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

# A LEI GERAL DE PROTEÇÃO DE DADOS E A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

Edison da Fonseca Guerra Alvares
Orientador: Guilherme Magalhães Martins

RIO DE JANEIRO

2022

Edison da Fonseca Guerra Alvares

# A LEI GERAL DE PROTEÇÃO DE DADOS E A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

Monografia apresentada à Faculdade de Direito da Universidade Federal do Rio de Janeiro, como requisito parcial para a obtenção do título de Bacharel em Direito.

RIO DE JANEIRO

2022

ALVARES, Edison da Fonseca Guerra.

A Lei Geral de Proteção de Dados e a Responsabilidade Civil dos agentes de tratamento dos dados pessoais /ALVARES, Edison da Fonseca Guerra – 2022.

56 f.

Monografia (graduação em Direito) – Universidade Federal do Rio de Janeiro, Centro de Ciências Jurídicas e Econômicas, Faculdade de Direito.

Referências: f. 54 - 56.

**Edison da Fonseca Guerra Alvares**

DRE: 117078358

Celular: (21) 988060613

E-mail: edison.guerra98@gmail.com

Ed.: Rua Franz Weissman 410, Bloco Termoli 802, Jacarepaguá, Rio de Janeiro – RJ

CEP: 22775-051

Turno: Integral

Professor Orientador: Guilherme Martins

## RESUMO

O direito à proteção de dados tornou-se pujante na sociedade brasileira, tendo em vista o compartilhamento em massa de informações na internet. Em um mundo onde os dados pessoais passaram a ser um ativo extremamente lucrativo, as empresas tentam explorar a coleta destes dados em seu máximo aproveitamento, fazendo com que a tutela dos direitos dos titulares dos dados torne-se ainda mais necessária. É neste contexto que no presente trabalho faz-se necessário analisar as ferramentas utilizadas na coleta, tratamento e compartilhamento de dados e, principalmente os limites da responsabilização dos agentes tratadores, a partir da Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, que trouxe inovações e conceitos importantes para o combate aos problemas gerados pelo compartilhamento de informações em massa na internet. Diante disso, o presente trabalho aborda, a partir da análise da legislação vigente, bem como de estudos de outros autores, o surgimento da legislação e suas motivações de início. Posteriormente, faz-se um recorte dos dados pessoais como direito da personalidade, além da demonstração da utilização destes como mercadoria e de outras ferramentas inerentes ao uso das novas tecnologias. Por fim, o trabalho passará a uma análise sobre as modalidades subjetiva e objetiva de responsabilização dos agentes de tratamento de dados, bem como a demonstração desta última como modalidade capaz de resolver de forma mais coerente os conflitos relacionados à Lei.



## ABSTRACT

The right to data protection has become thriving in Brazilian society, in view of the mass sharing of information on the internet. In a world where personal data has become an extremely profitable asset, companies try to exploit the collection of this data to its fullest, making the protection of the rights of data subjects even more necessary. It is in this context that in the present work it is necessary to analyze the tools used in the collection, treatment and sharing of data and, mainly, the limits of accountability of the processing agents, from the General Data Protection Law (LGPD), Law 13.709/ 2018, which brought important innovations and concepts to combat the problems generated by mass sharing of information on the internet. In view of

this, the present work approaches, from the analysis of the current legislation, as well as studies by other authors, the emergence of the legislation and its initial motivations. Subsequently, a cut of personal data is made as a right of personality, in addition to the demonstration of their use as merchandise and other tools inherent to the use of new technologies. Finally, the work will proceed to an analysis of the subjective and objective modalities of accountability of data processing agents, as well as the demonstration of the latter as a modality capable of resolving conflicts related to the Law in a more coherent way.
Mais sobre o texto original.

Palavras-chave: dados, GDPR, Lei Geral de Proteção de Dados, LGPD, Responsabilidade Civil Objetiva, Responsabilidade Civil Subjetiva.

*Key words*: *data, GDPR, General Data Protection Law, LGPD, Objective Civil Liability, Subjective Civil Liability.*

## DEDICATÓRIA

Pelo presente, diante do árduo processo de formação em Direito, na gloriosa Faculdade Nacional de Direito da UFRJ, agradeço primeiramente a mim mesmo por não desistir, diante da falta de motivação em alguns momentos, principalmente ao perceber que o caminho dentro da faculdade se mostrava demasiado teórico.

Gostaria de agradecer fundamentalmente à minha família, principalmente ao meu pai e minha mãe, que durante toda minha vida me amaram profundamente e se sacrificaram para investir tempo e dinheiro em meus estudos, além de serem pacientes com minha caminha e respeitarem minhas decisões durante o processo. Agradeço também à minha irmã que desde meus 7 anos de idade foi minha alegria sem tamanho, além da minha vó, a quem expresso eternamente minha gratidão por ter me dado o maior ensinamento da vida: ser Vasco da Gama. Agredeço à minha madrinha Thelminha e minha tia Edna por fazerem um pouco papel de mãe e me darem conselhos, companhia e amizade, apesar da distância física.

Agradeço profundamente à minha mulher e companheira de vida, Carol, com quem sou extremamente realizado e grato pois sempre me ajudou em tudo, me dá amor, carinho e apoio incondicional; com ela divido minha vida, sonhos e foi quem me deu a maior alegria que eu poderia ter: ser pai. Aproveito também para já agradecer o espírito dessa criança, o Nico, cujo nascimento ainda nem chegou, mas já me provém muito motivação para trilhar meu caminho.

Gostaria de agradecer à minha prima Fernanda, que por alguns anos morou comigo e dividiu suas experiências, tendo me ensinado muito na vida, além de junto do meu amigo Bruno, ter me dado uma alegria sem tamanho que são meus afilhados, Vicente e Joaquim.

Agradeço a meu primo Leo, que apesar da distância física, sempre tive grande afeto e carinho, além de admiração.

Gostaria de agradecer aos meus amigos do O.E.A. : Breno, Henrique, Leleco, Leo, Renan, Rolé e Xande, a quem agradeço por serem verdadeiros irmãos e estarem ao meu lado em todos os momentos. bem como os membros do L.D.: Igor, Magá e Fontes, tendo este último sido um grande mentor em meu primeiro estágio.

Agradeço aos amigos do Coreto da Nacional: Diego, Gustavo, Jamal, Mani e Renan, por compartilhar comigo os últimos momentos de gloria e de alento, os últimos suspiros da cultura barra brava dentro da faculdade, os fogos que soltamos por onde passamos, além da resenha que ficou para além da faculdade.

Agradeço aos meus amigos de bancada, de compartilhamento de alegrias em prol do Club de Regatas Vasco da Gama, nosso amor incondicional. Obrigado Turma da Regina: Bruno, Henrique, Fontes, Leleco, Magá, Renan, Renan Boyd, Rolé, Tauã e Thiago por compartilharem o alento, as viagens e o perrengue seguindo este clube que sempre será o clube do povo do Rio de Janeiro e sempre lutará contra toda forma de preconceito. Agradeço por nutrirem comigo uma rivalidade irracional contra o flamengo, clube derivado o qual nunca suportei e sempre estaremos no lado oposto. Que o Dr. Eurico Miranda esteja lá de cima com seu charuto olhando por nós. O alento não pode parar!

Agradeço minhas amigas Mariah, Lu e Gi por me acompanharem em tantos momentos na caminhada dessa vida e estarem sempre do meu lado.

Por fim, e nunca menos importante, expresso minha gratidão por meus sogros Roberto e Ana e meu cunhado Felipe por apoiarem a mim e a Carol na jornada de criar um novo ser.

**SUMÁRIO**

# INTRODUÇÃO

O avanço tecnológico mundial em diversos ramos da sociedade trouxe novas problemáticas e debates principalmente no que tange a atuação dos operadores dos direitos no sentido de alinhar as novas práticas com os princípios constitucionais e os valores sociais cultivados em território brasileiro. Em tempos de exasperação das desigualdades sociais, pandemia, trabalho remoto e em uma economia de cadastros digitais em plataformas de e-commerce, faz-se cada vez mais desafiador e necessário estudar e garantir a proteção e o tratamento adequado dos dados dos indivíduos, bem como a responsabilização dos que a estes causam danos.

Neste sentido, com entrada em vigor no ano de 2021 dentro do ordenamento jurídico brasileiro, a Lei Geral de Proteção de Dados (Lei 13.709/18), popularmente denominada "LGPD", trouxe uma gama de mudanças e inovações no que tange a proteção dos dados pessoais e a segurança da informação; inovação esta que acabou por ter seus reflexos na Constituição Federal de 1988 com a inclusão do inciso LXXIX no artigo 5º do mesmo diploma, ou seja, com a inclusão do direito à proteção de dados como direito fundamental, ocorrida pouco tempo após o STF julgar a ADIn 6.393, reconhecendo a proteção de dados pessoais e a autodeterminação informativa como direitos fundamentais autônomos. Tal fato tornou a proteção de dados pessoais um fator imprescindível para a articulação do direito privado diante dos interesses passíveis de tutela no contexto da informação.

O diploma da LGPD tem como inspiração o *General Data Protection Regulation*, regulamento europeu sobre o mesmo tema, do qual a legislação brasileira retirou parte de seu conteúdo, inclusive quase como tradução literal em alguns casos. Tal fato gera uma adequação ao modelo europeu que aponta para uma tendência de alinhamento típico de um mundo globalizado. Porém, dado que cada país tem seu ordenamento jurídico e que, na verdade, o GDPR é a lei de um continente, não de um único país e, por isso, não traz algumas definições expressas, deixando margem à interpretação das diferentes nações aderentes ao GPDR. Em decorrência dessa inspiração no modelo europeu, a LGPD acabou sofrendo diversas críticas de estudiosos do Direito por supostamente deixar alguns vácuos legislativos, tendo como um de

seus pontos principais a temática da responsabilidade civil dos agentes tratadores de dados pessoais, que será bastante abordada e discutida diante do presente estudo, principalmente sobre o conteúdo dos artigos 42, 43, 44 e 45 da versão brasileira do referido diploma legal.

Por conta das críticas , a parte do texto legal que trata sobre a responsabilidade civil dos agentes acabou por motivar grandes debates por parte destes estudiosos, bem como dos operadores do direito, devido à margem interpretativa encontrada na lei. O grande questionamento encontra-se voltado para a natureza quando da existência de obrigação de indenizar, se subjetiva – embasada pela falta de um dever de conduta imposto ao agente de tratamento - ou objetiva - fundamentada no risco da atividade desenvolvida. Porém, é verdade que na prática a legislação não possui vácuos; o que houve claramente foi uma tentativa de atores pró-mercado, de tentar subjetivar o modelo trazido pela legislação, fator que dificultaria a efetivação da tutela através da própria responsabilização. Tal fato será mais bem explorado em momento oportuno ao longo do presente estudo.

Fato é que a disseminação de dados pessoais na internet passou por grande aceleração no século XXI com a chegada de *smartphones* e, principalmente, da inteligência artificial, que a partir de ferramentas como a do *Big Data*, a ser explicada no presente estudo, tornou-se um grande negócio lucrativo, no qual agentes tratadores de dados, muitas vezes representados na figura de grandes empresas (como *Amazon, Netflix, Facebook, Twitter, Google, Microsoft* e outras), maximizam seu lucro e/ou controle a partir da quantidade de informações dos consumidores/cidadãos (denominados titulares de dados no presente estudo) que possuem em suas bases de dados. Este conflito trouxe certa preocupação para o mundo do Direito, bem como necessidade de entendimento sobre como reduzir a exposição dos titulares de dados pessoais frente à velocidade da internet atualmente. Hoje, na verdade, questiona-se se isso ainda é possível. De todo modo, caso se entenda que a redução desta exposição já não seja mais palpável, ao menos que sejam feitos esforços para, ao menos, mitigar seus efeitos, ou seja, para colocar os titulares de dados em uma posição na qual a reparação de danos seja viável de se buscar. Sobre tal assunto, vejamos o disposto por Bruno Bioni

> Nesse sentido, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e se movimentam a partir desses signos identificadores do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar

> informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações. (Bioni, 2019)

As respostas para este e outros possíveis questionamentos oriundos da Lei Geral de Proteção de dados não são exatas em virtude do momento de implementação prática da nova legislação ser ainda bastante recente, além de ter ocorrido de forma tardia, fator pelo qual se faz amplamente necessário estudar e aprofundar o tema, sem qualquer intenção de exaurir o debate, mas somente buscar soluções práticas tão úteis quanto às tecnologias que motivaram a idealização da LGPD. A lei trouxe inovações, sendo sua interpretação tão complexa quanto necessária para alcançar os avanços sociais pretendidos. Porém, as inovações tecnológicas são demasiadas e constantes, fator pelo qual sempre será necessário atualizar os pensamentos dos estudiosos, bem como o próprio texto legislativo, buscando novas soluções para os próximos problemas que surgirão.

Por fim, terminadas as considerações iniciais sobre os direcionamentos do presente trabalho, passa-se ao desenvolvimento da pesquisa, na qual foram utilizados artigos científicos, legislações, livros e outros meios vinculativos de informação sobre o tema a serem apresentados ao longo do estudo. A linha do tempo a ser utilizada apresentará desde a o surgimento da lei de proteção de dos dados no brasil, até a conclusão normativamente doutrinadora sobre a melhor aplicação dos modelos de responsabilidade civil no tratamento de dados.

## 1) SURGIMENTO E MOTIVAÇÃO PARA A CRIAÇÃO DE UMA LEI ESPECÍFICA

Desde o início da última década, empresas e usuários, bem como as autoridades, vêm buscando respostas para a questão da segurança no ambiente virtual, que ganham relevância com o crescimento exponencial dos crimes cibernéticos. 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. (Machado, 2018). É verdade que a Lei Geral de Proteção de Dados, bem como nenhum outro diploma legal sobre o mesmo tema, surgiu do dia para a noite. Sua idealização é, como já apontado, tardia, evidenciando certa tendência inevitável de apresentar respostas legislativas posteriores a uma atividade amplamente realizada na prática das mais diversas formas de relações cotidianas, cujos reflexos econômicos, políticos

e sociais são palpáveis enquanto fundamentos que justificam e explicam os motivos, enfoques principais e substrato jurídicos, envolvidos na concepção da LGPD.

## 1.1) SURGIMENTO

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. Com o objetivo de garantir a segurança de dados pessoais, a lei trouxe importantes mudanças no Marco Civil da Internet, de 2014.

De fato os Estados Unidos são tidos como iniciador das discussões doutrinárias e jurisprudenciais sobre o papel do Direito diante do fenômeno social dos direitos à privacidade, iniciadas a partir do clássico artigo "The right to privacy", escrito por Samuel Warren e Louis Brandeis, publicado na revista acadêmica "Harvard Law Review" em 1890. Já em um contexto internacional, a privacidade aparece na Declaração Universal dos Direitos Humanos de 1948, que em seu artigo 12 dispõe:

> Artigo 12:
>
> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.

Já no Brasil, a preocupação com a privacidade é algo evidente desde a Constituição de 1891, que em seu artigo 72, § 18, trazia que "é inviolável o sigilo de correspondência. Já na Constituição de 1988, atualmente vigente, pela primeira vez é vista a preocupação não só com a privacidade de modo geral, mas expressamente com a questão dos dados, em seu artigo 5º, incisos X e XII, dispondo que: " são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação" e "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Sobre tal mutação, temos os escritos de Samuel D. Warren e Louis D. Brandeis :

> Que o indivíduo deve ter total proteção pessoal e patrimonial é um princípio tão antigo quanto o common law*; mas tem sido considerado necessário, de tempos em tempos, definir novamente a natureza exata e a extensão de tal proteção. Mudanças políticas, sociais e econômicas implicam o reconhecimento de novos direitos, e o common law, em sua eterna juventude, cresce para atender às novas demandas da sociedade. Assim, em tempos muito antigos, a lei dava remédio apenas para a interferência física na vida e na propriedade, para transgressões vi et armis. Então, o "direito à vida" servia apenas para proteger o sujeito da agressão em suas várias formas; liberdade significava liberdade de restrições atuais; e o direito à propriedade assegurava ao indivíduo suas terras e seu gado. Mais tarde, veio o reconhecimento da natureza espiritual do homem, de seus sentimentos e seu intelecto. Gradualmente, o escopo desses direitos legais foi ampliado; e agora o direito à vida passou a significar o direito de aproveitar a vida – o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo "propriedade" cresceu para incluir todas as formas de posse – tanto intangíveis quanto tangíveis.* (Quintiliano, 2021)

Porém, a noção de dados pessoais ganha novo contexto com a disseminação em massa da internet. Neste sentido, a influência da União Europeia assume papel de grande influência nos rumos tomados posteriormente pela legislação brasileira. No ano de 2016, foi publicado o Regulamento Geral de Proteção de Dados Europeu (*GDPR*) e, a partir dele, a União Europeia passou a publicar um relatório de quais os países fora do bloco econômico possuiam níveis adequados de proteção de dados, criando obstáculos para aqueles que não obtivessem o resultado esperado. Dentre os requisitos, era esperado que o país tivesse legislação nacional relevante sobre o tema, contendo: a proteção de dados pessoais; medidas de segurança; direitos dos titulares de dados e; previsão de medidas administrativas e judiciais efetivas para assegurá-los etc.

Os requisitos supracitados, para além de ter "apressado" a implementação da LGPD, fizeram com que o GDPR também influenciasse a redação de diversos artigos na lei brasileira, sendo alguns inclusive tradução quase literal do diploma europeu. A questão da responsabilidade civil, por exemplo, motivadora de grandes problemas interpretativos na legislação brasileira, foi uma das partes bastante semelhantes à lei europeia. São muitas as semelhanças entre os diplomas, de maneira que o consentimento se faz amplamente resguardado e protegido por ambas as leis. A informação aos titulares dos dados sobre eventuais incidentes, prova do consentimento, portabilidade de dados, indicação e responsabilidade dos agentes encarregados pela operacionalidade dos dados e as regras de segurança para armazenamento, transmissão e manuseio são pontos essenciais e regulados pela LGPD que constam também no regimento da GDPR. Com isso, é possível compreender que as

convergências com o diploma europeu ocorreram com um propósito: facilitar e ser o elemento responsável por assegurar a "interoperabilidade" dos mencionados regimes, por seu turno essencial para os negócios globais e para o compliance por organizações de todos os tamanhos. Tal movimento é fator que aponta na direção da globalização e da atração de investimentos de países desenvolvidos para o Brasil.

## 1.2.) MOTIVAÇÃO

Ao analisar os "fundamentos da proteção de dados pessoais", a professora Ana Frazão aponta que os dados pessoais são imprescindíveis para o desenvolvimento de grande parte das atividades econômicas, colocando-os no centro de um "crescente e pujante mercado", cujas consequências, inevitavelmente, acabaram por respingar em uma reformulação das dinâmicas político-sociais, bem como na seara das liberdades privadas dos titulares dos dados. "Os dados ganharam uma importância transversal, tornando-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia" (Frazão)

Para fins de auxiliar o presente estudo, faz-se necessário que o conceito de dados pessoais refere-se àqueles que comumente são fornecidos em um cadastro, como nome, RG, CPF, gênero, data e local de nascimento, filiação, telefone, endereço residencial, cartão ou dados bancários. Mas também são dados pessoais algumas informações que nem sempre fornecemos de forma consciente, como localização via GPS, retrato em fotografia, prontuário de saúde, hábitos de consumo, endereço de IP (Protocolo da Internet) e cookies. Ou seja, tal definição não apresenta um rol taxativo, mas exemplificativo de que existe um mundo de informações sobre os indivíduos para a consideração de dados pessoais; além disso, o conceito já denota uma ideia do quão complexo é encontrar a melhor aplicação para um conceito que apresenta-se como tão abrangente e se manifesta em diversos graus de relevância.

A clara expansão da propagação de dados ocorre com o surgimento do *Big Data* e do *Big Analytics*, ferramentas proporcionadoras da consecução dos fins por eles almejados de maneira mais eficaz, veloz, massiva e diversificada. Assim foi que, na ausência de uma regulamentação

mais adequada, os procedimentos envolvendo o referido ativo passaram a ser realizados sem qaulquer limitação e com resultados que podem se projetar por tempo indeterminado.

Nos últimos anos, nos deparamos com vazamentos de dados, dos mais variados. Aliás, as professoras Ana Frazão e Caitlin Mulholland no podcast "Direito Digital" preferem utilizar o termo incidente de segurança, tendo em vista que vazamento denota uma conotação até pejorativa como se algúem tivesse violado algo, ou ainda alguém tivesse falhado. Fato é que diversos incidentes recentes ocorreram como foi o caso do Serasa e do Banco Itaú, expondo dados pessoais de milhões de brasileiros. Estes ocorridos nos fazem questionar se uma postura diferente das empresas poderia evitar a exposição, ou ainda uma maior regulamentação do poder público sobre o ambiente da internet.

No que tange a atuação de empresas como agentes tratadores de dados, há uma crítica bastante pertinente sobre a maneira como coletam os dados, ou seja, sobre a atuação da primeira etapa da cadeia de dados. Desde que a sociedade, e principalmente o setor do comércio começou a entender a importância do uso de dados pessoais para crescer a atuação no mercado, iniciou-se um movimento de coleta todo e qualquer tipo de dado dos consumidores. Com isso, começaram a surgir empresas movidas por dados, com uma cultura bastante agressiva de coleta, tornando o processo muitas vezes invasivo pro cliente. O mercado precisa compreender que nem sempre quantidade é qualidade. Aliás, quanto maior a quantidade, maior o risco para o agente tratador.

É justamente com o intuito de acabar com a coleta desenfreada de dados, que a LGPD traz o princípio da necessidade. que prevê que devem ser coletados apenas o estritamente necessário para atingir a finalidade pretendida, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Sobre o princípio, Marcio Pestana leciona:

> "A necessidade, ao seu turno, poderá ser compreendida como a adoção de um meio que, a par de preencher o requisito de adequação à finalidade almejada, seja o menos gravoso para o indivíduo e para o interesse público. A Administração Pública em inúmeras circunstâncias interfere no exercício da liberdade e da propriedade dos indivíduos, ora promovendo desapropriações, ora apreendendo alimentos deteriorados, estabelecendo condições para o exercício do comércio etc. Agora, sua intervenção, de acordo com o princípio da proporcionalidade, deverá

> dar-se por meio da adoção do ato administrativo mais suave à situação, constituindo-se, portanto, num elemento de intensidade e extensão, de graduação, em outras palavras".

Ou seja, um dado pode ser ou não considerado necessário, dependendo de cada caso de uso específico. O que isso significa na prática? Se um *e-commerce* tem um processo comercial 100% digital, onde não há qualquer possível interação via telefone, por exemplo, este *e-commerce* não deve tornar obrigatório para que os compradores forneçam seus telefones no momento da compra. Porém, a questão é muito mais complexa e, na prática, obviamente o que se observa é uma tentativa dos agentes tratadores de dados, principalmente quando se trata de empresas, de justificar pelo motivos mais absurdos algum tipo de tratamento que racionalmente seria considerado indevido.

Abordando os princípios dentro da LGPD, a lei também traz a questão da finalidade. No inciso I do artigo 6º, a lei fala em "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Ou seja, os propósitos do controlador (agentes que tratam os dados), devem ser específicos e legítimos para o tratamento de dados. Além disso, essa finalidade deve estar atralada ou princípio da transparência que, segundo o inciso VI do mesmo artigo dispõe: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Com isso, torna-se claro que a lei surge em um cenário não só de preocupação em entender quais dados são necessários, mas também de compreender os propósitos do tratamento, se são legítimos, bem como de fornecer aos titulares de dados a maior transparência possível quanto a destinação de seus dados. Aliás, o artigo 6º trouxe dez princípios diversos que motivam a legislação. Não com o intuito de esgotamento, mas os dez princípios, em conjunto com a boa-fé, motivam uma melhor aplicação dos anseios existentes quanto à proteção de dados.

Outro questionamento surgido mais recentemente foi quanto a estudos feitos nos Estados Unidos demonstrando que algoritmos de tratamento e classificação de dados pessoais utilizados pela inteligência policial e no contexto de procura e oferta de vagas de emprego acabaram por reproduzir padrões considerados racistas e discriminatórios, mesmo sem terem sido intencionalmente desenvolvidos para tanto e, tampouco, sem que tenha sido identificada

alguma “falha”, em sua estruturação, desenvolvimento ou programação. Tal fato, demonstra que a inteligência artifical, muitas vezes pode acabar reproduzindo certos padrões de comportamento humano considerados retrógrados.

Sobre o tema, importante trazer o estudo feito pelo professor, mestre em Comunicação pela UFBA, Tarcízio Silva. Ao abordar o Colonialismo de dados, em um dos trechos, o autor aborda a questão do racismo algorítmico:

> As práticas em torno da base de imagens etiquetadas ImageNet formam um dos exemplos mais loquazes sobre como o colonialismo de dados molda práticas e modelos que ganham incrementalmente camadas de opacidade até o ponto de serem tomados como naturais e promovem algoritmicamente o racismo. Esta base de imagens possui milhões de fotografias extraídas sem consentimento através de *web scraping* em buscadores. Foi etiquetada – ou seja, marcada com categorias para permitir o aprendizado de máquina – sobretudo através de trabalho do modelo *“crowdsourced”* realizado por profissionais precarizados em países como Filipinas e Índia. As imagens eram provenientes em sua absoluta maioria de países europeus e EUA, hipervisibilizando pessoas e ambientes destes países e invisibilizando estéticas do Sul Global. A partir deste treinamento de máquina, competições de construção de modelos algorítmicos para identificação de imagens foram realizados por centros científicos dos países afluentes. Como resultado, isto significou a reprodução opaca de modelos algorítmicos de interpretação de imagens em visão computacional que apaga ou interpreta erroneamente pessoas e ambientes não-eurocêntricos ao mesmo tempo que transferiu trabalho e recursos reproduzíveis e escaláveis para os centros afluentes da tecnologia global.

Outro caso bastante emblemático e similar ocorreu na rede social Twitter, no qual usuários fizeram o seguinte experimento: foram postadas várias fotos de pessoas com pele clara e de pessoas com pele escura utilizando as mesmas circunstâncias. Com isso, começou-se a observar que as fotos de pessoas com pele mais clara obtinham um alcance muito melhor em relação às fotos de pessoas com pele mais escura.

Tal análise nos permite compreender que o racismo, muitas vezes também presente no tratamento de dados, é algo premeditado e escolhido a dedo por atores relevantes do mercado. Muito se afirma que o algoritmo não é racista, pois é uma matemática, é algo baseado em uma estatística e fundamentado em matemática e não tem como ser racista, quem são racistas são as pessoas que programam os algoritmos. Porém, de todo modo não se pode falar em algo ocasional ou inerente ao uso das novas tecnologias, mas sim em uma reprodução dos preconceitos humanos que são responsáveis pela contaminação racista nas decisões das

máquinas. Além disso, o trecho de Tarcízio Silva nos traz importante reflexão a respeito das consequências de tal modelo. Nas eleições no âmbito político pelo mundo, percebe-se que as grandes empresas, justamente as maiores participantes da dinâmica descrita pelo autor, participaram ativamente na construção de opinião sobre os condidatos envolvidos. Com isso, surge o questionamento sobre os interesses empresariais servirem para manipular o pensamento cidadão por meio das redes sociais destas mesmas empresas. Recentemente, um exemplo brasileiro desta necessidade de tutela, é o inquérito das *Fake News*, no qual entendeu-se ser necessário cassar a candidatura de elegíveis que não se adequem às boas práticas e à legislação. Sem esse tipo de ameaça, se estava banalizando o compartilhamento de dados mentirosos sobre outros concorrentes, colocando em risco o próprio sistema democrático.

A partir do momento em que os atores sociais, políticos e econômicos passam a compreender que as novas tecnologias possuem grande potencial de correlacionar os dados constantes em uma rede social, a utilização destas informações se tornou base para o desenvolvimento de um bojo de estratégias para hipervigilância por parte do Estado e também pelos Oligopólios privados. Sendo que o conceito de vigilância aqui disposto engloba um mundo de monitoramento, controle, observação, classificação, checagem e atenção sistemática" (Bauman, 2013) dos indivíduos a partir do processamento de dados.

Em tempos mais remotos, a preocupação de vigilância existente era do povo em relação ao próprio Estado, em relação à possibilidade de concentração do poder estatal mediante o uso indiscriminado de dados constantes em bancos de dados centralizados, levando-nos *ao Big Brother* de George Orwell[1], na qual perpetua-se uma vigilância constante sob o olhar do Grande Irmão ( este representando a cultura de um grande chefe de Estado). Porém, nos tempos modernos, a preocupação é ampliada à figura das grandes empresas e da descentralização de dados. Se antes era possível entender que o Grande Irmão era o detentor de todos os dados em um centro de controle, hoje estas informações estão descentralizadas, mas ainda com grande, ou ainda maior, relação entre si; o controle e rastreio neste modelo descentralizado torna-se ainda mais difícil.

[1] Líder governamental do Estado distópico constante na obra literária 1984, de George Orwell.

É diante desta reflexão que a velha sociedade de vigilância transforma-se em capitalismo de vigilância, na qual pequenos Grandes Irmãos assumem o controle das informações e de dados pessoais, no intuito de influenciar e transformar o comportamento do cidadão. Com isso, o caminho leva o cidadão a uma economia de vigilância, na qual seus dados são o objeto mais bem avaliado no mercado, porém o próprio titular é o único integrante da cadeia que não obtém lucro com suas informações.

Através de um olhar baumaniano, a vigilância contemporânea é caracterizada por ser líquidez e fluidez, esparramada ao longo das diferentes camadas sociais (Bauman, Vigilância líquida, p.10, 2013), não sendo possível traçar suas origens com facilidade, em que o sistema de dominação é instalado de forma progressiva e dispersa, em oposição ao poder centralizado do sistema panóptico característico das sociedades disciplinares. Para Bauman, liquidez e vigilância não estão obrigatoriamente atrelados, mas é um elemento decorrente do atual estado da própria modernidade, que é, por si, líquida, "fluida e perturbadora" (Bauman, Vigilância líquida, p.10, 2013), na medida em que "todas as formas sociais se desmancham mais depressa que a velocidade com que se criam novas formas." (Bauman, Vigilância líquida, p.11, 2013). Não é apenas a vigilância que passou por porfunda tranformação; tal característica perpassa todos os campos afetados pela sociedade da informação.

Com isso, entende-se que a necessidade de uma legislação específica sobre o tema, tornou-se pujante, tendo em vista que diplomas esparsos não possuem mais a capacidade de adequação à complexidade temática. Com isso, a LGPD surge em um contexto de ameaça dos direitos individuais e da autodeterinação comportamental comprometidos frente a uma indústria de dados, cada vez mais capaz de manipular o comportamento do próprio titular desses dados. Para tal, faz-se impresncindível o respeito ao princípio da transparência. Este determina que os agentes precisam ser francos com os titulares dos dados, devendo, inclusive, informar aos proprietários dos dados sobre os respectivos agentes de tratamento, que são, basicamente, outras empresas envolvidas no processo de tratamento dos dados.

Sobre o grave retrocesso ocasionado pelo tratamento de dados pessoais em larga escala, Bioni comenta:

> observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade. (BIONI, 2020, p.96).

## 2) OS DADOS PESSOAIS COMO UM DIREITO DA PERSONALIDADE

Após a Revolução Industrial, a dependência do ser humano em relação a tecnologias tornou-se algo vital. Para o bem ou para o mal, o mercado virtual domina cada vez mais as relações sociais. Da utilização do Pix ao reconhecimento facial na tela do celular, estamos diariamente e quase que instantaneamente expondo dados para terceiros. Apesar da naturalidade com que o ser humano passou a fornecer estas informações, é assustadora a sensação que se tem quando estas e outras informações são veiculadas sem o consentimento do indivíduo. E é diante disso que surge uma maior preocupação com o direito à privacidade. Porém, tal inquietude já era observadas em tempos longínquos como na Roma antiga, a figura do *jus utendi, fruendi et abutendi*, que assegurava o controle e amparo à vida privada. (FERNANDES, 1996).

Porém, é só com o advento da internet que aumentam significativamente os anseios relacionados à privacidade. Sobre o avanço, Carlos Alberto Bittar leciona:

> Esse direito vem assumindo, paulatinamente, maior relevo, com a contínua expansão das técnicas de virtualização do comércio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade de locomoção, do círculo relacional do homem, obrigando-se à exposição permanente perante públicos os mais distintos, em seus diferentes trajetos sociais, negociais ou de lazer. É fato que as esferas de intimidade têm se reduzido com a internet e meios eletrônicos. (BITTAR, 2015, p. 173)

Para compreender tal avanço, faz-se necessário que a personalidade física e humana, esta que sempre foi conhecida desde os primórdios da sociedade, atualmente é estendida, ou melhor, acaba por criar uma outra personalidade daquele mesmo indivíduo, porém está como personalidade virtual.

É a partir dessa nova personalidade criada no mundo virtual que surgem as mesmas características oriundas do mundo físico. Cada indivíduo tem suas informações e preferências (cor, idade, lugares mais frequentados etc.). Ora, tais preferências que já se faziam existentes no mundo físico, merecem garantia de não serem violadas sem consentimento também no mundo digital. A noção de privacidade parte do direito à solidão, em outras palavras, ficar em paz ou sozinho (NOJIRI, 2005).

Ora, por correspondência, este direito a solidão ou privacidade, transforma-se, dentro do meio digital, conforme nos explica RODOTÁ (2008, p. 92), no direito do sujeito de manter o controle sobre as próprias informações. Nesse sentido, há de se valorizar as escolhas pessoais, levando em conta o novo direito do indivíduo sobre o tratamento de seus dados.

Diante de tal análise, entende-se que a não proteção dessa personalidade virtual criada significaria não proteger também a personalidade da pessoa física titular desta mesma *persona* digital.

A tutela supracitada refere-se não só à tutela dos dados por parte de seu titular, mas também o conhecimento do tratamento que está sendo feito em relação a estes, afinal, a defesa dos direitos da personalidade engloba por si só a defesa dos direitos fundamentais constitucionalmente garantidos.

Em resumo, faz-se necessário entender os direitos da personalidade não como um rol taxativo definido meramente através do código civil brasileiro, ora desatualizado em relação ao tema do presente estudo, mas em uma visão ampla, o que abre caminho para o reconhecimento do direito à proteção de dados com um novo direito da personalidade (BIONI, 2020, p. 50).

Aliás, a referida visão mais ampla é inclusive praticada pelo STF que recentemente, confirmou a existência de "um verdadeiro direito fundamental à proteção de dados pessoais", como um "direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo", conforme voto do ministro Gilmar Mendes no julgamento ADI 6.387/DF. Desta forma,

a proteção dos dados pessoais adequa-se a uma categoria autônoma dos direitos da personalidade.

## 2.1) OS DESAFIOS DA TUTELA DO DIREITO À PROTEÇÃO DE DADOS:

Na mesma proporção em que se observa tentativa de proporcionar, através da tutela, maior poder de controle do indivíduo sobre suas informações, há uma exposição em massa através de ataques *hackers* ou outras modalidades de incidentes de segurança, tornando extremamente árdua a tarefa da legislação em proteger, através da lei, os cidadãos.

A causa de tal dificuldade está principalmente atrelada à falta de protagonismo da privacidade em prol do mercado e da livre concorrência. Para a manutenção de tal modelo, é necessária coleta, tratamento, venda e distribuição de dados em uma velocidade avassaladora para prospecção de clientes, direcionamento de publicidade e propaganda, desenvolvimento da persona, entre outras técnicas com fins comerciais.

Tal fato ocorre, muitas vezes sem o consentimento do indivíduo que, segundo a LGPD, é fundamental para o tratamento de dados ser válido. Aliás, alguns dados pessoais sequer deveriam ser utilizados para fins negociais, como é o caso dos dados pessoais sensíveis, mas não é o que ocorre na prática. Estes dados são classificados como qualquer dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. As bases legais que autorizam o tratamento dos dados sensíveis encontram-se no artigo 11 da LGPD. A principal diferença entre o tratamento de dados pessoais e dados pessoais sensíveis é que nesse último, como regra, a base legal aplicada é o consentimento, de forma específica e destacada, para finalidades específicas.

Com essa algoritimização dos dados pessoais, a produção e o próprio marketing das empresas passa a ser bastante especializado, buscando atingir o consumidor a nível mais profundo possível. Para tal, a maneira como se faz a coleta dos dados torna-se imprescindível para um estratégia realmente lucrativo para o agente tratador.

Um dos meios de coleta mais utilizados atualmente é através de *cookies*, instrumento já bastante visto por qualquer usuário de internet atualmente, mas pouco compreendido. Os cookies são nada mais que pequenos arquivos compostos por cadeias de números, que, ao serem instalados em um computador, permitem a sua identificação, sendo tão preciso que, ao retornar ao site onde aceitou os cookies inicialmente, o indivíduo é reconhcido automaticamente, sendo desnecessário que insira suas informações novamente, inclusive informações extremamente sensíveis como login e senha do usuário. Porém, cabe lembrar que a atuação dos cookies não se limita ao site em que houve o registro inicial. Para muito além de meramente salvar as informações iniciais do usuário, eles também funcionam de modo a expandir a coleta para outros sites que o indivíduo venha a visitar no futuro, a fim de que o servidor reconheça o usuário por diversos sites em que navega da internet, possibilitando, por exemplo, que comecem a aparecer na tela do usuário uma gama de anúncios personalizados. Normalmente as pessoas se perguntam como aquela propaganda apareceu e a resposta está no rastreio do conteúdo navegado pela pessoa na internet. Assim, fortalece-se o *profiling*, ou seja, a técnica de formação de perfis dos usuários a partir de seus dados de navegação, gostos, hábitos e preferências pessoais. Ainda que haja grande utilidade dos *cookies* para o próprio funcionamento da internet, a sua onipresença causa certa preocupação no âmbito de proteção da privacidade, especialmente ao se tratar de *third-party cookies* – *cookies* inseridos por terceiros, que não o site visitado pelo indivíduo – e cookies adaptados, como os *Flash cookies*, que são mais eficazes no rastreamento dos usuários e muito mais difíceis de serem removidos que os cookies tradicionais. O rastreamento se torna ininterrupto, colocando o usuário em considerável posição de vulnerabilidade, uma vez que o *profiling* permite a identificação de dados sensíveis. Para além disso, a comercialização dos perfis de usuários implica a transformação do ser humano em mera mercadoria, reduzindo sua autonomia. Com isso, entende-se que a questão não trata apenas de invasão da privacidade, mas também uma drástica redução da esfera da liberdade individual, visto que o rastreamento e a vigilância são aprimorados de acordo com o comportamento online do indivíduo, mas conforme "uma lógica que está fundamentalmente fora de seu controle.

## 3) A ERA DO BIG DATA E OS DADOS PESSOAIS COMO MERCADORIAS

É notório nos últimos anos que o mercado de *e-commerce* assume maior protagonismo no setor de varejo mundo afora, bem como no Brasil. Tal fato demonstra a migração do consumo para o meio digital, sendo também uma migração em massa dos dados de clientes e possíveis clientes para o meio digital. Ora, se antes as grandes redes de loja obtinham informações dos consumidores e as armazenavam em pequenos cadernos ou já mais atualmente em computadores de tecnologias mais robustas, hoje se tem a era do *Big Data* com o armazenamento em nuvem e compartilhamento de informações em massa. Aliás, através de técnicas de *machine learning* é possível, inclusive, desvendar informações do cliente que este sequer apresentou em seu cadastro no endereço virtual da empresa. Torna-se evidente que esta nova via expõe muito mais e de forma mais rápida as preferências, afinal, é esta a ideia do e-commerce no varejo.

As transformações sociais moldam a evolução digital. De uma necessidade humana por mais informações e novos meios de desvendar o próprio comportamento dos indivíduos, nasce esta ferramenta apelidada de *Big Data*, que possibilita o cruzamento de dados de diferentes ramos para mapear resultados precisos.

Para Mayer-Schönberger e Cukier (2013), o termo *Big Data* refere-se à percepção e compreensão das relações entre informações que, até recentemente, tínhamos dificuldade para entender. Com o alastramento da internet mundo afora, a quantidade de dados gerados também aumentou. Em 2012 por exemplo, já foram gerados em torno de 2,5 quintilhões de bytes de dados e 90% destes dados foram produzidos nos dois últimos anos aanteriores, demonstrando um crescimento exponencial. Com isso, estamos sujeitos a decisões tomadas por sistemas autônomos de inteligência artificial impulsionada por uma quantidade enorme de dados que procuram facilitar a vida dos seres humanos.

O referido aumento ocasionou demanda por um gerenciamento mais efetivo desta enxurrada de informações. Aliado a isso, a facilidade de se apresentar um produto através da internet, gerou nas empresas o sentimento de necessidade de compreender mais profunda e rapidamento o comportamento do ser humano. Assim, o *Big Data* surge no intuito de auxiliar na formulação de perguntas e para processar os resultados da análise de forma eficaz.

Diante disso, entende-se que o *Big Data* está amplamente ligado à velocidade com que se processa uma infinidade de dados em crescimento exponencial, permitindo que dela sejam extraídas informações de extrema relevância em uma velocidade nunca antes atingida.

É notório, portanto, que os tempos atuais demonstram um acúmulo de capital centralizado na informação, conhecido como Capitalismo de Vigilância (ZUBOFF 2019). Tal fato, no que tange o mercado do varejo torna-se muito evidente, já que grandes empresas deste seguimento, possuem robusta estrutura de comunicação, negociação e trade marketing baseada em *Big Data*. Tal ferramenta possibilitou não só a manutenção de dados de clientes em um banco virtual, mas a sua combinação com outros dados que por sua vez passa a ser capaz de prever comportamentos daquele cliente, como o próximo produto que o indivíduo X tem mais chances de adquirir em um e-commerce imediatamente após comprar o produto Y, sem expressamente perguntar para o indivíduo se ele optaria por determinada escolha.

A ideia do *Big Data* é tão genial quanto complexa. Para Zuboff, não se pode limitar a meras previsões, mas para atingir resultados realmente lucrativos, será necessário que esses prognósticos sejam ainda mais exatos e, para tal, imprescindível minerar a maior quantidade de dados possíveis. Este processo, para Zuboff, seria capaz não só de prever o comportamento humano, mas também modificá-lo como meio de produzir receitas e controle de mercado.

## 3.1) A UTILIZAÇÃO DE DADOS PESSOAIS COMO FERRAMENTA DE MERCADO NO VAREJO:

Em um cenário mundial de globalização e de crescimento exponencial na divulgação de informações através da internet, as inovações tecnológicas assumem papel protagonista na produção de riquezas e acúmulo de capital. Com isso, a informação torna-se o ponto focal da organização econômico-social, redefinindo o comportamento humano e precificando-o. Sobre o tema, Barreto Júnior (2015), discorre:

> O advento do Informacionalismo é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no qual há uma gradativa valoração da

> informação como mercadoria e fator de geração de valor econômico, o que torna a National Association of Securities Dealers Automated Quotations (Nasdaq), bolsa de valores das empresas tecnológicas, tão estratégica, em termos de organização econômica, quanto a tradicional New York Stock Exchange, denominada bolsa de Wall Street. As megacorporações informativas (Google, Facebook e Yahoo, entre outras) acumulam vestígios de informações sobre os usuários da Internet, tais como seus padrões de navegação, compras realizadas online, preferências culturais, religiosas e ideológicas, websites de interesse, verbetes e expressões pesquisadas nos websites de busca, entre outras, "impressões digitais eletrônicas" que servem para estabelecer uma categorização minuciosa de cada usuário na rede. [...] Circunscreve-se no fato de que há inúmeros usos para esses perfis eletrônicos, tal como direcionamento de publicidade on-line, oferta de mercadorias relacionadas ao perfil do consumidor, além de montar cadastros de valor incomensurável sobre os cidadãos da sociedade em rede. (BARRETO JUNIOR, 2015, p. 410).

Diante de tal análise, percebe-se que a informação, não só é mercadoria, como tem capacidade de, através de uma análise com auxílio do *Big Data*, ser a locomotiva que guia os indivíduos a consumirem a mercadoria desejada por determinada empresa.

Nesse sentido, BIONI (2020, p. 11) afirma não bastar a consideração da informação para que esta seja produtiva para determinada estratégia empresarial: é preciso convertê-la em conhecimento aplicado acerca do comportamento humano, mais precisamente sobre hábitos de consumo das pessoas. Assim, a nova ordem econômica utiliza dessas informações, que são dados sobre experiências humanas, como matéria prima para fins comerciais, segmentando campanhas para perfis específicos de consumidores e criando produtos cada vez mais personificados, que acabam guiando as escolhas dos usuários (BIONI, 2020).

Para a conversão destas informações em conhecimento, as empresas utilizam cada vez mais a ferramenta do *Big Data,* tendo em vista as características deste modelo citadas no capítulo anterior.

Não se pretende, por parte dos líderes de empresas, compreender o porquê de um determinado comportamento ou nova tendência. O que se quer atingir, na verdade, é a capacidade de encontrar relação entre determinados dados e até prever o que se pode ocorrer no futuro.

Uma vez atingido tal objetivo, o ser humano torna-se cada vez mais dependente das novas tecnologias. Em um gestão, seja ela em empresas privadas ou no ambiente da administração

pública, já se começa a enxergar os benefícios de mapear e traçar objetivos através da inteligência artifical. Durante a pandemia da COVID-19, por exemplo, ficou claro o quanto a utilização de informações, bem como o cruzmento de dados, ajudou prefeitos de diversas cidades a entenderem a hora certa de flexibilizar ou não as medidas sanitárias.

A utilização do mesmo raciocínio ocorre no meio privado. Ora, se as empresas controlam todos os dados de seus clientes e entendem que uma determinada categoria de produtos está vendendo menos que o esperado para determinado público em determinada época, esta companhia pode fazer campanhas promocionais direcionadas à parcela de clientes com a qual ela não está satisfeita com o consumo.

Nesse sentido, compreende-se que, de fato, o *Big Data* contribui para melhorar, do ponto de vista empresarial, a utilização dos dados dos clientes como ferramenta de mercado. Ora, não só capital em caixa, mais informações de usuários, passam também a ser considerados ativos financeiros para uma determinada marca. Afinal, quanto maior a captação de dados relevantes e cruzmento entre eles, maior será a capacidade que determinada empresa terá em influenciar o consumo dos seus clientes. Ou seja, não se trata mais somente de ter em catálogo os produtos que os clientes desejam, pois isso uma gama de empresas terá, mas para estar a frente do mercado, torna-se imprescindível proporcionar ao usuário uma experiência personalizada única, capaz de conduzi-lo ao consumo daquilo que a companhia realmente deseja vender.

Para isso, a corrida pelos cadastros em bancos de dados é infinita. Afinal, para realmente atingir o objetivo destacado no parágrafo anterior, é preciso alimentar constantemente os estes repositórios, com o maior número de informações possíveis. O que se vive hoje, em verdade, é a observação permanente do comportamento dos indivíduos, cujas informações e dados pessoais são matériaprima a ser explorada para geração de riqueza (BIONI, 2020, p.6).

É essa guerra por cada detalhe da vida do indivíduo, seja sobre um hábito noturno ou preferências de destino nas férias, que deixa o consumidor cada vez mais vulnerável, em uma sociedade na qual a velocidade da informação é tão rápida, que o próprio titular de dados não é mais capaz de recordar a quantidade de plataformas as quais forneceu o consentimento para tratarem seus dados, muito menos qual nível de informação foi fornecida para cada plataforma.

A verdade é que, ao fazer o download de um aplicativo em seu celular e consentir com a política de tratamento de dados, o consumidor não possui a real noção sobre as consequências daquilo que se pode extrair com das informações geradas; ele apenas consente, em troca de liberar seu acesso a alguma plataforma inovadora. Nessa mesma linha Frazão afirma:

> […] o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro trade-off entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares. (FRAZÃO, 2019, p. 31).

Diante de tal visão, torna-se pertinente iniciar um debate acerca da legitimidade da adesão a tais políticas. Ora, é certo que o ordenamento jurídico aponta para o consumidor como o lado mais frágil da relação e, por isso, preocupa-se com a efetivação de leis que tragam equilibrio para esta balança.

Porém, no modelo de consentimento às políticas de aplicativos, tem-se modelo igual a um contrato de adesão, no qual o usuário não tem oportunidade de debater quais tipos de dados ele concorda em fornecer à plataforma, se é que concorda com algum item da política. Para ir mais além, na prática, a maioria dos usuários se quer abre para ler qualquer frase, mas fica apenas limitado a ansiedade de utilizar o aplicativo de imediato, levando-o a consentir sem ler os risco que este modelo de contrato possui para si.

Em razão deste fato, fica evidente que tal mecanismo na verdade só reforça a assimetria do mercado digital de informações. O suposto direito à privacidade do indivíduo está bastante longe das violações que este sofre ao clicar em um botão de “aceito” em determinado aplicativo.

Essa desvantagem do consumidor torna-se ainda mais defasada, segundo Bioni, em decorrência das limitações cognitivas do ser humano, que o impedem de calibrar efetivamente as “gratificações e as perdas mediatas e imediatas necessárias para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais” (BIONI, 2020, pág 138).

Diante disso, o consumidor não possui qualquer chance de controlar efetivamente o destino de seus dados ou o tratamento que lhes será dado, podendo sofrer danos irreparáveis com determinados tipos de conduta das empresas, que sequer podem ser previstos, colocando o indivíduo em vulnerabilidade: há uma sobreposição de fraquezas que são característicos de uma nova vulnerabilidade (BIONI, 2020, p.38).

O presente trabalho não pretende fazer juizo de valor sobre o cenário, muito menos apontar existência ou não de ética nos diversos tipos de tratamento de dados feitos pelos diversos tipos de empresas. Apenas faz-se necessário acender um alerta nas empresas, afinal, da mesma forma que os dados servem como ativos financeiros para as empresas, o seu mau tratamento, armazenamento ou destinação, pode ocasionar perdas seríssimas para as mesmas companhias. Além disso, dada a pressão existente após o advento da Lei Geral de Proteção de Dados, não seguir as recomendações desta implica em não ser bem visto dentro do mercado como uma empresa confiável para se relacionar.

Diante do mercado do varejo, é evidente que o consumo é contínuo, ou seja, os clientes em sua maioria compram mais de uma vez nas diversas plataformas existentes, muitos inclusive irão comprar mercadorias em determinadas plataformas de e-commerce do varejo por muitos anos. Tal fato demonstra ainda mais a importância da aplicação correta da LGPD em suas plataformas, pois além da imagem passada para o restante do mercado acerca da confiabilidade da plataforma, uma plataforma que usa as ferramentas de Big Data corretamente e traça boas estratégias de tratamento de dados dentro da lei, tende a conseguir prever e, como já visto, modificar o compartamento do seu consumidor, perpetuando-o em sua cadeia de compradores.

Inclusive, esse poder dos grandes players do mercado do varejo torna-se ainda mais perigoso, dado que, devido ao consumo contínuo, se está diante de um mercado ainda mais capaz de conduzir o consumidor a mudar seus hábitos para outros que mais interessam à empresa. Ora, as empresas oferecem novos produtos para o consumidor após uma compra e assim ocorre por anos. Com isso, o mercado começa a controlar o cidadão.

Essa busca pelo consumidor tornou-se um jogo da sociedade moderna. E é buscando melhor igualar as regras que surge a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), buscando uma regulação específica sobre o tema, capaz de oferecer ao consumidor (lado mais

frágil da relação jurídica) algum poder de barganha capaz de reparar suas assimetrias frente às empresas. A legislação criou a expectativa de ser a única capaz de exercer o "importante papel de reforçar a autonomia dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre os seus dados" (FRAZÃO, 2019, p. 31).

## 3.2) O COMPLIANCE COMO MECANISMO DE MAIOR CONFIABILIDADE DAS ORGANIZAÇÕES:

Dada a problemática relatada no início deste capítulo e a profundidade dos riscos para as empresas quanto ao tratamento incorreto de dados pessoais, torna-se fundamental que as companhias destinem maior atenção para as questões que tangem a LGPD.

Nesse sentido, cabe um aprofundamento de toda a empresa através de treinamentos, em torno do que é a cultura do *compliance* e como aprimorá-la. Basicamente este termo significa estar dentro de determinados padrões éticos, podendo assim ser definido:

> O compliance, dentro do cenário corporativo e institucional, pode ser compreendido como um conjunto de disciplinas ou procedimentos que tenham por escopo fazer cumprir (to comply) as normas legais e regulamentares, bem como as políticas e diretrizes institucionais, além de detectar, evitar e tratar qualquer desvio ou inconformidade que possa ocorrer dentro da organização. 1
>
> SILVA, Daniel C.; COVAC, José R. Manual de Compliance. São Paulo: Editora de Cultura. 2015. p. 12.

Ora, se os dados são um ativo para as organizações, é válido todo esforço para, dentro da lei, minimizar os riscos do tratamento. Tal medida deve ser capaz de atingir todas as camadas da organização e todos os setores.

Embora o instituto tenha sua origem atrelada ao mercado financeiro, o compliance é amplamente utilizado pelas organizações privadas e governamentais, com uma incidência maior entre aquelas que estão sujeitas à forte regulamentação e controle pelo setor público.

É no *compliance* das empresas que se encontra figura capaz de instrumentalizar procedimentos internos de controle, bem como realizar o monitoramento de operações,

regulando condutas e as vinculando às multas e outras penalidades em caso de descumprimento das regras.

## 4) RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS:

Primeiramente, cabe definir que a Responsabilidade Civil é um instituto do Direito das Obrigações, visando garantir que haverá reparação de danos que prejudiquem determinados direitos de outros relacionados a uma determinada ação ou omissão por parte do autor. A violação, portanto, é ato ilícito que gera a obrigação de reparar e cria um vínculo jurídico que outorga a uma parte o direito de exigir da outra que cumpra determinada prestação (GONÇALVES, 2016, p. 45). Em outra passagem mais complexa, (GONÇALVES 2011, p. 24) explica: "A responsabilidade civil tem, pois, como um de seus pressupostos, a violação do dever jurídico e o dano. Há um dever jurídico originário, cuja violação gera um dever jurídico sucessivo ou secundário, que é o de indenizar o prejuízo.

Um importante exemplo do instituto da Responsabilidade Civil encontra-se no artigo 932 do Código Civil:

> Art. 932. São responsáveis pela reparação civil:
>
> I- os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;
> II- o tutor e o curador, pelos pupilos e curatrelados, que se acharem nas mesmas condições;
> III- o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho, que lhes competir, ou em razão dele;
>
> IV- os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos".

Ainda, importante também a observação do artigo 936 do mesmo código:

> **Art. 936.** O dono, ou detentor, do animal ressarcirá o dano por este causado, se não provar culpa da vítima ou força maior.

Diante dos exemplos, importante destacar que a responsabilidade se confunde bastante com uma obrigação, e de fato ambas possuem profunda relação. Porém, é importa lembrar que

a obrigação é o próprio dever jurídico originário, moldando o comportamento dos cidadãos conforme o ordenamento jurídico brasileiro. Por outro lado, a responsabilidade é classificada como um dever jurídico sucessivo, decorrente de uma violação do mesmo ordenamento jurídico.

Historicamente, os primeiros registros de responsabilidade civil, que vem do Direito Romano, têm viés de vingança, como a lei de talião, na qual o princípio do "olho por olho, dente por dente" é expresso. Posteriormente, tal pena transformou-se em responsabilidade do poder do Estado.

Com o avanço da história, na França napoleônica, nasce a culpa como pressuposto da responsabilidade civil – a culpa que hoje entendemos como fator que enseja modalidade subjetiva. Esse instituto da culpa foi fundamental para o desenvolvimento do ordenamento jurídico brasileiro.

Faz-se importante ressaltar que o conceito da Responsabilidade Civil perante a LGPD aparece na Seção III, do Capítulo VI, intitulada "Da Responsabilidade e do Ressarcimento de Danos", é formada pelos artigos 42 a 45 da LGPD.

Para análise da responsabilidade, é preciso se ater a alguns pressupostos, necessários que que o ato jurídico possa ter início, sendo necessária a análise de três requisitos para verificar a responsabilização: conduta ilícita imputada ao agente, o nexo de causalidade desta e por último analisar a extensão do dano sofrido. Passemos a uma análise breve dos requisitos:

Primeiramente, quanto a observação da conduta ilícita, é necessário observar o Código Civil brasileiro:

> Aquele que por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral ou no caso do titular de um direito que, ao exercê-lo, excede manifestamente os limites de seu fim econômico, social, em ofensa à boa-fé e aos bons costumes, comete ato ilícito (BRASIL, 2002, n. p.).

Percebe-se que o ordenamento jurídico estabeleceu que aquele, ainda que involuntariamente, tenha uma conduta e decorrente desta, venha causar danos na esfera de

direitos de outrem, comete ato ilícito e assim fica obrigado a reparar tais 21 prejuízos. Isto é, o agente de tratamento que causar danos no exercício da atividade de tratamento de dados, terá que indenizá-los a quem sofreu (GONÇALVES, 2020, p. 63).

O segundo elemento trata-se do nexo causal, sendo este a relação ou aquilo que conecta a conduta de determinado agente e o dano por ele causado, sendo também indispensável para imputar a responsabilidade civil a um agente. Ora, se um agente que realiza tratamento de dados acaba por praticar uma conduta, mas o resultado que atinge o mesmo titular dos dados tratados é totalmente adverso e sem relação com a conduta do agente, este obviamente não pode ser responsabilizado, tendo em vista não ter sido ele quem deu causa ao dano ocorrido ao titular.

Por fim, o terceiro elemento analisado é o dano, sendo este o prejuízo efetivamente causado ao titular dos dados. A sua inexistência afasta tanto a responsabilidade objetiva quanto a subjetiva, tendo em vista que determinada falha de um agente não chegou a gerar prejuízos para o titular dos dados. Nos dizeres de Venosa (2013, p. 38) tem-se versão esclarecedora sobre dano:

> Dano consiste no prejuízo sofrido pelo agente. Pode ser individual ou coletivo, moral ou material, ou melhor, econômico e não econômico. A noção de dano sempre foi objeto de muita controvérsia. Na noção de dano está sempre presente a noção de prejuízo. Nem sempre a transgressão de uma norma ocasiona dano. Somente haverá possibilidade de indenização, como regra, se o ato ilícito ocasionar dano. Cuida-se, portanto, do dano injusto, aplicação do princípio pelo qual a ninguém é dado prejudicar outrem (neminem laedere) (BAPTISTA, 2003, p. 47).

Diante de tal defnição, pode-se concluir que o entendimento de qual foi o real prejuízo causado ao titular é que irá definir a proporcionalidade da indenização cabível ao agente. Dadas as explanações iniciais acima, parte-se para análise mais profunda da matéria.

Não obstante a Lei Geral de Proteção de Dados tenha estabelecido um conjunto de princípios e regras que procuram criar um ambiente de responsabilidade proativa, de cunho preventivo, o risco potencial de ocorrência de lesão na coleta e tratamento de dados pessoais, especialmente ante os riscos inerentes à uma sociedade de classificação (FRAZÃO, 2019, p. 35), demanda a existência de um sistema de responsabilidade civil capaz de propiciar a efetiva tutela da vítima e a reparação integral do dano.

A LGPD dedicou um capítulo inteiro para a abordagem da Responsabilidade Civil dos agentes causadores de danos no que tange o tratamento de dados pessoais. Tal matéria está disposta entre os artigos 42 e 45 da lei 13.709/2018.

No artigo 42, tem-se uma abordagem mais generalista, na qual a preocupação é uma cláusula geral de responsabilidade, ou seja, imputa-se ao agente causador do dano a obrigação de indenizar caso descumpra a legislação de proteção de dados, causando dano patrimonial ou extrapatrimonial aos titulares dos dados pessoais violados. Vejamos o inteiro teor do artigo:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Ainda sobre o texto legal, observa-se, da leitura do §2º do artigo supracitado, que o legislador também possui uma preocução com a assimetria na relação entre consumidor x grandes empresas ou titular x agente tratador de dados, pois o §2º possibilita ao magistrado que proceda à inversão do ônus da prova dentro do processo. Tal fato é prova da hipossuficiência do titular de dados pessoais, oriunda da dificuldade que este teria em eventual produção de provas em um processo, afinal não é este quem tem acesso a todo o aparato onde seus dados foram armazenados e tratados.

Avançando um pouco mais na matéria, da leitura do artigo 43 observa-se as hipóteses de exclusão da responsabilidade, sendo tal fato possível quando o agente provar que i) não realizaram o tratamento dos dados pessoais, ii) se o realizaram, não violaram as normas de proteção de dados pessoais ou iii) que o dano foi causado por terceiro ou pelo próprio titular (art. 43, I a III):

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Observa-se portanto que há um rol taxativo, extremamente restrito, capaz de afastar a responsabilidade civil, não havendo razoabilidade para ampliar o rol, sob pena de novamente pender a balança da relação jurídica contra o lado mais frágil da relação.

Dada a hipótese acima, em seguida o legislador preocupa-se em esclarecer sobre o tratamento irregular de dados. A chegada da LGPD e o volume de debates sobre o tema, induz o cidadão comum à percepção de que o tratamento de dados é algo ruim. O artigo 44 da LGPD prova exatamente o contrário, apontando que, na verdade, existem algumas falhas comuns no tratamento que levam a irregularidades. O dispositivo demonstra que será o tratamento irregular quando contrariar a lei ou, ainda qu não o faça, ensejará a responsabilidade civil caso o tratamento feito não fornecer a segurança legitimamente esperada pelo titular dos dados (art. 44, I a III):

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Por fim, no artigo 45, último da Seção, a lei enfatiza que as hipóteses de violação continuam sujeitas à regra de responsabilidade prevista no Código de Defesa do Consumidor (Lei 8.078/90).

Diante dos dispositivos apresentados, entende-se haver no legislador, no magistrados, estudiosos e na sociedade como um todo, esforços no sentido de buscar a melhor solução interpretativa para a via de responsabilidade civil a ser utilizada perante à LGPD. Sobre tal desafio, o professor Gustavo Tepedino explica:

> Tais linhas teóricas compartilham o esforço de definição das soluções mais adequadas aos novos problemas. Identificam-se, nesse sentido, variadas formulações que enunciam princípios éticos próprios para a regulação dos robôs e demais sistemas autônomos. As célebres Leis de Asimov servem como boa representação do quanto exposto: o temor (ou encanto) das novidades tecnológicas parece instigar a formulação de novas regras e novas soluções. Empreende-se, assim, grande esforço para a concepção de respostas que se possam reputar adequadas aos novos desafios suscitados pela inteligência artificial. (TEPEDINO; SILVA, 2019, p. 70).

É essa tentativa de formular novas regras e soluções que acabam por quebrar a unidade do sistema jurídico, dificultando a orientação sobre uma linha única de tratamento do tema.

> A rigor, a enunciação de novo ramo do direito voltado especificamente para as questões da robótica e da inteligência artificial traz consigo o grave risco de tratamento assistemático da matéria. Os fundamentos para a tutela das vítimas de danos injustos não devem ser buscados em novos e esparsos diplomas normativos, mas sim – e sempre – no ordenamento jurídico em sua unidade e complexidade. A disciplina ordinária da responsabilidade civil – tanto em relações paritárias quanto em relações de consumo –, embasada na tábua axiológica constitucional, serve de fundamento suficiente para o equacionamento dos problemas referentes aos danos causados por sistemas autônomos. Advirta-se, por oportuno: o tratamento sistemático ora propugnado deve levar em consideração o ordenamento jurídico em sua unidade e complexidade, sem se cair na armadilha da enunciação de um (mais um chamado micro) sistema próprio de valores da lex robotica. (TEPEDINO; SILVA, 2019, p. 70-71).

É fato que a mesma tentativa supracitada revelou uma dupla interpretação sobre os artigos 42 a 45 da LGPD.

## 4.1) RESPONSABILIDADE SUBJETIVA

Parte da doutrina entende que a modalidade de responsabilidade civil mais adequada para casos envolvendo o tratamento de dados pessoais, seria a subjetiva. Há ainda aqueles que acreditam na relação com o risco, gerando responsabilidade objetiva. Tal fato é decorrente da imprecisão normativa quanto ao sistema de responsabilidade civil adotado pela lei protetiva. O embate doutrinário é travado entre posições que afirmam ter a lei estabelecido um sistema baseado na responsabilidade objetiva ou subjetiva, sendo respeitáveis os posicionamentos em ambos os sentidos. (TASSO, 2020, p. 104). É verdade, portanto, que a LGPD não trouxe clareza na modalidade cabível, cabendo aos estudiosos encontrarem melhor solução para o caso.

É evidente que o modelo subjetiva encontra amparo na doutrina, como observado a seguir:

> Os trabalhos preparatórios da LGPD deixam claro que sua política legislativa refutou
>
> deliberadamente um regime de reponsabilidade civil objetiva. Há outros elementos

> normativos que, direta ou indiretamente, convergem para que haja um juízo de valor em torno da culpa do lesante. Algo que não está apenas cristalizado no rol de excludentes de responsabilidade, mas, também, na principiologia e em outras partes importantes e integrantes do texto da LGPD. É uma racionalidade inescapável e que está por trás da lógica do regime de responsabilidade civil em questão. (BIONI E DIAS, 2020, p. 9)

Aprofundando a temática, importante analisar os comentários de Gustavo Tepedino, Aline de Miranda Terra e Gisela Sampaio da Cruz Guedes:

> "A lógica da responsabilidade objetiva é outra: não cabe discutir cumprimento de deveres, porque a responsabilidade objetiva não decorre do descumprimento de qualquer dever jurídico". Quando se discute cumprimento de deveres, o que no fundo está sendo analisado é se o agente atuou ou não com culpa. Assim, apesar de a LGPD não ser explícita em relação à natureza da responsabilidade dos agentes de tratamento de dados, como é o Código de Defesa do Consumidor ao adotar a responsabilidade objetiva, a interpretação sistemática da LGPD leva à conclusão de que o regime adotado por este diploma foi mesmo o da responsabilidade subjetiva.
> Não obstante as semelhanças com o Código de Defesa do Consumidor, é essencial destacar que, enquanto o Código de Defesa do Consumidor tem pelo menos dois artigos expressamente indicando a natureza objetiva da responsabilidade (arts. 12 e 14 – ambos se valem da expressão "independentemente de culpa", que deixa clara a opção do legislador pela responsabilidade objetiva), não há qualquer norma análoga na LGPD. O art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva".

Neste diapasão, é coerente retirar das análises dos defensores da responsabilidade subjetiva que a centralização da problemática na figura do cumprimento de deveres, para os defensores, tende a apontar a LGPD para o modelo de responsabilidade subjetiva.

> Da mesma forma, quando a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados, há ressalva de que tal responsabilização somente é deflagrada se não foram adotadas as "medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação". Trata-se de elementos que afastam a aplicação do sistema deresponsabilidade civil objetiva. (BIONI E DIAS, 2020, p. 9)

Nesse sentido, o artigo 927 do Código Civil estabelece que a obrigação da reparação dos danos causados a outrem se dá devido à aferição de ato ilícito, conforme o disposto nos artigos 186 e 187 do mesmo código. Ainda, para os defensores, segundo o disposto no parágrafo único do artigo 927, a responsabilidade objetiva é utilizada para casos específicos e, por isso,

excepcional, por exemplo, por ocasião de atividade representante de risco inerente ou ainda por expressa determinação legal. Com isso, conclui-se que, a justificativa da responsabilidade civil subjetiva encontra-se em um entendimento de que a atividade como um todo não possuiria risco inerente. Porém, tal visão é no mínimo contraditória, afinal o conceito de dados pessoais, como já visto, é extremamente abrangente. Ou seja, tratar uma gama enorme de dados de uma pessoa impõe a riscos intrínsecos, que integram sim o "risco inerente" previsto na parágrafo único do artigo 927 do Código Civil e, portanto, devem ser mitigados por parte das autoridades e até pela prevenção por parte dos agente tratadores.

A análise, para os defensores da modalidade subjetiva, tem fundamento pois, para eles, a LGPD não possui qualquer determinação expressa sobre responsabilidade civil independente de culpa. Para além, a lei demonstra que a conduta do agente tratador deve ser em violação da LGPD, ou seja, diante da inobservância do cumprimento dos deveres trazidos pelo diploma, colocando a culpa em sentido amplo como fundamento da responsabilização. Com isso, a reprovabilidade da conduta do agente de tratamento se vincula à violação do dever de observar os preceitos da LGPD. Porém, tal argumento não poderia ser a base para a definição da modalide de responsabilização, tendo em vista que, em um diploma legal inspirado em outra legislação, é natural que algumas questões não estejam expressamente vinculadas. É nesse sentido que se faz imprescindível analisar o ordenamento jurídico como um todo e entender o as diferentes previsões legais, bem como em que direção caminha o avanço histórico da responsabilidade civil.

Diante de tal análise, surge também o questionamento sobre se realmente há o risco inerente a atividade de tratamento de dados, tendo em vista a grande variedade das atividades de tratamento de dados pessoais. Há claramente atividades que pressupõem um risco menor, principalmente no que diz respeito a informações de baixa relevância em pequenos estabelecimentos. Tal fato, para os defensores do modelo de responsabilidade subjetiva, demonstra que não é coerente o argumento de "risco inerente" se for referido a atividade do tratamento de dados como um todo. Porém, tão visão parece ser muito pró-mercado, ignorando que há sim um risco inerente a toda e qualquer atividade de tratamento de dados, por menor que seja, além de não olhar para o fato de que é o titular dos dados o lado mais frágil da relação, mas não o agente de tratamento.

Um outro questionamento por parte dos defensores da responsabilidade subjetiva encontra-se no fato de que a LGPD traz alguns princípios necessários ao tratamento de dados, como é o caso do princípio da transparência. Este, para os defensores do modelo, traz o entendimento de que há um claro incentivo à prevenção. Com isso, torna-se imprescindível que a análise da responsabilidade não seja meramente objetiva, levando-se em conta fatores subjetivos como o risco do caso concreto e as políticas prévias adotadas pelo agente tratador. De todo modo, para os defensores do modelo subjetivo, considerando o foco da lei na conduta dos agentes – tanto que a responsabilidade e a transparência são princípios para o tratamento de dados pessoais – o entendimento por um modelo de responsabilização objetiva torna-se contraditório diante da própria lei que impulsiona os agente às referidas práticas preventivas.

Porém, no presente estudo entende-se que a interpretação do parágrafo anterior é errônea. É fato que a LGPD preocupou-se com um incentivo à prevenção, porém tal fato não ocorre para servir de "prêmio" ao mercado. Na verdade, este incentivo ocorre devido a possíveis graves consequências para os titulares de dados oriundas de um risco inerente ao negócio. É tão grande essa preocupação com o risco inerente, que a palavra "risco" aparece em diversos trechos da lei. Como clássico exemplo temos o disposto no artigo 44, inciso II:

> **Art. 44.** O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> II - o resultado e os riscos que razoavelmente dele se esperam;

Este não é o único exemplo, tendo a lei ofertado a palavra "risco" no inciso XVII do artigo 15; no parágrafo único do artigo 38; no artigo 48; no artigo 50; entre muitos outros. Tal fato demonstra que esse incentivo à prevensão é na verdade para mitigar o risco inerente que claramente existe no negócio de tratamento de dados.

Por último, os defensores da modalidade subjetiva entendem que a responsabilização objetiva dos agentes tratadores seria o mesmo que culpá-los pelos danos aos titulares, sem que aqueles tenham praticado qualquer tipo de conduta efetivamente contrária à legislação. Ou seja, alguns autores possuem o entendimento de que os agentes poderiam ser responsabilizados por ocorrências de dano aos titulares que não decorressem de qualquer previsão legal ou regulatória

sobre os parâmetros necessários ao tratamento de dados. Nesse cenário, ficaria a dúvida: se a conduta do agente não importa para a aplicação da responsabilidade, qual a razão para a adoção de boas práticas ou o investimento em medidas de adequação custosas? Portanto, a visão dos defensores da responsabilização subjetiva aponta para a análise da existência de culpa no caso concreto, como se a própria atividade de tratamento de dados não possuísse risco inerente ao negócio. Porém, é um fato que tal pensamento denota uma abordagem pró-mercado, que peca ao não enxergar o titular dos dados como o lado mais frágil da relação jurídica. Ora, "ao mesmo passo que os provedores desenvolvem ferramentas e aplicações cada vez mais sofisticadas para a captação dos dados e categorização dos consumidores, pressionam para que a legislação os isente de promover a tutela da personalidade dos usuários". (Martins, 2021).

Diante da presente análise, entende-se que os ensinamentos de professores como Gustavo Tepedino, Aline de Miranda Terra e Gisela Sampaio da Cruz Guedes são enriquecedores para o debate objeto do presente estudo, porém parecem, sob a desculpa do liberalismo, limitar-se ao ponto de vista do lado mais forte da relação ou, no mínimo, majorá-la, em detrimento da tutela necessária aos titulares de dados. Sobre tal movimento, o professor Guilherme Magalhães Martins leciona:

> É bem verdade que, recentemente, em especial no Brasil, é possível notar claramente um movimento de recuo no caminho narrado, até então percorrido no direito civil, amiúde contrário ao princípio da dignidade da pessoa humana e à proteção dos vulneráveis. Trata-se dos retrocessos legislativos, jurisprudenciais e doutrinários supostamente legitimados por um discurso da "liberdade econômica", que esconde um método perverso de relegar a vítima à própria sorte, resgatar a culpa como elemento central da responsabilidade civil, esvaziar o conceito de dano moral como um mero aborrecimento e, ao fim e ao cabo, demolir as conquistas de direitos refletidas no campo do Direito de Danos, ressuscitando o elemento subjetivo e afastando-se do risco como fator principal de imputação.

Diante disso, passemos a uma outra proposta de análise do modelo de responsabilização dos agentes tratadores de dados, cujos parâmetros parecem ser mais coerentes com a melhor aplicação da responsabilização dos agentes tratadores de dados, no intuito de promover a adequada reparação ao danos sofridos pelos titulares de dados.

## 4.2) RESPONSABILIDADE OBJETIVA

Em uma outra abordagem, há aqueles que acreditam em um modelo de responsabilidade objetiva, sendo esta a posição majoritária da doutrina. Por mais zeloso que seja o agente tratador de dados, nenhuma atividade humana é livre de riscos (DEVLIN, 2015, p. 99). No presente estudo, foi proposto anteriormente que as empresas (aplica-se também para outros agentes tratadores de dados), assumissem uma postura mais proativa. Tal cobrança ocorre justamente pelo entendimento de que o agente tratador assume um risco ao iniciar sua atividade, afinal tal postura é capaz de trazer frutos bastante lucrativos para este, enquanto para os titulares de dados, as possibilidades de violação são igualmente grandes e bastante obscuras no que tange as consequências de seu alcance.

Diferente do que entendem os defensores da responsabilidade subjetiva, o risco inerente ao negócio do tratamento de dados é evidênciado no artigo 42 da LGPD que traz a expressão "em razão do exercício de atividade de tratamento de dados pessoais". Este trecho deixa claro que o legislador já apontou para o próprio negócio de tratamento de dados como capaz de assumir controvérsias, sendo necessário garantir a tutela. E é justamente em decorrência deste risco que torna-se evidente que o texto legal do art. 42 está falando de modalidade objetiva em relação aos agentes de tratamentos, restando estes entendidos tanto na figura do operador, quanto do controlador, pois é assim que definem os dois incisos do § 1o do artigo 42 da LGPD,. Tal fato decorre do artigo 927, parágrafo único, do Código Civil, que demonstra incidir a obrigação de indenizar o dano, independentemente de existência de culpa, nos casos especificados em lei, ou ainda, como ocorre no caso da proteção dos dados pessoais, quando a atividade normalmente desenvolvida pelo autor do dano trouxer, por si só, risco para os direitos de terceiros.

Apenas para fins de maior clareza na matéria, as duas figuras expostas no parágrafo anterior (controlador e operador), apesar de sujeitas à mesma modalidade de responsabilidade, apresentam algumas divergências no que tange as consequências para cada um. Explica-se:

A partir da leitura do artigo 42, principalmente nos dois incisos do parágrafo 1º do artigo, verifica-se que o operador e controlador possuem condições diferentes para responder por possíveis prejuízos causados. O operador irá responder solidariamente somente quando

descumprir as obrigações previstas em legislação ou quando deixar de seguir as instruções do controlador. Desse modo, há uma violação por parte do controlador que gera a sua responsabilização.

Por sua vez, os controladores dos dados sempre responderão pelo tratamento de dados. Isso pois a LGPD em vários momentos estabelece obrigações específicas ao controlador, fazendo com que seja inviável a sua figura não estar envolvida no tratamento. A LGPD ao adotar essas medidas impossibilita que o operador se olvide de sua obrigação de tutelar os dados que estão em seu poder.

Retomando a análise do tipo de responsabilidade, a partir da leitura do artigo 44 da mesma LGPD, depara-se com a exigência de um certo padrão comportamental por parte do agente que realiza o tratamento de dados pessoais, isto é, estabelece deveres de resultado, tendo seu não cumprimento como consequência a responsabilidade, não falando em prova de culpa. Através desta cobrança de padrão comportamental, fica ainda mais evidente que é desprovida de sentido aquela argumentação dos defensores da responsabilidade subjetiva, de que a atividade de tratamento de dados não se enquadra nas condições do parágrafo único do artigo 927 por não haver risco inerente ao modelo de negócios. Ora, qual seria o sentido do legislador exigir padrões comportamentais mínimos se não houve qualquer risco inerente ao negócio? É evidente que que o artigo 44 é a manifestação expressa de um receio quanto ao tratamento feito de forma irregular. Afinal, deixar o tratamento a cargo de cada a gente tratador significaria tornar impossível o controle do que é feito com os dados tratados. Além disso, o artigo 6º, inciso X, da LGPD demonstra claramente uma preocupação com a prevenção, sendo mais um fator que aponta para a existência de uma atividade de risco. É neste sentido que o livro "The right to Privacy" traz lição a favor da reparação sem aquela prova de culpa:

> Se a invasão de privacidade constitui um dano jurídico, existem os elementos para exigir reparação, uma vez que já é reconhecido o valor do sofrimento psíquico, causado por ato ilícito em si mesmo, como fundamento da indenização.

Deste modo, a legislação parece certeira ao atrelar a atividade como um todo ao risco. Afinal, também não faz sentido aquela argumentação de que se está inibindo o desenvolvimento econômico ao adotar a responsabilidade objetiva. Ora, se os grandes *players* do mercado global criam um grande sistema baseado em *big data e big analytics*, no qual é criado também um

*one-way mirror*, onde apenas o lado mais forte da relação (os agentes tratadores de dados) enxergam, não há qualquer absurdo em em exigir que os danos causados nos tratamentos de dados pessoais sejam reparados por aqueles que lucram com atividades feitas utilizando estes mesmos dados. Afinal, é de se convir que o custo dos riscos existentes, bem como de suas reparações, são infinitamente menor que a possibilidade de lucro característica do modelo de negócio.

> É racional imputar responsabilidade por danos a quem agiu exatamente como deveria ter agido quando o sujeito passivo da obrigação de indenizar ocupa posição econômica que lhe permita socializar os custos da sua atividade entre os beneficiários dela. Nessa posição encontram-se, por exemplo, os empresários, o Estado e as agências de seguro social (ULHOA, 2018, 528).

Muito se questiona também, principalmente por parte das empresas e daqueles que defendem a modalidade de responsabilidade subjetiva, quanto aos casos de incidentes de segurança alheios às políticas da empresa ou invasão de sistemas por terceiros (muito conhecida como invasão de *hackers*); há o argumento de não ser justo a quebra da liberdade econômica por prática de crimes alheios à conduta do agente tratador. Porém, segundo a professora Caitlin Mulholland, tais casos devem ser tratados como fortuito interno, não podendo ser afastada a obrigação de indenizar dos agentes de tratamento em virtude de tais fatos. (Mulholland, 2021). Ora, a análise da professora tem fudamento, pois se assim não fosse, não haveria de se implementar melhorias após uma invasão de terceiros, possibilitando com que estas se tornem cada vez mais recorrentes, uma vez descoberta a forma de "entrar" por parte dos invasores, principalmente se os prejuízos forem maiores para o consumidor e não para a empresa. Além disso, há de se abordar também que o artigo 6º, inciso VI, da LGPD demonstra a preocupação com a questão da transparência, vejamos seu teor:

> Artigo 6º:
>
> VI: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

Nesse sentido, conclui-se que há clara importância dentro da LGPD, não só da necessidade de maior prevenção, mas também de promover aos titulares de dados a informação precisa sobre quais foram as consequências exatas de uma eventual invasão de *hackers*, bem como evitar, ao menos na medida do alcance do agente tratador, que os efeitos da invsão se

perpetuem, aumentando o dano para o titular. Nesse sentido, entende-se que a responsabilização subjetiva não é coerente, pois mesmo após um eventual ataque hacker, a atuação do agente tratador, bem como sua responsabilidade, não se encerram.

Outro questionamento dos defensores da modalidade subjetiva manifessta-se no relato de que o próprio risco existe em diferentes níveis e que, supostamente, não faria sentido tratar dentro da mesma modalidade de negócio, agentes de realidades completamente diversas. Em uma grande plataforma de e-commerce que faz uso de inteligência artificial, por exemplo, tem-se um risco inerente muito maior se comparado a um pequeno negócio com volume de dados menor com destinação apenas informativa Tal fato, apesar de ser verdade, deve ser resolvido de outra forma. Não se deve, por existir diferentes níveis de tratamento, dar um grande benefício ao agente, afinal tal fato acabaria por desequilibrar a balança em desfavor dos titulares dos dados. A solução não pode ser oferecer o benefício da responsabilidade subjetiva. Na verdade, a política mais sensata a ser realizada deve ser a fiscalização baseada no princípio da prevenção, podendo ser exigido um maior nível de proatividade para grandes *players* do mercado, dada sua maior capacidade econõmica, bem como ser poder de influência dentro da sociedade.

No que tange a responsabilidade civil no âmbito das relações de consumo, menos ainda há qualquer sentido em argumentar contra a responsabilidade objetiva, pois tendo em vista uma visão do ordenamento jurídico brasileiro como um todo para a mitigação de eventuais vácuos em legislações específicas, é expressa a menção legal presente nos artigos 12 e 14 do Código de Defesa do Consumidor, que adere claramente a teoria do risco criado. Vejamos o teor dos artigos 12 e 14 da Lei 8.078/1990:

> Artigo 12:
>
> "o fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de seus projetos".

> Artigo 14:
>
> "O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos."

Além disso, não haveria qualquer coerência se a LGPD tivesse criado um sistema de proteção de dados pessoais se, na concretização deste, ele fosse débil ou factualmente inútil, propiciando uma situação de perpetuação do estado de lesão a um direito de personalidade (BARRETO JÚNIOR; CAVALCANTI; LEITE, 2018, p. 523). A própria tentativa de justificar a responsabilidade subjetiva parece ignorar a assimetria da relação jurídica entre o titular de dados pessoais e o agente tratador. Não se pode permitir que os grandes players se escondam atrás de uma escusa de liberdade econômica para evitar a reparação de danos. Como visto, a tendência precisa ser de facilitar a reparação, não torná-la impossível.

Para os estudiosos defensores da responsabilidade objetiva, entende-se que a argumentação a favor da responsabilidade subjetiva gira muito em torno da onerosidade para os agentes tratadores de dados. É quase como se estes admitisse a existência de falhas ou irresponsabilidades no tratamento. Não é uma interpretação que atrela a responsabilidade civil na LGPD ao risco que impossibilita o lucro, que é tão inerente ao negócio no tratamento de dados pessoais, quanto o seu risco. Pelo contrário, como já visto, uma postura voltada a ouvir o *compliance* da empresa, bem como nele investir, pode e deve ser capaz de reduzir riscos e maximizar lucros. Com isso, trazer uma interpretação de responsabilidade objetiva pode também servir como fator motivacional para exigir cada vez mais uma postura proativa dos agente tratadores de dados. Aliás, tal exigência deve ser vista não como uma falta de incentivo econômico, como alegam defensores da modalidade subjetiva de responsabilidade civil, mas como uma previsão legal capaz de proteger ainda mais o consumidor, baseada na prestação de contas prevista no artigo 6º, X, da própria LGPD, vejamos seu teor:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Tal dispositivo revela o princípio da prevenção, no qual torna-se possível que restrições sejam impostas aos grandes *players*, cujo potencial ofensivo é notavelmente maior para o titular dos dados.

Em direção oposta ao que afirmam os defensores da tese subjetiva, a imputação da responsabilidade objetiva no advento do Código Civil e do Código de Defesa do Consumidor,

não inibiu a inovação e o desenvolvimento de novas tecnologias, mas certamente as tornou mais seguras e impediu a socialização dos riscos de desenvolvimento (e dos danos a eles relacionados), imputando o dever de reparar àquele que exerce a atividade e assegurando a efetiva proteção das vítimas de danos injustos, a ponto de não surpreender a descoberta (ou desenvolvimento) de um ―princípio da proteção da vítima‖ na interpretação do sistema civil-constitucional vigente:

> Cuida-se, porém, de falso dilema, pois a história já demonstrou que a adoção dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não limitaram o desenvolvimento de novas tecnologias. Ao contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade fundado na atenção e no cuidado para com o lesado. Ademais, já pontuava Rodotà, o argumento de eventual aumento dos custos de proteção dos dados pessoais para as empresas não é decisivo, vez que não se pode considerar que interesses ligados à proteção de dados pessoais dos titulares sejam de status inferior aos interesses empresariais. (MORAES, 2019, p. 4)

Superadas questões relacionadas ao impedimento do desenvolvimento das tecnologias, torna-se importante demonstrar como o ordenamento jurídico europeu, através do GDPR, trouxe soluções para a controvérsia, já que a Seção sobre responsabilidade civil na LGPD é quase uma tradução literal da lei europeia.

## 4.3) SOLUÇÕES TRAZIDAS PELO GDPR PARA A RESPONSABILIDADE CIVIL:

Na Espanha, por exemplo, há a interpretação, através de uma conjunção com regras do direito interno, que o GPDR ilustra uma hipótese de responsabilidade civil objetiva, de modo que, uma vez verificada a ocorrência da infração de uma das obrigações relativas ao tratamento de dados pessoais prevista no RGPD que tenha ocasionado os danos suportados pela vítima, o responsável deverá repará-los sem que possa provar eventual ausência de culpa de sua parte (Puig, 2018), motivos pelos quais apenas são admitidas como teses de defesa as excludentes do nexo causal de praxe. Na mesma linha dos ibéricos, no Reino Unido, nação que adota o tort law como sistema de responsabilidade civil, interpreta-se que o art. 82 do GPDR encerra hipótese

de “strict liability”, ou seja, adota-se o entendimento de que o dever de indenizar será imputado ao agente causador do dano independentemente da prática de uma “fault” (Fortuna, 2020).

Porém, a definição não é de fácil conclusão. Em países como Portugal, por exemplo, tem-se uma interpretação da responsabilidade civil mais favorável ao modelo subjetivo. Talvez inclusive seja por isso que a GPDR procurou não dar uma definição para o modelo de responsabilidade a ser aplicado, no intuito de respeitar a tradição dos diversos países integrantes, o que não faz sentido no Brasil, tendo em vista que obviamente não há dentro do ordenamento, outros ordenamentos de outros países a serem respeitados. Tal fato, inclusive, reforça a hipótese supracitada de ser observar o ordenamento jurídico e seus diplomas anteriores à LGPD no Brasil para, assim, dar a interpretação mais coerente com a tradição nacional.

## 4.4) APLICAÇÃO PRÁTICA DA RESPONSABILIDADE CIVIL

Apesar de todo o exposto no campo teórico e tendo em vista que o presente estudo não se propoe a buscar respostas, mas sim a criar novos questionamentos, faz-se necessário passar a uma abordagem mais prática da matéria, visando compreender o que realmente ocorre no cotidiano do tratamento de dados. Como já visto no presente trabalho, as questões que permeiam a LGPD e o tratamento de dados pessoais não são uma unidade, possuindo particularidades a depender das partes envolvidas.

O ser humano em geral, em pleno 2022, já não consegue terminar um dia sequer, sem autorizar que alguém faça o tratamento de seus dados. Seja em um aplicativo de seu celular através dos *cookies* como já citados anteriormente, seja no balcão de atendimento de um médico, ou ainda ao participarmos de uma promoção, estamos constantemente aceitando políticas de uso e tratamento dos nossos dados. Sabemos mesmo do que se trata este “aceite” e quais as suas consequências?

Diante de tal fato, faz-se necessário compreender a importância da tutela feita através da legislação específica surgida com o advento da LGPD. É apenas com a legislação e a intensa fiscalização que se pode atingir a efetivação do direito de reparação do titular dos dados (lado mais fraco da relação) ou ainda a redução da quantidade de danos causados aos titulares, através

da exigência de proatividade incentivada pelo artigo 6º, inciso X, da lei. E é imperativo que, após toda a análise feita no presente estudo, a tutela seja buscada através de um modelo objetivo de responsabilização dos agentes tratadores de dados. Resta pontuar que qualquer tentativa de insistir em um modelo subjetivo de reparação, é na verdade um projeto de apagar parte dos avanços conquistados com a evolução histórica da responsabilidade civil, que passou da culpa para o risco. Aliás, este já é o entendimento adotado pelo judiciário brasileiro. Vejamos a atuação do TJSP ao condenar a Concessionaria da Linha 4 do Metro de Sao Paulo S.A. (via Quatro)

> Ante o exposto, JULGO PROCEDENTES EM PARTE os pedidos, com resolução do mérito, na forma do artigo 487, I do Código de Processo Civil, para (i) determinar que a requerida se abstenha de captar as imagens, sons e quaisquer outros dados pessoais dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4 Amarela do metrô, sem consentimento prévio do consumidor, confirmando a liminar anteriormente concedida pela decisão de fls. 327/332; (ii) determinar à requerida que, caso deseje readotar as práticas tratadas nos autos, deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e tratamento dos dados, com adoção das ferramentas pertinentes; e (iii) condenar a requerida ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00, corrigida segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo, desde a data da publicação da sentença, e com juros de mora de 1% ao mês, incidentes a partir da citação, por se tratar de ilícito contratual, na forma do artigo 405, do Código Civil, a ser revertido para o Fundo de Defesa de Direitos Difusos FDD, criado na forma do artigo 13 da Lei nº 7.347/85. Deixo de condenar a parte autora em honorários de advogado, custas e despesas processuais, pois ausente má-fé, na forma do artigo 18 da Lei nº 7.357/85. Em razão da sucumbência recíproca com relação ao IDEC e isenta a parte autora, condeno a requerida ao pagamento de metade despesas processuais e custas, incluindo as iniciais, observado o valor atualizado para 2021 e o teto de 3.000 UFESP, atualizadas monetariamente desde a data do desembolso segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo, e com incidência de juros de mora 1% ao mês, quando da execução definitiva, a partir do decurso do prazo de 15 dias para pagamento do débito ora fixado, consoante o artigo 523, do Código de Processo Civil, bem como honorários advocatícios em benefício do autor, arbitrados no patamar de 10% do valor corrigido da condenação, nos termos do artigo 85, §2º, do Código de Processo Civil e acrescido dos juros de mora de 1% ao mês, na forma acima mencionada para as custas e despesas. Com relação à Defensoria Pública, condeno a requerida ao pagamento das custas e despesas processuais, atualizadas monetariamente desde a data do desembolso segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo, e com incidência de juros de mora 1% ao mês a partir do decurso do prazo de 15 dias para pagamento do débito ora fixado, consoante o artigo 523, do Código de Processo Civil, , bem como honorários advocatícios em benefício do órgão, arbitrados, por equidade, em R$5.000,00, nos termos do artigo 85, §§2º e 8º, do Código de Processo Civil e acrescido dos juros de mora de 1% ao mês, na forma acima mencionada, a ser revertido ao fundo gerido pela Defensoria Pública, conforme artigos 85, §19º e 91 do Código de Processo Civil e

> artigo 4º, XXI da LC nº 80/94. Sem condenação em honorários com relação ao amicus curiae, por falta de amparo legal. Se interposto recurso de apelação, intime-se o(a) apelado(a) a apresentar contrarrazões no prazo de quinze dias e, após, remetam-se os autos à Seção competente do E. Tribunal de Justiça, acompanhados de eventuais mídias e objetos arquivados em cartório, independentemente de juízo de admissibilidade, nos termos do art. 1.010, § 3º, do Código de Processo Civil. Com o trânsito em julgado, aguarde-se por 5 (cinco) dias eventual pedido de cumprimento de sentença. Após, tomadas as medidas pertinentes para a cobrança das custas devidas, ao arquivo, observadas as cautelas legais. P.R.I. e ciência ao MP. Julgada Procedente em Parte a Ação

Para fins de maior explicação da atuação proposta, pontua-se que a utilização do modelo objetivo, diferentemente do que pensam os defensores da responsabilização subjetiva, não é uma utilização meramente teórica da lei. Pretende-se sim que a análise do modelo de responsabilização seja cada vez mais aberta, levando em consideração cada caso concreto como único, afinal a internet está em constante e rápida mutação. Nada obstante que surjam novas teorias daqui em diante. Porém, o que se pretende concluir no presente estudo é no sentido de que a responsabilização sempre deverá ser analisada priorizando os titulares de dados, afinal é na direção destes que surge a tutela proposta na LGPD.

## 5) CONSIDERAÇÕES FINAIS:

O crescimento tecnológico exponencial que tem sido observado desde meados do século XX, mas com maior clareza a partir do início do século XXI, torna a discussão sobre a proteção dos direitos à privacidade e principalmente aos dados pessoais mais relevante do que nunca. Se outrora a classificação da privacidade como simples direito de defesa pode ter sido suficiente para garantir a sua tutela, atualmente não o é mais. É certo que a era do *Big Data* e das grandes empresas de *e-commerce*, além das grande redes sociais chegou para transformar a velocidade da propagação de informações através do mundo digital, modificando também os problemas referentes ao Direito à Privacidade, tendo em vista que tal direito passou a ser enfraquecido em razão do avanço tecnológico. Não se trata de um enfraquecimento meramente ocasional em decorrência das máquinas e suas tecnologias, mas de um modelo programado pelos grandes atores políticos, econômicos e sociais para maximizar o lucro na sociedade da informação. Tal modelo, apesar de passar amplamente pela utilização de máquinas, é a pura aplicação da

mentalidade humana, em sua faceta cada vez mais capitalista e cada vez mais globalizada e descentralizada.

Com o surgimento do *Big Data*, as relações dentro da internet tornaram-se algo extremamente agressivo. Tal sistema, permitiu, principalmente a empresas e governantes, que fosse feita uma combinação com diversos dados, gerando resultados bastante significativos sobre os indivíduos e capazes até de mudar o comportamento deles. O problema é que isto não ocorre de maneira inofensiva. Desde o repasse de informações entre plataformas para encarecer um serviço para um indivíduo até influenciar em eleições de um páis, o advento do *Big Data* tornou-se algo tão genial quanto perigoso para a sociedade.

Em um mercado como o varejo, por exemplo, onde o consumo muitas vezes é contínuo, ou seja, há maior fidelização do cliente, a tendência é que após a compra de um item, o consumidor receba indicação de um novo item e assim ocorre eternamente. Com isso, aos poucos a empresa, através do *Big Data*, vai entendendo e prevendo o compartamento do indivíduo. Neste movimento, a empresa começa a tornar-se capaz de modificar o comportamento da população, através de um one-way mirror, derecionando as pessoas para onde o capital quiser e, como consequência, para onde quem tem capital e poder, quiser.

Em razão de uma disseminação de informações e dados em velocidade nunca antes vista, surge a necessidade de tutelar os direitos dos indivíduos dentro de uma tela, seja de computador ou de celular. É como se, metaforicamente falando, a personalidade do indivíduo começasse a aparecer do outro lado da tela, e o Direito reconhece isso. Os dados passam a ser reconhecidos como um direito da personalidade. Além disso, o assunto ganha *status* de Direito Fundamental através da Emenda Constitucional 115/2022.

É neste sentido que surge a LGPD, com o intuito de mitigar os efeitos da relação desigual entre usuários e grandes empresas, que se aproveitam de cada passo do consumidor para traçar suas estratégias de marketing e outros procedimentos. Bastante influenciada pelo GDPR europeu, inclusive com artigos traduzidos quase que literalmente do diploma europeu, a lei traz dispositivos importantes para o tema como o modo correto de realizar o tratamento de dados, bem como sua coleta, a necessidade de prevenção, além da importância de se basear em

princípios como os da necessidade, transparência e segurança, além de dispor sobre a responsabilidade civil dos agentes, tema este de bastante discussão como já visto.

Diante do já demonstrado impacto que o diploma da LGPD impõe principalmente aos cidadãos e às empresas, torna-se pujante a definição das obrigações dos agentes de tratamento de dados e, consequentemente, delimitar o regime jurídico para sua responsabilização, bem como analisar a possibilidade de ações individuais em decorrência de danos causados em violação ao disposto na lei.

Apesar das inovações, a lei motiva muitos debates de estudiosos e operadores do direito, entendendo-se como um dos focos do problema a fraqueza do método para adquirir o consentimento do titular do dado. Apesar de a LGPD definir o consentimento como uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados, não é o que ocorre na prática, mesmo quando falamos de dados pessoais, para os quais é exigido um consentimento mais específico. O modelo acaba por ser um contrato de adesão, na qual o consumidor não tem a possibilidade de negociar os termos e, inclusive, muitas vezes não os lê. Aliás, a política dos *cookies* é, no mínimo, controversa para o lado do consumidor, a partir do momento em que gera um rastreio constante das informações, além de possibilitar que elas envolvam outros sites visitados pelo usuário ( *third-party cookies*).

É desta forma que as empresas acabam conseguindo coletar uma número inimaginável de informações, elaborando grandes bases de dados, que violam o direito à privacidade desses indivíduos, bem como o livre desenvolvimento da personalidade humana e o direito à autodeterminação informativa, prevista expressamente ao longo da Lei Geral de Proteção de Dados (LGPD). A descentralização dessas bases torna possível a implementação do capitalismo de vigilância, dificultando o rastreio do destino das informações do usuário, fundamental para a manutenção do poder das grandes empresas e Estados sobre o cidadão, que ainda carece de maior proteção, mesmo com a entrada em vigor da Lei Geral de Proteção de Dados. Vive-se o famoso *one-way mirror*, pelo qual só quem enxerga são os agentes tratadores, mas nunca os titulares. Afinal, é esta a ideia dos tratadores: quando você não paga pelo serviço, é porque o serviço é você.

No intuito de mudar tal panorama, torna-se imprescindível que os agentes tratadores de dados de boa-fé reúnam seus esforços para maior adequação à Lei Geral de Proteção de Dados, dado sua previsão de que todos que realizarem tratamento de dados, devem atentar-se para o texto legal. É possível manter o alto padrão de lucro inerente ao sistema capitalista sem violar as regras da LGPD.

Porém, é um fato que não se pode esperar uma mudança advinda de quem somente espera a maximização de lucros, ou muitas vezes não consegue vislumbrar os benefícios de se adequar as leis.

Foi justamente não esperando que agentes tratadores e titulares de dados se autorregulassem, bem como visando uma aplicação mais coerente com o problema que a legislação se preocupou, nos seus artigos 42 a 45, em garantir a reparação dos danos causados ao lado mais frágil da relação. Tais prejuízos, como visto, são oriundos da existência de um risco inerente ao modelo de negócio do tratamento de dados como um todo, fator pelo qual, apesar da ausência de recomendação expressa, enseja a responsabilidade civil objetiva dentro da LGPD. Tal fato é o fator reparador, o peso faltando na balança da relação jurídica entre titular de dados e agentes tratadores de dados, balança esta que era provida de assimetria em prejuízo do lado mais fraco da relação. Além disso, dado que a própria responsabilidade civil como um todo evoluiu historicamente da culpa para o risco e que o titular de dados ficou ainda mais fragilizado com o avanço rápido da internet, por não possuir todo um aparato econômico por trás, não faz sentido aplicar o modelo subjetivo de responsabilidade, na qual a culpa precisa ser analisada e o tratador normalmente resta beneficiado.

O caminho para lograr a mudança pretendida pela legislação está também no âmbito da prevenção, com um maior investimento em programas de *compliance,* capazes de estipular novos programas para treinamento dentro das empresas, bem como regular internamente o correto tratamento dos dados os quais a empresa tem acesso. Porém, para que isto seja alcançado, torna-se pujante que seja exigida cada vez mais, por parte do judiciário, no que tange o julgamento dos casos, exigindo o cumprimento do artigo 6º, inciso X, da LGPD, no qual é incentivada a prevenção. Como visto, essa exigência não passar por ignorar o caso concreto e tratar todos os agentes tratadores como iguais, mas é justamente este trecho da lei o fator capaz

de diferenciar grandes *players* do mercado global e pequenos comerciantes, sem falar em ensejar a responsabilidade subjetiva.

Diante do que foi visto no presente estudo, bem como nos demais citados como referência, sem o intuito de esgotar o debate do tema ou extrair verdades universais, entende-se ser necessário criar uma cultura de tratamento ético dos dados pessoais. A atividade de tratamento de dados é de alto risco e não pode ser deixada meramente à *mercê* da escusa de liberdade econômica. É imprescindível uma boa tutela dos titulares de dados, no sentido de promover uma cultura de consumo mais consciente e mais justa, sem em qualquer momento reduzir o lucro inerente ao modelo privado de negócios, mas fazendo-o quando necessário para garantir os direitos da coletividade. Para os agentes de tratamento, sejam eles uma grande empresa privada ou um agente do Estado, a LGPD já pode se mostrar uma grande aliada às empresas que melhorarem sua forma de enxergar dados, podendo elevar seus lucros, sem deixar de respeitarem os direitos e garantias fundamentais dos indivíduos.

## REFERÊNCIAS:


BARRETO JUNIOR, Irineu Francisco. **Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (orgs.). Direito & Internet III. São Paulo: Quartier Latin, 2015. p. 100-127.

BAUMAN, Zygmunt. **Vigilância líquida:diálogos com David Lyon.** Rio de Janeiro: Zahar, 2013, p. 7.

BAUMAN, Zygmunt. **Vigilância líquida**. 2013. p. 10.

BAUMAN, Zygmunt. **Vigilância líquida**. 2013. p. 10.

BAUMAN, Zygmunt. **Vigilância líquida**. 2013. p. 11.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense. 2019. p. 63-65.

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

BIONI, Bruno Ricardo; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor.** Civilistica.com, Rio de Janeiro, ano 9, n. 3, p.1-23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 fev. 2021.

FRAZÃO, Ana. **Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados.** In: TEPEDINO, Gustavo;

FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: FRAZÃO, Ana;

GONÇALVES, Carlos Roberto. **Responsabilidade Civil.** 17. ed. São Paulo: Saraiva, 2016.

GONÇALVES, Carlos Roberto. **Responsabilidade civil.** 19 Ed. Saraiva Educação SA, 2020.

Harvard Law Review, vol. IV, 15 de dezembro de 1890, n° 51890. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Magalhães Martins, Guilherme. **The Brazilian General Data Protection Law (Law 13,709/2018) and its principiology.** Revista dos Tribunais | vol. 1027/2021 | p. 203 - 243 | Maio / 2021. DTR\2021\7888

MAYER SCHONBERGER, Viktor, Kenneth Cukier. **Big Data: A Revoution That Will Transform How We Live, Work and Think**, 2013.

MULHOLLAND, Caitlin. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. p. 3.

PUIG, Antoni Rubí**. Daños por infracciones del derecho a la protección de datos personales: El remedio indemnizatorio del artículo 82 RGPD.** Revista de Derecho Civil, [s. l.], v. V, n. 4, p. 53-87, out-dez. 2018, p. 10, tradução nossa.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008

SILVA, Tarcisio. **Colonialismo de dados é fruto e arma da supremacia branca.** 2021. Disponível em https://tarciziosilva.com.br/blog/colonialismo-de-dados-e-fruto-e-arma-da-supremacia-branca/

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor.** Cadernos Jurídicos: Direito Digital e proteção de dados pessoais, São Paulo, ano 21, n. 53, São Paulo, jan./mar. 2020, p. 97-116.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **Desafios da inteligência artificial em matéria de responsabilidade civil.** Revista Brasileira de Direito Civil – RBDCivil, v. 21, Belo Horizonte, jul./set. 2019, p. 61-86.

TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52. ISBN 978-85-5321-663-5. p. 24.

TEPEDINO, Gustavo; Terra, Aline de Miranda; Cruz Guedes, Gisela Sampaio da. **Fundamentos do Direito Civil** (pp. 236-252). Forense. Edição do Kindle. Harvard Law Review, vol. IV, 15 de dezembro de 1890, n° 51890. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

WARREN, S.; BRANDEIS, L. The Right to Privacy. civilistica.com, v. 2, n. 3, p. 1-22, 14 out. 2013. Tradução nossa

ZANFIR-Fortuna, Gabriela. Article 82. **Right to compensation and liability**. In: KUNER, Chistopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. The EU General Data Protection Regulation (GDPR): A commentary. Oxford: Oxford University Press; 2020. p. 1160-1179. p. 1176. No mesmo sentido: VAN ALSENOY, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, JIPITEC, n. 271, 7 (2017). Disponível em: [https://www.jipitec.eu/issues/jipitec-7-3- 2016/4506]. Acesso em 14/03/2021.