



**PUC
GOIÁS**



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÕES
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
MONOGRAFIA JURÍDICA

**CULPA OU RISCO: UMA ANÁLISE DA RESPONSABILIDADE CIVIL NA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

ORIENTANDO (A) – GILMARA KELLEN MACÊDO SANTOS
ORIENTADORA – PROF.^a DR.^a FERNANDA DE PAULA FERREIRA MOI

GOIÂNIA-GO
2022

GILMARA KELLEN MACÊDO SANTOS

**CULPA OU RISCO: UMA ANÁLISE DA RESPONSABILIDADE CIVIL NA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicações, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof.^a Orientadora Dra. Fernanda de Paula Ferreira Moi.

GOIÂNIA-GOIÁS

2022

GILMARA KELLEN MACEDO SANTOS

**CULPA OU RISCO: UMA ANÁLISE DA RESPONSABILIDADE CIVIL NA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Data da defesa: 28 de maio de 2022.

BANCA EXAMINADORA

Orientador(a): Prof. Dra. Fernanda de Paula Ferreira Moi.

Nota: ____

Orientador(a): Prof. André Aidar

Nota: ____

AGRADECIMENTOS

Gostaria de agradecer ao meu pai, Gilmar, por sempre acreditar e patrocinar meus estudos, minha mãe, Jael, por me ensinar desde criança como devem ser os caprichos na vida escolar, ensinamentos que trouxe comigo para a vida acadêmica. Ao meu namorado, Matheus pelo apoio com os livros e aparelhos eletrônicos, sem deixar de mencionar a inspiração nas fases de bloqueio. Aos meus amigos que conheci na faculdade a quem dedico enorme carinho e que tornaram essa jornada mais leve: Gefferson, Luenes, Izabella Menês, Haytanna, Gustavo, Roberta, Elisa, Andressa e Izabella Reis.

SUMÁRIO

RESUMO	6
ABSTRACT	7
INTRODUÇÃO	8
1 DO DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS	11
1.1 NOÇÕES DE DIREITO À PRIVACIDADE.....	11
1.2 CENÁRIO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS	16
1.3 A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO	21
2 DA RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO	26
2.1 CONCEITOS BÁSICOS	26
2.2 ELEMENTOS DA RESPONSABILIDADE CIVIL.....	27
3. ANÁLISE DA APLICAÇÃO DA LGPD EM CASOS CONCRETOS	33
3.1 TJ-SP – APELAÇÃO CÍVEL: 10168440320208260068	33
3.2 RECURSO INOMINADO: 0707016-12.2021.8.07.0016	36
CONSIDERAÇÕES FINAIS	40
REFERÊNCIAS BIBLIOGRÁFICAS	42

RESUMO

O presente trabalho tem como objetivo observar sobre a aplicação da responsabilidade civil, em sede de LGPD, no caso concreto. Para tanto, foi preciso refletir acerca do direito à privacidade e como a Lei Geral de Proteção de Dados Pessoais, bem como demais dispositivos que visam tutelar este direito fundamental. A ideia de privacidade atual, apesar de manter, em certo ponto, o traço individualista que possuía em anteriores veículos jurídicos, vai além do direito de solitude, e, como caráter de direito fundamental, busca igualdade e liberdade de escolha. Neste sentido, aponta-se um estudo dos dispositivos dentro do ramo do direito civil que dispõem a respeito do que concerne o direito à privacidade e do instituto da responsabilidade civil como um todo.

PALAVRAS-CHAVE: Direito. Privacidade. Responsabilidade civil. Dados Pessoais.

ABSTRACT

The present work has as a goal describe the application of civil responsibility on specific cases. For that, it was necessary to reflect about the right to privacy and General Personal Data Protection Law, and how other legal provisions claim to protect this fundamental right as well. The current idea of privacy, even though kept an individualistic that use to have on legal provisions, goes beyond the right to be left alone and, as a fundamental right, claims for equality and freedom of choice. About that matter, a study concerning the civil law was done to explain the right to privacy and the civil responsibility as a whole.

KEYWORDS: Law. Privacy. Civil Responsibility. Personal Data.

INTRODUÇÃO

O presente trabalho monográfico carrega em si o ousado objetivo de analisar em a aplicação da recente Lei brasileira de Proteção de Dados Pessoais, no que tange a responsabilidade civil neste e em outros dispositivos legais que mantenham relação com o direito fundamental à privacidade.

Todo o nosso ordenamento jurídico é voltado para a proteção de bens jurídicos. No estudo em prisma, o bem jurídico tutelado pela Lei Geral de Proteção de Dados Pessoais é a privacidade

O fornecimento de dados de origem pessoal é evidentemente necessário no cotidiano das relações sociais e comerciais. Isso se dá desde o preenchimento de um formulário para uma matrícula em academia, escolha ou universidade, até o cadastro de informações de e-mail para ter acesso algum site na internet. A partir de então, a maneira como tais plataformas e instituições fazem uso dos dados fornecidos podem gerar problemas e prejuízos financeiros, cabendo então, ao Direito entrar em atuação de forma a regular este âmbito das relações humanas.

O século XIX foi marcado pelo magnífico ensaio publicado por Warren e Brandeis, em 1890. A revista Harvard Law Review foi o veículo utilizado para a divulgação deste artigo. A partir de então, diante dos marcos da revolução tecnológica, o direito à privacidade tornou-se foco dos juristas, tendo, nessa época, uma conotação para o “direito de ser deixado só”.

A ideia de privacidade atual, apesar de manter, em certo ponto, o traço individualista de Warren e Brandeis, vai além do direito de solitude, e, como caráter de direito fundamental, busca igualdade e liberdade de escolha. A liberdade de escolha ligada à privacidade está intrinsecamente agregada à autodeterminação informativa, que também é um dos fundamentos da LGPD (art. 2o, inc. II). Por este fundamento, o indivíduo tem a liberdade de decidir sobre o tratamento de seus dados, podendo se opor ou interromper o tratamento.

Ademais, como direito fundamental, em nossa Constituição, a privacidade engloba a intimidade e a vida privada. Devido sua tamanha importância, esse bem jurídico também é assegurado em outras Cartas fundamentais, como a da União Europeia, onde também é garantido de forma em que a vida privada e, na Carta exemplificada, vida familiar, é inviolável.

Destarte, a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 18 de setembro de 2020, foi criada para proteger os direitos fundamentais de privacidade de cada indivíduo, bem como regular os direitos dos titulares de dados. Com um conhecimento mais concreto acerca do tipo de responsabilidade civil em se tratando de objetiva ou subjetividade, os titulares de dados, bem como os indivíduos que os forneceram, podem, antes de adentrar no contencioso, verificar mais facilmente se estão presentes os requisitos do dever de reparar exigidos pela LGPD. E, até mesmo já dentro de um processo judicial, suas partes – requerente, requerido e juiz – poderão se nortear em maior grau satisfatório no momento de colher e analisar o conteúdo probatório necessário à satisfação do conflito de interesses.

Em um levantamento realizado pela empresa Juit, até junho de 2021, foram contabilizados 598 processos judiciais que discutem a violação de dados pessoais por diversas empresas e corporações no Brasil.

Assim, podemos inferir que a LGPD pode se tornar, em um futuro demasiado próximo, um novo contencioso em massa. Tal evento ocorre em função do território novo abrangido pela nova Lei, que por vigência já vincula os agentes titulares de dados a evitarem a prática de possíveis atos ilícitos. Estes, podem ser penais, administrativos e civis, dos quais nos é relevante, neste trabalho, apenas o último.

Para tanto, é preciso refletir sobre como o direito à privacidade se relaciona com a proteção de dados pessoais, merecendo seu espaço como direito fundamental, de forma que um cidadão, caso precise da tutela jurisdicional se sinta amparado enquanto civil, consumidor, titular de dados, entre outras posições possíveis dentro dos ramos do direito alcançados por nosso ordenamento jurídico.

Posto isso, estudaremos como a reponsabilidade civil se comporta no direito brasileiro para que haja melhor compreensão do que o legislador pretendeu ao elaborar os artigos que fixam a responsabilização dos tratadores de dados em caso de ato ilícito danoso.

O primeiro pilar da responsabilidade civil é o ato ilícito. O art. 42, caput da LGPD, fixa que o indivíduo que causar dano a outrem, independentemente do tipo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Por meio deste artigo, podemos verificar o que determina um ato ilícito: uma conduta que causa dano a outrem ao infringir alguma norma. Mais precisamente, de acordo com Flávio Tartuce, 2018, o ato ilícito ocorre quando uma conduta humana age em

desacordo com a ordem jurídica e causa danos a alguém, ferindo direitos subjetivos e privados.

Como segundo pilar da responsabilidade civil, temos o abuso de direito. Este, ao contrário do ato ilícito, tem um conceito fluido, que pode ser melhor consolidado no caso concreto

Por fim, há de se expor os casos concretos escolhidos para análise, a fim de que se observe não só o olhar do legislador acerca da temática estudada, mas também a visão do judiciário, bem como a importância da proteção da vida privada e da intimidade do cidadão na prática.

1 DO DIREITO À PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

1.1 NOÇÕES DE DIREITO À PRIVACIDADE

Privacidade é uma palavra de origem latina, derivada do verbo *privare*, sendo seu adjetivo *privatus* (DONEDA, 2021, p. 105). Apesar de suas percepções estarem associadas, originalmente, ao sentido de “fora do grupo, algo separado do coletivo”, como noção de propriedade. Ainda hoje, principalmente em países de *common law*, as normas de tutela da privacidade possuem fundamento na proteção da propriedade privada. Mas não somente nos Estados com herança da *common law* tratam da privacidade na conotação de propriedade. No Brasil, por exemplo, a inviolabilidade do domicílio e da correspondência são de matéria da privacidade, ainda atrelada à propriedade.

De início, com a privacidade tendo ligação direta com a noção de propriedade, variavam entre “situações subjetivas patrimoniais e não patrimoniais” (DONEDA, 2021, p. 112). A herança deixada pelo direito romano, bem como as contribuições do cristianismo, aliadas às vozes da filosofia tiveram papel fundamental para a criação desse direito que tutelaria a vida privada, que apresenta um caráter subjetivo. Subjetivo porque, a noção que existe uma dicotomia entre o público e o privado, evidencia que existe uma exclusão, que é de escolha do indivíduo.

Embora já houvesse o reconhecimento da necessidade de tutela desse novo direito da personalidade, sua origem se deu apenas de forma doutrinária, não sendo tratado em nenhum Código Civil, tampouco Constituições durante o século XIX.

A privacidade, em diferentes períodos e sociedades, era utilizada com suas fartas acepções, por meio de costumes, tendo, porém, palco como direito fundamental após a Segunda Guerra Mundial, com a Declaração Universal dos Direitos do Homem, aprovada em 1948, na Assembleia Geral das Nações Unidas.

A noção de privacidade, em si, não é recente – com os diversos sentidos que apresenta, pode ser identificada nas mais variadas épocas e sociedades. Porém, a privacidade começou a ser concretamente abordada pelo ordenamento jurídico somente no final do século XIX para, enfim, assumir as suas feições atuais apenas muito recentemente (DONEDA, 2020, p. 29).

A Guerra gerou uma necessidade maior da valorização dos direitos da pessoa humana, pois, é impossível negar que no período entre Guerras, bem como durante, houve grande negligência dos direitos humanos fundamentais. Em consequência, a proteção desses direitos se tornou temática principal das Convenções Internacionais em escala mundial, tais como a Convenção Europeia dos Direitos do Homem, Convenção Americana dos Direitos do Homem, também conhecida como “Carta de San José”, bem como a Carta dos Direitos Fundamentais da União Europeia. A partir de então, tendo abrigo como direito fundamental, a privacidade consegue maior espaço para ser tutelada nos ordenamentos jurídicos dos Estados Nacionais.

A revolução tecnológica também trouxe maior urgência em discutir a necessidade de se definir os moldes do direito à privacidade, uma vez que os novos mecanismos tecnológicos, tais como a fotografia e seu auxílio a jornais e veículos de comunicação ampliaram a viabilidade de disseminação de informações condizentes à vida privada das pessoas.

O artigo “*Right to privacy*”, de Brandeis e Warren - obra de demasiado apreço no tocante ao direito à privacidade – traz uma reflexão justamente acerca dos novos inventos tecnológicos, em especial a fotografia que aprimorou o trabalho da imprensa. Os autores apontam no artigo que a *como law* deve ser transformada para que o direito à privacidade seja respeitado à medida que novas tecnologias de cunho informático surjam.

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right to be let alone. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life (...) (...) and the question whether our law will recognize and protect the right to privacy in this and other respects must soon come before our courts for consideration (BRANDEIS, WARREN, 1890, p. 195-196)¹.

A *privacy* norte-americana, então, abordada no artigo supracitado, difunde o direito à privacidade como “o direito a ser deixado só”, que transmite uma noção individualista da temática, com a segurança de que cada individual possui o direito de

¹ Invenções recentes e métodos de negócios chamam atenção para o próximo passo que deve ser tomado para a proteção da pessoa e para a segurança do indivíduo – o que o Juiz Cooley chama de o direito de ser deixado só. Fotografias instantâneas e a iniciativa do jornal tem invadido locais sagrados da vida privada e doméstica (...) e o questionamento de que nosso direito reconhece e protege o direito à privacidade nesse e em outros aspectos deve chegar em breve em nossos tribunais para consideração.

determinar, ordinariamente, quais extensões de seus pensamentos, sentimentos e emoções podem ser comunicada a outros.

Já o direito brasileiro tutela o direito à privacidade dividindo-o em dois bens jurídicos, que, em teoria, são distintos: “intimidade” e “vida privada” (art. 5º, X, da CF/88). A distinção presente nos bens jurídicos é baseada na Teoria das Esferas de Henrich Hubmann.

O embasamento da distinção do Constituinte brasileiro pode ser encontrado na teoria das esferas de Heinrich Hubmann, segundo a qual o sentimento de privacidade do indivíduo pode ser compreendido a partir de um esquema de círculos concêntricos, que representam diferentes graus de manifestação da privacidade: no núcleo estaria a esfera da intimidade ou do segredo (Geheimsphäre); em torno dela, viria a esfera privada (Privatsphäre); e em torno de ambas, em um círculo de maior amplitude, encontrar-se-ia a esfera pessoal (Öffentlichkeitsbereich), que abrangeria a vida pública do indivíduo (MENDES, 2008, p. 21).

A propósito, além das terminologias utilizadas pelo legislador constituinte, nosso ordenamento jurídico também faz uso de vocábulos como: sigilo, segredo, intimidade da vida privada, dentre outros que podem variar de acordo com o interesse jurídico em questão. Essa diversidade de nomenclaturas não ocorre apenas no âmbito jurídico brasileiro, sendo possível observá-la também, por exemplo, no sistema doutrinário norte-americano, com a *privacy*, que, apesar de consolidada, é amplamente utilizada dentro de inúmeras situações. Situações estas que, para um jurista brasileiro, não estariam relacionadas com a privacidade.

Isso ocorre devido à evolução histórica do direito brasileiro, que vem de uma tradição oriunda do *civil law*. Desta forma, qualquer jurista que tenha seu direito resultante do *civil law*, pode encontrar dificuldade em pautar as situações abrangidas pela *privacy* norte-americana, a qual possui suas origens nos moldes *common law*. A diferença básica entre tais modelos jurídicos está localizada na fonte imediata do direito. Ou seja, a jurisprudência como fonte imediata do direito, característica da *common law*, concede um leque maior de cenários que a *privacy* consegue abarcar. Enquanto, no *civil law*, a fonte em questão é a lei, possuindo o legislador, então, o condão de determinar as respectivas circunstâncias que podem ser englobadas pelos vocábulos que a privacidade pode compreender.

No *civil law*, ocorre a codificação das leis, com um direito escrito, de forma que a lei exerce maior peso nas decisões judiciais, e, a jurisprudência, apesar de ser

relevante, não se sobressai ao lado da lei predeterminada. Sendo assim, para o jurista brasileiro, é mais relevante compreender os cenários da privacidade conhecida pelas terminologias abrangidas pela lei e não os entendimentos jurisprudenciais que podem trazer cenários diferentes, que não são, para a lei, concernentes ao direito à privacidade.

A privacy norte americana, o droit au secret de la vie privée ou simplesmente la protection de la vie privée na França; o diritto alla riservatezza (ou a segretezza) na Itália (ou mesmo a privacy, termo usado no país); a reserva da intimidade da vida privada (Portugal); o Derecho a la intimidad na Espanha; a noção da Die Privatshphäre, que divide a autonomia individual e a vida social, presente na doutrina da Alemanha; a integritet da Suécia, que compreende a noção pela qual as pessoas têm direito de serem julgadas de acordo com um perfil completo e fiel de sua personalidade; são algumas das designações utilizadas para se referir ao complexo de interesses que remetem ao termo privacidade (DONEDA, 2021, p. 101)

O termo “vida privada” no contexto da Carta Maior brasileira implica que existe uma divisão entre o que é de vida pública e vida privada. Enquanto que “intimidade” faz referência às circunstâncias particulares e pessoais, subjetivas da pessoa, que são determinadas pela confiança individual.

Mesmo com a ocorrência da presente diferenciação em nosso conjunto legislativo, entre “intimidade” e “vida privada”, na prática, quando há uma violação do direito à privacidade, a distinção conceitual entre os vocábulos não é suficiente para suscitar em uma sequela jurídica significativa (PEREIRA, 2021). Para que haja relevância jurídica, o discernimento entre “intimidade” e “vida privada” deve ser funcional, uma vez que o perigo à violação do direito à privacidade não está intrinsecamente ligado ao nível de intimidade, tampouco ao sigilo de determinado dado. O que determina a gravidade da violação deste direito é seu potencial discriminatório.

Sob essa perspectiva, é importante retomar a distinção conceitual efetuada pela Constituição Federal entre “vida privada” e “intimidade”. Muito embora a norma suprema mencione ambos os termos, tal distinção não deve operar efeitos jurídicos na tutela da privacidade pelo direito brasileiro, porque, tanto o seu âmbito de proteção, como as suas limitações, assim como os efeitos de sua violação, independem da distinção entre “vida privada” e “intimidade”, razão pela qual se entende que tal distinção não deve ser tratada juridicamente. Isso porque a gravidade da violação ao direito à privacidade não estará relacionada necessariamente ao grau de intimidade ou de sigilo de determinada informação armazenada, mas, por exemplo, ao seu potencial

discriminatório, como ocorre nos casos de dados sensíveis (MENDES, 2008, p. 22)

Além disso, a própria doutrina ao tratar da temática não refinou a questão a ponto de eleger apenas um termo e, sendo a primeira vez que o constituinte brasileiro explora o tema como direito fundamental, provavelmente decidiram manter um leque maior de terminologias para que a norma não tivesse sua aplicação reduzida.

Pelos motivos expostos acima, embora nosso ordenamento jurídico utilize ambos os termos supracitados na tutela do direito em questão, para a explanação aqui objetivada, a terminologia “privacidade” é ampla e suficiente. Afinal, a própria jurisprudência brasileira utiliza do termo na seara de suas decisões, como observa-se no RESP nº 306570/SP: “O contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais (...)” (rel. Min. Eliana Calmon, D.J. 18/02/2002); e também no Mandado de Segurança n. 23639/DF, onde o Ministro Celso de Mello, do STF (D.J. 16/02/2000) verifica uma “eventual ruptura dessa esfera de privacidade das pessoas” no contexto de uma errônea escuta telefônica. Em suma, a aceitação da terminologia “privacidade” para tratamento da temática é satisfatória e de aceitação na alçada jurídica brasileira.

Na visão de Gustavo Nojosa Pereira (2021, posição 359), o direito à privacidade é um “controle do indivíduo sobre suas informações”, “consiste na possibilidade de a pessoa controlar, tanto quanto possível a massa de informações sobre si mesma a que outros podem ter acesso”. Trata-se de uma autodeterminação informativa, onde a informação pessoal é de substância objetiva e cabe à pessoa humana, que é um ser de direitos, construir sua esfera privada livremente. Para Alan Westin (1967, p. 7), “privacidade é a reivindicação de indivíduos, grupos, instituições para determinar, quando como e em que extensão, informações sobre si próprios devem ser comunicadas a outros”.

Nesse prisma, pode-se concluir que privacidade é a possibilidade de escolher a se opor ou não acerca da interferência alheia no que é de informação pessoal de cada ser humano, sem excluir o direito de obter acesso a qualquer dado que venha a ser coletado por outros, no que tange a personalidade individual de cada indivíduo.

O direito à privacidade, entretanto, não se traduz em um direito absoluto, pois, sendo o homem um ser social, não pode e não consegue ser excluído da vida em sociedade. Para a manutenção da interação social, este direito é limitado para que haja um equilíbrio entre os direitos individuais e coletivos.

Para que haja a harmonia entre o coletivo e o privado, o direito à privacidade não pode ser utilizado para ferir “outros direitos e princípios do ordenamento jurídico, tais como a liberdade de imprensa, a criação cultural, a segurança dos cidadãos, a autonomia pública, entre outros” (MENDES, 2008 p. 26).

A tutela do direito à privacidade, em seu aspecto de autodeterminação informativa, evoluiu, então, por intermédio das normas de tratamento de dados pessoais. Nas palavras de Gustavo Nojosa (2021, posição 567): “tanto o direito à privacidade, como a proteção de dados pessoais fundamentam-se na proteção da personalidade e da dignidade do indivíduo”.

Sabe-se que na atual fase tecnológica em que a sociedade se encontra, **a informação é um dos bens de maior valor**. Por esta razão, **a sua proteção deve ser questão de importância máxima, merecendo a atenção do legislador** (FINKESTEIN, 2019, p. 5, grifo nosso)

Diante do exposto, torna-se evidente que a divulgação e utilização de algum dado pode afetar diretamente a privacidade de um indivíduo. Para evitar que o direito à privacidade seja violado, as normas evoluíram, de forma que legisladores de diversos estados nacionais passaram a elaborar dispositivos para tratamento de dados pessoais, assunto que será abordado a seguir.

1.2 CENÁRIO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS

Como previamente estabelecido, privacidade, nos moldes atuais, atua como um direito fundamental voltado para a autodeterminação informativa, ou seja, possui uma estrutura voltada para a informação ligada, especialmente aos dados pessoais.

Com as novas tecnologias que possibilitaram maior veiculação de dados pessoais, dos indivíduos, o tema passou a ter maior palco em composições jurisprudenciais e legislativas nas últimas décadas. O Tribunal Constitucional Alemão foi um grande impulsionador da autodeterminação informativa, com ideais voltados para garantir o direito de acesso de informações armazenadas por instituições públicas.

O olhar voltado para a proteção de dados pessoais permite que a privacidade e os princípios que a norteiam sejam reavaliados de modo que diversas perspectivas, em especial, novas formas de controle “tornadas possíveis com o tratamento de dados

personais” (DONEDA, 2021, p. 177). O Ministro Ruy Rosado, no âmbito do Recurso Especial 22.37/RS (grifo nosso), proferiu em voto:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar a devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de direitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.

Percebe-se então que o tratamento de dados pessoais é uma atividade de risco, pois, carrega em si o perigo de ser utilizado de forma abusiva e errônea. Assim, fica evidente a urgência para a criação de instrumentos que permitam ao indivíduo o controle sobre seus dados. Afinal, trata-se de um direito fundamental necessário para garantia da proteção da pessoa humana.

A doutrina aponta a década de 1970 como a principal em relação ao surgimento de intentos legislativos voltados para a tutela de dados pessoais, abrangendo leis classificadas como de “primeira” e “segunda geração”.

Entre as precursoras, a já mencionada Lei do Land alemão de Hesse, em 1970, a primeira lei nacional de proteção de dados que foi, na Suécia, o Estatuto para bancos de dados de 1973 – *Datalog* (1973:289) (que por sua vez também criava um inspetor para o uso de dados pessoais – o *Dataispektionen*), além do *Privacy Act* norte-americano em 1974 (DONEDA, 2021, p. 179)

As leis de proteção de dados pessoais de primeira geração estavam voltadas para a atuação do Estado. Ou seja, as normas de proteção informacional de cunho pessoal eram voltadas para os órgãos estatais administrativos e estes seriam os responsáveis pela colheita e administração dos dados pessoais. Sendo assim, o poder

de concessão de permissões para abertura de bancos de dados era de competência apenas do Estado.

Contudo, em razão do aumento elevado de núcleos processadores de dados, as normas de primeira geração não eram suficientes para abarcar e gerir demasiado crescimento de bancos de dados. Por isso, os conteúdos normativos se tornaram obsoletos em curto tempo. Em consequência, ainda na década de 1970, sobrevieram as leis de segunda geração para cuidar do tratamento de dados pessoais.

A segunda geração de leis sobre a matéria surgiu a partir da segunda metade da década de 70, já com a consciência da “diáspora” dos bancos de dados informatizados; pode-se dizer que o seu primeiro modelo foi a lei francesa de proteção de dados pessoais de 10978, intitulada *Informatique et Libertés* (...) Como representante desta geração de leis, podemos mencionar também a lei austríaca, além de que as menções às constituições portuguesa e espanhola, já mencionadas, apontam neste sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde (DONEDA, 2021, p. 181-182).

Essa geração de leis foi responsável por fazer uma inserção do cidadão na decisão de como seus dados seriam tratados. Assim, os legisladores voltaram o olhar para a privacidade como uma liberdade negativa, de maneira que o Estado teria uma menor atuação na matéria.

Isso se deu, pois, além do crescimento de centros processadores de dados, já mencionado anteriormente, os cidadãos passaram a sofrer ainda mais com a utilização de suas informações pessoais por terceiros e, o Estado já não conseguia defender tais ofensas de forma a preservar os interesses individuais de cada cidadão. As normas dessa geração criaram mecanismos que possibilitaram ao indivíduo detectar se suas informações estavam sendo utilizadas de forma indevida, e desse modo, o mesmo poderia tomar ações para melhor proteger sua privacidade.

O paradigma tecnológico mudou em relação às leis anteriores, e assim as técnicas de controle utilizadas não se dirigiam diretamente à tecnologia. O mecanismo de autorização para o funcionamento de bancos de dados se apresenta diluído, quando não substituído por mera notificação de sua criação; a atividade de supervisão das autoridades de controle transforma-se em uma atuação como *ombudsman*, como auxiliar da administração pública ou mesmo como órgão para-jurisdicional (DONEDA, 2021, p. 182).

Da mesma maneira que as leis de primeira geração, as de segunda geração também enfrentaram impasses. Agora, com a liberdade do processamento de dados

voltada para o cidadão, tornou possível refletir que a entrega de certos dados pessoais era imprescindível para a manutenção da ativa presença do indivíduo na vida em sociedade. Já não era mais viável a efetiva participação do cidadão no exercício de sua liberdade interromper o curso de certos dados, pois, este feito passou a acarretar, em regra, na exclusão do sujeito de algum prisma da vida social. Ora, se o exercício de um direito agora provoca a lesão de outro direito, é evidente a necessidade de um aprimoramento na gestão do tratamento das informações pessoais humanas.

Diante dos novos impasses, na década de 1980, surgiu a terceira geração de leis voltadas para a proteção de dados pessoais. A partir dessa geração, os legisladores buscaram priorizar o contexto em que os dados dos cidadãos eram requeridos, de maneira que ainda haja uma escolha do indivíduo proprietário do dado pessoal, podendo este exercer sua liberdade, sem que seja excluído de qualquer âmbito do convívio social. O maior objetivo dessa geração de leis era garantir o real implemento da autodeterminação informativa. Nas palavras de Lugati e Evangelista de Almeida (2020, p. 5) “A terceira geração de leis se preocupa mais com a tutela do direito à privacidade, indo além da liberdade de ceder ou não os dados, mas sim em garantir a efetividade deste direito”.

Apesar das leis priorizarem maior participação dos cidadãos, o exercício do direito de autodeterminação informativa ainda era privilégio que apenas uma minoria conseguia exercer, uma vez que demandava recursos econômicos e até mesmo sociais que nem todos tinham acesso. Por isso, assim como as outras gerações normativas, a terceira não foi suficiente para atender aos interesses individuais de proteção de dados para todos.

Pelos motivos acima expostos, urgi a necessidade de uma quarta geração de leis, na qual já reconhecia a complexidade de “basear a tutela dos dados pessoais simplesmente na escolha individual”, nas palavras de Doneda (2021, p. 184). A partir de então, os legisladores focaram, principalmente, em conseguir efeitos concretos com a aplicação das normas.

As leis de quarta geração, como as que existem hoje em vários países, caracterizam-se por procurar suprir as desvantagens do enfoque individual existente até então. Nelas, está presente igualmente uma forte dose de pragmatismo, voltado para a busca, de resultados concretos (DONEDA, 2021, p. 183).

Os principais traços dessa quarta geração de leis se encontram na forma diferenciada de tratamento de alguns tipos de dados. Com a experiência proveniente das demais gerações, percebeu-se que certos dados pessoais carecem de uma tutela superior, e, nesses casos, a escolha individual não é suficiente para sanar tal necessidade. Por isso, na quarta geração, houve a criação de leis de cunho mais específico, havendo ramificações, por exemplo, em tratamento da área consumista, de saúde, educação, entre outras.

Nos primórdios da década de 1980, houve um consenso comum acerca dos princípios essenciais no que tange a proteção de dados pessoais. A Convenção 108 do Conselho da Europa é conhecida por ser um dos maiores instrumentos relativos à proteção de dados pessoais com aceitação em nível global, possuindo, atualmente 55 signatários e oito países observadores (FACHINETTE e CAMARGO, 2021).

Os princípios estabelecidos por esta Convenção, em suma, são os seguintes: princípio da publicidade; princípio da exatidão; princípio da finalidade; princípio do livre acesso e princípio da segurança física e lógica.

Pelo princípio da publicidade, entende-se que não pode existir um banco de dados sem prévia autorização, tampouco pode existir em sigilo, devendo a autoridade responsável ser notificada. Já o princípio da exatidão exige que os dados coletados não podem extrapolar a realidade, nem a distorcer, bem como devem se manter atualizados. O princípio da finalidade é imprescindível na prática, entendendo que o tratador de dados deve seguir a finalidade estipulada pelo titular do dado no momento de sua coleta, de forma que as informações não sejam passadas a terceiros desinteressados.

O princípio do livre acesso tem o objetivo de garantir que o cidadão consiga acessar os bancos de dados que possuam suas informações, podendo este fazer a correção em caso de algum dado se encontrar incorreto, de forma que o princípio da exatidão também seja honrado. Finalmente, o princípio da segurança física e lógica preconiza que os dados devem ser resguardados para que não sofram perigo de “extravio, destruição, modificação, transmissão ou acesso não autorizado” (DONEDA, 2021, p. 187). Tais princípios serviram como base para o desenvolvimento de regimes de proteção de dados, tanto em países adeptos à *common law*, quanto *civil law*.

Contudo, apesar dos princípios guias estabelecidos na Convenção 108 do Conselho da Europa, cada país ainda fazia aplicação diferenciada do que nela foi acordado. Afinal, já existiam leis nacionais para proteção de dados antes de cada país

adotarem a Convenção, bem como sua implementação poderia se dar de formas diversas aos países, uma vez que não possuía um plano de execução bem elaborado.

Com o intuito de diminuir discrepantes aplicações da Convenção nos estados nacionais, que causavam atritos entre ordenamentos nacionais, a União Europeia decidiu por editar a Diretiva 95/46/EC, acerca do processamento de dados pessoais.

A Diretiva foi aprovada em 24 de outubro de 1995 e entrou em vigor em 1998. Para que a harmonização do nível de proteção dos dados pessoais entre os países signatários, uma nova remessa de direitos foi elaborada, mas manteve-se os princípios acordados na Convenção. Na prática, cada país membro deve criar uma agência de proteção de dados, que utilize de um agente do estado que atue como supervisor, garantindo que os princípios sejam aplicados, sendo que os setores público e privado deveriam ser submetidos à mesma supervisão.

Em 2002, para adequação diante das novas tecnologias, foi elaborada outra Diretiva, a 2002/58/CE, pelo Parlamento Europeu. Os princípios e normas da Diretiva anterior foram mantidos, inovando-se apenas em instrumentos para manutenção da proteção de dados face à comunicação em rede.

De 2012 em diante, começou-se a discutir pelos países membros da União Europeia uma nova legislação interna. Porém, somente em 2018, no dia 25 de maio, foi promulgada a *General Data Protection Regulation* (GDPR). Seu objetivo também era de adaptação em face das novas tecnologias de informação, com normas de maior rigor, visando a proteção dos dados que formam a identidade do indivíduo. Afinal, as inovações tecnológicas criaram novos ambientes, como lojas virtuais, redes sociais, entre outros, que possibilitam maior exposição de dados de seus usuários.

A GDPR exerceu papel fundamental para a criação da Lei Geral de Proteção de Dados Pessoais, uma vez que grande parte do texto da legislação europeia foi adaptado para o cenário brasileiro. Ambas as legislações visam a proteção dos direitos fundamentais no âmbito do tratamento de dados pessoais, como será comentado a seguir.

1.3 A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO

A especificidade da proteção de dados pessoais no direito brasileiro é uma estrutura recente. As disposições acerca do assunto eram encontradas em dispositivos relacionados, por exemplo, ao direito do consumidor, bem como ao direito

de propriedade, entre outros ramos da legislação ordinária. Isso, porque, a própria Constituição não é específica em relação a tutela de informações pessoais, tratando da mesma através de garantias como “direito à informação”, “liberdade de expressão”, proteção à vida privada e à intimidade, inviolabilidade de sigilo de correspondência e domicílio.

Na legislação ordinária, o Código de Defesa do Consumidor também aborda garantias acerca de tratamento de dados pessoais. Em seu art. 43, podemos ver a garantia do princípio do livre acesso, sendo estipulado que o consumidor “terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre eles, bem como sobre as suas respectivas fontes”. Entretanto, a tutela de dados pessoais neste dispositivo é limitada, pois trata-se aqui apenas do âmbito consumerista.

Tal técnica legislativa acabou por fundamentar uma interpretação no mínimo temerosa no que diz respeito à matéria: se por um lado, a privacidade é encarada como um direito fundamental, **as informações pessoais em si pareciam, a uma parte da doutrina, serem protegidas somente em relação à sua “comunicação”**, conforme o art. 5º, XII, que trata da inviolabilidade da comunicação de dados (DONEDA, 2021, p. 270, grifo nosso)

Ou seja, a ausência de uma legislação específica, aliada à dispersão dos dispositivos acerca da tutela da privacidade e da proteção de dados pessoais, abriram palco para houvesse uma interpretação simplificada da Constituição acerca da matéria, sem que fosse levada em consideração a proteção de informações pessoais separadamente, de forma indireta. Pois, é evidente que o uso arbitrário de certos dados pessoais pode acarretar o ferimento do direito fundamental à privacidade.

Para sanar tal impasse, o legislador brasileiro colocou em pauta a Proposta de Emenda à Constituição nº 17 (ainda em votação), para que seja adicionado o direito fundamental à proteção de dados pessoais, *in verbis*:

Art. 5º (...)

XII – 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, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

Art. 22. Compete privativamente à União legislar sobre: (...)

XXX – proteção e tratamento de dados pessoais.

Outro instituto presente na Constituição de 1988, que trata da tutela de informações pessoais é o *Habeas Data*. Este, trata-se de um remédio constitucional, com atuação processual, que possui o fito de dar à pessoa física ou jurídica a garantia de acesso às suas informações armazenadas em bancos de dados de órgãos públicos e equiparados e, em caso de informações equivocadas, a garantia de retificação dos dados. O instrumento se encontra disposto no art. 5º, LXXII da Constituição e possui regulamentação própria pela Lei 9.507/1997, a qual versa sobre os tramites processuais do *habeas data* e o direito ao acesso informacional.

Além dos dispositivos legais mencionados, é cediço tratar protagonista do tema em prisma: a Lei nº 13.709/18, a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em 18.09.2021, após dois anos de *vacatio legis*. O âmago desta lei visa proteger a liberdade e a privacidade, direitos fundamentais essenciais na construção da personalidade da pessoa natural, dentro do respeito ao princípio da boa-fé no interim de cada tratamento de dados pessoais, sendo estes dados sensíveis ou não.

Conforme mencionado anteriormente, a LGPD tomou como inspiração a GDPR, mantendo demasiadas semelhanças conceituais e técnicas em seus dispositivos. Quanto à organização, a LGPD está dividida em dez capítulos, abrangendo 65 artigos.

Para maior compreensão da norma, o legislador, em seu art. 5º elencou conceitos importantes para a aplicação da lei no cotidiano, como se pode observar:

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

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

II - dado pessoal sensível: 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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

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

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

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

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

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

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

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

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Como principiologia, além do princípio da boa-fé, o art. 6º elenca os seguintes princípios: finalidade; adequação; necessidade; livre acesso, qualidade dos dados; transparência; segurança; prevenção; não discriminação e responsabilização e prestação de contas. Em seguida, a norma regulamenta seu objeto desde a coleta até o momento do término do tratamento de dados, devendo cada etapa respeitar os princípios supracitados, bem como as medidas de segurança também fixadas por esta legislação.

Vários artigos da lei carecem de complementação futura, devendo esta complementação ser suprida pela Autoridade competente. Sendo assim, foi criada a Autoridade Nacional de Proteção de Dados (ANPD). Sua atuação está regulada nos

arts. 55-A ao 55-K da LGPD. A ANPD é responsável por fiscalizar a aplicação da Lei, bem como garantir a aplicação de sanções e multas estipuladas pelo ordenamento.

A ANPD está incumbida de tornar a LGPD mais clara, acessível e ajustável para a realidade do Brasil pós-pandemia, tanto para os titulares de dados, quanto para os agentes de tratamento, garantindo maior segurança jurídica às transações que envolvem o tratamento das informações pessoais, já que essas são uma das competências da Autoridade, conforme o art. 55-J, da Lei Geral de Proteção de Dados (PINHEIRO, 2021, p. 68)

Em caso de violação à legislação em foco, com resultado danoso que prejudique a outrem, de forma patrimonial ou moral, o responsável pelo controle de dados tem a obrigação de repará-lo (art. 43 da LGPD). Tal obrigação gera a responsabilidade civil, e, seu caráter é justamente o objeto de estudo do presente trabalho, e carece, portanto, de maior palco para esclarecimentos. Sendo assim, o próximo capítulo cuidará desta explanação.

2 DA RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO

2.1 CONCEITOS BÁSICOS

Nosso ordenamento jurídico é alimentado por normas que visam garantir um convívio social harmonioso em todos os âmbitos. Contudo, demasiadas ações do ser humano corroboram para o surgimento de óbices que prejudicam essa convivência harmônica, causando desequilíbrio. Com o intuito de reparar o desequilíbrio causado pela ação humana, o legislador, então, designou determinadas normas, dentre elas, temos a previsão do instituto da responsabilidade civil.

A discussão acerca da responsabilidade civil orbita em torno de desobediência em razão de obrigação inadimplida ou pela inobservância de alguma norma reguladora de vivência social. No primeiro caso, estamos diante da responsabilidade civil contratual ou negocial (fundamentada pelo Código Civil de 2002 nos artigos 289, 390 e 391), e, no segundo caso, temos a responsabilidade civil extracontratual (abordada nos artigos 186 e 187).

Apesar dessa divisão, a doutrina prega que o legislador, em futuras normas, optará por extinguir essa dicotomia, unificando a responsabilidade civil. Como exemplo, temos o Código de Defesa do Consumidor, que não faz a distinção referida.

Como bem afirma Fernando Noronha, a divisão da responsabilidade civil em extracontratual e contratual reflete “um tempo do passado”, uma vez que os princípios e regramentos básicos que regem as duas supostas modalidades de responsabilidade civil são exatamente os mesmos (TARTUCE, 2018, p. 467).

Diante do esclarecido, passaremos à explanação acerca da responsabilidade civil extracontratual, uma vez que esta é o foco do presente trabalho.

O Código Civil de 2002 baseia sua responsabilidade civil dois pilares: ato ilícito e abuso de direito, fundamentados, respectivamente, nos arts. 186 e 187 do referido código:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa fé ou pelos bons costumes.]

Ou seja, a responsabilidade civil extracontratual decorre do descumprimento de um dever legal: o dever de não lesar. A reparação de danos, portanto, se trata de uma obrigação secundária consequente da transgressão da obrigação primária de não causar dano. Dentro dessa dinâmica, podem ser observados alguns elementos, os quais se encontram elencados a seguir.

2.2 ELEMENTOS DA RESPONSABILIDADE CIVIL

Para que seja constituída, a responsabilidade civil deve apresentar os seguintes elementos: conduta ou ato humano, nexo de causalidade e dano. A depender do cenário, pode se fazer presente um elemento acidental, verificando-se, nesse caso, a presença da culpa.

A conduta ou ato humano carrega em si a voluntariedade, onde pode haver uma ação ou omissão. Sendo assim, em razão da ação ou omissão ocorrer em caráter voluntário, o indivíduo está ciente da conduta, que, além de positiva ou negativa, pode decorrer de ato lícito ou ilícito. Aqui, é preciso identificar se a pessoa pode ser civilmente condenada ou não, não sendo relevante, nesse contexto, se foi dela a conduta ou de terceiro em sua responsabilidade.

Nesse sentido, a conduta pode ser direta ou indireta, dependendo se a sua prática se der pessoalmente pelo indivíduo ou pelo terceiro ligado a ele, respectivamente.

A regra é a ação ou conduta positiva; já para a configuração da omissão é necessário que exista o dever jurídico de praticar determinado ato (omissão genérica), bem como a prova de que a conduta não foi praticada (omissão específica) (TARTUCE, 2021, p. 464).

No tocante ao nexo de causalidade, este se trata da conexão entre o ato humano à consequência danosa. É um elemento imperioso para que a responsabilidade civil se concretize, pois, se não existe uma causa que gere um liame entre conduta e dano, não haverá, portanto, a obrigação de indenizar. Como ensina Venosa (2017, p. 474):

O conceito de nexo causal, nexo etiológico ou relação de causalidade deriva das leis naturais. É o liame que une a conduta do agente ao dano. É por meio do exame da relação causal que se conclui quem foi o causador do dano. Trata-se de elemento indispensável. A responsabilidade civil dispensa a

culpa, mas nunca dispensará o nexa causal. Se a vítima, que experimentou um dano, não identificar o nexa causal que leva o ato danoso ao responsável, não há como ser ressarcida.

Como é cediço, cuida-se o dano de lesão sofrida pelo indivíduo, que pode ser individual ou coletiva, moral ou material. Afinal, o dever de indenizar pressupõe a existência de um prejuízo que deve ser demonstrado. Alvim (1966, p. 171-172, apud GONÇALVES, 2019, p. 378) aduz o seguinte:

Dano em sentido amplo, vem a ser a lesão de qualquer bem jurídico, e aí se inclui o dano moral. Mas, em sentido estrito, dano é, para nós, a lesão do patrimônio; é o conjunto das relações jurídicas de uma pessoa, apreciáveis em dinheiro. Aprecia-se o dano tendo em vista a diminuição sofrida no patrimônio. Logo, a matéria do dano prende-se à da indenização, de modo que só interessa o estudo do dano indenizável.

Assim sendo, com a presença dos elementos citados, forma-se a responsabilidade civil. Agora, como mencionado, em alguns cenários a culpa se faz presente, e, com isso, a dever de indenizar pode ser apreciado dissemelhantemente, de forma subjetiva ou objetiva.

Para Chironi (1935, p. 5) “a culpa pode ser conceituada como o desrespeito a um dever preexistente, não havendo propriamente uma intenção de violar o dever jurídico” (apud TARTUCE, 2021, p. 466). Tal ensinamento, nos permite concluir que, na culpa, o agente se preocupa apenas com a conduta ativa ou omissiva, sem se preocupar com os efeitos que sua ação pode ocasionar. Por isso, o dolo, quando presente no direito civil, está abrangido pela culpa.

Deste modo, quando presente a culpa, a responsabilidade civil é subjetiva, visto que o agente apresentou conduta voluntária e, por negligência, imperícia ou imprudência (art. 186 do Código Civil atual), ocasionou dano a terceiro. Como é cediço, a negligência ocorre pela ausência de atenção, pois esta, se presente, poderia evitar o resultado danoso; a imprudência se manifesta quando o indivíduo se precipita, agindo sem cautela; já o a imperícia acontece quando o indivíduo não possui habilidade ou formação para exercer a conduta em questão.

Em suma, para que o indivíduo responda civilmente pela prática de uma conduta danosa, na responsabilidade civil subjetiva, é necessário que a culpa seja atestada, sendo ela com intenção de prejudicar ou com imprudência, imperícia ou negligência.

Como mencionado, a culpa é um elemento accidental, podendo se apresentar ou não na prática, como se vê:

Ao analisarmos **especificamente a culpa**, lembremos a **tendência jurisprudencial cada vez mais marcante de alargar seu conceito, ou de dispensá-lo como requisito para o dever de indenizar**. Surge, destarte a noção de culpa presumida, sob o prisma do dever genérico de não prejudicar (VENOSA, 2017, p. 442, grifo nosso)

Apesar de alguns autores destacarem a culpa como elemento essencial da responsabilidade civil, no caso concreto, a jurisprudência não a tem recebido como requisito para a obrigação de ressarcir. A teoria do risco surge para explicar como a ausência deste elemento pode ensejar, ainda, o dever de indenizar.

A referida teoria prega que qualquer dano é indenizável, sendo que o nexo de causalidade indicará o responsável por este dever. Ora sendo, é suficiente que exista um liame para unir dano e conduta para estarmos diante da responsabilidade civil objetiva. O dispositivo do Código Civil que representa tal responsabilidade dispõe da seguinte maneira:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, **independentemente de culpa**, nos casos especificados em lei, **ou** quando a **atividade normalmente desenvolvida pelo autor do dano implicar**, por sua natureza, **risco para os direitos de outrem** (grifo nosso).

Através deste artigo o legislador fixou duas oportunidades para que a responsabilidade civil objetiva ocorra:

- a) em situações conjeturadas por lei expressa, como, por exemplo, a presente no Código de Defesa do Consumidor, que estabelece a responsabilidade civil objetiva para prestadores e fornecedores; **ou**
- b) quando a atividade (lícita, uma vez que a lei permite) do agente naturalmente ensejar algum risco a direitos de outrem. A I Jornada de Direito Civil, em seu enunciado de n. 38 (grifo nosso) interpretou:

A responsabilidade **fundada no risco da atividade**, como prevista na segunda parte do parágrafo único do art. 927 do novo Código Civil, configura-se quando **a atividade normalmente desenvolvida pelo autor do dano causar a pessoa determinada um ônus maior do que aos demais membros da coletividade**.

Apesar do antagonismo evidente entre a responsabilização subjetiva e a objetiva, nosso ordenamento jurídico, em seus moldes, suporta conflitos entre normas, podendo existir diferentes interpretações a depender do caso concreto.

O art. 7º da Constituição Federal, em seu inciso XXVIII, garante: “seguro contra **acidentes de trabalho**, a cargo do empregador, **sem excluir a indenização a que este está obrigado, quando incorrer em dolo ou culpa**” (grifo nosso). Pelo olhar constitucional, o empregador está sujeito à responsabilização civil subjetiva, decorrendo, pois, de culpa. Ora, no mesmo cenário há espaço para a responsabilidade objetiva, sob o prisma do art. 927, parágrafo único do Código Civil, que também prevê a indenização cível em casos de atividade de risco, independentemente de culpa.

Neste exemplo, estamos diante de um conflito de normas, sendo a Carta Magna hierarquicamente superior, todavia, devido à especificidade da lei civil, o antagonismo ainda prospera. Para superar o impasse, cabe ao judiciário, face ao caso concreto, utilizar das analogias, costumes e princípios gerais, dando prioridade às exigências do bem comum (art. 4º e 5º da Lei de Introdução às normas do direito brasileiro).

Assim como no exemplo apresentado, a Lei Geral de Proteção de Dados permite interpretação para responsabilidade objetiva e subjetiva. O art. 42 da LGPD é responsável por regular a indenização cível, o que o faz nos seguintes termos:

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.**

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento **quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador**, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei

[...] (grifo nosso).

A redação deste artigo nos remete ao art. 186 do Código Civil, que versa sobre a responsabilidade civil subjetiva em decorrência de cometimento de ato ilícito “em violação à legislação de proteção de dados pessoais”, podendo ser tal ação ou

omissão praticada por negligência, imperícia ou imprudência “quando não tiver seguido as instruções lícitas do controlador”.

Ocorre que, o tratamento de dados, a depender do cenário, também pode ser considerado atividade de risco, como já explanado no capítulo anterior. O próprio art. 5º, inciso XVII da LGPD prevê o procedimento a ser adotado em caso de tratamento de risco:

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

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de **tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais**, bem como **medidas, salvaguardas e mecanismos de mitigação de risco**; (grifo nosso).

O Ministro Ruy Rosado, no âmbito do Recurso Especial 22.37/RS (grifo nosso), proferiu em voto:

A inserção de **dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno**, onde o uso da informática e a **possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar a devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade**; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer seu resultado, retificá-lo ou cancelá-lo. E **assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de direitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica**. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.

Sendo, portanto, o tratamento de dados uma atividade de risco, o parágrafo único do art. 927 também se aplica como obrigação de indenizar. É claro que a norma mais específica deve prevalecer, sendo, nesse caso, a LGPD. Entretanto, não se pode ignorar que o tratamento de dados é sim uma atividade de risco, e, como já esclarecido pela Jornada de Direito supracitada, o dano causado ao titular de dados, pode deixá-lo exposto a um dano em demasiado maior que aos demais membros da sociedade.

No âmbito da LGPD, o agente responsável pelo tratamento de dados é o operador, o que o faz seguindo os comandos do controlador, como já explicado no capítulo antecedente a este.

O §1º do art. 42 da LGPD prevê a responsabilização solidária dos agentes (controlador e operador). Para mais, visando o melhor interesse do titular dos dados em tratamento, o §2º desta lei permite a inversão do ônus da prova, quando houver verossimilhança em suas alegações e este for hipossuficiente no que tange à produção de provas ou até mesmo quando a produção de provas por parte do titular ser exorbitantemente onerosa.

Face aos dispositivos pertinentes ao tema (Constituição Federal, Código Civil e LGPD, para melhor compreensão da aplicação destes, passemos então para a análise de cenários concretos.

3. ANÁLISE DA APLICAÇÃO DA LGPD EM CASOS CONCRETOS

Com o objetivo de visualizar a aplicação da LGPD no caso concreto, em especial, para os fins deste trabalho, os arts. 42 e 43, os quais cuidam da responsabilidade civil na lei em prisma, passemos então para os casos concretos selecionados.

3.1 TJ-SP – APELAÇÃO CÍVEL: 10168440320208260068

O caso narrado a seguir se encontra em segredo de justiça, motivo pelo qual o nome da parte autora não é mencionado e a síntese dos fatos se encontra concisa.

Na comarca de Barueri, em São Paulo, um cidadão teve seu prontuário médico vazado, no qual indicava que este era portador do vírus HIV. Tal exposição o deixou constrangido em seu ambiente de trabalho. Essa desventura ocorreu em porque, para ter acesso ao prontuário, era necessário apenas que fossem informados CPF e data de nascimento, dados estes, de fácil acesso por terceiros. De tal forma é que a própria supervisora do emprego em que o apelante deste caso em tela conseguiu os dados médicos através do portal da prefeitura. Os abalos emocionais que este indivíduo sofreu após ser exposto acabaram resultando no desligamento da empresa.

O autor arguiu que utiliza o Sistema Único de Saúde (SUS) do município para tratar de sua doença (HIV), e, como muitos exames e consultas eram necessários, sua supervisora começou a investigá-lo em meados de novembro de 2019. Com o simples acesso, a supervisora obteve a relação completa de todos os exames e consultas de seu funcionário. Este, questionado por sua supervisora, confirmou que fazia tratamentos médicos antirretrovirais, e pediu sigilo, contudo, também foi questionado por outra funcionária acerca de seu tratamento.

Em janeiro de 2020, o autor recebeu a comunicação de desligamento da empresa, onde foi informado por sua supervisora que uma das razões determinantes de sua demissão teria sido justamente seu tratamento.

Este ingressou, portanto, com ação de obrigação de fazer com pedido de tutela provisória c/c indenização por danos morais e materiais, onde colegas de trabalho declararam por escrito terem acesso aos dados médicos do autor facilmente

através do portal da saúde da prefeitura. Entretanto, não concordando com o valor fixado pelo magistrado de primeiro grau, interpôs apelação.

Vejamos, então, a ementa da Apelação em tela (grifo nosso):

APELAÇÕES CÍVEIS. DANOS MORAIS. DANOS MATERIAIS. DIVULGAÇÃO DE PRONTUÁRIO MÉDICO. HIV. Dados médicos do autor disponibilizados ao público no site da prefeitura mediante a simples inserção de seu CPF e sua data de nascimento, informações essas de fácil acesso. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho. **A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexos causal entre a conduta e este dano e a ausência de culpa excludente da vítima** (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. **Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade.** Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. **Danos morais configurados. Quantum indenizatório majorado.** Danos materiais não configurados. Ausência de prova de nexos de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. (TJ-SP-AC: 10168440320208260068 SP 1016844-03.2020.8.26.0068, Relator: Heloísa Martins Mimessi, Data de Julgamento: 05/07/2021, 5ª Câmara de Direito Público, Data de Publicação: 07/07/2021)

O município também apelou, arguindo em razões ser isento de responsabilidade neste cenário, uma vez que o autor é quem não cuidou de suas informações pessoais (CPF e data de nascimento). Esclareceram que o autor começou a ser investigado no trabalho em meados de dezembro de 2019, em consequência de demasiadas consultas e exames médicos.

Argumentou, ainda, que a municipalidade “não pode controlar e ser responsável pelos atos praticados por terceiros a quem o requerente repassou suas informações pessoais”. Alegou, por fim, que este caso não deveria ser analisado pela teoria objetiva, mas sim pelo critério subjetivo.

Todavia, como observado na ementa supracitada, o Tribunal de Justiça do Estado de São Paulo, aplicou sim a responsabilidade objetiva ao caso concreto, esclarecendo que foi configurado o dano moral uma vez que a simples divulgação de informação sigilosa por si sustenta o pedido de indenização. Além disso, o quantum foi majorado e o município, em sede de tutela provisória foi obrigado a aplicar medidas

com o fito de impedir a maneira indiscriminada de acesso às informações pessoais médicas dos cidadãos.

A decisão foi fundamentada nos seguintes dispositivos: art. 5º, inciso X e art. 37, §6º ambos da Constituição Federal; art. 42 da 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018.

Como é cediço, o art. 5º da CF elenca os direitos fundamentais, onde, nesse caso, foi violado o disposto no inciso X deste artigo, o qual garante, *in verbis* (grifo nosso): “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**”.

O art. 37 da CF, em seu §6º, dispõe que as pessoas jurídicas de direito público e privado que prestam serviços públicos, respondem pelos danos que causarem a terceiros. Trata-se, aqui, da responsabilidade civil objetiva do Estado, que, para que esta ocorra dano causado a terceiro em consequência da prestação de um serviço público por uma entidade ou pessoa jurídica de direito público ou privado.

A sentença também não poderia deixar de ser fundamentada pela Lei n. 13.787/2018, que cuida justamente da utilização de sistemas informatizados que manuseiam e armazenam prontuários de paciente. O caput do art. 4º desta lei diz o seguinte: “Os meios de armazenamento de documentos digitais **deverão protegê-los do acesso, do uso**, da alteração, **da reprodução** e da destruição não autorizados” (grifo nosso).

Ora, claramente o artigo acima foi descumprido nesse caso concreto, visto que os dados que forneciam acesso às informações médicas do paciente eram de fácil acesso, e, em razão dessa facilidade, tais informações foram distribuídas sem permissão do titular.

Por fim, o art. 42 da LGPD, versa sobre a responsabilização civil em caso de desobediência à esta legislação que trata da proteção de dados pessoais, como já asseverado no capítulo anterior, redação deste artigo nos remete à responsabilização subjetiva, em casos de negligência, imperícia e imprudência. Entretanto, como o operador de dados se trata de uma entidade pública, também prestadora de serviço público, não resta espaço para análise de culpa.

Neste caso concreto, é evidente que em virtude da fácil exposição não autorizada de informações médicas, houve violação de direito fundamental do autor, no qual desventurou-se ao ver sua vida exibida em seu ambiente de trabalho.

O julgamento designado a este recurso ocorreu sob a ótica da responsabilidade civil objetiva. Isto porque o responsável pela proteção dos dados pessoais em prisma se trata de entidade pública, devendo, portanto, ser aplicada a responsabilidade objetiva do Estado. Contudo, como explicado no capítulo anterior, essa teoria não exclui a culpabilidade em si, apenas a torna objetiva, onde não é preciso analisar a existência de vontade causadora de dano.

Fica o questionamento: a responsabilidade civil também seria julgada objetivamente se o tratamento dos dados pessoais não ocorresse na tutela da prestação pública? Vejamos então no próximo cenário concreto.

3.2 RECURSO INOMINADO: 0707016-12.2021.8.07.0016

Arnaldo José, após ser vítima de um golpe (popularmente conhecido como “golpe do motoboy”), ajuizou Ação Declaratória de Inexistência de Débito c/c Repetição do Indébito. O ocorrido foi que, Arnaldo recebeu uma ligação, por meio da qual os estelionatários se passaram por funcionários do Banco do Brasil S/A, e enganaram o autor, dizendo que seu cartão havia sido clonado. A vítima, após confirmação dos dados referentes ao cartão pelos meliantes, seguiu as instruções dadas por estes, qual seja de telefonar para o número contido no verso do cartão de forma a realizar o bloqueio imediato.

Os golpistas, entretanto, conseguiram ardilosa e sutilmente manter a ligação original, simulando apenas o redirecionamento para um *call center* falso. Apesar de não solicitarem nenhuma senha, através dos registros de digitação e por intermédio de um software, os enganadores decifraram os números digitados.

Ao selecionar a opção de “falar com um atendente”, outro charlatão conduziu a segunda parte do golpe, confirmando a fraude no cartão e fingindo prosseguir com o cancelamento do cartão. Para tanto, informaram à vítima que esta deveria enviar os cartões ao banco e enviar uma carta pedindo o cancelamento e estorno das quantias sacadas, a fim de finalizar o cancelamento e emitir novos. Para completar o golpe, foi informado ao autor da ação que um emissário compareceria à sua residência, o que foi feito por meio de mais um falsário atuando como funcionário do referido banco.

Acreditando ter tomado os devidos cuidados, a vítima apenas aguardou a emissão de seus novos cartões. Foi se dar conta do golpe que sofreu somente depois de dez dias, ao conversar com sua filha (aposentada do Banco do Brasil).

Apesar de ser correntista do banco há mais de 44 anos, a real instituição financeira nem sequer questionou a Arnaldo acerca de suas movimentações repentinamente atípicas.

Quando questionado, o banco justificou que o golpe narrado estava ocorrendo com demasiada frequência e confirmou as operações feitas a partir da data em que o golpe fora finalizado, com um prejuízo total de R\$ 30.795,00 (trinta mil setecentos e noventa e cinco reais), exposto na inicial que tal prejuízo aconteceu por decorrência de “sucessivas operações realizadas no mesmo dia e em exíguo intervalo de tempo”.

Não suficiente, após registro de ocorrência na delegacia, e mesmo diante da fraude configurada, após contestação dos valores junto ao banco, a instituição informou que as operações de crédito da bandeira utilizada foram recobradas, ou seja, a instituição ‘nada fez para evitar os prejuízos financeiros. Por esta razão, não restou alternativa ao Sr. Arnaldo senão procurar a tutela do judiciário, através do juizado especial cível (por se tratar de causa, cujo valor não excede quarenta vezes o salário-mínimo, como manda o art. 3º da Lei 9.099/95).

Em sede de contestação, o banco alegou ter apenas exercido seu direito à cobrança e se escusou da responsabilidade atribuindo a culpa à parte autora e apresentou a preliminar de ilegitimidade passiva e falta de interesse de agir.

Ainda em primeiro grau, na sentença, a juíza rejeitou a liminar proposta pelo banco e verificou a presença de interesse de agir do autor, uma vez que este procurou a via administrativa para dirimir a lide, entretanto, como narrado, não obteve sucesso. Ademais, a julgadora reconheceu que houve falha na prestação de serviço por parte do banco réu, visto que este não efetuou bloqueio imediato diante das operações evidentemente atípicas e fora do padrão de seu cliente correntista há mais de quarenta anos. Asseverou a juíza:

É dever da instituição financeira adotar mecanismo de segurança interna que se voltem à proteção de seu cliente, como é o caso da guarda de informações sigilosa confiadas pelos correntistas, bem como da devida segurança dos cartões utilizados nas operações bancárias, mormente, quando há compras fora do perfil e do padrão de consumo do cliente. BRASIL. 4º Juizado Especial Cível de Brasília. Magistrada: Maria Rita Teizen Marques de Oliveira. Processo n. 0707016-12.2021.8.07.0016, ID 100897501.

Diante disso, a magistrada determinou que o banco procedesse com o cancelamento das referidas dívidas, bem como estornos de eventuais descontos

feitos na conta bancária do autor. O banco, insatisfeito com a sentença de primeiro grau, interpôs recurso inominado:

JUIZADOS ESPECIAIS CÍVEIS. DIREITO DO CONSUMIDOR. IDOSO. COMPRAS UTILIZANDO O CARTÃO DE CRÉDITO E DÉBITO. PRELIMINAR DE ILEGITIMIDADE PASSIVA. REJEITADA. PRELIMINAR DE EFEITO SUSPENSIVO. REJEITADA. LANÇAMENTOS DE COMPRAS NÃO REALIZADAS PELO TITULAR. FRAUDE PERPETRADA POR TERCEIROS ESTELIONATÁRIOS. ENTREGA DE CARTÃO BANCÁRIO AO MOTOBOY. RESPONSABILIDADE OBJETIVA. DANOS MATERIAIS. FRAGILIZAÇÃO DE DADOS. LGPD (LEI 13.709/2018). RESPONSABILIDADE SOLIDÁRIA. RECURSO CONHECIDO. PRELIMINARES REJEITADAS E NÃO PROVIDO. [...]

8. Diante da fraude, restou provado que a recorrente deixou de atender aos critérios de segurança para monitoramento das compras realizadas nos cartões de crédito e débito da parte autora, que eram incongruentes com o seu perfil de usuário. **O Banco do Brasil e a Operadora de Cartão de Crédito vinculada a ela possuem aparato tecnológico para detecção de fraudes, restando caracterizada a falha na prestação do serviço, a qual trouxe prejuízo à parte autora de ordem financeira. Havendo fragilização dos dados do correntista, tal como se extrai do caso concreto dos autos, porque os estelionatários, de antemão, já tinham os dados do autor, é de se aplicar os comandos da Lei Geral de Proteção de Dados, Lei 13.709/2018, arts. 42 e seguintes, confirmando a responsabilidade da instituição financeira em ressarcir os prejuízos comprovados pelo autor. Portanto, não há falar em culpa concorrente.** 9. Recurso CONHECIDO. Preliminares rejeitadas. No mérito, NÃO PROVIDO. Sentença mantida por seus próprios fundamentos.

(TJ-DF 07070161220218070016 DF 0707016-12.2021.8.07.0016, Relator: ARNALDO CORRÊA SILVA, Data de Julgamento: 22/11/2021, Segunda Turma Recursal, Data de Publicação: Publicado no DJE: 01/12/2021. Pág.: Sem Página Cadastrada) (grifo nosso).

Novamente, houve falha na segurança no que tange a proteção de dados pessoais, pois, para que o golpe narrado só foi possível, os estelionatários já estavam em posse dos dados do autor, ensejando, mais uma vez, a aplicação do art. 42 e seguintes da LGPD.

É possível refletir, também, que a responsabilidade objetiva novamente se fez presente. Entretanto, outra vez, isso não se deu em razão da LGPD em si, mas sim por outro dispositivo legal, qual seja, nesse cenário, o art. 14 do Código de Defesa do Consumidor, que determina:

Art. 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.

O serviço será defeituoso quando não oferece a segurança devida ao consumidor, onde são consideradas circunstâncias relevantes (art. 14, § 1º do CDC), sendo que, no caso concreto em prisma, a falha na prestação de serviço se deu em virtude do resultado (prejuízo financeiro).

Diante de todo o exposto, conclui-se que a responsabilidade civil na LGPD e seu modo de aplicação – objetivo ou subjetivo – será determinado de acordo com o incumbido de tratar das informações pessoais questionadas no caso concreto. Isso ocorre, pois, esta legislação se aplica a todos, sem exceção de qualquer categoria profissional (art. 4º da LGPD), e, em respeito ao princípio da especialidade – que rege todos os ramos do direito brasileiro – é preciso observar as normas já existentes referentes a cada pessoa (física ou jurídica), com fins públicos ou particulares.

A bem da verdade, sob o prisma de um olhar geral, a proteção de dados apresenta riscos tanto para o titular dos dados, quanto para seu controlador. Se trata de uma legislação recente, mas ao levarmos em consideração a velocidade com que os avanços tecnológicos têm aparecido nessa era da informação, é de se esperar que a lei nova rapidamente se torne obsoleta. É preciso, para o bem de todos, seja titular ou controlador, que mantenham a ética e boa-fé, assumindo sua responsabilidade ao ler os termos antes de aceitar um cookie (titular), bem como transparência ao redigir tais termos (operador).

Dessa forma, podemos usufruir das novas tecnologias e ampliar as facilidades que elas trazem, sem aumentar os riscos já existentes.

CONSIDERAÇÕES FINAIS

Diante de todo o exposto, foi possível observar o que é privacidade, sua merecida posição como direito fundamental (intimidade e vida privada) e como a negligência desse direito pode gerar riscos e danos em todas as esferas da vida de um indivíduo. Esta reflexão foi proposta com a finalidade de criar palco para o verdadeiro questionamento que envolve este trabalho: a responsabilidade civil na Lei Geral de Proteção de Dados Pessoais possui seu fundamento na culpa ou no risco?

Ainda com o fito de responder a indagação, foram estudados os artigos mais importantes da lei em tela, bem como os dispositivos da lei civil e constitucional que envolvem a responsabilidade civil. Por meio dos artigos iniciais da LGPD, tornou viável entender as terminologias importantíssimas para interpretação da norma, quais sejam: titular, tratamento de dados, dados pessoais, dados sensíveis, dados anonimizados, anonimização, consentimento, operadores, controladores e encarregados. Outrossim, os artigos iniciais da referida lei cuidaram também de apresentar os princípios norteadores e determinar sua aplicação geral, ou seja, para todos, sem deixar de fora nenhum setor de atuação profissional.

Através dos ensinamentos no que tange a responsabilidade civil no direito brasileiro, foi possível compreender as diferenças entre sua aplicação subjetiva e objetiva, bem como observar conflitos de normas a seu respeito, onde, como é cediço, prevalece a norma mais específica. Os últimos dispositivos abordados para que a análise dos casos concretos pudesse tomar palco, foram os arts. 42, 43, 44 e 45, sendo estes os essenciais utilizados nas decisões do judiciário expostas no último capítulo deste trabalho.

Finalmente, foram descritos dois casos concretos. No primeiro, o controlador dos dados pessoais se tratava de entidade pública, como a LGPD foi omissa no que tange o dever de indenizar objetivo ou subjetivo, o magistrado incumbido do caso aplicou o que manda a Constituição (art. 37, §6º), ou seja, a responsabilidade civil de entes que prestam serviço público. O segundo cenário concreto evidenciou uma pessoa jurídica de direito privado. Novamente, foi responsabilizada objetivamente pelos danos causados ao titular dos dados, mas desta vez com fundamentação legal encontrada no Código de Defesa do Consumidor, além, é claro, dos artigos 42 a 45 da LGPD.

Apesar da conclusão alcançada por meio do presente estudo em conjunto das decisões judiciais, é essencial lembrar que o tratamento de dados pessoais, carrega consigo um caráter delicado e, no andar que caminhamos no que se refere a *internet* e seu futuro, será preciso gradativamente mais olhar com maior cautela o que consentimos neste referido meio. Assim sendo, não sobrarão espaço para uma análise de culpa, sendo imperioso se atentar ao enorme risco que envolve a exposição de informações que compõem o ser humano.

Em especial, na presente era onde tudo é realizado online, a vida está se transferindo aos poucos para este meio e nessa estação de aclamações e cancelamentos, é imprescindível que as pessoas se atentem à maneira que conduzem sua vida no ambiente virtual, desde o aceitar dos termos e condições de *cookies* até a exposição do cotidiano em uma rede social, de forma que não reste espaço para culpa e nem para risco.

REFERÊNCIAS BIBLIOGRÁFICAS

BATISTA, Maria Fernanda; MARTINS, Dayane. **Decisões judiciais sobre LGPD**. Tecnoblog, 2021. Disponível em: <<https://www.privacidade.com.br/decisoes-judiciais-sobre-a-lgpd>>. Acesso em: 29/03/2022.

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

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29/03/2022.

BRASIL, Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29/03/2022.

BRASIL, Lei n. 8.078 de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 29/03/2022.

BRASIL, Lei no 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 29/03/2022.

DONEDA, Danilo César Maganhoto. **Da privacidade à proteção de dados pessoais** (livro eletrônico): elementos da formação da Lei Geral de Proteção de Dados. 2ª edição. São Paulo: Thomson Reuters Brasil, 2020.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 14ª edição. São Paulo: Saraiva Educação, 2019.

MOTA NOVAKOSKI, André Luís; HAYDÉE DAL FARRA NASPOLINI, Samyra. **Responsabilidade Civil na LGPD: Problemas e Soluções**. Conpendi Law Review, 2020. Disponível em: <<https://www.indexlaw.org/index.php/conpedireview/article/view/7024>>. Acesso em: 29/03/2022.

SANTOS DIVINO, Sthéfano Bruno, MACENA DE LIMA, Taissa. Responsabilidade Civil na Lei Geral de Proteção de Dados Brasileira. Revista Univem, v. 20 n. 1, 2020. Disponível em < <https://revista.univem.edu.br/emtempo/article/view/3229>> Acesso em: 29/03/2022.

TARTUCE, Flávio. **Manual de Direito Civil**: volume único. 8ª edição. São Paulo: Método, 2018.

TASSO, Fernando Antônio. **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, Ano 21 – número 53 – janeiro-março, 2020. Disponível em: <<https://epm.tjsp.jus.br/Publicacoes/CadernoJuridico/60662?pagina=1>>. Acesso em: 29/03/2022.

UNIÃO EUROPEIA, **Directiva 95/46/CE do Parlamento Europeu e do Conselho**. 1995. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046>. Acesso em: 29/03/2022.

UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho**. 2016. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 28/03/2022.]

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, 1890.