RESPONSABILIDADE CIVIL DOS AGENTES DE PROTEÇÃO DE DADOS NO BRASIL (LGPD)

João Rafael Costa Veiga[1]
Emmanuelli Gondim[2]

RESUMO

Este trabalho, em formato de artigo científico, considerando que a proteção de dados é fundamental para a efetivação dos direitos da personalidade, tem como objetivo principal analisar a natureza jurídica e limites da responsabilidade civil dos agentes de proteção de dados no Brasil, determinados a partir da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que estabelece os conceitos e delimita a atuação dos agentes de tratamento de dados para que seja possível enfrentar os problemas causados pela exploração das novas tecnologias. Foram aplicados os métodos de pesquisa de forma Comparativa, pois serão consideradas, ao longo do trabalho, opiniões e diferenças de opiniões doutrinárias, servindo de base para uma fundamentação e argumentação consistente; explicativa, diante da exposição de situações que contribuem para a resolução do problema de pesquisa e histórico, uma vez que será demonstrada a evolução histórica. Para atender ao objetivo do presente trabalho, procedeu-se exploração da legislação vigente, de modo a complementar o que está estabelecido na LGPD, além de fazer uso de doutrina que versa sobre a responsabilidade civil e a LGPD, para construir um melhor entendimento e interpretação do assunto. Constatou-se que, a LGPD cumpre, então, o seu papel de elo entre os diferentes diplomas para a da proteção de dados.

Palavras-chave: LGPD. Agentes de proteção de dados. Responsabilidade civil. Dados Pessoais.

CIVIL LIABILITY OF DATA PROTECTION AGENTS IN BRAZIL (LGPD)

ABSTRACT

This work, considering that data protection is fundamental for the realization of personality rights, has as main objective to analyze the legal nature and limits of civil liability of data protection agents in Brazil, determined from the General Law of

Protection of Data (Law nº 13.709/2018), which establishes the concepts and delimits the performance of data processing agents so that it is possible to face the problems caused by the exploitation of new technologies. The research methods were applied in a comparative way, as opinions and differences of doctrinal opinions will be considered throughout the work, serving as a basis for a consistent foundation and argumentation; explanatory, given the exposure of situations that contribute to the resolution of the research and historical problem, since the historical evolution will be demonstrated. In order to meet the objective of the present work, the current legislation was explored, in order to complement what is established in the LGPD, in addition to making use of the doctrine that deals with civil liability and the LGPD, to build a better understanding and interpretation of the subject. It was found that the LGPD fulfills its role as a link between the different diplomas for data protection.

Keywords: LGPD. Data protection agents. Civil responsibility. Personal data.

[1] Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: joao.veiga@rn.sebrae.com.br
[2] Professora Orientadora do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. E-mail: emmanuelli@unirn.edu.br

1. INTRODUÇÃO

O princípio da dignidade da pessoa humana se propaga pelas Constituições mundo afora, sobretudo após a Segunda Guerra Mundial, a partir da constatação de que era necessário assegurar que as atrocidades cometidas até então não se repetissem. Assim como a perspectiva do direito patrimonialista e individualista perdia força com a constatação de que a interpretação do Direito deve levar em consideração princípios universais, como a dignidade da pessoa humana, e que a dignidade se materializava com a promoção do bem comum e com a tutela de valores essenciais dos indivíduos.

No Brasil não foi diferente. A redemocratização possibilitou a evolução da legislação e a promulgação da Constituição Federal de 1988, que fundou uma nova forma de interpretar o ordenamento pátrio. Passou-se a reinterpretar a legislação a luz da Carta Magna e com foco na promoção dos fundamentos do Estado Democrático de Direito.

Mediante o desenvolvimento tecnológico, que proporcionou uma nova maneira de organização, as novas tecnologias de transmissão, coleta, armazenamento e processamento na internet permitiram que as informações fossem cada vez mais usadas para o desenvolvimento da eficiência econômica, ao passo que foi possível estabelecer uma relação mais eficaz na relação com os consumidores. Ou seja, passou a ser possível que a produção e a divulgação dos produtos fossem mais efetivas. Porém, o lado negativo é que o indivíduo titular dos dados e consumidor dos bens foi se tornando cada mais vulnerável, uma vez que as informações passaram a circular entre os agentes econômicos e a sua intimidade e capacidade de escolha foi sendo suplantada pelos interesses das grandes corporações.

Em síntese, esse foi o contexto que ensejou a discussão sobre a necessidade de regulamentação da exploração econômica dos dados pessoais a partir das novas tecnologias para o desenvolvimento econômico. Foi estabelecido que é preciso estipular limites para tal atividade, de modo que preserve a intimidade e a autodeterminação do indivíduo, porém que não inviabilize a exploração econômica, assim como o desenvolvimento tecnológico, que é proveitoso e importante para o desenvolvimento da sociedade.

A necessidade de proteção dos dados pessoais dos titulares, que foi possível com o uso de novas tecnologias, é uma questão que já vem sendo muito discutida no âmbito acadêmico. O estabelecimento do direito à privacidade como um direito fundamental, no âmbito da constitucionalização do Direito Civil, e a sua aplicação a proteção desses dados é uma questão central na doutrina majoritária. Desse modo, verificou-se que a legislação vigente não delimitava de maneira clara quais os princípios e regras que deveriam ser aplicados, assim como de que maneira a proteção se materializava.

É nesse contexto que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) foi sancionada e já começa a mobilizar a sociedade e o mercado. vários pesquisadores e profissionais passam a se especializar na proteção de dados para desenvolver formas de adequar as atividades, hoje desenvolvidas por empresas e órgãos públicos que lidam diretamente com coleta e tratamento de dados pessoais, à nova lei.

Diante da ineficiência da legislação até então vigente para a proteção dos direitos da personalidade no uso das novas tecnologias, esse novo marco legal surge objetivando suprir esta necessidade. A LGPD então veio para regulamentar as relações estabelecidas entre os titulares e os controladores e operadores dos dados, de modo a instituir um órgão administrativo para regulamentar e fiscalizar a questão além de uma positivação clara das atribuições, regras e punições cabíveis para o descumprimento do bom uso e sigilo das informações coletadas nas atividades com fins econômicos.

Sendo assim, é de fundamental importância o mecanismo de reparação civil insculpido na lei, que estabelece os encargos que permitem identificar os responsáveis pela proteção das informações dos titulares. Porém, a interpretação dos dispositivos da LGPD que tratam da responsabilidade civil não pode deixar de considerar os mandamentos gerais estabelecidos em outros diplomas. Na verdade, é possível vislumbrar que esse novo elemento fixado na LGPD contribui para a atualização do instituto em tela aos novos desafios que ora nos tocam.

Tendo em vista que a LGPD é um marco importante na proteção de dados e estabeleceu princípios, conceitos, procedimentos, normas e punições acerca do tema, é fundamental ressaltar que a responsabilidade civil é questão central.

Os recentes episódios de vazamento de informações de usuários por agentes de tratamento de dados pessoais deixam claro que um dos aspectos mais importantes do novo marco legal será, não só o regramento do que pode ser coletado e tratado, mas, principalmente, a responsabilização daqueles que não conseguirem garantir a integridade do direito fundamental em tela. A referida lei estabelece os conceitos e delimita a atuação dos agentes de tratamento de dados para que seja possível enfrentar os problemas causados pela exploração das novas tecnologias.

Sendo assim, é de suma importância que se faça uma interpretação acerca da natureza jurídica e limites da responsabilidade civil na referida lei, a partir da confrontação entre a lei específica sobre proteção de dados e as normas gerais sobre responsabilidade civil presentes no Código Civil, Código de Defesa do Consumidor e a Constituição Federal. Esse cotejamento se faz necessário para estabelecer os limites da responsabilidade na nova área que se abre com o regramento da proteção de dados, em que pese a escassez doutrinária e jurisprudência ainda quase que inexistente sobre o tema. É preciso então atualizar a doutrina sobre responsabilidade civil tomando como ponto de partida a LGPD, para subsidiar as futuras discussões sobre os casos concretos, quando da entrada em vigor de todos os seus dispositivos.

Considerando que a exploração das atividades de coleta, compartilhamento, armazenamento e processamento de dados dentro dos limites estabelecidos pela lei é relevante para o desenvolvimento econômico e, assim, de interesse da sociedade. Além disso, considerando que o descumprimento de deveres ou a afronta a direitos de outrem podem trazer danos, e este enseja a reparação, é pacífico que a responsabilidade civil é um dos principais aspectos da lei objeto deste estudo.

Por isso, o presente trabalho tem como objetivo geral delimitar qual a natureza jurídica da responsabilidade dos agentes de proteção de dados e, a partir daí, elucidar como a reparação se dará frente aos futuros casos de violação dos deveres legais neste domínio.

Os questionamentos suscitados no objetivo geral serão elucidados a partir das seguintes etapas: identificar os conceitos fundamentais, princípios,

agentes e suas atribuições contidos na Lei Geral de Proteção de Dados; verificar a legislação nacional acerca da responsabilidade civil e proteção de dados; e analisar os limites e especificidades para reparação dos danos pelos agentes de proteção de dados.

Para isso, parte-se da Constituição Federal de 1988, que inaugurou um novo momento no âmbito nacional, implicando num texto moderno em que o princípio democrático é levado a cabo e que possui relação direta com a reorganização do ordenamento de modo a estabelecer como um dos fundamentos, a dignidade da pessoa humana. Vale ressaltar que a proteção de dados é um direito fundamental, constitucional, prevista no art. 5º LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

Por conseguinte, a legislação infraconstitucional foi reinterpretada sob um novo fundamento de validade conforme os novos ditames constitucionais. Sendo assim, o Código de Defesa do Consumidor (Lei nº8.078/90) e o Código Civil de 2002(Lei Nº 10.406/2002) formam a expressão de tal movimento, à medida que se distanciaram do caráter patrimonial e privatístico e instituíram a concepção de que não é possível pensar os institutos do direito privado sem submetê-los as novas bases constitucionais.

Já recentemente, sob o contexto da sociedade da informação, verifica-se uma vulnerabilidade dos indivíduos em relação às grandes organizações que desenvolvem atividades com tratamento de dados pessoais, pois não havia nalegislação esparsa regramento específico.

Outrossim, a LGPD também estabelece os agentes de proteção de dados com seus deveres e direitos para a exploração das atividades com fins econômicos. Com efeito, esses agentes têm o dever de zelar pela segurança dos dados a partir das orientações da Autoridade Nacional de Proteção de Dados (ANPD), evitando assim que informações pessoais sejam usadas de maneira inadequada e causem dano aos titulares. Por isso, é necessário que se busque elucidar a natureza jurídica dessa responsabilidade através do cotejamento com a doutrina clássica do direito civil.

Em suma, para atender ao objetivo do presente trabalho, pretende-se

explorar a legislação vigente, de modo a entender como a LGPD definiu o tema. Além disso, para subsidiar a discussão, pretende-se fazer uso de doutrina que verse sobre a responsabilidade civil e a LGPD, para que se construa uma melhor interpretação do assunto. Por isso, utiliza-se o método bibliográfico de pesquisa.

2. A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados se situa como meio de efetivação dos direitos da personalidade (COELHO, 2019). Através de princípios e regras, estabelece o regulamento nacional sobre o tratamento de dados, a fim de evitar que ocorram distorções no tratamento de informações consideradas dados pessoais.

A LGPD entrou em vigor em setembro de 2020 para todos os direitos, deveres e obrigações previstos. Portuno destacar, que a LGPD entra em vigor junto uma intensa migração digital que foi acelerada pelo cenário da pandemia COVID-19, isso nos força a enfrentar com mais qualidade e celeridade os novos desafios trazidos com sua implementação. Desafios esses que não devem ser subestimados, isso porque a proteção de dados se tornou um diferencial determinante no mercado.

Depois do Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) é, seguramente, o maior avanço legislativo brasileiro em termos de proteção da informação que circula na web. De certa forma, sua entrada em vigor não deixa de ser uma resposta à publicação do Regulamento Geral sobre a Proteção de Dados (GDPR) europeu em 2018. Seja como for, as empresas que usam o ambiente digital para fazer negócios devem se ajustar ao que diz a nova lei. Isso porque ela afeta diretamente a forma como os dados de usuários são coletados e tratados.

A Lei Geral de Proteção de Dados foi sancionada, no Brasil, com a publicação da Lei Nº 13.709 em 14 de agosto de 2018. Em seu preâmbulo, fica exposto que o objetivo é garantir a segurança de dados pessoais. Por isso, a LGPD promove importantes alterações no Marco Civil da Internet de 2014. Aliás, deve-se destacar que ambas as leis se fundamentam em princípios muito parecidos. Nesse sentido, diz o artigo 2º do Marco Civil, que trata das disposições

preliminares:

> A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I – o reconhecimento da escala mundial da rede; II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; III – a pluralidade e a diversidade; IV – a abertura e a colaboração; V – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VI – a finalidade social da rede.

No mesmo sentido é expresso nas disposições preliminares da LGPD.

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

A LGPD é resultado de um movimento espontâneo da sociedade e autoridades brasileiras. Desde o início da década, empresas e usuários vêm buscando respostas para as questões de segurança virtual, que ganham relevância em função da escalada do cibercrime. Em 2018, segundo um estudo da McAfee publicado na revista Veja, o Brasil registrou perdas progressivas com crimes virtuais, chegando a R$ 10 bilhões por ano. Somos uma das “potências” mundiais nesse quesito, ao lado de Índia, Vietnã, Rússia e Coreia do Norte. Assim sendo, a LGPD surge do esforço conjunto de diversas instâncias no sentido de combater as fraudes e crimes online que, com o tempo, crescem vertiginosamente no Brasil. É por isso que a lei é considerada um avanço, até mesmo por se aplicar em todo o território nacional.

No dia 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115 em sessão solene no Congresso Nacional, incluindo a proteção de dados pessoais no rol de direitos fundamentais. Além de representar um marco histórico, a emenda simboliza um grande avanço quanto ao amadurecimento do país em relação à garantia da proteção de dados pessoais que passa a ser assegurado pelo art. 5º., LXXIX da Constituição Federal. Consequentemente, sendo alçado como direito fundamental autônomo, o tema proteção de dados passa a ser estudado a nível constitucional.

Ness contexto, o primeiro artigo da LGPD atua como uma introdução da Lei

Geral de Proteção de Dados, pois define os objetivos das normas. O intuito é a preservação do direito constitucional à liberdade e à privacidade por meio da proteção de informações sensíveis. A lei é válida em todo o território brasileiro e se sobrepõe às leis municipais e estaduais. Inclusive, tem validade tanto em meios digitais quanto analógicos, englobando desde páginas na internet até fichas em papel.

A LGPD entende que os cidadãos devem ter controle sobre suas informações pessoais, por isso, precisam conhecer como e com quais fins seus dados são utilizados. O intuito é preservar a imagem dos brasileiros, evitando que as informações sejam usadas com fins prejudiciais. No entanto, destaca-se que não há a intenção de prejudicar empresas que utilizam o tratamento de dados. Portanto, o tratamento é liberado, mas deve ser feito com total transparência, pedindo consentimento aos cidadãos e informando como as informações serão usadas.

Trata-se de uma lei sucinta, porém bastante coerente, que apresenta desde o início quais são as suas diretivas principais e que são de suma importância para a compreensão e desenvolvimento de atividades no âmbito do tratamento de dados.

Por isso, o presente capítulo discorre sobre a lei geral de proteção de dados, seus encaminhamentos, fundamentos e princípios. Apresentando, desta maneira, o modo como a lei se constitui.

2.1 ENCADEAMENTO DA PRODUÇÃO LEGISLATIVA, TRAMITAÇÃO E RELAÇÃO COM GDPR. (REGULAMENTO GERAL DA PROTEÇÃO DE DADOS)

Com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e assim possibilitar o livre desenvolvimento da personalidade da pessoa natural, foi criada a Lei Geral de Proteção de Dados, Lei nº13.709/2018. Ela traz a ressalva que todo tratamento de dados pessoais, exceto casos especiais enumerados na lei, serão objeto de suas disposições. Então, apesar de ter sido fruto de um movimento que tomou corpo com o desenvolvimento tecnológico, ela não se restringe ao ambiente virtual.

Porém, é inegável que o tratamento de dados pessoais alcançou um

patamar nunca visto, à medida que a tecnologia de processamento e transmissão se desenvolveram e alcançaram uma popularidade maior. A coleta e processamento de dados *off-line* tem limitações estruturais relevantes que a tornam menos rentável e atentatória aos direitos fundamentais agora tutelados. Por isso, as referências diretas a proteção de dados serão feitas as realizadas no âmbito da tecnologia, haja vista quesão mais presentes no nosso cotidiano.

Tendo em vista que a tecnologia aproxima as distâncias físicas e ultrapassa fronteiras, a sociedade sofreu transformações que a levaram a uma nova forma de organização, em que a informação tem papel central no desenvolvimento econômico (CASTELLS, 2000). As novas tecnologias de transmissão, coleta, armazenamento e processamento na internet permitiram que as informações fossem cada vez mais usadas para o desenvolvimento da eficiência econômica, ao passo que foi possível estabelecer uma relação mais eficaz com os consumidores. Ou seja, passou a ser possível que a produção e a divulgação dos produtos fossem mais efetivas. Porém, o lado negativo é que o indivíduo, titular dos dados e consumidor dos bens, foi se tornando cada mais vulnerável, uma vez que as informações passaram a circular entre os agentes econômicos e a sua intimidade e capacidade de escolha foi sendo suplantada pelos interesses das grandes corporações.

É por esse motivo que a proteção dos dados pessoais não poderia continuar se aplicando apenas a temas específicos e preso por limites geográficos que não têm mais a mesma influência do passado. Considerando-se que as atividades relacionadas a coleta e tratamento de dados envolve vários atores, de múltiplas origens, exercendo diferentes atividades, não há outro caminho, a não ser o da tentativa de universalização coordenada, respeitando a competência específica de cada cenário, da regulação, até para preservar a livre iniciativa e possibilitar o pleno desenvolvimento de novos modelos de negócio.

No Brasil, há um cenário de discussões sobre a privacidade e os direitos da personalidade bem antes da aprovação da Lei Geral de Proteção de Dados, Lei nº 13.709/2018. Já havia uma série de leis setoriais que tangenciavam o assunto, mas que formavam uma “colcha de retalhos”, como destaca Bruno Ricardo Bioni (2019). Todos esses diplomas servem de base para proteção de

dados, porém não previam, e nem havia como, a dimensão que tomaria o mercado de dados, como conhecemos hoje.

Só com o Marco Civil da Internet, instituído como Lei nº12.965/2014, é que se tem propriamente uma lei que trate da proteção de dados pessoais em todas as esferas, mas principalmente do que concerne a novas tecnologias, pois estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Trata-se da lei que inaugurou a positivação de normas, baseada no debate sobre a importância que tem a internet na vida cotidiana.

Por fim, depois de toda produção legislativa, o Brasil finalmente aprova o projeto de lei nº 4060/2012 e cria a lei que recebe o número 13.709/2018, a Lei Geral de Proteção de Dados, objeto central deste estudo. Como já vimos, ela foi fruto de vários anos de debate e o projeto, como era de se esperar, sofreu várias modificações em sua tramitação.

> A Lei nº 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolvao tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao usode um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionadas às pessoas (PINHEIRO, p. 15).

Dessa forma, vale ressaltar que, com essa lei o Brasil estabeleceu seu diploma legal central acerca da proteção de dados, e caminhou para o alinhamento com os países mais avançados no assunto, notoriamente a União Europeia.

É justamente na União Europeia que está a vanguarda da proteção de dados. Foi lá que se desenvolveu a GDPR, General Data Protection Regulation, (EU) 2016/679, que deu o pontapé inicial para a universalização da proteção da privacidade e o livre desenvolvimento da personalidade das pessoas naturais. É certo que já havia, tanto no âmbito da União Europeia quanto no Brasil, diplomas que tratavam do assunto de forma setorial, porém essa nova codificação visava alargar a área de atuação da proteção de dados. Ou seja, quando se diz que a legislação foi inovadora não significa que ela pode ser descolada de tudo que veio antes. Na verdade, a inovação legislativa está em, ao se utilizar daquilo que já

tinha sido construído e percebendo as novas demandas, oferecer uma resposta à altura.

Da mesma forma, a LGPD não nasceu alheia às discussões e de forma totalmente espontânea, existe um aspecto econômico importante. A GDPR é gestada com o pressuposto de que o mercado de dados tem uma facilidade, maior do que outras atividades econômicas, de superar fronteiras. Por isso, corria-se o risco de, com o estabelecimento das regras do setor, a atividade migrasse e mesmo assim continuasse a atingir a população local. O encadeamento de atividades concernentes à exploração desse novo ativo econômico, que é exploração de dados, situa empresas e atores de vários países como parceiros.

A cooperação internacional por meio da LGPD e GDPR é forma de relacionamentos pessoais, comercias entre países, resguardando os direitos indisponíveis das pessoas sejam físicas ou jurídicas de Direito privado, bem como de Direito Público, que participam dessas relações que ultrapassam as fronteiras do país. Os mecanismos de legislações compatíveis na proteção de dados, partem de um sistema de cooperação internacional de proteção.

Portanto, foi fundamental para que os outros países, com os quais a União Europeia mantinha relações comerciais, fossem incentivados a criarem normas para disciplinar o assunto, que se estabelecesse uma reciprocidade. Para isso, a GDPR incluiu no seu texto um critério para a manutenção dos fluxos de dados. Para que haja a transferência de dados pessoais em tratamento ou destinados a transformação, da UE para um país terceiro, devem ser observados os requisitos estabelecidos na GDPR e as garantias vigentes no país terceiro.

Ou seja, era necessário que, os países interessados em participar do ciclo dos dados com entidades europeias, demonstrassem que têm legislação própria, com condições mínimas de segurança e garantias de proteção desses dados.

Desse modo, podemos dizer que a LGPD teve a sua tramitação no Congresso Nacional agilizada pela necessidade do mercado nacional de apresentar compatibilidade com a legislação europeia para continuar suas atividades.

2.2 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Os princípios constituem indispensável elemento da interpretação dos textos legais. Porém, despertam um profícuo debate acerca de sua definição e relação com as regras. Todavia, não nos cabe neste breve estudo adentrar nesse debate.

Importa apenas explanar que quando uma norma é denominada de princípio significa dizer que esta tem uma forma específica de interpretação. Não se trata da generalidade ou do grau, mas de sua aplicação no caso concreto (ALEXY, 2006).

Nesse sentido, define Robert Alexy, *in verbis*:

> O ponto decisivo na distinção entre regras e princípios é que princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. O âmbito das possibilidades jurídicas é determinado pelos princípios e regras colidentes (ALEXY, 2006, p. 90).

Dessa forma, os princípios são sempre aplicados, em maior ou em menor medida, ao contrário das regras, que são aplicadas ou não ao caso concreto. A aplicação de uma regra implica o afastamento de outra que, em tese, estaria em colisão.

Logo depois o autor define as regras como:

> […] normas que são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve se fazer exatamente aquilo que ela exige; nem mais, nem menos. Regras contêm, portanto, determinações no âmbito daquilo que é fática e juridicamente possível. Isso significa que a distinção entre regras e princípios é uma distinção qualitativa, e não distinção de grau. Toda norma é ou uma regra ou um princípio (ALEXY, 2006, p. 91)

Isto posto, os princípios elencados na LGPD têm importância clara na compreensão e aplicação da norma. O legislador então escolheu colocá-los de maneira explícita para que não restasse dúvida sobre a metodologia necessária na sua aplicação.

Os princípios então são enumerados nos incisos do art. 6º da LGPD, mas já no caput deste artigo se vê que, além dos princípios, deve-se observar a boa-

fé. A boa-fé, nesse caso, objetiva, ou seja, relações jurídicas em que interessam as repercussões de certas condutas, principalmente em relações jurídicas de caráter obrigacional (LÔBO, 2017).

Portanto, se faz necessário analisar cada princípio individualmente, e é o que faremos a seguir.

2.2.1 FINALIDADE

O princípio da finalidade, determina a força do que é pactuado entre as partes. Nesse caso, pretende-se dar ao titular dos dados a prerrogativa de poder analisar se aquele dado que será coletado tem razão de ser.

Tendo em vista que só se pode tratar dados a partir da autorização do titular, é preciso garantir que não haverá desvirtuamento da finalidade da coleta e tratamento pactuados no contrato. A pessoa a quem pertencem os dados, deve ser instruída e esclarecida devidamente, quanto a utilização, ou finalidade de utilização dos dados

De acordo com o artigo 4º da GDPR, o termo “violação de dados” (*personal data breach*) diz respeito a uma infração de segurança que tenha por efeito a destruição, alteração, divulgação, perda ou acesso não autorizado a dados pessoais sujeitos a qualquer tipo de tratamento, de modo acidental ou ilícito.

Um exemplo famoso de violação de dados que ocorreu em 2018 é o do Facebook. A condenação do Facebook foi de 5 bilhões de dólares, além de um acordo de restrições de atuação e análise trimestral de seus serviços e produtos, após ter usado de forma indevida as informações de 87 milhões de usuários da rede social no escândalo Cambridge Analítica. Segundo a sentença, a rede social de Mark Zuckerberg falhou em proteger os dados de seus usuários de empresas terceirizadas e mentiu para os seus clientes sobre a informação de que os sistemas de reconhecimento facial estavam desativados por padrão.

Sendo assim, o controlador e operador estão submetidos a finalidade pactuada previamente, para evitar que sejam utilizados artifícios para que se possa dar destino não autorizado aos dados. Cria-se então uma obrigação de ficar restrito a tal pacto, de modo que os controladores terão de ter bem delimitado, desde a concepção do projeto, para que finalidades serão utilizados

os dados.

Por outro lado, esse princípio também qualifica tais propósitos, conforme atribui a este, os requisitos legítimos, específicos, explícitos e informados ao titular. Na verdade, se verifica que é a materialização da boa-fé, juntamente com os adjetivos que devem orientar a manifestação de vontade plenamente válida.

Ou seja, impede que as cláusulas sejam obscuras ou dúbias quando se referem a finalidade, considerando que o titular deverá avaliá-las para anuir com a operação.

2.2.2 ADEQUAÇÃO

O princípio da adequação refere-se à compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

O vocábulo adequação, como se sabe, apresenta diversas acepções. Para o ambiente da LGPD, refere-se ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento e a finalidade objetivada, tal como previamente informada ao titular.

Estabelece, portanto, relação lógica entre o tratamento e a finalidade objetivada; o tratamento e a comunicação transmitida ao titular; a finalidade almejada e a comunicação transmitida ao titular; e, entre os três elementos, integradamente considerados, ou seja, entre o tratamento, a finalidade objetivada e a comunicação transmitida ao titular.

O tratamento, no caso, ao se realizar, somente assim o será, porque tudo leva a crer, naquele determinado recorte de tempo e espaço, que estabelecerá um liame valioso e relevante para o atingimento do objetivo, do qual o titular tem ciência induvidosa.

O dispositivo que define o princípio da adequação impede que a finalidade acertada esteja adequada a forma que se opera o tratamento de dados. Está diretamente ligado ao princípio da finalidade, pois estabelece que esta desse ser observada para evitar abuso no tratamento dos dados pessoais.

Trata-se de mais um caso em que o titular poderá questionar caso se

descubra que os dados estão sendo coletados e tratados para além daquilo que foi pactuado como sua finalidade.

Acontece da seguinte forma: quando o controlador alarga a finalidade a que se destina a coleta dos dados e realiza um novo tratamento ou cede os dados para empresa com fim não previsto.

2.2.3 NECESSIDADE

Previsto no inciso III do referido dispositivo, o princípio da necessidade consubstanciase na limitação do tratamento de dados pessoais ao mínimo necessário para realização da finalidade objetivada, com abrangência dos dados pertinentes e proporcionais.

Isso quer dizer que os agentes devem utilizar apenas os dados estritamente necessários para alcançar a uma finalidade previamente delimitada e aprovada pelo titular dos dados correspondentes e nos limites do que se mostrarem imprescindíveis para que essa finalidade seja alcançada. Nem poderia ser diferente, pois seria impróprio tratar dados impertinentes ou excessivos.

O princípio da necessidade também está relacionado com o princípio da finalidade, pois estabelece que devem ser coletados e tratados o mínimo de dados possíveis para uma determinada causa. Ou seja, tendo em vista que se deve coletar dados, que sejam coletados os estritamente necessários para desempenhar a função a que se propõe.

Um possível exemplo de utilização que viola o princípio da necessidade seria um aplicativo de mapa, que depende apenas do sinal de localização do aparelho, solicitar acesso ao microfone, com a autorização para gravação inclusive. A não ser que haja a função de ativação por comando de voz, não há necessidade de o aplicativo do caso hipotético ter acesso ao microfone.

2.2.4 LIVRE ACESSO

Previsto no inciso IV, este princípio possibilita a clareza para o titular dos dados sobre a forma e duração do tratamento de suas informações. Deve haver um canal para que o titular tenha acesso aos dados que estão sob a tutela do agente de tratamento. Note que esse princípio gera uma obrigação, isto porque

o agente fica incumbido na tarefa de abrir o seu arquivo para que o titular possa avaliá-lo, mas somente em relação aos dados que lhe dizem respeito. Essa consulta deve ser gratuita.

Trata-se de princípio que, em especial, possibilita a transparência para o titular dos dados sobre as suas informações, e é chamado de livre acesso. Nada mais justo que este tenha acesso livre às informações sobre a forma e duração do tratamento, assim como a garantia de que estarão planos.

Vale ressaltar que o princípio do livre acesso está diretamente ligado a efetividade dos direitos personalíssiomos, e aos princípios constitucionais da liberdade, do acesso à informação e da privacidade.

O princípio da liberdade é encontrado no inciso do II do art. 5º da Constituição da República Federativa do Brasil de 1988, onde é estabelecido que “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude da lei”; em outras palavras quer dizer que ninguém está autorizado a obrigar ninguém a não ser determinado por lei.

Já o princípio do acesso a informação é uma das garantias previstas no artigo 5º da Constituição Federal. Por meio do inciso XXXIII, é assegurado que Todos têm direito a receber dos órgãos públicos informações particulares, ou do interesse de um grupo. Essas informações serão dadas para nós no prazo estabelecido pela lei, sob pena de responsabilização. A não ser que o fornecimento dessas informações possa de alguma forma colocar em risco a segurança da sociedade e do Estado.

O princípio da privacidade presente no art. 5º, X, da Constituição da República, prevê que à pessoa que se sentir lesada em relação a intimidade, vida privada, honra e imagem é garantido o direito de ingressar com ação judicial para pleitear a devida indenização.

Portanto deve haver um canal para que o titular tenha acesso as suas informações que estão sob a tutela do controlador. O princípio do livre acesso gera uma obrigação, visto que o titular fica incumbido na tarefa de abrir o seu arquivo, para que o titular possa avaliar se está acontecendo de forma correta.

A integralidade diz respeito a perfeição dos dados. Não é permitido que

sejam manipulados nem excluídos de forma arbitrária pelo controlador.

2.2.5 QUALIDADE DOS DADOS

O consentimento do titular dos dados é dado para que os dados sejam coletados da melhor forma possível. Se o titular libera acesso aos seus dados, o mínimo que pode esperar é que não contenham imprecisões, por isso, com este princípio pretende-se estabelecer a qualidade dos dados.

Para isso, é preciso que o dado seja atualizado, claro e exato. É preciso que ele reflita da melhor maneira possível a realidade, como alerta Rony Vainzof (In: MALDONADO e BLUM, 2019):

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta (MALDONADO e BLUM, 2019, p. 149).

O que o autor quer dizer nesse trecho é que, na verdade, a imprecisão dos dados pode ser prejudicial ao titular e, por isso, o controlador tem a responsabilidadede tomar medidas que mantenham a integridade desses dados.

Para que a integridade dos dados seja mantida é necessario seguir a chamada Política de Privacidade. A Política de Privacidade se refere a informações específicas de coleta, armazenamento e proteção de dados pessoas de usuários de um site ou aplicativo. Termos e Condições Gerais de Uso servem para indicar as regras que devem ser respeitadas ao utilizar a plataforma.

2.2.6 TRANSPARÊNCIAS

O princípio da transparência é o mais caro o entre as disposições do tratamento de dados. É o princípio que, ausente, inviabiliza toda a efetividade da lei. Vimos que, na verdade, a particularidade dos princípios está em, justamente, poder ser satisfeito em grau diferente. Porém, é notório que uma norma que trate de proteção de dados é bastante dependente da transparência em todo o processo.

Acontece que, este princípio deve ser observado de maneira especial desde antes do fornecimento do consentimento, por parte do titular. Tem

vinculação direta com o fato de o titular ter de estar inteiramente informado sobre os termos da coleta, finalidade, tratamento, requisitos e chega até o fim do processamento e descarte dos dados, salvo os segredos industrial e comercial.

Tudo isso só tem sentido se o titular tiver a possibilidade de conhecer, entender e decidir se aceita ou não os termos. Qualquer alteração ou descumprimento posterior, por parte dos agentes de tratamento de dados estarão infringindo a lei e serão passíveis das consequências legais.

> O titular dos dados carece de ampla informação sobre o tratamento dos seus dados para que consiga enxergar, cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade. Assim, terá condições para refletir sobre o tratamento e tomar decisões de acordo com os seus direitos. A transparência deve ser diretamente proporcional ao poder do tratamento dos dados pessoais (qualitativo e quantitativo) e à capacidade de assimilação dos titulares dos novos e dinâmicos produtos e serviços apresentados para o seu uso (MALDONADO e BLUM, 2019, p. 150).

É possível inclusive, verificar isso em casos que precedem a entrada em vigorda LGPD. A primeira medida das autoridades é questionar informações que teriam sido negadas aos usuários, que se tivessem prévio acesso, talvez não anuíssem. E ainda, diante do descumprimento, só é possível responsabilizar os culpados quando há informações sobre o processo.

Por isso, pode-se dizer que a principal força da LGPD e de outros diplomas vêm do sistema de *accountability* formado pelas regras e princípios. No que diz respeito às regras, podemos destacar os arts. 9º, 18 e 19 que determinam, em suma, que o titular tem o direito de ter o acesso às informações necessárias de forma facilitada. O que se pretende é, na verdade, que este seja o primeiro fiscal sobre as práticas dos agentes de tratamento de dados.

2.2.7 SEGURANÇA

O princípio da segurança – art. 6, VII, – compreende as 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. A ideia central desse princípio, que atua junto ao princípio da prevenção, é de preservar o ambiente seguro, utilizando e aprimorando técnicas de segurança para mitigar e prevenir eventuais incidentes.

Para Pestana, em caso de incidentes, segundo esse princípio, é irrelevante se a perda, acesso, alteração ou difusão resulte de uma conduta voluntária, ou seja, resultado de negligência, imprudência ou imperícia: a proteção dos dados é uma obrigação e o tratador deve prever todos os cenários de possíveis riscos e se precaver contra todos eles. Já para Oliveira (2019), a culpa não será presumida, mas oriunda de verificação técnica de determinada violação (OLIVEIRA, 2019, p. 22)

Pode parecer redundante, mas para a proteção de dados é imprescindível a observância da segurança. Isso significa aplicar todos os meios possíveis, à época do tratamento, para manter a segurança dos dados.

É responsabilidade dos agentes de tratamento de dados oferecer ao titular um aparato técnico capaz de evitar acessos não autorizados e vazamentos de dados. Isso implica na responsabilidade de possíveis danos causados por incidentes, à medida que, em regra, a culpa não será presumida, mas oriunda de verificação técnica daquela violação.

Dessa forma, os riscos do empreendimento devem ser mitigados pela aplicação de técnica capaz de obstar as tentativas e falhas no processo de tratamento de dados.

2.2.8 PREVENÇÃO

A prevenção vem dos pilares da Segurança da Informação, onde é necessário se precaver de eventuais eventualidades que possam ocorrer, adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Para garantir que a informação esteja protegida e ter uma Segurança da Informação efetiva, além de investir em tecnologia, é essencial também trabalhar com alinhamento de processos e conscientização de pessoas de toda a organização. Assim, com o desenvolvimento de Políticas de Segurança da Informação, alinhadas a processos organizacionais, utilização adequada de tecnologias e conscientização das pessoas em como lidar com as informações e recursos corporativos

O princípio da prevenção estabelece que devem ser tomadas medidas desde a concepção do projeto. A prevenção deve ser a tônica da segurança, considerando que, com o potencial da rapidez da tecnologia, uma falha pode significar danos inimagináveis, pois a capacidade de transmissão e armazenamento potencializam seus efeitos danosos.

Nesse ponto específico, é necessário frisar a importância do encarregado, definido no art. 5º, inciso VIII, como a pessoa indicada pelo controlador para atuar na comunicação entre o controlador, titulares dos dados e a Agência Nacional de Proteção de Dados, e para receber as instruções desta para aplicar ao tratamento, orientando os funcionários quanto às práticas mais acertadas.

2.2.9 NÃO DISCRIMINAÇÃO

O presente princípio por seu nome já diz sua finalidade. O tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos. Não se pode ter exclusão de titulares de dados pessoais no momento de seu tratamento de dados por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

Não é dizer que nunca poderá ter uma setorização de tratamento de dados, porém somente poderá ocorrer tal restrição em condições específicas e previstas em lei, como por exemplo um tratamento de dados de alunos optantes por cotas, perante a Lei de Cotas 12.711/2012, a condição de tratamento de dados pessoais será a partir de seu histórico educacional, sendo ele oriundos integralmente do ensino médio público, em cursos regulares ou da educação de jovens e adultos.

O processamento de dados possibilita a classificação de informações de uma maneira muito mais simples e corriqueira. Não há dúvida de que isso é extremamente útil nos tempos atuais e de que é justamente o processamento de dados que possibilita, através da montagem de padrões, um aumento na eficiência eprodutividade das empresas.

Acontece que, há sempre a possibilidade de esse procedimento de predição declinar para uma situação discriminatória, principalmente quando tocam dados sensíveis, como os elencados no Art. 5º, II da LGPD. Mas uma

associação simples de dados não sensíveis e, aparentemente, inofensiva, pode enveredar pelo campo da discriminação, isso já foi motivo de punição no Brasil, quando constatado que uma empresa praticou *geo pricing* e *geo blocking.*

Por isso, constitui um dos princípios da lei a não discriminação. Para que isso seja efetivamente cumprido, é necessário que haja o cumprimento de um princípio em especial, que é, como já falamos, o da transparência. Guardados os segredos empresariais, é preciso que a controladora apresente suas justificativas, que, no caso de suspeita, serão avaliadas para determinar se há ou não violação ao princípio da não discriminação

2.2.10 RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Finalmente, no último princípio, encontramos um resumo de tudo aquilo que expressa todos os outros. Enquanto o princípio da transparência é pedra fundamental para efetivação dos demais, o princípio da responsabilização e prestação de contas nos remete às consequências do descumprimento da lei. Ou seja, o tratamento de dados é lícito e regular quando atende aos ditames legais, em caso de descumprimento e dano ao titular, haverá responsabilização.

> Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos (MALDONADO e BLUM, 2019, p. 166-167).

Como disse o autor, este princípio foi assim colocado por ter importância central na disciplina do tratamento de dados, uma vez que, como observa Nelson Rosenvald (2017), a responsabilidade civil vai além da função apenas restaurativa, pois se presta também a uma função preventiva, cumprindo um papel civilizatório.

Por isso, têm o controlador, e aqueles que participarem da empreitada, os operadores, o ônus de responderem por seus atos, na medida de suas ações ou omissões. Para que isso não aconteça, é necessário, ao menos,que sejam cumpridos todos os requisitos legais e que se comprove a efetividade das medidas adotadas.

Pode-se dizer que o princípio da responsabilização e da prestação de contas dispõe que o agente tratador dos dados pessoais (controlador ou operador), deverá demonstrar todas as medidas eficazes e capazes de comprovar o cumprimento da LGPD e, ainda, a eficácia das medidas aplicadas.

Em outras palavras, é dizer que o controlador ou operador tem o dever de prestar contas, ante a sua responsabilização, de demonstrar a autoridade delegante que os objetivos propostos foram cumpridos, sejam elas técnicas e/ou preventivas, e que esses processos guardaram adequação (conformidade) com as regras e princípios estabelecidos, que comprovem a efetividade e a observância da proteção aos dados pessoais.

3. RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

A responsabilidade civil é um instituto relativo ao ramo do direito obrigacional que decorre do reconhecimento dos direitos pessoais. A partir do momento que o ordenamento estabelece direitos, o faz para que seja disciplinada a relação entre as pessoas e que se impeça que tais direitos sejam violados. A violação, então, no caso do direito civil, é ato ilícito que gera a obrigação de reparar. Sendo assim, cria-se um vínculo jurídico que outorga a uma parte o direito de exigir da outra que cumpra determinada prestação (GONÇALVES, 2016, p. 45).

A Constituição Federal de 1988 teve papel importante no desenvolvimento da responsabilidade civil. O seu texto não apresenta uma teoria geral sobre o assunto, mas pacificou pontos importantes, como a questão da indenização pelo dano moral, nos incisos V e X do artigo 5º.

> 15 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> V - É assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ouà imagem;
>
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Além da decretação da responsabilidade objetiva do Estado, que está presente no §6º do artigo 37, a todos os prestadores de serviço público. Outro exemplo de determinação constitucional para a aplicação da responsabilidade objetiva é nos

danos decorrentes de instalações nucleares, previsto na alínea d, inciso XXIII do artigo 21, porém essa incluída por Emenda Constitucional.

Por fim, um aspecto importante que foi gestado na Constituição, e que culminou com a transformação da responsabilidade civil no Brasil, foi a defesa do consumidor, que discutiremos nos próximos tópicos deste capítulo.

3.1 RESPONSABILIDADE CIVIL NO CÓDIGO DE DEFESA DO CONSUMIDOR

Como já visto, as transformações no direito e na responsabilidade civil são indiscutíveis. Alguns, como o professor Sérgio Cavalieiri Filho (2019), chamam o que aconteceu de verdadeira revolução, pois reorganizaram de maneira profunda o entendimento sobre o tema. Quando nos debruçamos, atualmente, sobre essas transformações, podemos ter a impressão de que foram, na verdade, parte de uma evolução, pois todas as inovações caminhavam nesse sentido. O termo para designar tal fenômeno não interfere muito para os fins deste trabalho, pois, de qualquer modo, o que se pretende é verificar que fazem parte um movimento comum em que, à medida que a legislação fica mais robusta, a proteção avança.

Dessa forma, um marco intransponível no que tange a responsabilidade civil é o Código de Defesa do Consumidor, Lei nº 8.078 de 1990. Esta lei, sancionado pouco tempo depois da Constituição, como já foi dito, foi gestada na Carta Magna.

A Constituição, ao determinar que o Estado promovesse a defesa do consumidor, estabelecer a competência da União para legislar sobre dano causado ao meio ambiente, e ordenar que o Congresso Nacional elaborasse o Código de Defesa do Consumidor, reconheceu de forma definitiva a vulnerabilidade do consumidor.

Consequentemente, no Código de Defesa do Consumidor, a responsabilidade pelos danos causados em decorrência da relação de consumo independe de prova de culpa. Tudo o que foi dito anteriormente sobre o aumento da complexidade das relações em virtude das mudanças na forma de produção, são materializadas no CDC.

O Estado então reconhece mais uma vez que, há uma dificuldade na prova da culpa que, independentemente da atividade, que tende para o desequilíbrio nas

relações. Estabelece então, que a intervenção é necessária para que seja reestabelecido o equilíbrio entre as partes, diante da importância social e econômica que tem.

> O regime jurídico dessa reparação do dano sofrido pelo consumidor é o da responsabilidade objetiva pelo risco da atividade. Essa é a regra do CDC sobre responsabilidade civil. Qualquer que seja a natureza do dano, há o dever de indenizar pelo risco da atividade (GRINOVER, 2017, p. 555).

Como podemos ver, essa é a regra geral do CDC. Há a previsão de uma exceção, no art. 14, §4º, que disciplina a responsabilidade em caso de serviços prestados por profissionais liberais em que se deve apurar a culpa. Em todos os outros casos, se aplica a regra da responsabilidade objetiva.

Além disso, nesse contexto de responsabilidade objetiva, não há como discutir cláusulas de exclusão da responsabilidade, pois esse tipo de cláusula ataca o nexo de causalidade da conduta ao excluir a culpa do agente, que só são válidas para a verificação na responsabilidade subjetiva (GRINOVER, 2017), a não ser por culpa exclusiva da vítima ou de terceiros.

É extremamente relevante que se destaque também, que a responsabilidade é solidária entre o fabricante, produtor, construtor, nacional ou estrangeiro e o importador, conforme a redação do art. 12. Ou seja, o CDC aumenta as possibilidades de o consumidor buscar reparação de eventuais danos. a legislação fixa o entendimento de que todos aqueles que concorreram para a prestação do serviço são responsáveis pelas eventuais consequências negativas.

É por esses motivos que o CDC é o diploma mais avançado na proteção do indivíduo e se firma como verdadeiro paradigma, no que tange à legislação nacional, pois guarda total coerência com a necessidade de adequação a multiplicidade de relações.

3.2 RESPONSABILIDADE CIVIL NA LGPD

Como podemos verificar quando abordamos os princípios da LGPD, a responsabilidade dos agentes é ponto central da proteção de dados. O mercado de dados, em virtude do incremento tecnológico, está cada vez mais presente em nossos dias e tem importância no cotidiano. Com isso, a possibilidade de dano ao titular é consequência direta do tamanho da sua importância econômica e da sua abrangência.

A LGPD inova ao trazer uma série de condições para que o tratamento seja realizado. Aparece como um marco essencial para que as empresas e órgãos que trabalham com dados possam se adequar à nova realidade de proteção da personalidade.

Mas, é preciso atentar para o fato de que, como já afirmado, é uma atividade que envolve riscos e que pode acabar, por descumprimento da lei ou por algum outro fator, causando danos ao titular, seja dano patrimonial ou moral.

Para esses casos, em que ocorre dano decorrente do tratamento de dados, é que a lei instituiu uma série de regras sobre como deve proceder o ressarcimento. Nesse momento, tudo o que vem sendo discutido, sobre fundamentos, princípios e regras, serve de base para a reparação dos danos sofridos pelo titular dos dados.

Disciplinado entre o art. 42 e o 45 da Lei, a responsabilidade civil dos agentes de tratamento de dados, controlador e operador, em relação ao titular dos dados é dividida em dois tipos. O primeiro deles, contido no caput do art. 42, trata da regra geral e acaba por reproduzir aquilo que é definido no Código Civil de 2002 como forma de reparação de danos, que é a responsabilidade subjetiva. A responsabilidade objetiva é a exceção na LGPD, o que não significa que terá menos questionamentos que a tomam por base.

A responsabilidade civil na LGPD pressupõe o reconhecimento do risco no tratamento de dados pessoais. Dessa forma, pouco importa na prática se qualificarmos a responsabilidade da LGPD como objetiva ou como subjetiva com culpa presumida. Fato é que o dever de indenizar surge quando houver o dano, a violação à norma e o nexo causal.

A Lei Geral de Proteção de Dados também prevê expressamente as hipóteses em que não haverá responsabilidade civil dos agentes de tratamento de dados, sendo estas: quando não tiverem realizado o tratamento de dados que lhes é atribuído; quando o dano for decorrente de culpa exclusiva do titular dos dados ou de terceiro e quando não houver violação à legislação de proteção de dado. Essas hipóteses são aplicáveis tanto na exclusão de responsabilidade de pessoas de direito privado, quanto pessoas de direito público.

Também é previsto na LGPD a definição dos “dados sensíveis”, que são dados

cujo tratamento pode ensejar a discriminação do seu titular por se referirem, por exemplo, à opção sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas. Os dados sensíveis, pelo potencial discriminatório que apresentam, de acordo com a proposta em questão, devem ser protegidos e responsabilizados de forma mais rígida.

A Lei de Proteção de Dados Pessoais é muito calcada na perspectiva de risco. Isso significa dizer que você pode e deve esperar mais daqueles agentes de tratamento de dados pessoais cujas atividades têm um risco maior. Ou seja, o peso da lei vai ser calibrado de forma intensa para quem, por exemplo, trata dados pessoais sensíveis em larga escala. Por essa razão, não se pode perder de vista os princípios da prestação de contas e da responsabilidade.

3.3 RESPONSABILIDADE CIVIL SUBJETIVA

No que se refere a responsabilidade civil na LGPD, há uma clara separação entre as relações civis e relações de consumo. Na primeira, que tem como pressuposto o aspecto contratual, se aplica a regra geral do Código Civil, que é a responsabilidade em que se leva em conta a culpa do agente, tendo em vista que a responsabilidade objetiva, se fosse o caso, deveria estar indicada de forma expressa.

Vale também destacar que há a previsão da responsabilidade não só do controlador, mas também do operador. Já vimos que o operador está submetido aos comandos do controlador, porém ele desenvolve atividades de tratamento de dados submetido aos ditames da Lei da mesma forma. O operador tem a responsabilidade, assim como o controlador, de observar as regras da Lei e tomar as medidas necessárias para a segurança dos dados, da mesma forma. Além de que, é uma atividade que o beneficia e contém riscos, por isso pode incorrer em ilícito.

Outro aspecto importante é que a reparação pode ser feita em relação a um indivíduo específico ou a uma coletividade. Em virtude da própria natureza das atividades de tratamento de dados, que se torna mais precisa e rentável à medida que atinge mais pessoas, é mais provável que os danos acometam uma coletividade.

Após essas determinações iniciais, a seção da LGPD que trata da responsabilidade começa a desenvolver uma série de normas de maneira mais

específica para a atividade de tratamento de dados. A Lei institui que há solidariedade, entre controlador e operador, na obrigação de reparação dos danos, conforme inciso I, §1º, do art. 42. Tendo em vista que o cumprimento da Lei e a segurança da atividade é relativa a todos os agentes de tratamento, não importando se algum deles está submisso aos comandos do outro. Isso significa que a reparação pode ser exigida de um deles, ou dos dois. Como o enunciado do §1º coloca, é uma das regras que visa garantir a "efetiva indenização ao titular de dados".

O tratamento de dados é desenvolvido, normalmente, por uma rede complexa. Vários agentes concorrem para a seu funcionamento, e existem várias formas de arranjo para essa cadeia produtiva. Por isso, é possível que, em uma situação específica, se encontre uma multiplicidade de agentes composta de tal forma, que seja constituída por mais de um controlador, inclusive. Nesse caso, o inciso II do §1º, expressa que serão solidários todos os controladores. Isso aumenta de forma considerável as possibilidades de adequação da regra da reparação aos casos que surgirão, o que ajuda a garantir a reparação.

Decorre dessa concepção o fato de haver a possibilidade de ação de regresso, conforme §4º, do mesmo art. 42. Como há a solidariedade e a obrigação pode ser cumprida por todos ou por um deles, aquele que cumpri-la, pode exigir dos outros, "na medida de sua participação no evento danoso", o ressarcimento das quotas de cada um.

Por outro lado, no que concerne a produção de prova para a comprovação da culpa, o legislador adotou as mesmas regras gerais, exceção e teoria que fundamenta a inversão que as utilizadas no Código de Processo Civil de 2015. O ônus da prova no CPC é determinado, em regra geral, pela posição que as partes ocupam na demanda. Diz o art. 373 que incumbe ao autor provar fato constitutivo de seu direito e ao réu fato impeditivo, modificativo ou extintivo. Acontece que o §1º institui a teoria da distribuição dinâmica do ônus da prova (FILHO, 2018).

Esta teoria estabelece que o ônus da prova não é estático, pode ser invertido em determinadas situações, para ajudar na resolução do mérito de forma mais ágil e acertada possível. Da mesma forma determina a LGPD, no §2º do art. 42. É uma medida importante, pois presume-se que os agentes de proteção de dados têm maior

facilidade na produção de provas, porque detém todas as informações acerca da atividade. É também por isso que, como já vimos, exige-se que estes mantenham registro da atividade de tratamento.

Posteriormente, a Lei prevê as excludentes da responsabilidade no art. 43. O dispositivo determina as situações em que é afastada relação entre a conduta do agente e o dano sofrido pelo titular.

A reparação do dano só pode ser exigida de quem realizou o tratamento de dados de alguma forma. Se a cobrança é feita do agente que não participou, não há como configurar o nexo de causalidade entre dano e suposto ato ilícito. Sendo assim, o agente se desincumbe de reparar.

Outra possibilidade é quando, apesar de haver dano, o agente não descumpriu as normas de segurança determinadas pela LGPD e pela Autoridade Nacional de Proteção de Dados. Sendo assim, afasta-se a culpa agente, de modo a impossibilitar o pleito titular.

Por fim, é afastada a obrigação de reparação quando o agente prova que o dano foi causado por culpa exclusiva do titular ou de terceiros. O titular age de modo a contrariar seus interesses quando descuida da segurança ou subestima os riscos de uma determinada medida. Isso acarreta riscos que se somam aos normalmente ligados ao tratamento de dados, e foge completamente ao controle do controlador. Por isso, não pode ser responsável por possíveis danos resultantes.

Pode-se perceber que essas excludentes dependem da produção de prova por parte do agente. Portanto o processo será muito mais complexo e extenso. As condições para a produção de prova, porém, são mais acessíveis a estes agentes, por terem uma capacidade técnica e contextual mais favorável.

A ilicitude do procedimento dos agentes é determinada pelo descumprimento da legislação ou pela frustração da expectativa do titular sobre o procedimento, tendo em vista que é uma relação contratual, que preza pela transparência e respeita a boa-fé. O fato de a expectativa do titular ser um critério subjetivo a ser verificado no caso concreto pode, ao primeiro contato, parecer refúgio de insegurança. Porém, o legislador faz questão de esmiuçar, nos incisos I a II, tal regra, do art. 44, e determinar

que seja avaliado pelo julgador o “modo pelo qual é realizado” o tratamento, “o resultado e os riscos que razoavelmente dele se esperam” e as técnicas disponíveis à época.

Portanto, ao analisar os dispositivos que disciplinam a responsabilidade civil subjetiva dos agentes de tratamento de dados, pode-se observar que guarda grande semelhança com a legislação civil nacional, e, por isso, se mostra plenamente capaz de dar resposta a eventual necessidade de reparação de danos.

Contudo, levando em consideração que a maioria das atividades de tratamento de dados se dão em decorrência de relações de consumo, a responsabilidade objetiva, que é a exceção, será mais comumente aplicada. Porém, essa é uma hipótese que deverá ser verificada com o tempo e instrumentos específicos.

3.4 RESPONSABILIDADE CIVIL OBJETIVA

A responsabilidade civil objetiva é aplicada, por determinação legal, em casos que o legislador julga que há uma vulnerabilidade estrutural de uma das partes. Essa forma de reparação, sem levar em conta a culpa, então, configura forma e especial que decorre da Lei.

No caso da LGPD, está prevista em duas situações: tratamento de dados no âmbito das relações de consumo, por força do art. 45 da Lei, e tratamento de dados pelo poder público, conforme art. 37, §6º da Constituição.

Especificamente em relação ao poder público, existe entendimento do Supremo Tribunal Federal de que se aplica a responsabilidade objetiva em atos comissivos (MALDONADO e BLUM, 2019). É um entendimento que ainda não enfrentou a especificidade do tratamento de dados, e que deve ser observado em estudos posteriores.

Por outro lado, o Código de Defesa do Consumidor é paradigma na aplicação da responsabilidade civil objetiva. Efetivou mandamento constitucional de proteção ao consumidor e instituiu vários direitos que asseguram ao consumidor, vulnerável, proteção contra danos decorrentes da relação de consumo.

Por isso, a LGPD determina expressamente que, nas relações de consumo

este diploma deve ser aplicado, pois, por ser mais favorável ao consumidor, se presta melhor ao objetivo de prover reparação dos agentes que tem superioridade econômica e informacional sobre a atividade.

O defeito do produto ou do serviço, que gera dano ao consumidor, então é protegido através da solidariedade dos agentes, da inversão do ônus de prova e ao acesso a informações precisas.

Dessa forma, a LGPD se alinha com toda a legislação vigente, de modo coerente e seguro, na busca pela reparação efetiva e justa, guardando as especificidades de todos os contextos.

4. CONCLUSÃO

O presente trabalho trouxe como tema a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, a qual constitui um marco para as instituições privadas e públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais. A mesma apresenta inovação legislativa no Brasil quando se utiliza daquilo que já havia sido constituído na EU (União Europeia) e percebe novas demandas ao passo que apresenta novas respostas.

A LGPD possui em sua composição sete fundamentos e dez princípios, os quais têm por finalidade, respectivamente, explicar os objetivos da lei e auxiliar na compreensão e aplicação da mesma em cada caso. Seus fundamentos são organizados de modo a priorizar a proteção do indivíduo, contemplar a ordem econômica e apresentar consequências dos casos. Seus princípios, por sua vez, mesmo segmentados, atuam de forma interligada.

O rol de hipóteses estabelecidas no artigo 7º da LGPD são de suma importância, uma vez que é descrito o modo como a lei se aplica e a maneira como se comporta diante de cada situação, sendo assim, se constituem como um fator indispensável para podermos julgar se determinado tratamento está, ou não, em conformidade com os seus ditames.

O estudo e profunda interpretação dos aspectos e possibilidades da LGPD são merecedores de pontual atenção uma vez que as novas tecnologias de transmissão,

coleta, armazenamento e processamento na internet permitem que as informações sejam cada vez mais usadas para o desenvolvimento da eficiência econômica, ao passo que é possível estabelecer uma relação mais eficaz com os consumidores. Deste modo, passou a ser possível que a produção e a divulgação dos produtos fossem mais efetivas. Em contraponto, o lado negativo desta relação é que o indivíduo titular dos dados e consumidor dos bens foi se tornando cada mais vulnerável, uma vez que as informações passaram a circular entre os agentes econômicos e a sua intimidade e capacidade de escolha foi sendo suplantada pelos interesses das grandes corporações.

Diante de tal, admite-se afirmar que a Lei Geral de Proteção de Dados, ao fazer uso de seus aspectos para o tratamento dos dados, é satisfatória ao ponto que de acordo com o texto da EC 115, foi acrescido um inciso LXXIX ao artigo 5º, CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (Incluído pela Emenda Constitucional nº 115, de 2022), Reconhecer a proteção de dados como um direito fundamental. Portanto é eficiente em atender as mais diversas demandas relacionadas a proteção de dados pessoais. Institui um sistema de transparência, objetividade e segurança que assegura a identificação de falhas e possibilidade o restabelecimento de seus efeitos. Implementa um sistema de reparação que distingue bem as relações que se aplicam a responsabilidade civil subjetiva e objetiva, de modo a efetivar a reparação do titular, preservando os fundamentos constitucionais.

O trabalho mostrou que, a partir da análise da origem e texto da LGPD, cotejamento com outros diplomas e pesquisa doutrinária é possível identificar os conceitos fundamentais, princípios, agentes e suas atribuições contidos na Lei Geral de Proteção de Dados; verificar a legislação nacional acerca da responsabilidade civil que corrobora com a Lei de Dados para a efetiva satisfação dos prejuízos decorrentes do desrespeito a proteção de dados; e analisar os limites e especificidades para reparação dos danos atribuídos aos agentes de proteção de dados. Constatou-se que, a LGPD cumpre, então, o seu papel de proteção de dados, pois assegura aos titulares a forma mais justa e moderna de responsabilização civil que há no nosso ordenamento jurídico. Dessa forma, se diz que os objetivos deste trabalho puderam ser contemplados.

5. REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. 1. ed. São Paulo: Malheiros Editores, 2006.

CASTELLS, M**. A Sociedade em Rede**. 3. ed. São Paulo: Paz e Terra, 2000.

BIONI, B. R. **Proteção de dados pessoais**: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

COELHO, A. C. B**. A Lei Geral de Proteção de Dados Pessoais Brasileira como meio de efetivação dos direitos da personalidade**. João Pessoa: [s.n.], 2019.

FILHO, M. M. **Novo Código de Processo Civil Comentado**. 3. ed. São Paulo: Atlas, 2018.

FILHO, S. C. **Programa de Responsabilidade Civil**. 13. ed. São Paulo: Atlas, 2019

GODINHO, A. M. **O fenômeno da constitucionalização**: um novo olhar sobre o Direito Civil. Revista Libertas, Janeiro 2013.

GONÇALVES, C. R. **Responsabilidade Civil**. 17. ed. São Paulo: Saraiva, 2016.

GRINOVER, A. P. **Código Brasileiro de Defesa do Consumidor - Comentado pelos Autores do Anteprojeto**. 11. ed. Rio de Janeiro: Forense, 2017.

JÚNIOR, S. R. C. D. S. **A Regulação jurídica da proteção de dados pessoais no Brasil. Trabalho de Conclusão de Curso (Bacharelado em Direito) PUC Rio.** Rio de Janeiro: [s.n.], 2018.

LÔBO, P. **Direito Civil**: parte geral. 6. ed. São Paulo: Saraiva, 2017.

MALDONADO, V. N.; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados comentada. 1. ed. São Paulo: Revista dos Tribunais, 2019.

PINHEIRO, P. P. **Proteção de Dados Pessoais**: Comentários à Lei nº 13.709/2018. 1. ed. São Paulo: Saraiva Educação, 2018.

ROSENVALD, N. **As funções da responsabilidade civil**: a reparação e a pena civil. 3. ed. São Paulo: Saraiva, 2017.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Congresso Nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 de Setembro de 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 20 de Setembro 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709. htm. Acesso em: 22 de Setembro de 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 22 de Setembro de 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 20 de Novembro de 2022.