecer apenas no campo das ideias. Assim, a boa-fé foi positivada, sendo alocada como regra ou princípio de que regem as relações jurídicas (COTS; OLIVEIRA, 2019, p. 76).

Neste sentido, a boa-fé pode ser analisada sob dois aspectos, quais sejam, a boa-fé subjetiva e a boa-fé objetiva. No primeiro caso, o esforço é o de tão-somente não prejudicar o próximo. Já no segundo caso, a boa-fé deixa de ser passiva e começa a se mostrar por meio de uma conduta preventiva e proativa a fim de que outrem não seja prejudicado (COTS; OLIVEIRA, 2019, p. 76).

b) Princípio da finalidade

Oliveira ensina que o tratamento de dados precisa ter uma finalidade a ser alcançada. Assim, o referido princípio serve não apenas para restringir o objetivo final do tratamento, como também para tornar previsível o que dele se espera, impossibilitando tratamento posterior desvinculado com a finalidade original (COTS; OLIVEIRA, 2019, p. 79).

Não obstante, a lei protecionista passou por uma recente alteração, realizada por meio da Lei n. 13.853/2019, incluindo um parágrafo no art. 7º, conforme se vê abaixo (BRASIL, 2019):

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> [...]
>
> 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019).

Entretanto, a crítica que a doutrina faz é a possibilidade de serem dadas novas finalidades aos dados pessoais de acesso público, o que acabaria por contrariar o princípio em epígrafe (COTS; OLIVEIRA, 2019, p. 80).

Desta forma, nota-se que o legislador foi incoerente ao acrescentar o dispositivo acima na lei protecionista, uma vez que está pondo em risco a aplicabilidade não apenas o princípio em comento, como também de todo o arcabouço normativo.

c) Princípio da adequação

O referido princípio, nas palavras de Oliveira, visa a preservar a relação entre as finalidades informadas e o tratamento dispensado, evitando, assim, a desvirtuação (COTS; OLIVEIRA,

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

2019, p. 80).

Neste sentido, o autor aponta que a principal diferença que distingue o princípio em epígrafe do princípio da finalidade reside no fato de que o último se preocupa na regularidade da finalidade em si, enquanto o segundo aborda o procedimento realizado para se alcançar a finalidade pretendida (COTS; OLIVEIRA, 2019, p. 80).

d) Princípio da necessidade

O princípio em epígrafe aponta que devem ser tratados apenas os dados necessários, descartando-se os excessivos ou desnecessários.

Não obstante, Oliveira ressalta que nem sempre a necessidade nasce diretamente no negócio jurídico com o titular, sendo possível que a lei obrigue o controlador a tratar determinado dado (COTS; OLIVEIRA, 2019, p. 81).

O autor cita, por exemplo, a data de nascimento, que antes era um dado dispensável na maioria das compras online e, após a vigência da LGPD passou a se tornar um dado necessário, haja vista o tratamento diferenciado de dados pessoais de menores de idade e idosos que foi imposto pelo referido diploma legal (COTS; OLIVEIRA, 2019, p. 81).

e) Princípio da não discriminação

O princípio da não discriminação prevê a vedação de tratar dados para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018).

São exemplos de violação ao referido princípio: a) realizar senso para dispensa de empregados de determinada religião; b) realizar ofertas de produtos ou serviços apenas para pessoas de determinada nacionalidade; c) não admitir como usuário pessoas do sexo feminino (COTS; OLIVEIRA, 2019, p. 81).

f) Princípio da transparência

Agir com transparência no âmbito da Lei n. 13.709/2018, de acordo com Oliveira, significa agir com o fim de garantir informações claras, precisas e acessíveis aos titulares no que se refere ao tratamento de seus dados pessoais (COTS; OLIVEIRA, 2019, p. 81).

g) Princípio do livre acesso

O referido princípio encontra amparo no art. 9º da lei protecionista. O dispositivo em comento prevê o seguinte, *in verbis* (BRASIL, 2018):

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

Nos ensinamentos de Oliveira, é direito do titular ter acesso às informações sobre o tratamento de seus dados que deverão ser disponibilizadas de forma clara, adequada e ostensiva (COTS; OLIVEIRA, 2019, p. 100).

Contudo, o autor destaca que as referidas informações não devem necessariamente ser apresentadas pela internet, uma vez que há o tratamento de dados *on-line* e *off-line* (COTS;

OLIVEIRA, 2019, p. 100).

Nesse sentido, assim como a revogação do consentimento, o autor entende que a disponibilização das informações deve ser da mesma forma ou pelo mesmo meio por meio do qual o tratamento de dados se iniciou (COTS; OLIVEIRA, 2019, p. 100).

Assim, se o tratamento se iniciou pela internet, deve ser por ela que as informações de tratamento devem ser apresentadas, já se foi em um local físico, é nele que devem ser acessadas (COTS; OLIVEIRA, 2019, p. 100).

h) Princípio da qualidade de dados

A lei protecionista prevê que o titular de dados tem direito a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (BRASIL, 2018).

Neste sentido, o art. 18 da lei protecionista prevê alguns direitos que se referem ao tratamento de dados entre titular e controlador, que serão comentados a seguir. Saliente-se que o exercício de tais direitos é realizado mediante requisição, ou seja, não se trata de pedido ou solicitação, não podendo o controlador se opor, salvo nos casos previstos na lei protecionista (COTS; OLIVEIRA, 2019, p. 130).

Pois bem, o art. 18 destaca como um dos direitos do titular a confirmação acerca da existência de tratamento, acesso aos dados tratados e a possibilidade de correção deles, quando incompletos, inexatos e desatualizados. Saliente-se que os referidos direitos estão vinculados aos princípios da transparência, livre acesso e qualidade dados (COTS; OLIVEIRA, 2019, p. 130).

Não obstante, por se tratar de uma requisição, Oliveira lembra que o titular, ainda que não tenha conhecimento técnico, poderá exigir quaisquer das ações acima mencionadas, cabendo necessariamente ao controlador adotar a medida mais adequada (por exemplo, se o titular exigir que determinados dados sejam anonimizados, caso o controlador decida que estes devam ser excluídos em benefício do titular, deverá se utilizar do procedimento de eliminação de dados) (COTS; OLIVEIRA, 2019, p. 130).

O referido dispositivo ainda prevê o direito do titular acerca da portabilidade de seus dados de um fornecedor de produtos ou serviços para outro, como acontece, por exemplo, na portabilidade de números telefônicos (COTS; OLIVEIRA, 2019, p. 131).

Entretanto, a doutrina salienta que não se deve confundir os dados pessoais e o produto do tratamento destes. Suponha, por exemplo, que um *site* de vendas, com base na navegação do usuário logado, cria um perfil de consumo de modo que ofereça produtos de acordo com os interesses do cliente, utilizando-se, para isso, de estudo de mercado, *softwares* de outras técnicas (informações dos *cookies*, por exemplo). Caso o titular solicite a portabilidade, o *site* não é obrigado a reunir os dados e informações advindos do tratamento, mas apenas os dados coletados (COTS; OLIVEIRA, 2019, p. 131).

Ainda, deve-se frisar que a portabilidade precisa ser expressa, não escrita, ou seja, poderá ser feita por qualquer meio que transmita de forma precisa a vontade do titular (COTS; OLIVEIRA, 2019, p. 131).

O art. 18 prevê, ainda, que o titular tem direito a informação sobre o compartilhamento de seus dados, sendo que o conteúdo da informação deve trazer a finalidade e abrangência de

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

tal compartilhamento. Contudo, até então, a maioria dos controladores não possuíam controle adequado do compartilhamento que realizavam, o que provavelmente deve mudar com a nova lei (COTS; OLIVEIRA, 2019, p. 131).

Nesse ínterim, importante mencionar a relevância acerca do compartilhamento de dados e a sua principal consequência, quando se trata de procedimentos os quais (o titular) requisita. A lei n. 13.853/2019, neste sentido, acrescentou o § 6º ao art. 18, o qual aduz o seguinte (BRASIL, 2019):

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> [...]
>
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019).

Depreende-se do exposto acima que o controlador tem a obrigação de informar imediatamente aos demais agentes de tratamento quaisquer das ações acima mencionadas, caso tenham sido realizadas, para que estes repitam procedimento idêntico. Tal fato se justifica na necessidade de haver total controle sobre as demais entidades públicas e privadas que tenham recebidos os dados pessoais (COTS; OLIVEIRA, 2019, p. 132).

Por fim, o referido dispositivo prevê o direito do titular de saber das consequências da negativa de consentimento para tratamento de dados pessoais. Frisa-se que, em alguns casos, as consequências poderão envolver a impossibilidade de fechamento de negócio jurídico, como por exemplo, o não consentimento para elaboração de proposta comercial ou contrato (COTS; OLIVEIRA, 2019, p. 132).

Entretanto, a doutrina ressalta que para que a consequência seja negativa, é necessário lembrar os princípios da necessidade, finalidade e adequação, pois, se os dados pessoais foram desnecessários ou abusivos, não se justifica o tratamento (COTS; OLIVEIRA, 2019, p. 132).

i) Princípio da segurança

Além dos princípios já mencionados, o art. 18 traz como princípio basilar, e talvez o mais importante de todos, o da segurança. Estabelece o dispositivo que a segurança no tratamento de dados se refere a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (BRASIL, 2018).

j) Princípio da prevenção

O princípio da prevenção, de acordo com a lei protecionista, trata da adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (BRASIL, 2018).

O referido princípio é mais bem explicado no art. 47 da lei protecionista, que prevê o

seguinte, *in verbis* (BRASIL, 2018):

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta lei em relação aos dados pessoais, mesmo após seu término.

O referido artigo trata da garantia da segurança da informação. Depreende-se do dispositivo em comento que o agente se responsabilizará pelo tratamento, respondendo por seus empregados, contratados, prestadores de serviços e quaisquer outras pessoas, físicas ou jurídicas, sob as suas ordens (COTS; OLIVEIRA, 2019, p. 196).

Assim, o melhor entendimento é, mesmo que o dispositivo acima mencionado fale em "qualquer outra pessoa", tal fato não isenta o agente de tratamento, mas abre um caminho mais claro e seguro para que ele se utilize de ação regressiva contra o causador do dano, voltado, notadamente, à questão da segurança de informação, conforme o art. 934 do Código Civil ou do art. 462, da CLT, a depender da natureza da relação entre agente e infrator (COTS; OLIVEIRA, 2019, p. 196).

Ainda, o art. 47 trata da segurança permanente, que consiste na obrigação dos agentes de tratamento ou seus contratados em garantir que a segurança da informação permaneça mesmo após o término do tratamento (COTS; OLIVEIRA, 2019, p. 196).

k) Princípio da responsabilização e prestação de contas

O princípio em epígrafe, de acordo com a Lei n. 13.709/2018, trata da demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar e observância e o cumprimento das normas de proteção de dados e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

O referido princípio é abordado com maior clareza no art. 42 do mencionado diploma legal, que trata da responsabilidade e do ressarcimento de danos ao titular de dados.

No que se refere a responsabilização do agente de tratamento (controlador ou operador), nos casos em que houver dano patrimonial, moral, individual ou coletivo, este deverá reparar (BRASIL, 2018).

Para fins de indenização, é necessário distinguir as duas figuras de agentes que a Lei n. 13.709/2018 prevê. Assim, o controlador é aquele que detém todo o poder decisório sobre o tratamento de dados, enquanto o operador apenas executa as instruções passadas pelo primeiro (COTS; OLIVEIRA, 2019, p. 180).

No que se refere à responsabilidade civil dos agentes, segue a regra geral prevista nos artigos 186, 187 e 927 do Código Civil (BRASIL, 2002):

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Não obstante, a lei protecionista criou duas hipóteses de responsabilidade solidária, nas

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

quais o operador responderá ao lado do controlador pelos danos causados, que são as seguintes: a) quando o operador violar a LGPD; e b) quando o operador não seguiu as instruções de tratamento estabelecidas pelo controlador.

Saliente-se que as duas hipóteses não são cumulativas, mas pode-se dizer que detém certa relação de dependência, à medida que se a segunda ocorrer, poderá impactar diretamente nos princípios previstos na LGPD, gerando a sua violação indireta (COTS; OLIVEIRA, 2019, p. 181).

Há, ainda, a previsão da inversão do ônus da prova, que segue a regra do art. 373 do Código de Processo Civil (BRASIL, 2015):

> Art. 373. O ônus da prova incumbe:
>
> I - Ao autor, quanto ao fato constitutivo de seu direito;
>
> II - Ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor.

Neste sentido, o CDC (BRASIL, 1990) já previa a inversão do ônus da prova com base no mesmo raciocínio, haja vista que nas relações em que há posição de desvantagem de umas das partes (p. ex. técnica, econômica) as regras processuais devem se adequar, facilitando a perseguição dos direitos da parte em desvantagem (COTS; OLIVEIRA, 2019, p. 182).

Portanto, a LGPD, considerando a sua finalidade precípua, levou em conta a realidade social já consolidada: o titular, recorrentemente, encontra-se em posição de desvantagem ou fragilidade diante dos agentes de tratamento (COTS; OLIVEIRA, 2019, p. 183).

Tal fato teve grande peso para que o legislador decidisse por incluir o instituto processual da inversão do ônus da prova também nas relações de tratamento de dados pessoais (COTS; OLIVEIRA, 2019, p. 183).

Assim, para que a inversão do ônus se opere, deve ser considerando o seguinte: a) a alegação do titular deve conter indícios de veracidade; e b) deve haver hipossuficiência para fins de produção de prova ou quando a produção de prova for muito onerosa (COTS; OLIVEIRA, 2019, p. 183).

3 Tratamento de dados pessoais

O tratamento de dados pessoais, nos ensinamentos de Oliveira, deve ser feito mediante o enquadramento em uma das bases legais do art. 7º, da Lei n. 13.709/2018 (COTS; OLIVEIRA, 2019, p 83).

Contudo, por se tratar de um rol exaustivo, serão abordadas apenas as bases legais que detém relação com a proteção de dados do consumidor.

Assim, o dispositivo em comento prevê que o tratamento de dados poderá ser realizado nas seguintes hipóteses:

a) Mediante o fornecimento de consentimento do titular;

b) 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; e

c) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No que se refere à primeira hipótese, salienta-se que o consentimento do titular de dados é de fundamental importância para que se garanta a qualidade e segurança no tratamento de seus dados.

Dessa forma, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso de dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e privacidade (PINHEIRO, 2020, p. 85).

Já a segunda hipótese remete à teoria geral dos contratos, já abordado em tópico anterior deste trabalho.

Não é demais relembrar, de forma sintética, que o contrato é o acordo de duas ou mais vontades [...] destinado a estabelecer uma regulamentação de interesses entre as partes, com o escopo de adquirir, modificar ou extinguir relações jurídicas de natureza patrimonial (DINIZ, 2008, v. 3).

Neste sentido, Oliveira destaca que a fase antecedente da contratação geralmente envolve a proposta ou o contrato preliminar, sendo que ambas dependem do tratamento de dados pessoais para a adequada identificação das partes ou de seus representantes (COTS; OLIVEIRA, 2019, p. 86).

Portanto, ao redigir a hipótese em comento, o legislador optou por não permitir o tratamento de dados pessoais na fase de formação dos contratos, mas tão somente em sua execução, ou seja, antes disso, o tratamento só poderá ser realizado mediante o consentimento legal do titular (COTS; OLIVEIRA, 2019, p. 86).

Quanto à hipótese de proteção de crédito, salienta-se que esta hipótese já foi aborda em tópico anterior, quando se explicou acerca do banco de dados e cadastros de consumo.

Não obstante, importante destacar aqui alguns pontos relevantes acerca do crédito financeiro, uma vez que se trata de uma ferramenta trivial para a movimentação da economia (COTS; OLIVEIRA, 2019, p. 90).

Pois bem, o crédito financeiro viabilizar tanto o desenvolvimento pessoal quanto o empresarial, injetando importantes recursos no mercado nacional e impactando beneficamente seus personagens como um todo (COTS; OLIVEIRA, 2019, p. 90).

Contudo, a referida atividade oferece riscos, podendo ser concretizado pela inadimplência, degradação de crédito ou, ainda, pela degradação de garantias (COTS; OLIVEIRA, 2019, p. 90).

Neste sentido, foram criados mecanismos por meio dos quais o mercado tenta se precaver dos riscos desconhecidos ou, ainda mapear a abrangência de riscos conhecidos, sendo o principal as entidades de proteção de crédito (COTS; OLIVEIRA, 2019, p. 90).

Nesse contexto que surgiu a Lei do Cadastro Positivo (Lei n. 14.414/2011), prevendo a criação de banco de dados de adimplentes, fazendo com que o risco pelo oferecimento de crédito a si fosse menor do que para pessoas que não constavam em tal cadastro (COTS; OLIVEIRA, 2019, p. 90).

Salienta-se que a referida lei foi uma das precursoras à criação da lei protecionista, uma vez que muito do que consta na primeira, serviu de base normativa para a segunda.

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

4 Adoção de boas práticas a fim de se resguardar a proteção dos dados do consumidor

Por fim, comentar-se-á, aqui, acerca da segurança e boas práticas para que se torne possível a qualidade na proteção e tratamento de dados do consumidor.

A Lei n. 13.709.2018 prevê, em seu art. 46, que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de:

a) Acessos não autorizados;

b) Situações acidentais (nos casos de culpa: negligência, imprudência ou imperícia); ou

c) Ilícitas (cometidas com dolo).

Neste sentido, a respeito da segurança da informação, a norma ISO/IEC 17799:2005 a define como sendo "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos, maximizando o retorno sobre os investimentos e as oportunidades de negócio" (BRASIL, 2005).

Assim, Oliveira ressalta que as medidas de segurança são de elevada importância, porém, não geram seus efeitos sendo aplicadas de forma isolada, dependendo, para isso, de medida técnicas e administrativas (COTS; OLIVEIRA, 2019, p. 191).

Salienta-se, ainda, a comunicação em caso de incidentes, prevista no art. 48 da lei protecionista. O referido ato guarda muita semelhança com o denominado *recall*, previsto no art. 10, do CDC (BRASIL, 1990):

> Art. 10. O fornecedor não poderá colocar no mercado de consumo produto ou serviço que sabe ou deveria saber apresentar alto grau de nocividade ou periculosidade à saúde ou segurança.
>
> § 1° O fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários.

Não obstante, a comunicação prevista na Lei n. 13.709/2018 deve observar algumas formalidades em seu conteúdo, contendo o seguinte: a) descrição da natureza dos dados pessoais afetados; b) informações sobre os titulares envolvidos; c) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; d) riscos relacionados ao incidente; e) motivos da demora, no caso de a comunicação não ter sido imediata; e f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

No que se refere ao encaminhamento da comunicação, a lei n. 13.709/2018 prevê que deve ser feito pelo controlador. Entretanto, se houver incidente no âmbito do operador, este deverá comunicar o controlador imediatamente, a fim de que ele cumpra com sua obrigação legal (COTS; OLIVEIRA, 2019, p. 199).

A lei protecionista estabeleceu também a possibilidade de controladores e operadores, sozinhos ou coletivamente, criarem boas práticas corporativas para o tratamento de dados pessoais (COTS; OLIVEIRA, 2019, p. 201).

Desta forma, haverá a possibilidade de ser implementado o que a LGPD denominou "programa de governança em privacidade", semelhante a já conhecida política de segurança

da informação, porém focado no cumprimento na nova lei, assim como demonstrando o comprometimento do agente de tratamento em cumprir e fazer cumprir a lei em relação aos seus contratados (COTS; OLIVEIRA, 2019, p. 203).

Portanto, de acordo com a doutrina, a disposição no art. 50 pactua com as atuais políticas empresariais de governança e *compliance*[2], que visam, de modo geral, a realizar uma adequada gestão de riscos, por meio de boas práticas, atendimento da legislação e regulamentos incidentes sobre o negócio e a criação de controles internos (COTS; OLIVEIRA, 2019, p. 203).

Logo, nota-se uma forte tendência da LGPD no âmbito do tratamento de dados pessoais, notadamente nas relações de consumo virtuais, no sentido de que eles sejam gestados pelas empresas de forma a se assegurar prioritariamente a integridade, segurança e transparência acerca das informações que são levadas ao consumidor, proporcionando, via de consequência, um ambiente adequado para a manutenção de seus dados e informações cadastrais.

5 Considerações finais

Esta pesquisa se dedicou essencialmente a investigar a aplicabilidade que a lei protecionista estabelece para a guarda e manutenção de dados do consumidor no âmbito das relações de consumo virtuais.

A referida lei traz o instituto do consentimento, que é uma das espécies de negócio jurídico, previsto no CC/2002. Para que o fornecedor/arquivista possa utilizar os dados pessoais de seu cliente, é obrigatório o seu consentimento legal. Assim, a Lei n. 13.709/2018 cuidou de disciplinar o referido instituto, tornando-o uma das bases legais para o tratamento de dados, haja vista, a necessidade que há em se obter a autorização para tratamento de dados pessoais de um indivíduo.

Dessa forma, o consentimento muito se aproxima com o princípio da privacidade, prevista na CF/88. A Lei Maior é enfática ao apontar a privacidade do indivíduo como um dos fatores indispensáveis para a manutenção da dignidade humana.

Portanto, uma vez que essa privacidade é violada, também estão sendo violados a dignidade da pessoa humana e os direitos humanos previstos na Constituição.

Logo, resta claro que o consentimento, como sendo um ato jurídico, deve seguir a base constitucional e, ainda, ser norteado pelo respeito à privacidade do indivíduo, com destaque à proteção de seus dados pessoais. Destarte, o que se extrai desta pesquisa é o nível da proporção que a lei protecionista pretendeu abarcar com a sua vigência.

Trata-se de uma lei multidisciplinar, pois não apenas trouxe para o ordenamento jurídico brasileiro institutos seguradores da proteção de dados pessoais (com, por exemplo, os princípios que a Lei Geral de Proteção de Dados elenca), como também previu uma política de segurança de informação com base no estabelecimento da relação de consumo, permitindo, assim, uma maior eficiência no tratamento de dados pessoais.

---

2 O termo *compliance* significa "estar em conformidade com", obedecer, satisfazer o que foi imposto, comprometer-se com a integridade. No âmbito corporativo, uma Organização "em *compliance*" é aquela que, por cumprir e observar rigorosamente a legislação à qual se submete e aplicar princípios éticos nas suas tomadas de decisões, preserva ilesa sua integridade e resiliência, assim como de seus colaboradores e da Alta Administração. In: EDITORA FORUM. *Entenda o que é Compliance e descubra os princípios benefícios para as empresas*. 2020. Disponível em: <https://www.editoraforum.com.br/noticias/entenda-o-que-e-compliance-e-descubra-os-principais-beneficios-para-as-empresas/>. Acesso em: 26 abr. 2021.

Revista Amor Mundi | Santo Ângelo | v. 2 | n. 6 | p. 7-27 | junho 2021.
DOI: https://doi.org/10.46550/amormundi.v2i6.111

Muito do que se esperava na legislação até então existente, foi concretizada na LGPD, a partir do momento em que se tornou possível prever os benefícios e riscos na gestão de dados pessoais de um determinado indivíduo, e as consequências de seu tratamento em desconformidade com a lei. Desta forma, surgiram os agentes de tratamento – controlador e operador – personagens indispensáveis para a concretização do procedimento de gestão de dados pessoais.

Logo, a Lei n. 13.709/2018 se trata essencialmente de uma ferramenta de combate às ilegalidades no tratamento de dados pessoais, visa a estabelecer uma zona de segurança para quem consente o uso de seus dados, principalmente ao consumidor que utiliza a internet para realizar compras e contratar serviços, porém, o que se nota, na atualidade, é a ausência de políticas públicas para que se concretize o a finalidade precípua da referida lei dentro do e-commerce, que é estabelecer uma zona de segurança para o consumidor no tocante à guarda e manutenção de seus dados pessoais.

Referências

BASTOS, Celso Ribeiro. *O princípio da Livre Concorrência na Constituição Federal.* Revista dos Tribunais – Cadernos de Direito Tributário e Finanças Públicas, n. 10, São Paulo, RT, 1995.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo: Saraiva, 1990. v. 7.

BENJAMIN, Antônio Herman de Vasconcellos e. *Código brasileiro de defesa do consumidor:* comentado pelos autores do anteprojeto. Direito material (arts. 1º a 80º e 105 a 108). Rio de Janeiro: Forense, 2011, v.1.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais – A função e os limites do consentimento*. 2ª edição. Rio de Janeiro: Forense, 2020.

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018.

BRASIL. *Constituição Federal de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 22 de jun. de 2021.

BRASIL. *Código de Defesa do Consumidor*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 22 de jun. 2021.

BRASIL. *Código Civil de 2002.* Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 09 de ago. 2021.

BRASIL. *Norma ISO/IEC 17799:200.* 2005. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=60452>. Acesso em: 26 de jun. 2021.

BRASIL. *Código de Processo Civil.* Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 09 de ago. 2021.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09 de ago. 2021.

BRASIL. *Decreto n. 8.771, de 11 de maio de 2016*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 09 de ago. 2021.

BRASIL. *Lei n. 13.853/2019 - Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 26 de jun. 2021.

BRASIL. *Medida Provisória n. 869, de 27 de dezembro de 2018*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 26 de jun. 2021.

CANOTILHO, J. J. Gomes. *Direito Constitucional*. Coimbra: Almedina, 1991.

COELHO, Fábio Ulhoa. *Curso de direito civil:* parte geral, volume 1. 5ª edição. São Paulo: Saraiva, 2012.

COTS; Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada.* 3ª Edição. São Paulo: Thomson Reuters Brasil, 2019.

DINIZ, Maria Helena. *Curso de direito civil brasileiro*. São Paulo: Saraiva, 2008, v. 3.

EFING, Antônio Carlos. *Banco de dados e cadastro de consumidores*. São Paulo: Revista dos Tribunais, 2002.

GONÇALVES, Carlos Roberto. *Direito civil esquematizado:* volume 1. 2ª edição. São Paulo: Saraiva, 2012.

G1. *Falha em aplicativo do Banco do Brasil expõe contas, dizem usuários*. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/12/falha-em-app-do-banco-do-brasil-expoe-contas-dizem-usuarios.html>. Acesso em: 09 de ago. 2021.

PINHEIRO, Patrícia Peck. *Proteção de dados do consumidor: comentários à Lei n. 13.709/2018*. 2ª edição. São Paulo: Saraiva Educação, 2020.

ROB, Peter. *Sistemas de bancos de dados:* projeto e implementação. Trad. All tasks. São Paulo: Cengage Learning, 2011.

SENADO. *Lei Geral de Proteção de Dados Pessoais entra em vigor.* Site do Senado Federal, 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 24 de jun. 2021.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo.* 15ª edição. São Paulo: Malheiros, 1998.