

CENTRO UNIVERSITÁRIO UNIDADE DE ENSINO SUPERIOR DOM BOSCO – UNDB  
CURSO DE DIREITO

**KÉSSIA CHRISTINA ROSA SILVA**

**RESPONSABILIDADE CIVIL DAS EMPRESAS À LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD): um estudo de caso sobre a adequação da LGPD na  
Empresa Assunção Promotora Eireli em São Luís/MA**

São Luís

2022

**KÉSSIA CHRISTINA ROSA SILVA**

**RESPONSABILIDADE CIVIL DAS EMPRESAS À LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD): um estudo de caso sobre a adequação da LGPD na  
empresa Assunção Promotora Eireli em São Luís/MA**

Monografia apresentada ao Curso de Graduação em  
Direito do Centro Universitário Unidade de Ensino  
Superior Dom Bosco como requisito parcial para  
obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Dra. Josanne C. R. Façanha

São Luís

2022

Dados Internacionais de Catalogação na Publicação (CIP)

Centro Universitário – UNDB / Biblioteca

Silva, Késsia Christina Rosa

Responsabilidade civil das empresas à luz da Lei Geral de Proteção de Dados (LGPD): um estudo de caso sobre a adequação da LGPD na empresa Assunção Promotora Eireli em São Luís/MA. / Késsia Christina Rosa Silva. \_\_ São Luís, 2022.

68 f.

Orientador: Profa. Dra. Josanne C. R. Façanha.

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2022.

1. Lei Geral de Proteção de Dados (LGPD). 2. Responsabilidade civil. 3. Vida privada. 4. Empresa - Assunção Promotora. I. Título.

CDU 347.72:342.721(812.1)

**KÉSSIA CHRISTINA ROSA SILVA**

**RESPONSABILIDADE CIVIL DAS EMPRESAS À LUZ DA LEI GERAL DE  
PROTEÇÃO DE DADOS (LGPD): um estudo de caso sobre a adequação da LGPD na  
empresa Assunção Promotora Eireli em São Luís/MA**

Monografia apresentada ao Curso de Graduação em  
Direito do Centro Universitário Unidade de Ensino  
Superior Dom Bosco como requisito parcial para  
obtenção do grau de Bacharela em Direito.

Aprovado em 14/ 12 / 2022

**BANCA EXAMINADORA**

---

**Profa. Dra. Josanne Cristina Ferreiro Ribeiro Façanha (Orientadora)**  
Centro Universitário Unidade de Ensino Superior Dom Bosco

---

**Prof. Me. Daniel Almeida Rodrigues**  
Centro Universitário Unidade de Ensino Superior Dom Bosco

---

**Prof. Esp. Johelson Oliveira Gomes**  
Centro Universitário Unidade de Ensino Superior Dom Bosco

À Deus, a minha mãe, meus irmãos, bem como as demais pessoas que desde sempre acompanharam minha trajetória pessoal e profissional.

## AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me concedido a graça de poder chegar até aqui, à minha mãe, Núbia Cristina Ramos Rosa, por sempre ter me encorajado a estudar com persistência, e ter me impulsionado a colocar meus estudos em primeiro lugar, por ter sempre acreditado que eu seria capaz, e por estar ao meu lado em momentos imprescindíveis. Aos meus irmãos, Carlos Ivan Machado Silva Filho e Ivan Carlos Rosa Silva, e principalmente ao meu irmão mais velho que sempre foi uma das minhas maiores inspirações nos estudos, provando-me, que podemos chegar onde queremos se persistirmos. Ao meu irmão mais novo, encorajou-me a ser sua referência e por isso nunca me deixei abater pelas adversidades da vida.

Agradeço de mesma forma as minhas amigas Sandra Correia e Larissa Salazar, na qual tive a oportunidade de dividir minha trajetória na UNDB, e certamente deixaram essa caminhada mais leve, além do que, sempre estiveram comigo quando necessitei de um ombro amigo, vocês fazem parte dessa história.

De mesma forma, agradeço aos meus chefes Panmalla Bacellar e Rafael Bacellar, que sempre se mostraram compreensivos com a minha trajetória acadêmica e por muitas vezes me ajudaram dentro do ambiente de trabalho. Decerto que a flexibilidade me dada no final complexo de um curso superior foi fundamental para que eu pudesse finalizar essa caminhada.

Agradeço a minha orientadora, Dra. Josanne Façanha, que desde o primeiro momento no qual conversamos a respeito do tema objeto deste trabalho, mostrou-se disposta a me auxiliar e a discutir as questões envolvendo o tema, com muito interesse e, acompanhadas de correções e sugestões sempre pertinentes. Além do que, pelo enorme carinho e admiração que tenho desde que foi minha professora no Pitágoras, por toda sua trajetória acadêmica e de vida.

Por fim, aos demais professores, colegas de sala e amigos que sempre estiveram comigo, em especial a Dona Francisca Costa, que teve um papel crucial quando passei na bolsa do Prouni ao me ajudar de forma financeira, sem ela, talvez nada disso seria possível. À Dona Domingas Pereira, por me dar abrigo e por ter sempre cuidado de mim como se fosse sua filha. Em especial também, a minha tia Gisélia Moreira, que me abrigou em sua casa por quase um ano, sou muito grata. Cada uma delas, de sua maneira particular, contribuíram para a construção do período mais intenso que experimentei até o momento durante minha trajetória.

“Quando for a hora certa, Eu o Senhor, farei acontecer”. Isaías 60:22

“Nunca deixe que alguém te diga que não pode fazer algo. Se você tem um sonho, tem que protegê-lo. As pessoas que não podem fazer por si mesmas dirão que você não consegue. Se quer alguma coisa, vá e lute por ela. Ponto final”.

— À Procura da Felicidade

## RESUMO

Este trabalho tem como objetivo geral enfrentar questões sobre a responsabilização de empresas privadas no processo de fiscalização da LGPD, além de analisar o cenário no qual foi promulgada e seus objetivos esperados na sociedade, descrevendo os processos de aplicação da norma, visto que, tem influência direta na intimidade e na vida privada, devendo ser vista de forma analítica para sua melhor aplicação enquanto direito da personalidade. Ademais, possui interesse em conceituar a responsabilidade civil e sua aplicação dentro da perspectiva da LGPD, relacionando os debates sobre a vida privada e a colisão de princípios constitucionais como intimidade e informação. Além de analisar qual teoria dentro da Responsabilidade Civil será utilizada para definir a responsabilidade daqueles que infringirem a norma, e ainda, explorar e entender como está sendo realizado os julgamentos e sentenças nesses casos pelo judiciário brasileiro. Nesse intuito, utiliza-se o método qualitativo de abordagem, pesquisa bibliográfica de caráter exploratório, estudo de caso da empresa Assunção Promotora, com aplicação de questionário a um dos funcionários responsáveis pelo processo de implantação da LGPD na empresa estudada, além de pesquisa por meio da exploração da legislação vigente, doutrinária e documental. Após apresentação da doutrina e aplicabilidade da lei no processo já existente, verifica-se que as empresas vêm sendo responsabilizadas pelos conceitos já existente dentro da responsabilidade civil, contudo, não está havendo tantas condenações em indenizações, os magistrados buscam um viés ainda mais educativo que obrigam a parte a se adequar ao processamento correto dos dados, pois, o processo de coleta e armazenamento de dados envolvem direitos fundamentais que atingem todo uma coletividade.

**Palavras-chave:** LGPD; responsabilidade civil; vida privada; estudo de caso; Assunção Promotora.



## **ABSTRACT**

The general objective of this work is to address questions about the accountability of private companies in the LGPD inspection process, in addition to analyzing the scenario in which it was enacted and its expected objectives in society, describing the processes of application of the norm, since it has a direct influence on intimacy and private life, and should be seen analytically for its best application as a right of personality. In addition, it is interested in conceptualizing civil liability and its application within the perspective of the LGPD, relating the debates on private life and the collision of constitutional principles such as intimacy and information. It also analyzes which theory within Civil Responsibility will be used to define the responsibility of those who violate the norm, and also, explore and understand how judgments and sentences are being carried out in these cases by the Brazilian judiciary. For this purpose, a qualitative method of approach is used, bibliographical research of an exploratory nature, a case study of the company Assunção Promotora, with the application of a questionnaire to one of the employees responsible for the implementation process of the LGPD in the company studied, in addition to research through the exploration of current legislation, doctrinal and documental. After presenting the doctrine and applicability of the law in the existing process, it appears that companies have been held accountable for existing concepts within civil liability, however, there are not so many convictions in indemnities, judges apply an even more educational procedure that obliges the party to adapt to the correct processing of data, since the process of collecting and storing data involves fundamental rights that affect an entire community.

**Palavras-chave:** LGPD; Civil responsibility; private life; case study; Assunção Promotora.

## **LISTA DE SIGLAS**

STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal
LGPD	Lei Geral de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
ANPPD	Associação Nacional dos Profissionais de Privacidade de Dados

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b> .....	12
<b>2</b>	<b>LEGISLAÇÃO SOBRE PROTEÇÃO DE DADOS NO BRASIL</b> .....	14
2.1	Contexto normativo para aprovação da lei 13.708/18 (LGPD).....	14
2.2	Princípios e fundamentos básicos da lei geral de proteção de dados.....	18
2.3	O paradigma da privacidade e a lei geral de proteção de dados e a colisão entre direitos à vida privada versus liberdade de expressão.....	22
<b>3</b>	<b>RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO</b> .....	27
3.1	Correntes doutrinárias de interpretação.....	27
3.1.1	Responsabilidade subjetiva e objetiva.....	28
3.1.2	Corrente dualista e perspectivas contrárias à culpa e ao risco.....	34
3.2	O consentimento do titular dos dados e a responsabilização civil de terceiro.....	37
3.3	A responsabilidade civil na LGPD e as empresas privadas.....	40
<b>4</b>	<b>A TUTELA COLETIVA NA PROTEÇÃO DE DADOS PESSOAIS</b> .....	45
4.1	A questão dos legitimados para judicialização de ações.....	45
4.2	Ações civil públicas ou privadas e processo de judicialização da LGPD.....	48
4.3	Estudo de caso: adequação da LGPD na empresa Assunção Promotora Eireli.....	50
4.3.1	Caracterização da área de estudo: organização da empresa quanto ao armazenamento e tratamento de dado.....	51
4.3.2	Coleta de dados: entrevista e análise de dados.....	56
<b>5</b>	<b>CONCLUSÃO</b> .....	61
<b>6</b>	<b>REFERÊNCIAS</b> .....	64

## 1 INTRODUÇÃO

A eclosão da tecnologia de informação com todas as suas novas formas de comunicação, trouxeram grandes avanços econômicos e sociais, facilitando de forma considerável a vida da sociedade em geral. Esses novos meios de intercomunicação, apesar de serem um marco nas relações sociais e econômicas, vieram acompanhados de grandes aproveitadores e criminosos, pessoas que se utilizam dessas ferramentas para hackear os aparelhos de usuários e divulgar informações de forma ilegal.

Atualmente, os meios cibernéticos apesar de todas as formas pensadas de segurança existentes, não podem garantir a segurança de dados dos usuários, exemplo de tal fato foi quando Julian Assange por meio de sua organização *wikileaks* hackeou de forma ilegal informações sigilosas do Governo Americano. Nesse caso, após diversos escândalos nessa ordem, viu-se a impotência de direcionar essa problemática para a ordem jurídica, coibindo as ilegalidades e a má gestão de dados na internet por intermédio de leis completas e robustas que versem sobre o tratamento e o armazenamento de dados (BBC, 2021).

Desse modo, visando o bem coletivo e a forma que vinham sendo tratadas os dados e as diversas violações de princípios básicos como privacidade e vida a íntima, a União Europeia editou *General Data Protection Regulation (GDPR)*, que versava sobre tratamento dados e elencava sanções ao seu descumprimento. O Brasil, após a determinação da União Europeia de que só iriam se relacionar comercialmente com os países que tivessem normas no mesmo sentido, e também aliada ao fato de diversas lides levadas ao judiciário, promulgou em 2018 a Lei Geral de Proteção de Dados, que entrou em vigor em 2020 e inicia suas sanções desde julho de 2021.

Assim, a LGPD se aplica tanto a órgãos públicos quanto privados, uma de suas principais preocupações é deixar que o titular das informações tenha mais poder e controle com seus dados solicitados em diversas plataformas e ambiente virtuais e até mesmo em entrevistas de emprego. Conseguir entender e cobrar os motivos reais para a solicitação de seus dados e como são manuseados O sentido da lei é proteger a vida íntima e sobretudo a privacidade.

As empresas privadas nesse panorama, viveram uma enorme modificação em toda a sua estrutura, tanto tecnológica, quanto em conscientização dos próprios funcionários sobre a importância de observar os ditames da LGPD. Para isso, as empresas tiveram grandes gastos com toda a implementação de mudanças em sistemas de servidores e de recursos tecnológicos para armazenar e tratar os dados de forma correta. Só que, nem todas as empresas têm poder econômico para modificar quase toda a estrutura construída nesse negócio. A principal

inquietação e dúvida são se essas empresas poderão vir a sofrer sanções judiciais pelo descumprimento parcial ou total da legislação.

Nesse viés, entender o conceito e as bases jurídicas que embasam se deve haver ou não a responsabilidade civil das empresas privadas é de suma importância, até porque o cumprimento da Lei Geral de Proteção de Dados se relaciona diretamente com o cumprimento de Dignidade da Pessoa Humana e de princípios fundamentais da pessoa. Outrossim, a disseminação de dados fere direitos cruciais que devem ser tutelados pelo Estado, sendo Direito a vida privada e privacidade. Nesse caso, outro princípio também que poderá ser lesado é o da informação, se o viés da LGPD for de fato munir o titular de expor somente aquilo que autoriza e não gera constrangimento.

Um dos quesitos que já vem sendo debatida nos tribunais antes mesmo da edição da norma é sempre no sentido se proteger a vida privada e a intimidade. A lei retrata claramente que os dados podem ser sim solicitados e expostos, caso haja uma motivação legal para aquilo e que seja controlado. Não pode é qualquer empresa ou órgão cobrar dados sensíveis como a sexualidade ou relacionada a cor e raça, caso seja solicitado, deve haver motivações jurídicas. Apesar de o Princípio da Informação e Privacidade serem extraídos da constituição, no caso a caso, sempre será aplicado aquele que preservar a Dignidade da Pessoa Humana.

Para este trabalho, utiliza-se o método qualitativo de abordagem e uma pesquisa bibliográfica de caráter exploratório, além de estudo de caso com aplicação de questionário. E, em termo de estrutura, o trabalho foi dividido em três capítulos. O primeiro denominado por Legislação da Proteção de Dados no Brasil, faz a construção do contexto normativo da criação da LGPD, além de trazer de forma detalhada os princípios norteadores da lei, sendo referenciada por autores como Bioni (2018). Após isso, discute o paradigma da privacidade e a colisão entre os Princípios da Liberdade de Expressão e da privacidade, acolhida por autores como Doneda (2006).

O segundo capítulo, nomeado como Responsabilidade Civil no Ordenamento Jurídico faz menção a Responsabilidade Civil, trazendo esse contexto para a Lei Geral de Proteção de dados, trabalhando as teorias de embasamento e descrevendo como as empresas privadas podem ser responsabilizadas civilmente, encontra amparo nas doutrinas de Gagliano e Pamplona Filho (2019).

Por fim, o terceiro capítulo, cuja tema é A Tutela Coletiva de Dados Pessoais, remonta sobre a tutela coletiva na proteção de dados pessoais, discutindo a questão dos legitimados para propor ações judiciais e como seria a judicialização de ações que tratam sobre a LGPD a longo prazo.

## 2 LEGISLAÇÃO SOBRE PROTEÇÃO DE DADOS NO BRASIL

Este capítulo irá discutir o contexto normativo no qual surgiu a Lei Geral e Proteção de Dados (Lei 13.709/18). Analisando-se os motivos determinantes da sua criação e como era tratada essas questões no judiciário no cenário anterior a lei. Expõem também de que forma os tribunais nacionais tem visto e decidido nesses casos e como faziam quando a lei ainda não estava em vigência.

Após isso, irá trabalhar com os princípios norteadores da LGPD, que dão base e solidificam a ideia da lei, além de explicar todos os processos e os motivos pelos quais devem ser cumpridos à risca. Entende-se, assim, o porquê é importante somente pedir ou guardar somente dados imprescindíveis para a situação prática e que a ilegalidade vai muito além da invasão de *hackers* e criminosos. Estabelece também sanções ao descumprimento da lei.

Desse modo, o assunto tratado aborda de mesma forma o paradigma da privacidade, ou seja, qual o modelo seguido pela LGPD dentro da questão do Direito a Privacidade, que na verdade é um dos temas mais comentados na norma. Com isso, demonstra, como ao longo do tempo após a revolução tecnológica esse princípio vem sendo violado e estabelece as diretrizes para pugnar tais práticas.

Em suma, discute as ideias de que há uma colisão de princípios dentro obrigatoriedade e cumprimento da LGPD. Ao que se mostra durante o discurso, os princípios devem sempre ser sobrepesados e prevalecer aquele que na situação real conceda e reflita direitos de Dignidade da Pessoa Humana.

### 2.1 Contexto normativo para aprovação da lei 13.708/18 (LGPD)

Para Bauman (2011, p. 8) crítico da pós-modernidade, o mundo líquido e os sentimentos de uma sociedade líquida contribuíram para a busca de constantes mudanças que resultaram na construção e organização social que se tem hoje. Os aparelhos tecnológicos que nos conectam e ao mesmo tempo nos desconectam das pessoas fazem parte das “autoestradas de informação que nos conectam de imediato, em tempo real, a todo e qualquer canto do planeta”. A grande facilidade de trocar informações e de realizar alguma atividade cotidiana se tornou simples e fácil e o melhor, basta apenas um *click*.

Sendo assim, com o surgimento de uma nova era informacional que teve seu “boom” em 1970, e nas reformulações dos meios de comunicação, a possibilidade de compartilhamento de dados e trocas de informações, tornou-se um “fenômeno mundial de

interconexão”. A mudança nas relações não atingiu somente as pessoas comuns, mas empresas, órgão públicos e privados, afinal, trouxe consideráveis modificações no que tange a comunicação (MARINELI, 2017, p. 1).

A regulamentação do tratamento de dados é um fenômeno global, por isso, muitos países editaram leis que pudessem enfrentar essa nova perspectiva social. Muito embora, o Brasil tenha sido pioneiro na criação de uma lei que tratasse do assunto, promulgando a lei 12.965/2014, o Marco Civil da Internet (BIONI, 2018). Manteve-se inerte na fiscalização e na verificação do que a lei do Marco Civil não tratava, mas que era constantemente judicializada e cobrada ao Poder Judiciário posicionamentos e decisões por meio de interpretações de princípios extraídos da Constituição Federal de 1988.

Conforme aponta Bastos (2018) apesar de todas as movimentações do Brasil na tentativa de regulamentar as nuances que envolviam o tratamento de dados e o perigo da internet, ainda assim, permaneceram lacunas com a Lei do Marco Civil que necessitavam de preenchimento. Dessa forma, observa que chegou um determinado momento que a legislação específica precisava ser editada. Bastos relata o seguinte:

Necessitava-se, portanto, de maior regulamentação no âmbito do direito digital. Assim, o Marco Civil da Internet se destacou por prever princípios, garantias, direitos e deveres para o uso da Internet no Brasil. No entanto, ele próprio deixava uma importante lacuna: a questão dos dados pessoais no direito digital. Reconheceu as relações jurídico-virtuais e os efeitos delas no ordenamento. Dispôs, por exemplo, acerca dos crimes cibernéticos. Mas deixou de abordar como os dados fornecidos pelos usuários poderiam ser utilizados pelas empresas (2018, p. 1).

Ao decorrer do tempo, constatou-se que os ambientes virtuais e as atividades realizadas nesses espaços, tratavam-se de algo muito mais sério e complexo do que se pensava. Nessa linha Mendes (2014, p. 20), estuda que em seguimento a essa oportunidade de expansão e capacidade dos indivíduos “os meios de comunicação e informação ampliam, na mesma medida, os riscos a que os indivíduos estão submetidos. Estando, assim, diante de um fenômeno com duas vertentes ao mesmo tempo que traz benefícios possuem diversas consequências prejudiciais”.

Ocorre que, a implementação dessa era tecnológica resultou em uma facilitação na vida das pessoas, no âmbito empresarial, e nos demais campos de trabalho. As propagandas se tornaram mais acessíveis e fáceis de produzir, os serviços se tornaram mais rápidos e a economia de tempo é um fator crucial que por muito tempo fez com que as autoridades fechassem os olhos para o que vinha acontecendo.

No mesmo pensamento GAGLIANO e PLAMPLONA FILHO (2019) observam que os avanços tecnológicos trazem consigo diversas problemáticas, pois, os crimes que antes eram feitos de forma pessoal, agora são digitais, dificultando a identificação dos criminosos. Dessarte, atentados a vida privada tem se tornando mais frequentes, não raro, as próprias empresas obterem os dados de usuários com o propósito de ofertar seus produtos, fazendo sua propaganda de forma ilegal e que gera desconforto.

O mesmo foi observado em julgamento realizado pelo Min. Luis Felipe Salomão da 4ª Turma do STJ, onde expõem por meio de seu voto que é de suma importância que haja autorização dos clientes de seus dados em relação a identificação de seu padrão de consumo, sendo abusiva e ilegal seu consentimento obrigatório por cláusula contratual.

“De fato, a partir da exposição de dados de sua vida financeira abre-se leque gigantesco para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se sua maneira de viver e a forma com que seu dinheiro é gasto. Por isso a imprescindibilidade da autorização real e espontânea quanto à exposição. Não bastasse o panorama traçado acima, considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.” (STJ, 2017)

Iniciou-se, assim, diversas discussões em julgamentos acerca do tratamento de dados, que apesar de não ter legislação até então específica, era visto como correta e sempre favorável a proteção de dados pessoais, buscando justificativa na proteção de princípios constitucionais. O relator Min. Sebastião Geraldo de Oliveira julgou improcedente o recurso de danos morais em razão da divulgação de dados pessoais do trabalhador, corroborando em seu voto que “a exposição de dados pessoais da autora gera constrangimentos decorrentes da imediata afetação da intimidade e vida privada da reclamante, valores resguardados constitucionalmente” (TRT-3, 2017).

De mesma forma, como aponta Bioni (2018, p. 114) a expansão das ferramentas tecnológicas fez com que o tratamento de dados fosse além do domínio governamental, direcionando-se a novos autores nessa relação. A demonstração de uma mudança mostrou-se indispensável nesse ambiente. É notório que o entendimento em relação ao tratamento de dados foi se modificando ao longo do tempo até se chegar no que é hoje, onde se tem ainda a caracterização de dados sensíveis e não sensíveis (BIONI, 2018, p. 117).

Quando se trata da Lei Geral de Proteção de Dados, pensa-se ser algo novo dentro de um cenário desconhecido, só que, a lei já estava em discussão desde 2010, ano que foi feita uma consulta pública de um anteprojeto de lei. Percebe-se que nos anos de 2010 a 2014 não foi algo tão discutido, contudo, escândalos mundiais começam a eclodir, como quando o americano



Eduard Snowden revelou os esquemas de espionagem praticados por determinados países. Afirmou em seu discurso que os governos tinham capacidade e poder para espionar e vigiar qualquer pessoa do planeta, fomentando ainda mais a importância de se ter uma lei própria sobre o assunto (BIONI, 2018).

Por isso, houve uma aceleração no fazimento do Projeto de Lei referente ao Marco Civil da Internet, que foi aprovada. Todavia, viu-se que não incluía tudo aquilo que deveria tratar dentro do ambiente cibernético do tratamento de dados. Sendo assim, em 2015 iniciou novas discussões para criação de uma nova lei que tratasse do tema com mais propriedade. Daí a criação da LGPD. Carvalho e Pedrini afirmam que:

Evidencia-se que, no viés de proteção do usuário perante o ambiente virtual, deve-se considerar os preceitos principiológicos e diretrizes do 24 Marco Civil da Internet, uma vez que são verdadeiras conquistas dos internautas frente ao mundo tecnológico. Entretanto, há, ainda, outro comando legislativo que deve ser igualmente observado, trata-se, pois, da LGPD, que trata detalhadamente e especificamente da proteção dos usuários, quando suas informações estão dispostas em banco de dados públicos ou privados (2019, p. 374-375).

Ver-se que o pontapé principal para que o Brasil iniciasse a adequação de controle de informações de usuários foi com a Lei do Marco Civil, porém, como dito, não exauria todas as situações de conflitos e lides no judiciário. A LGPD exige o cumprimento de adequações e normas e prevê a fiscalização dos órgãos públicos e privados, o que se mostra uma lei mais robusta e completa.

Importante salientar, que após escândalos em ordem internacional como aconteceu também com a plataforma Facebook que em 2018 disponibilizou dados de seus usuários a empresa Cambridge Analytica foram decisivos para a conclusão da discussão e criação da General Data Protection Regulation (GDPR), lei criada pela União Europeia com objetivo de punir e punir práticas criminosas na internet. O ponto crucial foi a determinação de que só teriam relações comerciais com os países que tivesse uma regulamentação e fiscalização no mesmo sentido (GOGANI, 2018). Bione ainda destaca que:

Ainda faltava o ingrediente mais quente para eclodir a pauta da proteção de dados pessoais em 2018: o escândalo da Cambridge Analytica escancarou como a desproteção de dados pessoais impacta não só a vida de um cidadão em específico, mas de toda uma coletividade e os alicerces do que se entende por democracia. Logo depois, houve uma sessão temática no Senado para debater, pela primeira vez no plenário em uma das Casas do Congresso Nacional, o tema. E, em maio de 2018, a Câmara dos Deputados realizou também um seminário como decorrência do referido escândalo (BIONI, 2018, p. 1).

Seguindo a linha do que foi exposto acima por Bioni (2018), após a edição da lei europeia, diversos países criaram normas no mesmo sentido, Segundo Ronaldo Lemos, a GDPR é uma legislação que tem um caráter “viral”, o que se mostrou verídico, pois, após sua edição diversos países se regulamentaram nesse sentido (PACETE, 2018). A criação da Lei da União Europeia foi decisiva para que o Brasil editasse a Lei de nº 13.709/2018, Lei Geral de Proteção de Dados. Além disso, a possibilidade de lesar princípios constitucionais como a privacidade, intimidade e honra fomentou ainda mais essa edição.

Vale sublinhar, que apesar de a LGPD ter sido editada em 2018 só veio entrar em vigor em 2020 e sua fiscalização só deu início em 01 de agosto de 2021. Entra em vigor, em um momento tão ímpar, que foi com a eclosão da pandemia do covid-19, onde empresas e todas as pessoas que se mantiveram reclusas de forma obrigatória necessitaram utilizar totalmente os recursos digitais para fins de comunicação e trabalho.

Pugnar as ações de criminosos, tornou-se também um objetivo importante da lei dentro da plataforma que expõem as pessoas e sua intimidade, desrespeitando princípios como a vida privada e privacidade. O objetivo não é a proteção dos dados em si, mas sim do detentor dos dados que vê sua vida exposta sem seu consentimento ou sequer sabe que seus dados pessoais são vendidos e difundidos a outras empresas (MENDES, 2014).

A forma mais eficaz de fazer com que criminosos não tenham mais vazão para acessos e compartilhamento de informações pessoais é adequando todos os órgãos e empresas para que criem mecanismos de armazenamento e defesa. A princípio, o que aparenta no âmbito empresarial e até mesmo público é punir desenfreadamente as empresas, mas o foco é adequar todos sobre esse novo quadro social.

## 2.2 Princípios e fundamentos básicos da Lei Geral de Proteção de Dados

O art. 6 da LGPD demonstra com grande afinco quais os princípios que balizam a lei 13.709/2018 e que orientaram sua formulação. É possível notar a exaustão que passa o legislador ao tentar pelo artigo preencher quaisquer situações que possam vim a envolver o compartilhamento e a manutenção dos dados. Isto significa, a busca por acompanhar, bem como, fiscalizar todos os processos existentes.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:  
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular [...]

- II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades [..]
- IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais [...]
- V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados [..]
- VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento [..]
- VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados [...]
- VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar [...] de proteção de dados pessoais [..]

Nesse sentido, o consentimento do titular dos dados deve ser compreendido e aplicado observado o texto do art. 6 da LGPD. Os princípios que regulam a Lei de Dados têm o cunho de delimitar o uso desses dados, trazendo mais segurança ao usuário. Porém, qualquer determinação feita, além de observar a Lei de Dados, deve sempre se atentar aos princípios constitucionais da jurisdição brasileira.

O princípio da finalidade também contido no referido artigo exige que titular dos dados esteja completamente ciente do que irá ser feito com seus dados, caso contrário a aceitação será dada como inválida. Tal princípio é revelado quando no art. 6, da referida lei é dito que deverá haver a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018).

Nesse ínterim, o fito primordial do Princípio da Finalidade nada mais é que exigir que os dados sejam utilizados somente para as finalidades firmadas em contrato concedidas pelo titular dos dados. Por isso, qualquer mudança ou desvio daquilo que permitiu o usuário, será considerado como ilegal (SANTOS, D., 2019).

O Princípio da Adequação traz um complemento ao Princípio da finalidade, pois, determina que os tratamentos dos dados pessoais devem estar exatamente conforme o que foram preestabelecidos entre as partes. Seria como exigir informações desnecessárias para fins desconhecidos que não se relacionam com o que busca o usuário, como a obrigatoriedade de informar dados de saúde para que o usuário pode obter informações de notícias de esportes. Nesse caso, seria desnecessário o pedido dessas informações e o Princípio da Adequação busca a correspondência à finalidade pretendida pelo contratante. Ou seja, o tratamento de dados

personais deve se limitar ao essencial mínimo para a realização da atividade informada ao titular dos dados (SANTOS, D., 2019).

No que tange ao princípio da necessidade, a própria lei faz entender que os dados devem ser coletados de modo restrito, sendo pertinentes, imprescindíveis para a realização da atividade, não podendo ser excessivos, os dados armazenados devem ser os suficientes para servir para o fim firmado entre as partes. Deve-se sempre ao tratar esses dados pessoais se munir com o Princípio da Proporcionalidade, balanceando aquilo que é indispensável e aquilo que não é (BRASIL, 2018).

No aspecto empresarial, Lima (2020, p.1) argumenta o seguinte

isso significa que ao fazer o levantamento e a varredura dos dados pessoais armazenados e suas expectativas naturezas, o empresário têm a inédita a oportunidade de propor uma revisão da sua estrutura de armazenamento e segurança de informação para aqui é essa seja a adequada ao tamanho de sua operação.

As empresas, nesse caso, devem ser extremamente criteriosas tanto nos dados que solicitam, quanto no armazenamento, visto que, é necessário que se demonstre a necessidade de armazenar o dado diante da operação realizada pela empresa. Por isso, sua guarda deve estar justificada, não somente vislumbrando a lei, mas aplicando para o ramo que atua e o que de fato é importante preservar, mesmo que não sejam dados sensíveis.

Na visão de Lima (2020), no que se refere o princípio da qualidade é a possibilidade que deve ser concedida ao titular dos dados de verificação da exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da formalidade de seu tratamento. Lima (2020, p. 1) ainda desta que:

Conforme vemos na própria Lei Geral de Proteção de Dados, o titular dos dados tem o direito de correção de dados incompletos, inexatos ou desatualizados e, ainda, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Sendo assim, a LGPD, confere poderes ao titular dos dados, que poderá solicitar e obter diversas informações sobre seus dados. A empresa, com isso, está obrigada a fornecer toda a linha de controle dos dados. Ou seja, quais dados estão sendo guardados, se estão atualizados, se foram compartilhados e com quais outras empresas houve a transferência de seus dados. Tendo ainda, a possibilidade, dependendo do caso, de exigir a exclusão de seus dados.

O Princípio da Transparência também denominado de Princípio da Publicidade é criado paralelamente ao Princípio da Finalidade. Significa dizer que ao detentor de seus dados é garantido e assegurado a prestação de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento. Então, deve ser de conhecimento público a existência de dados conforme elenca o art. 9 § 1, da Lei de 13.709/2018 (SANTOS, D., 2019).

No mesmo art. 6 da LGPD, encontra-se o Princípio da Segurança, uma comprovação incontestável do resguardo dos Direitos Fundamentais, prevendo a utilização de medidas técnicas e administrativas a fim de protegê-las de acessos não autorizados. E, ainda, a proteção contra acidentes, atos ilícitos, como a perda, destruição e até difusão dos mesmos (BRASIL, 2018).

O princípio da Prevenção constante na lei, vem para gerar obrigação de medidas preventivas pelo guardião do acesso ou aquele que detém e faz o armazenamento desses dados, deverá criar mecanismos de defesa para evitar ocasionais danos e sua responsabilização pela perda e compartilhamento dos dados (BRASIL, 2018).

Ainda buscando efetivar o cumprimento da Lei, o legislador ainda engloba o Princípio da não discriminação, pelo qual é vedado a utilização de dados pessoais com o fim discriminatório, abusivo e ilícito (SANTOS, D., 2019). Assim, o objetivo do art. 6, IX, da LGPD, é de quando se falar em dados, saber que de forma nenhuma podem ser utilizados para fins impróprios, vexatórios e discriminatórios (LIMA, 2020).

Importante se fazer uma observação sobre o tema, veja-se:

Não se pode ter a exclusão de titulares de dados pessoais no momento de seu tratamento de dados por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, globalizações, filiação sindical, estado genético ou de saúde ou orientação sexual. Não é dizer que nunca poderá ter uma setorização de tratamento de dados, porém somente poderá ocorrer tal restrição em condições específicas e previstas em lei, como por exemplo um tratamento de dados de alunos optantes por cotas, perante a Lei de Cotas 12.171/2012, a condição de tratamento de dados pessoais será a partir de seu histórico educacional, sendo ele oriundos do ensino médio público, em cursos regulares ou da educação de jovens e adultos (LIMA, 2020, p.1)

Por isso, o que deve ser verificado na questão do manuseio dos dados não é o conteúdo que foi colhido do detentor dos dados, mas sim, para que fim serão utilizados. Uma empresa, por exemplo, não poderá solicitar dados desnecessários para realização da seleção de seus funcionários, impor a selecionado que compartilhe no processo dados de cunho racial, religiosos e sexual.

Tem-se, ainda, para completar o rol dos princípios que balizam a Lei Geral da Proteção de Dados, o Princípio da Responsabilização e Prestação de Contas, que obriga os contratados a realização de condutas e de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. O objetivo é assegurar o proprietário dos dados um amplo controle daquilo que está sendo feito com as informações fornecidas (SANTOS, D., 2019).

Os princípios que concederam rumo para embasar a LGPD têm como intuito de criar diretrizes que devem ser seguidas à risca por todos nos relacionamentos contratuais, pessoais e de mera comunicação. Possibilitam o seguimento de boas práticas obrigatórias para garantir a validade das bases legais escolhidas.

### 2.3 O paradigma da privacidade e a Lei Geral de Proteção de Dados e a colisão entre direitos à Vida Privada versus Liberdade de Expressão e Informação

O direito contido na Carta Magna do Brasil a privacidade e vida íntima é também elencado nas constituições mundo afora, e inclusive, motivos de discussões e de comprometimento de cooperação a nível internacional por meio de pactos firmados entre os Estados. Isso apenas demonstra o quão importante é o resguardo desse direito, que no Brasil é garantido por meio de cláusula pétrea, ou seja, não pode ser modificado (BRASIL, 1988).

Em 1966, o Pacto Internacional de Direitos Civis e Políticos, resguardou em seu art. 7, a proteção à privacidade quando afirmou que: “Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação”

Na verdade, esse foi e é um dos motivos principais e mais discutidos dentro da Lei Geral de Proteção de dados no Brasil e em outras leis editadas por outros Estados. Tonou-se tão crítico a conectividade excessiva da vida moderna proporcionada pela internet e aparelhos eletrônicos que culminou na necessidade de criar formas que permitissem o resguardo da intimidade, tendo em vista que, no momento atual é cada vez mais esfacelada.

Os inventos criados pelos grandes cientistas e estudiosos facilitaram de uma forma estrondosa a vida das sociedades em geral, de forma a trazer facilitadores para desde pedir uma refeição em aplicativos de restaurantes ou até realizar uma reunião de trabalho. De uma forma ou de outra, toda a tecnologia envolvida e disponibilizada trouxe consigo a violação da vida privada das pessoas, pela clara exposição que as pessoas têm e seus dados (ZANINI, 2015)

Após o término das guerras mundiais e com a Declaração Universal de Direitos Humanos no ano de 1948, houve uma grande discussão acerca dos direitos básicos para a existência humana, à época, isso começou a ser prioridade para os juristas. O desafio era encontrar um padrão de definição para que com ele pudessem estabelecer leis e pontos de referência nos casos práticos do dia a dia.

Nessa esteira, a previsão de direitos de personalidade, que se remetiam justamente a ideia de direitos básicos humanos, foi vislumbrada na Constituição da Alemanha (Constituição Weimar), onde foi incluído que os direitos para livre desenvolvimento da personalidade deveriam ser resguardados. Foi dada a mesma ênfase no Brasil no Código Civil de 1916, onde os doutrinadores já verificavam a importância da tutela dos direitos da personalidade. Já no Código Civil atual essa garantia é expressamente prevista (BIONI, 2018, p. 55-56).

Dentre o rol de direitos que são resguardados pela personalidade, um deles é o Direito a Privacidade, o qual, conforme afirma Mendes (2014, p. 102), “atua a serviço da promoção da dignidade da pessoa humana”. O Direito a privacidade faz parte dos direitos básicos que concedem Dignidade ao cidadão.

Como aludido, falar de garantir direitos de Personalidade é se referir a Privacidade. Reconhece-se que o Direito há muito tempo já vem tratando sobre essas problemáticas, só que, todos de forma geral só vieram se atentar o quanto é crítico a questão do compartilhamento dados após diversos escândalos e exposições midiáticas.

Em vista disso, Marineli (2017, p. 1) destaca que “entre as violações perpetradas por pessoas e redes sociais mal-intencionadas, os danos à privacidade ganham destaque e já figuram entre as principais preocupações dos internautas”. Essas grandes exposições de muitas pessoas e criação de um mercado lucrativo ilegal de compartilhamento de dados foram o que resultou em leis de adequação para que houvesse um bloqueio dessas ações de baixo para cima.

Segundo Doneda (2006, p. 60) à época de sua obra já previa aquilo que era notório a muitos, destacando que o problema da privacidade “sempre foi diretamente condicionado pelo estado da tecnologia da sua época” e seu fundamento principal era condicionado de acordo com a evolução tecnológica do momento vivido. Com o tempo, foi o que aconteceu, com o crescimento tecnológico e a difusão de informações que cada vez mais crescia desenfreadamente e sem limites. Um mundo que ainda era novo e pouco explorado pelo juristas e doutrinadores que ainda tentavam entender como aconteciam as situações para expressar teses e opiniões.

Ao que pese tudo isso, falar de Privacidade é também falar de sigilo, podendo ser mais específico, refere-se a sigilo de contas bancárias ou de senhas de redes sociais, informações de movimentações e de chaves de aplicativos de bancos que permitem a invasão e a fraudes de diversos tipos. É exatamente este o paradigma da privacidade, que seja, a proteção contra invasões para roubo de informações que podem ser usadas por outros indivíduos para fins ilícitos, gerando transtorno e prejuízos.

E, quando se fala em proteção de dados, não se pode pensar somente em estelionatários, chantagistas, hackers e golpistas, mas também em terceiros que atuam de forma legítima, ou seja, você assina um contrato, cede seus direitos e informações, que são mascarados com cadastros, assinaturas ou até mesmo de pesquisas opinativas. Muitas empresas que se envolvem nessas ações, após a vigência da LGPD sofrerão fiscalizações, e caso seja encontrado algo fora das diretrizes da lei, a empresa ou órgão público será multado em advertências que vão de pagamentos iguais a 2% do faturamento, até um limite de R\$ 50 milhões.

Com essa nova dimensão, a Lei de Dados não deve somente se prestar a lidar com o óbvio, mas sim, com todas as nuances que fazem parte desses diálogos.

“Em perspectiva histórica mais recente, Tapper (1973) identifica duas maneiras de violação de privacidade. A primeira consiste na coleta de informações pessoais a segunda concentra-se no seu uso. O primeiro modo de violação da privacidade pode ser realizado de dois modos: ilícito, quando clandestinamente, alguém coleta informações pessoais, a fim de descobrir aquelas que ainda não se tornaram públicas; lícito quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa.” (FORTES, 2016)

Como já debatido, dentro das diversas facetas de possibilidades de tratamento de dados ilegais, tem-se a invasão propriamente dita e mascarada como um termo aparentemente legal ao usuário, sem saber, seus dados são usados para fins díspares do que foi autorizado. Isso diz muito sobre o quanto é relevante contar com uma legislação que consiga manter a confidencialidade dos dados. Ademais, com a popularização de atos como *revenge porn*, que é quando por vingança o ex-companheiro ou qualquer outra pessoa divulga amplamente vídeos e fotos íntimas com alegações que forma concedidas à época pelo titular.

A lei, em seus próprios princípios já abarca todas essas questões quando prevê que nenhum dado mesmo consentido poderá ser usado com caráter vexatório e ilegal, estabelecendo punições aqueles que agirem de forma contrária. Aliada a isso, desde 2012 já se tem Lei 12.737/2012, Lei Carolina Dieckman, onde se inseriu o artigo 154-A e 154-B ao Código Penal, tonando crime o ato da invasão a dispositivos para obter vantagem ilícita. Esse é um exemplo claro de ataque a privacidade e intimidade do cidadão.



No que se refere a colisão dos princípios de Liberdade de Expressão e vida privada, passou-se a discutir muitos imbróglios que são trazidos com a norma, como conflito entre os princípios da dignidade, privacidade, intimidade e honra versus os princípios da informação, liberdade de expressão e publicidade dos atos público, todos previstos na Constituição Federal de 1988. Do ponto de vista histórico, na dimensão empírica, os direitos fundamentais são, originalmente, direitos humanos (GUERRA FILHO, 2003).

De acordo com o pensamento de Bobbio (2004) os sujeitos desses Direitos Pessoais são a família, o povo, a nação e a própria humanidade, sendo assim, uma vez que é infringido, atinge a todos e não somente as pessoas presentes na situação em questão. E quando há colisão de direitos, eles devem ser sobrepostos analisando a aplicabilidade da melhor decisão que resultem em resguardo da Dignidade da Pessoa Humana, com base na situação prática, a melhor decisão.

Fato é, que desde a primeira semana de julho de 2021 essas lides foram levadas a debates no judiciário, conforme levantamento realizado pela entidade *Juit*, demonstrando que entre setembro de 2020 e junho de 2021 já ocorreram aproximadamente 600 decisões judiciais com fulcro na Lei Geral de Proteção de Dados. Boa parte dessas ações se referia a exposição pessoais de dados em sites de buscas como a Google e Yahoo. O pedido principal é que seja excluído dados que são encontrados facilmente ao buscar seu nome, podendo encontrar um processos trabalhistas ou processos onde sofreram uma condenação, por exemplo (SOPRANA, 2021).

A situação da colisão desses princípios se torna mais crítica se vê as decisões dos tribunais superiores com repercussão geral, que, no Recurso Extraordinário nº 1.010.606/RJ (sobre pedido para que não fosse mais divulgadas informações e reconstituições referentes ao assassinato de Aída Jacob Curi, ocorrido no ano de 1958, na cidade do Rio de Janeiro), votou em 11 de fevereiro de 2021 contra o direito ao esquecimento.

Ressalta-se que o direito à liberdade de expressão e vida privada se encontram em pontos significativos e se contrapõem em outros, a linha de encontro é tênue, vez que o direito de expressão possibilita para além da liberdade de o cidadão se expressar, que esse mesmo cidadão possa ser informado, todavia essas notícias não podem entrar em choque com o direito a vida privada, um não pode de forma alguma se justapor ao outro. O vazamento de dados faz com que ocorra o contrário disso, por mais que seja justificado o direito à informação, jamais poderá se colidir com a vida privada, uma vez feito isso, o cidadão está fora de seus direitos, prerrogativas legais e dignidade.

A constituição Federal de 1988 elenca em seu preâmbulo o seu objetivo primordial que é “*instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos (...)*”. Melhor dizendo, se há dúvidas entre a aplicação de um princípio e outro, deve-se sempre priorizar aquele que traga bem-estar e justiça, impedindo que se gere atitudes ilegais e preconceitos. Portanto, o princípio da dignidade, honra e imagem devem ser prioridade (BRASIL, 1988).

Essa previsão também está situada no art. 3º, inciso IV, prescreve que “constituem objetivos fundamentais da República Federativa do Brasil promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação” ao passo que o artigo 4º, inciso II, determina que “a República Federativa do Brasil se rege nas suas relações internacionais pelo princípio da prevalência dos direitos humanos” (BRASIL, 1988).

O art. 5 da CF/88, elenca uma série de incisos listando diversos princípios que reforçam direitos e garantias fundamentais, descrevendo várias vezes os direitos personalíssimos, excepcionalmente o direito à dignidade, honra e imagem, decretando, por exemplo, que “ninguém será submetido a tortura nem a tratamento degradante” (inciso III) ou que “*é inviolável a liberdade de consciência e de crença, o sigilo da correspondência e comunicações telemáticas*” etc.

Logo, a privacidade não pode ser defendida e vista apenas de uma única ótica, a privacidade como um direito pessoal e um direito que faz parte dos direitos fundamentais ao ser humano. Desse jeito, deve haver um controle no início com a captação e posteriormente no processamento e armazenamento, que é o foco da LGPD.

Verifica-se, ainda, que apesar de haver uma considerável colisão entre os dois direitos constitucionais, o Direito a Privacidade será reduzidos, assim como o da informação, com objetivo de permitir a existências de ambos e não sobrepor um ao outro. Decerto que o princípio da dignidade, intimidade, privacidade, honra e imagem, pela previbilidade legal dentro da constituição, mesmo que não sejam direitos absolutos, devem se sobrepor sobre quaisquer outros princípios e direitos quando há dúvida ou dicotomia entre os princípios.

### **3 RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO**

O presente capítulo abordará as correntes doutrinárias de interpretação que são base para o entendimento da Responsabilidade Civil, que irá ser aplicada no contexto da LGPD no que tange a responsabilização das empresas. Além disso, traz os conceitos dos tipos de responsabilidades, que são a subjetiva e objetiva, apresentando suas diferenças. No mesmo desenrolar, demonstra as correntes dualistas de interpretação e uma outra visão dada à culpa e ao risco, critérios trabalhados na responsabilização civil.

Na sequência, buscará desenvolver os aspectos sobre a permissividade e consentimento do titular dos dados, demonstrando os limites desse consentimento e até onde isso concede legalmente direito a divulgação destes. Disto isso, apresentará como esses dados devem ser tratados e os limites legais de sua utilização e compartilhamento. E ainda, esclarecer como ocorre a responsabilidade de um terceiro nessa relação e quais consequências podem ser sofridas em razão de más condutas.

Em síntese, discutirá de que forma as empresas privadas poderão ser responsabilizadas civilmente, trazendo isso para após a vigência da LGPD ter surgido a obrigatoriedade de adequação das empresas, sob pena de responderem civilmente pelo seu descumprimento. Conceituando e de mesma forma norteando como será feita essa responsabilização e aplicação do que já se tem hoje como Responsabilidade Civil.

#### **3.1 Correntes Doutrinárias de Interpretação**

No decorrer do tópico, far-se-á uma apresentação de posicionamentos doutrinários a respeito dos critérios utilizados na Responsabilidade Civil, bem como aplicada a LGPD. De forma que, exponha o que é feito hoje e o que é consolidado entre os doutrinários brasileiros, além de expor como já está sendo trabalhado esses conceitos dentro dos processos existentes que tratam de Responsabilidade Civil na LGPD. Nesse cenário, irão ser apresentadas as teorias utilizadas para caracterização e Responsabilidade e qual aplicada atualmente pelo judiciário brasileiro e como isso irá refletir na imputação de responsabilidade para àqueles que transgredirem as normas convencionadas na LGPD.

### 3.1.1 Responsabilidade Civil subjetiva e objetiva

A Responsabilidade Civil nasce de um dever de indenizar o outro quando estiver provado que houve prejuízo a terceiro por conduta causada a quem recaí o dever de indenizar, que pode ser contratual ou extracontratual. GAGLIANO; PAMPLONA FILHO (2019, p. 51) define responsabilidade civil como o que se “pressupõe a atividade danosa de alguém que, atuando a priori ilicitamente, viola uma norma jurídica preexistente (legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar)”.

Dias (2015, p. 01) revalida o conceito supracitado e menciona que “toda manifestação da atividade humana traz em si o problema da responsabilidade”. Com base nisso, o Código Civil de 2002, dispõe em seus artigos 186 e 187 o que segue:

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. (BRASIL, 2002)

Desse modo, pode-se compreender que responsabilidade civil para o Direito brasileiro é aquilo que “deriva da agressão a um interesse eminentemente particular, sujeitando, assim, o infrator, ao pagamento de uma compensação pecuniária à vítima, caso não possa repor in natura o estado anterior de coisas” (GAGLIANO; PAMPLONA FILHO, 2019, p. 51).

No sistema da Responsabilidade subjetiva, deverá haver a caracterização do dolo e culpa. Dessa forma, alguém deverá agir com intenção de se obter um resultado danoso a outrem ou agir com a falta de cuidado devida, parâmetros imprescindíveis para ter a obrigatoriedade do dever de indenizar. Nas palavras de GAGLIANO; PAMPLONA FILHO (2019, p.57):

“A noção básica da responsabilidade civil, dentro da doutrina subjetiva, é o princípio segundo o qual cada um responde pela própria culpa — unuscuque sua culpa nocet. Por se caracterizar em fato constitutivo do direito à pretensão reparatória, caberá ao autor, sempre, o ônus da prova de tal culpa do réu. Todavia, há situações em que o ordenamento jurídico atribui a responsabilidade civil a alguém por dano que não foi causado diretamente por ele, mas sim por um terceiro com quem mantém algum tipo de relação jurídica”

Nesse sentido, existe a possibilidade de responsabilizar o causador direto do dano e o terceiro que possui alguma ligação dentro do nexo de causalidade que gera o dever de

indenizar. Sendo assim, é o mesmo previsto no art. 42 da LGPD, que dispõem “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”. A lei faz recair responsabilidade em ambos, tanto do controlador dos dados, quanto de quem faz a operação desses dados.

A LGPD não traz em seu arcabouço jurídico qual seria a teoria utilizada para discernir quando haveria Responsabilidade Civil e quando não. O texto expõe desde os critérios para reparação de danos às circunstâncias que caracterizam um tratamento irregular, mas não especifica o regime. Diante disso, não fica claro se deve haver comprovação de culpa para haver indenização. Pelo que se extrai do Código Civil, há uma prevalência na aplicação da Responsabilidade Subjetiva, onde precisa haver a configuração de culpa para se ter responsabilidade.

As professoras Gisela Sampaio da Cruz Guedes e Rose Melo Venceslau Meireles (2019), por mais que sejam defensoras da aplicação da responsabilidade subjetiva, relatam que nenhum dos quatro artigos “deixam claro qual foi a espécie de responsabilidade adotada pelo legislador”, afirmando ainda que “a LGPD deveria ter sido explícita em relação à natureza da responsabilidade, porque isso evitaria uma série de controvérsias que inevitavelmente vão surgir em razão dessa falta de clareza”.

Diante da ausência da Lei, resta a análise dos artigos. É necessária uma análise sistemática dos dispositivos, onde pela breve leitura se conclui que se fala da culpa. Dessa forma, é observado por Gisela Sampaio da Cruz Guedes e Rose Melo Venceslau Meireles (2019), o seguinte “se o que se pretende é responsabilizar os agentes, independentemente de culpa de fato, não faz sentido criar deveres a serem seguidos, tampouco responsabilizá-los quando tiverem cumprido perfeitamente todos esses deveres”.

Tão logo que, os arts. 46 a 51, da Lei, que nomeia o capítulo “da segurança e das boas práticas”, destacando-se os art. 50, bem como o art. 6, X, onde se verifica a utilização dos termos “princípio da responsabilização e prestação de contas”, intitulado pela lei como a necessidade de demonstrar que há o cumprimento devido da lei de proteção de dados pessoais, e ainda a o êxito em sua aplicação.

De modo que, conforme observam as professoras Gisela Sampaio da Cruz Guedes e Rose Melo Venceslau Meireles (2019), a perspectiva trazida pela lei, torna evidente o estabelecimento de uma “um verdadeiro standard de conduta”, que se baliza em um conceito de “culpa normativa”. Para isso, há um afastamento do que se compreende do conceito tradicional de culpa na Responsabilidade Civil, não sendo pautado por uma análise

comportamental, mas sim, pelo cumprimento ou não da norma jurídica vigente. À vista disso, a lei trabalha na especificação dos comportamentos obrigatórios e esperados, e o que foge disso será tido como motivo justificado de culpa.

Com isso, para as professoras, torna-se entendido que há caracterização de culpa, todavia, de uma linha diferente do que é feito atualmente na aplicação de Responsabilidade Civil aos agentes causadores dos danos. Outro ponto caracterizador da ideia de culpa é observado na excludente da responsabilidade no art. 43, II: a ausência de “violação à legislação de proteção de dados”. O dispositivo, não se relaciona a nexos de causalidade e colide com incisos do art. 12, § 3, do CDC, que inspirou a criação do art. 43 da LGPD.

Pode-se entender pelo que disciplina o art. 43, II, o agente que trata os dados pode se eximir de responsabilidade quando mesmo existindo nexos causal, conseguir comprovar que cumpriu todos os deveres impostos e obrigatórios pela LGPD. Assim, verifica-se que a culpa é um dos requisitos para reparar o dano, contudo, ela se faz valer quando houver comprovadamente ausência de violação da lei (GUEDES; MEIRELES, 2019).

É possível identificar que além da responsabilidade civil subjetiva, existe aplicação e previsão legal da responsabilidade objetiva no Código Civil de 2002. Dentro da Responsabilidade objetiva, não é necessário sequer ser caracterizada a culpa, pois, o dolo ou culpa são irrelevantes juridicamente, será preciso somente a existência do elo de causalidade do dano e da conduta do agente para que haja o dever de indenizar (GAGLIANO; PAMPLONA FILHO, 2019).

No mesmo pensamento de que há culpa no dever de indenizar proposto pela LGPD, deve-se observar o que conclui Bruno Bioni e Daniel Dias (2019, p.7), que fazem análise do mesmo art. 43, II, da LGPD, concluindo que a lei não faz somente uma excludente de ilicitude como prevista no CDC. Para os autores, acrescido a principiologia e a “outras partes importantes e integrantes do texto da LGPD” (a seção específica sobre “boas práticas e governança” e a previsão dos “relatórios de impacto à proteção de dados pessoais”, por exemplo), afastam o que se entende pelos doutrinadores brasileiros de responsabilidade civil objetiva, tendo em vista que se tem a existência de “elementos normativos que, direta ou indiretamente convergem para que haja um juízo de valor em torno da culpa do lesante”.

Os autores Bruno Bioni e Daniel Dias (2019), apesar de defenderem a tese de que a existência de culpa é um ponto chave para responsabilizar o agente na LGPD, apontam que é inegável que o titular dos dados está em relação de hipossuficiência perante o controlador e operador. Além do que, muitas vezes o titular nem tem ciência que seus dados foram

armazenados e como estão sendo tratados, o controle dos dados é de uma certa forma totalmente de conhecimento do operador e controlador, e o titular fica à margem de tudo isso.

Para isso, a lei convencionou que “a culpa e autoria do agente de tratamento de dados são presumidas”, e determina pela leitura do art. 43, excludentes de responsabilidade, ao que passo que no disposto no art. 42, §2, “pode haver a inversão do ônus da prova quanto aos demais pressupostos”. Dessa forma, fecham seu pensamento que além da discussão da binariedade do dever de indenizar, existe ainda uma discussão profunda sobre aplicação e determinação da culpa, e assim conforme afirmado por TASSO (2020, p. 105), estar-se diante “de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade”.

Na mesma linha de raciocínio dos autores citados, o entendimento do juiz do Tribunal de Justiça da Bahia, Cícero Dantas Bisneto (2020, p.14-15), é o de que a falta de clareza da lei, considerando que é “a coleta e tratamento de dados constitui atividade de risco”, deturparia a regra geral como a utilização do art. 927, parágrafo único, do Código Civil. Ainda relata que o fato de se ter uma cláusula geral de responsabilidade objetiva, não quer dizer que autoriza a quem interpreta e aplica “uma discricionariedade sem limites, como se a generalidade do dispositivo normativo concedesse ao aplicar do direito os meios para se atingir qualquer fim pretendido, ainda que sob a justificativa de uma suposta equidade”.

Os doutrinadores Leonardo Corrêa e Tae Cho, coadunam para o mesmo entendimento, considerando ainda pontos-chaves do porquê a culpa deve estar presente dentro da responsabilização civil na LGPD. Pois, trata-se de uma lei “criada especificamente para tratar de dados em uma sociedade de informação digital”, onde rejeitar o seu entendimento conjuntamente com outra lei seria “um desprezo ao desenvolvimento tecnológico, um desserviço ao país e um mal-uso do processo legislativo que culminou com a LGPD”. Outro argumento, tomando como base a implementação do entendimento da responsabilidade objetiva seria que “o país poderá dar passos gigantes para trás no que se refere à tecnologia, com custos enormes para a sociedade como um todo”.

É possível identificar que além da responsabilidade civil subjetiva, existe aplicação e previsão legal da responsabilidade objetiva no Código Civil de 2002. Dentro da Responsabilidade objetiva, não é necessário sequer ser caracterizada a culpa, pois, o dolo ou culpa são irrelevantes juridicamente, será preciso somente a existência do elo de causalidade do dano e da conduta do agente para que haja o dever de indenizar (GAGLIANO; PAMPLONA FILHO, 2019).

No que concerne a responsabilidade civil objetiva, os elementos que constituem esse ponto são apenas o dano e o nexo causal para que seja designado a obrigação de indenizar,

ou seja o elemento da culpa é presumido por isso não é dispensável. Nessas situações, há atribuição de Responsabilidade Civil a alguém por dano que não foi causado diretamente por ele, e sim por um terceiro que mantém relações (COELHO, 2020).

De forma mais abrangente, Cavalieri Filho (2019) atrela o conceito de Responsabilidade civil objetiva à teoria do risco, nesta linha, o autor compreende esta teoria de modo que:

Todo prejuízo deve ser atribuído ao seu autor e reparado por quem o causou, independentemente de ter ou não agido com culpa. Resolve-se o problema na relação de causalidade, dispensável qualquer juízo de valor sobre a culpa do responsável. Na responsabilidade objetiva é irrelevante o nexó psicológico entre o fato ou atividade e a vontade de quem a pratica. Enquanto “a culpa é vinculada ao homem, o risco é ligado ao serviço, à empresa, à coisa, ao aparelhamento. (CAVALIERI FILHO, 2019, p.351– 352).

Por esse ângulo, basta que a conduta do agente, gere resultado danoso a outrem, mesmo que sem intenção, já que, a configuração da culpa não é necessária, mas tão somente a prática do ato. É isso que no entendimento geral a LGPD aplica, as exposições das condutas pelo legislador, é justamente para que possa haver uma adequação geral, uma vez que, não poderá haver alegação de falta de intenção dentro da conduta executada.

Os autores que se alinham a esse entendimento, tai como Danilo Doneda e Laura Schertel Mendes (2018, p. 469-483), verificam que “o tratamento de dados apresenta risco intrínseco aos seus titulares”. Baseando-se na ideia central trazida pela lei de que se tenta restringir ao máximo o cenário no qual o tratamento de dados é permitido, limitando a coleta de dados para situações realmente necessárias e justificadas, restringindo o compartilhamento e coleta de forma desordenada dos dados dos titulares.

Nesse contexto, correspondem suas ideias ao disposto no art. 7 da LGPD, que conta com os pontos específicos nos quais os dados podem ser coletados; a exposição do art. 6, que versa sobre III (“princípio da finalidade”) e II (“princípio da adequação”, cujos termos prescrevem que o tratamento não deve ser admitido quando for inadequado ou desproporcional “em relação à sua finalidade”); o art. 16 impõe “eliminação dos dados quando seu tratamento esteja encerrado”. E ainda, a exposição da lei no que se refere ao fato da obrigação “de se levar em conta o risco presente no tratamento de dados” (DONEDA; MENDES, 2018, p. 469-483).

Desse modo, entende-se que a conclusão dos autores para a existência de Responsabilidade objetiva é a preocupação da lei em dirimir as hipóteses permitidas de tratamento, criando restrições, e caracterizando a atividade de tratamento de dados como sendo



de risco. Sendo tal fator, motivação suficiente para atrair responsabilidade independente de ter agido com conduta culposa.

No mesmo raciocínio de configurar que a atividade de tratamento “impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade”, tem-se a opinião de Caitlin Mulholland (2020, p.1)), que alinha seu estudo à um viés diferente do que aponta Danilo Doneda e Laura Schertel Mendes. Nessa perspectiva, para a autora o que faz se entender pelos riscos nas operações de dados é que se trata de “danos a um direito fundamental”, e outro ponto é de que “tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que por si só, já justificaria a adoção da responsabilidade civil objetiva”.

Outra autora que também entende nesse sentido de responsabilização objetiva em razão da proteção de dados se tratar de um direito fundamental é José Carlos Massarelli Jr., Verônica Scriptor Freire e Almeida (2019, p.538-539), que é posição descrito no art. 8º da Carta de Direitos Fundamentais da Comunidade Europeia. Outrossim, não se encontra na análise dos autores Sthéfano Bruno Santos Divino e Taisa Marina Macena de Lima (2020), exclusão dos pressupostos de responsabilidade objetiva no art. 43 da LGPD, sendo assim, não pode ser utilizado como meio de se evadir.

Nesse aspecto, a utilização do art. 43 da LGPD, está sendo interpretado de forma dúbia do que se pretende, vez que, em nenhum momento cita a retirada dos pressupostos de culpa, mas tão somente expõem pontos excludentes do dever de indenizar, pois, a própria lei estabelece o que deve ser observado pelo agente. Além do que, em nenhum momento é exposto pelo art. 43, que “verificação de culpa ou dolo como elementos necessários à caracterização do dever de reparar” (GODINHO; QUEIROGA NETO, TOLEDO, 2020, p.15)

Compreendendo de forma diferente, o autor Walter Aranha Capanema, aponta em toda sua análise da lei, que o fato de se enxergar o titular dos dados como hipossuficiente é já motivo suficiente de se entender que é descartável que seja configurado o elemento culpa para atribuir responsabilidade. Indo além, pela Autoridade Nacional de Proteção de Dados estabelecer norma de cunho administrativo, o descumprimento da lei poderá ser atrelado tanto ao descumprimento de norma jurídico e técnicas (CAPANEMA, 2020).

No que se refere a tese de que entender que a Responsabilidade Civil é um retrocesso, reafirma-se que, desde o advento do CDC, estar-se diante de uma sociedade altamente tecnológica, ainda mais no que se trata de crimes cometidos para dados tratados de forma digital. Logo, não haverá injustiças, pois, para que seja imputada responsabilidade, deveria ser feito sob análise do que trata a lei que especifica exatamente as normas a serem

observadas e ainda elenca no art. 43, excludentes de responsabilidade caso haja cumprimento das normas (PAIM; GONÇALVES, 2020)

Entendendo-se que a nova concepção no Brasil é de que existe um duplo entendimento do conceito de Responsabilidade, em que temos a vigência da Responsabilidade Civil subjetiva, em simultaneidade com a Responsabilidade Civil Objetiva. Assim, evidencia-se que a Responsabilidade civil, em seu bojo, contém a presença da reparação e do sujeito passivo como elementos indispensáveis pautados na relação jurídica que se institui em detrimento da ocorrência de uma violação à ordem jurídica.

Desta maneira, analisando o que traz a lei, bem como seus pressupostos obrigatórios, é inegável o sentimento de que não há clareza na linha de raciocínio do legislador, ainda que, exija-se pontos que se remetem a responsabilidade subjetiva, de outro lado, haverá situações que a percepção objetiva irá prevalecer. Muito embora seja possível o entendimento dos artigos no entendimento completo da lei, as lacunas deixadas pelo legislador poderão gerar conflitos em posteriores discussões judiciais.

### 3.1.2 Corrente dualista e perspectivas contrárias à culpa e ao risco

Conforme observado nos conceitos de responsabilidade civil subjetiva e objetiva mencionadas no tópico anterior, dentre os aspectos que compõem as concepções conceituais existem elementos fundamentais que são como requisitos às modalidades de responsabilidade civil e, dessa forma, faz-se pertinente tratar destes elementos no presente tópico.

Nesse contexto, o presente tópico abrange o entendimento de que as chamadas “correntes dualistas” contemplam as concepções doutrinárias que asseveram uma solução intermediária em comparação às demais, haja vista que entendem a perspectiva que mesmo quando aplicáveis as disposições da LGPD, é possível que o causador do dano seja responsabilizado ou subjetiva, ou objetivamente, tal parâmetro irá depender diretamente da análise de cada caso concreto.

Ferreira (2019, p. 134), no que tange a responsabilização no âmbito da aplicação da LGPD, enfatiza que em linhas gerais, aplica-se a responsabilidade subjetiva, considerando a questão da omissão legal, e que, em tese, “o tratamento de dados não é uma atividade que traz graves riscos aos titulares, a ponto de atrair a aplicabilidade de “alguma das teorias do risco”.

Ainda na perspectiva dualista, Schreiber (2021, p. 319) aponta para uma outra análise ao fazer uma crítica à própria letra da lei da LGPD:

“O próprio texto legal da LGPD, o qual, segundo sua perspectiva, “não foi extremamente feliz no desenho das normas atinentes à responsabilidade civil”, de modo que existem “falhas e omissões que podem e precisam ser sanadas pelo intérprete” na busca por uma solução “a um só tempo, coerente e eficaz. No que tange ao artigo 42 apesar de, por um lado, o dispositivo não aludir “em sua literalidade, à culpa”, também é verdade que, por outro, deixa de se valer da expressão “independentemente de culpa”, motivo pelo qual, à luz especificamente do referido preceito normativo, dele se pode inferir, porquanto incontroversa a omissão, “uma preferência pela responsabilidade subjetiva”.

Desse modo, diante de tal crítica, o autor faz uma ressalva no que tange a aplicação da letra da lei LGPD, de maneira que infere que a interpretação dos dispositivos legais não pode ser feita de forma isolada e centralizada, para que não se recaia em omissões impõe-se a leitura e interpretação desses dispositivos em conjunto com outras disposições que lhes são conexas e poderão contribuir para uma melhor análise do caso concreto.

Nesse sentido, quanto ao disposto no artigo 42, Tasso (2020, p. 45) preleciona “que são utilizados apenas dois critérios objetivos para fundamentar a responsabilidade, quais sejam, o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados”, assim, para o autor, o disposto no referido artigo não prevê e tampouco exclui o elemento culpa. Diante disso, compreende-se que a falta de clareza da letra lei quanto à responsabilização civil pressupõe que há uma determinada imprecisão normativa no que tange a temática adotada pela LGPD.

O referido autor, menciona que adere a teoria dualista, uma vez que a aplicação do tipo de responsabilidade civil dependerá de cada caso concreto, mensura que:

Dessa forma, segundo o entendimento do Supremo Tribunal Federal, a responsabilidade estatal no espectro das atividades de tratamento de dados pessoais é analisada segundo os critérios da responsabilidade objetiva para os atos comissivos, aqui exemplificados como o tratamento e o compartilhamento irregular de dados e, por outro lado, segundo os pressupostos da responsabilidade subjetiva em se tratando de ato omissivo, como, por exemplo, a não observância das normas de prevenção e de segurança da informação a oportunizar o vazamento de dados pessoais dos cidadãos (TASSO, 2020, p. 105).

Portanto, o autor responde de forma concisa as imensas lacunas legais nos quais a lei não esclareceu, prevendo que para atos em que o agente tenha praticado conduta que incorra em infração da lei, será responsabilizado por meio da tese objetiva; já quando não houve observância das normas de proteção de dados deverá ser aplicado a tese subjetiva, muito embora a lei não direcione corretamente esses pontos, os entendimentos dos artigos conduzem a esse entendimento.

Todavia, embora seus estudos corroborem para o entendimento desta corrente dualista, Tasso (2020, p. 113) assim como outros doutrinadores, ponderam que a própria LGPD adotou a Responsabilidade Civil subjetiva em suas aplicações no caso concreto:

A despeito dos embates doutrinários, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza.

Verifica-se que apesar desse entendimento, não pode ser tido como verdade absoluta, pois, os embates jurídicos ainda estão acontecendo de forma tímida, levando em consideração que se trata de uma lei nova. Apesar de sua publicação em 2018, somente começou sua vigência em 18 de setembro de 2020, à exceção das sanções administrativas, que passaram a ser exigíveis a partir de 1º agosto de 2021, nos termos da Lei nº 14.010/2020. Pelos próprios estudos divergentes que já existem, os debates em âmbito legais serão ainda desenrolados e acalorados, atentando ao fato que a própria lei confere interpretação as duas correntes.

Assim, a respeito deste debate acadêmico, Bioni e Dias (2020) concluem que a LGPD elegeu a responsabilidade civil subjetiva, porém possui em seu bojo um alto grau de objetividade que recai principalmente sobre o dever de indenizar, por tanto, mencionam que a análise do caso concreto vá além da escola da teoria a ser adotada mas que o foco seja voltado para as questões normativas acerca do elemento culpa, por esta razão destacam:

Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade. (BIONI; DIAS, 2020, p.22).

Em suma, com base nas discussões, pode-se apreender que a própria Lei Geral de Proteção de Dados em si elegeu o sistema de responsabilidade civil subjetiva, conforme elucidado por alguns autores supracitados, com intuito precípuo de fomentar o fortalecimento de uma cultura de proteção de dados no Brasil.

Em contrapartida, depreende-se, com base em parte da doutrina, que há a possibilidade de haver a responsabilização objetiva na aplicação da LGPD no que se refere ao

tratamento de dados quando se tratar de relação de consumo com base no que estabelece o Art. 45 da LGPD que dispõe que ao se estar diante de hipóteses de violação no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas no CDC.

### 3.2 O Consentimento do titular dos dados e a responsabilização civil de terceiro

O consentimento do titular dos dados recebeu guarida destacada pelo legislador na elaboração da LGPD, estabelecendo em seu art. 7, quando os dados poderão ser colhidos, e ainda ressalva, que em muitos casos não somente o consentimento do titular será suficiente, visto que, em caso de dados sensíveis, necessitará de uma motivação legal. Esse aspecto do consentimento segue o modelo europeu e de diversas outras leis que abordam o assunto de tratamento de dados (TEPEDINO; TEFFE, 2019).

Nessa esteira, para o consentimento dos dados é analisado o art. 7 da lei, que estabelece os critérios de como o consentimento deve ocorrer. Contudo, para os dados sensíveis, esses foram exemplificados de forma mais rígida no art. 11, que inclusive, verifica o tratamento dos dados de menores de idades, que devem ter o consentimento dos responsáveis para poder coletá-los.

Em um momento em que nunca se falou tanto em tecnologia e que houve reorganização nas formas de comunicação, sendo que, a previsão é que seja cada vez mais tecnológico, criou-se uma mercantilização dados. Ora, com determinados dados se consegue traçar um perfil do usuário e saber exatamente como direcionar propagandas, produtos e até mesmo limitar a opção do titular, que em muitas das vezes está alheio ao que acontece consigo.

Por isso mesmo, importante foi a decisão que entendeu a proteção de dados como de cunho de um direito fundamental, pois se relaciona com a promoção da personalidade e que delimita a esfera privada. Referindo-se a autodeterminação existencial e informacional do ser humano, decerto que é imprescindível para a proteção do indivíduo e de sua intimidade, bem como de controlar seus dados (DE TEFFÉ; VIOLA, 2020).

A LGPD traça o consentimento como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Art.5º, XII). Mantendo exatamente o que preleciona a GDPR, veja-se “manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”.

Os autores DE TEFFÉ; VIOLA (2020, p. 22), preveem que esse consentimento se espalha a todo e qualquer âmbito, gerando grandes impactos em diversas áreas, veja-se:

Após a previsão relativa ao consentimento, afirma-se que o tratamento de dados pessoais poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador, como obrigações trabalhistas, deveres oriundos da lei anticorrupção e a guarda de registros por determinados provedores na forma do Marco Civil da Internet. Outro exemplo são as empresas do setor de seguros ou do mercado financeiro, as quais estão submetidas a várias regras legais e regulatórias e devem cumprir obrigações que eventualmente poderão exigir o tratamento de dados pessoais de seus clientes. Uma política de privacidade e tratamento de dados bem desenhados e transparente pode ajudar a melhor esclarecer o uso dessa base legal pela instituição.

A regulação do consentimento do titular gera impactos gigantescos, em razão de forçarem os mais variados ramos e setores a se adequarem para fornecer esse tipo de informação caso solicitado. Toda essa modificação reflete obviamente em custos para os setores públicos, bem como os privados. Mesmo que a lei não trate disso de forma objetiva, serão esses os impactos gerados com as modificações e consentimento de mais poder ao titular.

O artigo 9º da LGPD, estabelece os limites de controle que o titular dos dados pode ter sob um viés legal, ou seja, caso o controlador não obedeça fornecendo as informações que se tornaram obrigatórias com a vigência da lei, incorrerá em descumprimento e poderá ser responsabilizado. Veja-se o que propõem o art. 9 da lei, in verbis:

Art. 9º - O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.

O art. 11 da LGPD, faz alusão ao tratamento de dados sensíveis, inicia o caput com a seguinte demanda “o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses”, prevendo as hipóteses nas quais o operador ou controlador poderá realizar a coleta desses dados. Ademais, descreve de forma detalhada diversas situações que podem ser enfrentadas na tratativa de dados sensíveis, e dispõem qual seria a conduta certa a ser tomada (BRASIL, 2018)

Em seu primeiro inciso já contém a seguinte disposição “I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas”. Nesse sentido, além de exigir de forma explícita a concessão do titular dos dados, é

imprescindível que a coleta seja justificada e devidamente descartada após a sua finalidade ser completado. Até porque, os dados sensíveis são informações muitas das vezes que se expostas ou compartilhadas sem nenhum cuidado podem gerar constrangimentos e danos na esfera moral irreparáveis.

É o que conclui os autores DE TEFFÉ; VIOLA (2020, p.3), quando diz “não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que seja considerado legítimo e lícito, sendo possível inclusive cumular as mesmas, assim como no GDPR”.

O art. 9, por seu turno, apresenta alguns dos direitos do titular no que tange às suas informações e seu tratamento, de modo que seja garantido a observância do princípio do livre acesso, de modo que tal dispositivo elenca:

[...]  
 I - finalidade específica do tratamento;  
 II - forma e duração do tratamento, observados os segredos comercial e industrial;  
 III - identificação do controlador; IV - informações de contato do controlador;  
 V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;  
 VI - responsabilidades dos agentes que realizarão o tratamento; e  
 VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. [...]. (BRASIL, 2018).

Com base neste princípio, elenca-se, ainda, os princípios da transparência e da qualidade dos dados; à vista disso, verifica-se que ao titular dos dados é garantido o direito de confirmar a existência de tratamento de seus dados, de modo que poderá ter acesso aos dados e a sua correção em caso de informações incompletas, inexatas ou desatualizadas (COTS E OLIVEIRA, 2019). Representa para o titular instrumento de controle sobre as suas informações pessoais e de garantia de direitos”; para Bioni (2020, p. 118) a respeito do consentimento do titular, pressupõe-se que:

A sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno de um controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular (...)

A preocupação dos debates em torno da temática do consentimento que permeia a Lei de Proteção de Dados, baseia-se no intenso anseio em torno do alcance do consentimento do titular para o tratamento de seus dados pessoais diante do contexto sócio histórico vivenciado

por uma sociedade cada vez mais intelectual que é orientada e movida por dados nas mais diversas áreas.

No que tange à figura de uma terceira pessoa no tratamento de dados, pode-se aferir que o §5º, ainda do artigo 7º dispõe que, para a comunicação ou compartilhamento de dados entre controladores diversos deve haver consentimento específico pelo titular. Cots e Oliveira (2019) sinalizam que, em contrapartida, até há a possibilidade de haver tratamento de dados pessoais de acesso público sem o consentimento do titular, de modo que se respeite as bases legais; os autores fazem a ressalva que nesses casos, os dados são públicos, como por exemplo, os encontrados em diários oficiais.

No que se estima sobre a responsabilização do vazamento de dados por terceiros, os autores supracitados afirmam que a LGPD, de certa forma, se mostra omissa e generalista quanto a questão; assim, compreende-se que quando houver vazamento de dados por ato de terceiros, os agentes responsáveis pelo tratamento estariam isentos da responsabilização frente ao titular dos dados.

Entretanto, sob o viés do que se tem hoje em relação a Responsabilidade Civil, principalmente a objetiva, o terceiro envolvido será também responsável, caso esteja dentro do nexo de causalidade. Apesar de a lei não tratar de forma explícita sobre isso, baseia-se no Código Civil de 2002, que trabalha tais conceitos quando houver terceiro dentro da relação no que tange a responsabilidade. Como a LGPD ainda não teve esses recortes, que acontecerão após a judicialização, ainda não se tem um parâmetro exato de como será atribuída essa responsabilidade legalmente ao terceiro.

Para tanto, deve-se ter o entendimento claro de que a ação de terceiros deve estar fora do ciclo de fornecimento de tratamento de dados, somente assim isentará o controlador de responsabilidade, para esse fim, compreende-se que a conduta lesiva ou a falha do terceiro deve ser exclusiva dele, de maneira que o controlador não pode ter agido com culpa no processo que ensejou tal vazamento.

### 3.3 A Responsabilidade Civil sob a ótica da LGPD e as empresas privadas

Pode-se verificar que o debate acerca da proteção dos dados pessoais é relevante e se faz pertinente no ordenamento jurídico, diante de uma sociedade que vive em constante mudança e se mostra dinâmica em relação às evoluções, denota-se que há uma crescente demanda virtual no que se refere aos tratamentos de dados das redes sociais até sistemas de



armazenamento e tratamento de dados de empresas privadas, o que mostra a grande necessidade de aprofundamento deste debate no que tange aos marcadores de responsabilização.

A revolução tecnológica, fez com que os setores privados e públicos modificassem sua forma de trabalhar e se adaptassem às novas dinâmicas. Sendo assim, grandes empresas tiveram que acompanhar à dinamicidade da sociedade, de acordo com Demócrito (2002, p. 26):

A disseminação do uso de computadores fez com que, nos dias atuais, não somente as agências governamentais que tradicionalmente coletavam dados pessoais, a exemplo dos Correios, os Departamentos de Trânsito e as repartições do Fisco, funcionassem como poderosos centros de processamento de informações pessoais, mas também todas as empresas privadas hoje adquiriram os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo

Pode-se compreender que no decorrer dos anos e das atualizações constantes que perpassa a sociedade e suas tecnologias surge, dessa forma, a constante necessidade de uma reflexão acerca da maneira de tratamento e controle sobre os dados pessoais, de maneira que cada vez mais os sujeitos são inseridos na relação jurídica e na proteção jurídica a seus direitos.

O art. 46 da lei, determina que o responsável pelo controle e operação irá responder pelos danos causados se deixarem de adotar as medidas de segurança, referindo-se ao “agente de tratamento”, que em sua maioria são empresas, que tem o dever legal de adotar medidas de segurança, buscando pugnar o vazamento de dados. Adotar medidas de segurança, técnicas e administrativas são um dever, para que não haja situações ilícitas ou mesmo destruição de informações importante. De mesma forma, incorrerão em responsabilidade quando houver perda, alteração, comunicação ou qualquer tratamento inadequado ou ilícitos sobre as informações (BRASIL, 2018).

Dessa forma, diante das últimas atualizações trazidas pela LGPD, há que se falar na adaptação de grandes empresas como multinacionais, empresas de capital aberto e empresas de grande porte em geral; vislumbra-se que para estes tipos de empresas o processo adaptativo é considerado mais fácil, de maneira que algumas dessas tiveram se antecipando após a publicação da Lei para se adequarem as exigências trazidas pela norma e verificar as condutas passíveis de responsabilização e culpabilização no tratamento de dados pessoais de seus clientes e/ou colaboradores.

Em relação a empresas menores, de pequeno porte e pessoas jurídicas privadas, a Resolução CD/ANPD N° 2, regulamenta a conduta de empresas desse porte que realizam tratamento de dados pessoais e que assumem obrigações típicas de controlador ou de operador:

Art. 9º Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada. Art. 10. A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da regulamentação específica. Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD. Art. 13. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro: I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, §§ 3º e 5º da LGPD, nos termos de regulamentação específica; II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos de regulamentação específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada regulamentação; III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD; IV - em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

As empresas de pequeno porte apesar de terem vantagem na simplificação tanto de tratamento dos dados quanto ao parecer obrigatório, de demonstração da entrada de dados e demais informações obrigatórias, não foram eximidas. Nota-se que, empresas que muitas vezes estão no limite de gastos orçamentários irão ter que desembolsar valores ainda que de forma simplificada para realizar adaptação, sob pena de sofrer uma responsabilização em âmbito administrativo e até judicial.

Pelo já mencionado, resta claro que irão ser passíveis de pagamento de danos. No processo nº 1080233-94.2019.8.26.0100, a juíza Tonia Yuka Koroku, da 13ª Vara Cível de São Paulo, julgou o processo e realizou condenação de uma empresa que atua no ramo imobiliário ao pagamento de R\$ 10 (dez) mil reais a um cliente, que sem seu consentimento teve suas informações compartilhadas com outra empresa. Observe-se trecho da decisão:

“Um dos direitos fundamentais do consumidor é de acesso à informação adequada acerca dos serviços que lhes são postos à disposição. Especificamente sobre o assunto referente ao tratamento de dados, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados LGPD) prescreve que são fundamentos da disciplina da proteção de dados, dentre outros, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade (art. 2º).

[...]

Patente que os dados independentemente de sensíveis ou pessoais (art. 5º, I e II, LGPD) foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD).

A decisão inaugurou em 29 de setembro de 2020, como primeira decisão judicial que tratou sobre o tema no estado de São Paulo, até então no desenvolver dessa pesquisa, que foi noticiado em sites e jornais de grande circulação. Portanto, as decisões de Responsabilidade serão trazidas para o mesmo contexto, analisando a situação e apregoando exatamente o que disciplina a lei.

Por isso, é de extrema importância a nomeação de um DPO para a empresa, a tradução do inglês é de “Chefe de Proteção de Dados”, será o encarregado de manter o canal de comunicação entre o operador e o controlador. O DPO será o elo entre todas as escalas de comunicação dessas tratativas, quais sejam cliente ou usuário e a empresa coletora dos dados. A outra principal é criar estratégias dentro da empresa para evitar o sancionamento de multas pela ANPD, Sanções estas que podem ir de advertência simples até multa de R\$ 50 milhões, dependendo do fraturamento da empresa (BRASIL, 2028).

Para a função de DPO é necessário relevante conhecimento técnico sobre a nova legislação e um conhecimento vasto sobre o organograma da empresa controladora dos dados, assim como a carteira de cliente e sobre sua atuação no mercado. Os requisitos para ocupação do cargo não se limitam a ser pessoa física ou jurídica, bem como necessariamente a profissão de advogado, precisa o domínio do assunto para ser nomeado ao cargo (MARTINS JUNIOR, 2020).

No Brasil, a obrigatoriedade do DPO não está nivelada ao que dispõem a GDPR, é o mesmo que descreve TRIVINO (2012, p.1):

“E quais são as atividades do Encarregado de Dados? (I) – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (II) – receber comunicações da autoridade nacional e adotar providências; (III) – orientar aos funcionários e aos contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (IV) – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Sendo assim, podemos concluir que o papel do Encarregado de Dados é obrigatório, possuindo um papel determinado, até que a ANPD diga ao contrário. Pode ser uma pessoa física ou jurídica, desde que com expertise para atuar em tal função”.

Dessa forma, para cargo será exigido de todas as empresas obrigadas a disponibilizar informações nesse sentido a ANPD, até que o órgão se manifeste sobre os casos que não necessitará que a empresa faça essa contratação ou direcionamento de cargo dentro de sua empresa. A problemática está em o estresse gerado, principalmente em empresas de pequeno porte a adequação e ainda ter que lidar com a contratação ou mesmo promoção de um funcionário a DPO.

Em pesquisa realizada pela PK HUB, que possui sede na cidade de São Paulo, realizou pesquisa em 2020 com diversas empresas que possuem setores que trabalham com assuntos relacionados a LGPD; o resultado foi: 53,3% das empresas pesquisadas ainda não nomearam um encarregado para a proteção de dados (DPO); 66,7%, ou seja, dois terços, ainda não treinaram seus colaboradores sobre as práticas a serem adotadas em relação à Lei de Dados; e por fim, um bem alarmante, 73,3% das empresas pesquisadas ainda não estabeleceram políticas adequadas sobre os riscos à privacidade dos dados (MARTINS JUNIOR, 2020).

Pelo que se extrai dos estudos de MARTINS JUNIO (2020), além de entender que o serviço do DPO não é algo de tarefa simples, sua pesquisa demonstrou que mesmo após a LGPD ter entrado em vigor, não houve movimentação das empresas, que ainda não trabalharam os aspectos básicos da lei que são um programa de governança em privacidade, que, caso existisse, facilitaria o trabalho do DPO.

Verifica-se que pode se tratar de um grande problema, pois, existem diversas sanções que podem sofridas pelas empresas que não observarem os ditames legais. Veja-se algumas das sanções que podem ser cumpridas, elencadas no art. 52 da LGPD:

1. Advertência, com indicação de prazo para adoção de medidas corretivas;
2. Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 por infração;
3. Multa diária, observado o mesmo limite total referido acima;
4. Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
5. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
6. Eliminação dos dados pessoais a que se refere a infração;
7. Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
8. Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período;
9. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados

Nessa perspectiva, para que haja um processo harmônico de adaptação para todos os tipos de empresas, sejam elas privadas ou não, é de suma relevância que se tenham conhecimento sobre cada artigo mencionado no desenvolvimento desse tópico, bem como os dispositivos trazidos pela própria LGPD, principalmente para as empresas de pequeno porte, para que assim possam permanecer no controle correto sobre os dados de seus clientes e não sejam responsabilizadas civilmente sobre quaisquer vazamentos.

## 4 A TUTELA COLETIVA NA PROTEÇÃO DE DADOS PESSOAIS

O desenvolvimento desse capítulo irá abordar no primeiro tópico sobre quem são os legitimados para judicializar as ações em que há o descumprimento da LGPD, e expondo de mesma forma como já estão sendo decididas as ações que já tramitaram e estão tramitando, como exposto, por ainda estarem em um curso em sede de primeiro grau, ainda não se tem entendimento consolidado. Entretanto, o cenário é muito diferente do que previsto por especialistas da área, que entendiam que haveriam inicialmente um judicialização, mas, não foi o que aconteceu.

O segundo tópico trata sobre as ações públicas e privadas no processo de judicialização da LGPD, que demonstra que com a instituição da proteção de dados como um direito constitucional, há total possibilidade de propositura de ações civis pública pelo Ministério Público. E, ainda, de ações privadas por aqueles que sentirem que seu direito foi violado. Além de ter tido o reconhecimento pelo judiciário sobre a representatividade de associações e entidades civis que defendem os interesses da sociedade na Justiça nas chamadas ações coletivas.

O terceiro tópico, traz um estudo de caso no qual demonstra de que forma a Empresa Assunção Promotora Eireli, objeto do estudo, realizou sua adequação da LGPD diante da abordagem da nova legislação. O estudo foi realizado por meio de dados coletados ao decorrer da implantação, bem como por meio de questionário realizado ao responsável pela adequação da empresa.

### 4.1 A questão dos legitimados para judicialização de ações judiciais

No tocante à judicialização acerca do vazamento de dados pessoais após a vigência da LGPD, pode-se mensurar que a referida legislação dispõe sobre a aplicação de sanções administrativas pela ANPD - Autoridade Nacional de Proteção de Dados aos responsáveis pelo vazamento de dados e pelo seu não tratamento, tais sanções visam, em caráter pedagógico, erradicar a cultura de não-proteção de dados que ainda assola o Brasil na contemporaneidade.

Porém, embora havendo previsão de sanções administrativas, as ações indenizatórias pertinentes à Lei Geral de Proteção de Dados perante o Poder Judiciário já é uma realidade bem recorrente no Brasil. Pressupõe-se que ao ocorrer um dano em relação ao vazamento de dados sem o consentimento do titular, rompe-se o equilíbrio contratual e o fundamento jurídico-econômico da vítima, assim, faz-se necessário tentar recompensar a vítima

a um estado similar que ela estava antes da lesão, na maioria das vezes, isto significa uma indenização pelo dano gerado, tal indenização tem seu pontapé inicial na propositura da ação judicial pelo titular lesado.

Sobre a temática, aponta-se para o entendimento do STF acerca da proteção de dados e o respeito aos direitos fundamentais a liberdade, privacidade e a personalidade:

Os dados pessoais representam toda informação relacionada a pessoa natural ou identificável (artigo 5º, inciso I, LGPD). Segundo o artigo 5º, inciso X, da LGPD, o tratamento de dados pessoais consiste nas atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência, difusão ou extração, bem como a avaliação ou o controle da informação pessoal disponibilizada pela pessoa natural a quem se referem os dados pessoais que são objeto do tratamento - o titular dos dados (artigo 5º, inciso V). (STF, 2021)

Nessa perspectiva, com a LGPD em vigor, tem-se em mente que deve haver um propósito de criar uma perspectiva de segurança jurídica no poder judiciário frente as demandas inerentes ao vazamento ilegal de dados, de modo que deve haver a padronização de normas e práticas como tem sido feita no Brasil nos últimos tempos, para promover a proteção, de forma igualitária, aos dados pessoais de todo cidadão que esteja no Brasil.

Denota-se que no período de *vacatio legis* da LGPD que apenas entrou em vigor em 2021, a máxima insegurança jurídica no Brasil, neste início de adaptação das empresas às normas dispostas na LGPD foram enfrentados muitos desafios e muito foi deixado a desejar no tocante ao cumprimento dos dispositivos. Nessa esteira, no início da entrada em vigor da lei, foram ajuizadas as primeiras ações judiciais em que a causa de pedir era baseada na Lei Geral de Proteção de Dados, sobre a legitimidade ativa, evidenciou-se tanto o Ministério Público como polo ativo nas demandas, como também pessoas físicas que se sentiram lesadas de alguma forma.

Aborda-se a seguir um julgado recente acerca da responsabilização do agente que comentou o vazamento e a probabilidade do direito do titular dos dados que se viu afetado por tal conduta:

Sendo assim, em análise preliminar e não exauriente, como é própria das decisões de tutela de urgência, considero pertinente o entendimento de que a comercialização dos dados pessoais sem o consentimento, ainda que não caracterizados como dados sensíveis, **ferre a legislação específica e tem potencial para ensejar violação à privacidade, intimidade e imagem das pessoas, o que evidencia a probabilidade do direito.** (grifou-se) (TJ-DF - Agravo de Instrumento 0749765-29.2020.8.07.0000, Relator: Cesar Loya, Data de Julgamento: 26/05/2021 , 2ª Turma Cível, Data de Publicação: Publicado no DJE: 31/05/2021)

Dessa forma, compreende-se que a LGPD tem como objetivo primordial a proteção de direitos fundamentais do ser humano, de maneira que deve-se garantir os direitos da pessoa natural à liberdade, à privacidade e o livre desenvolvimento da personalidade em relação aos seus dados; nesse contexto, por muitas vezes as sanções administrativas não dão conta de afastar os problemas quanto aos riscos de vazamentos, o que leva ao principal interessado que teve seus dados expostos, buscar o poder judiciário para a resolução do conflito.

Todavia, de acordo com Leal (2021) há que se ressaltar que considerando que o assunto é, de certa forma, novo devido ao pouco tempo de vigência da LGPD, entende-se que a grande maioria das demandas ainda se encontra no primeiro grau, por esta razão, deve-se considerar que o tema ainda não possui um entendimento consolidado pela jurisprudência brasileira, os casos ainda estão passíveis de análise pelos tribunais superiores.

Acerca dessa questão ainda tímida no poder judiciário brasileiro no que tange ao tratamento jurídico ofertado para a responsabilização desses agentes, Pioli (2022, p. 01), mensura que:

Por enquanto o volume de ações é tímido e as decisões divergem (inclusive de forma antagônica). Temia-se a ocorrência de muitas condenações em ações pedindo indenização por danos morais por conta de vazamento de dados, mas o que se percebe é uma divisão de entendimentos, havendo várias decisões que entendem que o simples vazamento dos dados, sem efetivo dano, não gera o dever de indenizar. Exemplificativamente, o TJSP assim já se posicionou: “Ausência de provas, todavia, de violação à dignidade humana da autora e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autora que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, houve a ocorrência de danos mora. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa” (Apelação Cível 1000794-59.2021.8.26.0554).

Diante do supracitado, a autora preleciona que, ao observar o comportamento do poder judiciário frente às demandas que surgem, a jurisprudência nacional vem apontando para o entendimento de que o mero vazamento de dados pode não ser suficiente para uma caracterização de evidência de danos causados e probabilidade do direito, para, assim, gerar indenização, ainda que se trate de dados sensíveis e pessoais.

Assim, a importância deste órgão na judicialização destas demandas se expressa como figura essencial na proteção e defesa dos direitos dos lesados, Souza (2021, p. 20), aponta que:

ao figurar como polo ativo em demandas judiciais que tenham como objeto a aplicação da LGPD, o Ministério Público deslocará o eixo de enforcement de proteção de dados pessoais em direção ao Poder Judiciário, que aceitará o seu protagonismo como força capaz de fazer cumprir a LGPD, não se eximindo de resolver as lides. A

atuação do MP, entretanto, não usurpará a competência outorgada pela Lei unicamente à ANDP

No que tange à legitimidade do Ministério Público, pode-se apreender que o Ministério Público, antes mesmo da aprovação da LGPD em 2018, já desempenhava importante papel inerente a proteção dos direitos dos consumidores em relação a proteção de seus dados frente aos prestadores de serviço de internet, por exemplo.

Com base nisso, o tópico seguinte pretende apresentar alguns dos julgados referente às ações civis públicas no âmbito do processo de judicialização da LGPD com base nos legitimados para propositura da ação, que ganha cada vez mais força no cenário jurídico brasileiro.

#### 4.2 Ações civis públicas ou privadas no processo de judicialização da LGPD

Ainda se tratando de legitimidade do Ministério Público na propositura de ação Civil Pública, no que tange à defesa coletiva, compreende-se que, há previsibilidade no Código de Defesa do Consumidor, ao se apreender que além de o serviço prestado pelas empresas ser considerado falho no que tange a segurança dos dados dos usuários, há a questão da falta de informação como pressuposto do direito do consumidor.

Por esta razão, evidencia-se o art. 51 do CDC, que desde a sua instituição já admitia expressamente a legitimidade do Ministério Público para propor ação anulatória de cláusulas contratuais abusivas ou ilegais:

Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:

[...] § 4º É facultado a qualquer consumidor ou entidade que o represente em 11.02.2021 36 Idem 23 requerer ao Ministério Público que ajuíze a competente ação para ser declarada a nulidade de cláusula contratual que contrarie o disposto neste código ou de qualquer forma não assegure o justo equilíbrio entre direitos e obrigações das partes.

Por outro lado, há que se falar, ainda, na legitimidade estabelecida pelo art. 81, 82, IV do CDC, referente à entidades civis na propositura de ação civil pública, de modo que conquista o status deferido ao Ministério Público, dispõe os referidos artigos:

Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo. Parágrafo único. A defesa coletiva será exercida quando se tratar de:



I - Interesses ou direitos difusos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato;

II - interesses ou direitos coletivos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base;

III - interesses ou direitos individuais homogêneos, assim entendidos os decorrentes de origem comum.

Art. 82. Para os fins do art. 81, parágrafo único, são legitimados concorrentemente

I - o Ministério Público,

II - a União, os Estados, os Municípios e o Distrito Federal

III - as entidades e órgãos da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses e direitos protegidos por este código;

IV - as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este código, dispensada a autorização assemblear.

Nessa perspectiva, no tocante a ação civil pública e a responsabilização dos agentes que cometem vazamento de dados e que geram indenização, entende-se que o ressarcimento pelos danos individuais em sede de ação civil pública está expressamente previsto no artigo 95 do CDC, uma vez que este dispõe que a condenação será genérica para que a fixação dos valores seja feita em sede de liquidação individual prevista no artigo 97 da mesma norma.

No que tange a jurisprudência, apresenta-se alguns julgados sobre ação civil pública e o dano moral coletivo diante da propositura. O primeiro relaciona-se ao entendimento do STJ na questão da legitimidade de entidades civis na propositura de ações:

PROCESSUAL CIVIL. RECURSO ESPECIAL. VIOLAÇÃO DE DISPOSITIVO CONSTITUCIONAL. DESCABIMENTO. EMBARGOS DE DECLARAÇÃO. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. MATÉRIAS DE ORDEM PÚBLICA. QUESTÃO NÃO DECIDIDA. PRECLUSÃO PRO JUDICATO. NÃO OCORRÊNCIA. DIREITO DO CONSUMIDOR. AÇÃO COLETIVA DE CONSUMO. LEGITIMIDADE AD CAUSAM. ASSOCIAÇÃO. AUTORIZAÇÃO ASSEMBLEAR. DESNECESSIDADE. ART. 82, IV, DO CDC. SUCESSÃO NO POLO ATIVO. COLEGITIMADO. POSSIBILIDADE. ARTS. 9º DA LEI 4.717/65 E 5º, § 3º, DA LEI 7.347/85. (...)9. Na substituição processual, por outro lado, não se leva em conta a titularidade do direito material, mas sim a efetividade da tutela jurisdicional empreendida, razão pela qual a legislação prevê expressamente a possibilidade de terceiros defenderem em juízo direito alheio em nome próprio. 10. Por se tratar do regime de substituição processual, a autorização para a defesa do interesse coletivo em sentido amplo é estabelecida na definição dos objetivos institucionais, no próprio ato de criação da associação, sendo desnecessária nova autorização ou deliberação assemblear. Precedentes. (...).RECURSO ESPECIAL Nº 1.800.726 - MG (2018/0054195-0) MINISTRA NANCY ANDRIGHI

Diante do exposto acima, entende-se que a 3ª Turma do Superior Tribunal de Justiça (STJ), em relatora de Ilustre Ministra Nancy Andrigli, com decisão unânime, reconheceu a

representatividade de associações e entidades civis que defendem os interesses da sociedade na Justiça nas chamadas ações coletivas.

O próximo julgado diz respeito a probabilidade do direito no âmbito do dano moral coletivo:

“TRIBUTÁRIO. PROCESSUAL CIVIL. AUSÊNCIA DE PREQUESTIONAMENTO. SÚMULA 211/STJ. ACÓRDÃO FUNDAMENTADO EM MATÉRIA CONSTITUCIONAL. COMPETÊNCIA DO STF. AÇÃO CIVIL PÚBLICA. DANOS MORAIS COLETIVOS. CABIMENTO. 1. Descumprido o necessário e o indispensável exame dos dispositivos de lei invocados pelo acórdão recorrido, apto a viabilizar a pretensão recursal da recorrente, a despeito da oposição dos embargos de declaração. Incidência da Súmula 211/STJ. 2. Não cabe recurso especial contra acórdão fundamentado em matéria eminentemente constitucional. 3. Nos termos da jurisprudência pacífica do STJ, é possível a condenação em danos morais coletivos em sede de ação civil pública. Precedentes:EDcl no AgRg no AgRg no REsp 1.440.847/RJ, Rel. Ministro MAURO CAMPBELL MARQUES, SEGUNDA TURMA, julgado em 07/10/2014, DJe 15/10/2014; REsp 1.269.494/MG, Rel. Ministra ELIANA CALMON, SEGUNDA TURMA, julgado em 24/09/2013, DJe 01/10/2013. 4. "A possibilidade de indenização por dano moral está prevista no art. 5º, inciso V, da Constituição Federal, não havendo restrição da violação à esfera individual. A evolução da sociedade e da legislação têm levado a doutrina e a jurisprudência a entender que, quando são atingidos valores e interesses fundamentais de um grupo, não há como negar a essa coletividade a defesa do seu patrimônio imaterial. O dano moral coletivo é a lesão na esfera moral de uma comunidade, isto é, a violação de direito transindividual de ordem coletiva, valores de uma sociedade atingidos do ponto de vista jurídico, de forma a envolver não apenas a dor psíquica, mas qualquer abalo negativo à moral da coletividade, pois o dano é, na verdade, apenas a consequência da lesão à esfera extrapatrimonial de uma pessoa." ( REsp 1397870/MG, Rel. Ministro MAURO CAMPBELL MARQUES, SEGUNDA TURMA, julgado em 02/12/2014, DJe 10/12/2014) Agravo regimental improvido.” (STJ - AgRg no REsp 1541563 / RJ – Ministro Humberto Martins – Segunda Turma – DJE 16/09/2015)

Assim, verifica-se que há entendimento pacificado do STJ no que tange a possibilidade de ser fixada indenização pelo dano moral da coletividade. Dessa forma, em suma, a respeito dos embates no âmbito jurídico, verifica-se que A Lei Geral de Proteção de Dados adere a um sistema de responsabilidade civil compatível com o Código Civil e o Código de Defesa do Consumidor de modo que suas relações jurídicas de direito privado baseado no tratamento de dados pessoais são reguladas por tal legislação e encontram precedentes jurídicos quanto a proposituras de ações coletivas na defesa destes direitos fundamentais violados.

#### 4.3 Estudo de caso: adequação da LGPD na empresa Assunção Promotora Eireli

Pontua-se que, além da pesquisa bibliográfica, foi realizada uma pesquisa de campo durante o terceiro trimestre de 2022, que resultou em um estudo de caso. Denota-se que a intenção deste estudo foi responder aos objetivos propostos neste Trabalho de Conclusão, sobretudo acerca da compreensão da forma que a empresa pesquisada realizou sua adequação

interna após a vigência da LGPD, a fim de que se pudesse analisar quais meios adotados pela empresa, no que se refere à segurança da informação de seus clientes e demais entradas de dados.

Nesse sentido, pretende-se neste tópico apresentar um estudo de caso sobre a Empresa Assunção Promotora Eireli, localizada na cidade de São Luís – Maranhão, de modo a evidenciar a forma de atuação da empresa no que tange à sua adequação aos parâmetros da Lei Geral de Proteção de Dados e ao tratamento com os dados fornecidos pelos clientes.

No que se refere ao percurso metodológico, inerente ao estudo de caso, Mazzotti (2006) elucida que este tipo de método está intrinsecamente ligado a uma investigação empírica que tem por objetivo precípuo o estudo de um fenômeno contemporâneo dentro de seu contexto da vida real, de maneira que sua contextualização com a temática se dará de forma dialética.

#### 4.3.1 Caracterização da área de estudo – organização da empresa quanto ao armazenamento e tratamento de dados

A empresa Assunção Promotora Eireli, faz parte de um grupo composto por 6 (seis) empresas, sua fundação ocorreu em 2007, voltando sua atuação ao ramo financeiro com ênfase em contratos mútuos de empréstimos consignados, realizando a captações de clientes diretos por suas filiais físicas em São Luís- MA e Imperatriz- MA; a empresa desempenha seu nicho trabalhando com diversos prestadores de serviços por todo Brasil. Além do que, atualmente, possui contratos de prestação de serviços com cerca de 20 (vinte) Instituições Bancárias.

Ressalta-se que, conforme verificado durante o estudo, a instituição aqui abordada sempre demonstrou preocupação com a segurança das informações de seus clientes. Tal constatação é evidenciada no momento em que se verificam as políticas de atuação e até mesmo sua antecipação em adequações das obrigatoriedades da LGPD às instituições antes do recomendado.

Compreende-se que um conjunto de medidas foram adotadas visando proteger e preservar as informações utilizadas nas atividades diárias da Instituição, de modo que foram enviados comunicados pelo Bancos, um deles, foi a Bradesco Financiamentos e em abril de 2022 à Assunção Promotora, pois, havia sido contratado uma empresa de auditoria, Ernst & Young (EY), esta que é uma Big Four em auditorias, estando entre as quatro maiores do mundo, que realizaria a auditoria das empresas para verificar se estavam em compliance; tal notificação enviada foi informando sobre o início do Ciclo de Monitoramento de Correspondentes de 2022,

ou seja, deliberações acerca de novas exigências de adequações das instituições financeiras às exigências de confiabilidade no tratamento de dados, de acordo com a LGPD.

Neste informativo, que constará em anexo, a empresa deveria se atentar à regras como:

- (i) Relacionamento com o cliente,
- (ii) Políticas de Governança,
- (iii) Tecnologia da Informação,
- (iv) Aprendizado e Conhecimento e
- (v) **Adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), nos quais estão incluídos os aspectos da Autorregulação.**

Por esta razão, verifica-se que à empresa em estudo deveria seguir as regras estabelecidas no intuito de assumir suas responsabilidades no que tange ao tratamento, bem como coleta e o armazenamento de dados de seus clientes, de maneira a potencializar o desenvolvimento de três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (PEIXOTO, 2020). Com base nesses parâmetros o informativo em questão prelecionou que:

A ASSUNÇÃO PROMOTORA EIRELI deverá adotar todas as medidas necessárias para manter a mais restrita confidencialidade a respeito dos dados e informações estratégicas, comerciais, mercadológicas e quaisquer outras fornecidas durante o processo de monitoramento, sendo desautorizada a sua distribuição, cópia, fornecimento, comercialização ou, por qualquer outra forma ou meio, revelação desses dados e informações a terceiros, incluindo a própria Instituição Financeira contratante, a qualquer título que seja e a qualquer tempo (BRADESCO FINANCIAMENTOS, em anexo).

É importante ressaltar que, antes da obrigatoriedade de adequação à LGPD, a empresa possuía investimento em Segurança da Informação, como maneira de criar uma cultura de proteção de dados na instituição, o que proporciona um ambiente mais organizado e confiável com maior controle dos riscos pelos colaboradores; nesta perspectiva, como característica preponderante da empresa em estudo, tem-se a organização quanto ao tratamento de dados de seus clientes.

Nesse contexto, apresenta-se o Relatório de Impactos e Proteção de Dados, realizado pela Assunção Promotora Eireli, com objetivo de sistematizar suas operações e tratamentos de dados para viabilizar melhorias e avaliações. O Relatório de Impacto à Proteção

de Dados Pessoais (RIPD) visa descrever os 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.

Assim, em relação à caracterização da área de estudo evidencia-se de que forma se dá atuação da empresa no que tange à proteção de dados; em relação aos agentes que compõem a logística de tratamento de dados, a empresa apresenta a parceria com:

- Banco Bradesco S/A
- Banco BMG S/A
- Banco Bonsucesso
- Olé Consignado S/A
- Banco do Estado do Rio Grande do Sul S/A
- Banco Daycoval S/A
- Banco Pan S/A
- Banco Paulista

Na elaboração do Relatório para fins de avaliação e melhoria, alguns parâmetros que foram utilizados como indicativos de que determinadas ações de tratamento necessitem de avaliações, em razão do maior grau de risco que represente aos seus titulares de dados. Tais parâmetros são utilizados pela Assunção Promotora no exercício de seu direito atuando de forma preventiva no intuito de mitigação de riscos, dessa forma, os parâmetros são:

1. Monitoramento sistemático
2. Dados sensíveis ou de natureza altamente pessoal
3. Tratamento de dados em larga escala
4. Combinação de conjunto de dados
5. Dados de titulares vulneráveis Dados tratados com a finalidade de permitir ou negar o acesso do titular a determinado serviço ou realização de um contrato

No que se refere ao tratamento de dados propriamente dito, os procedimentos adotados e os dados tratados nas operações de empréstimos consignados e demais produtos financeiros, ofertados pelas instituições bancárias controladoras por intermédio da Assunção Promotora Eireli, seja na condição de CoControladora e/ou Operadora que possam gerar riscos aos Titulares de dados.

Pode se determinar que os dados são processados em âmbito nacional, e que apenas são coletados os dados exigidos pelas instituições financeiras controladoras, conforme roteiros operacionais e contratos, que em regra são documentos de identificação pessoal com número de RG e CPF, comprovante de endereço, contracheque, número do benefício do INSS e dados bancários, que podem variar dependendo do convênio ou instituição contratada.

O processamento destes dados é fundamental para que possa ser atingida a finalidade pretendida pelo titular dos dados, que neste caso será a concessão do empréstimo bancário. O grupo "Assunção Promotora" fundamenta este procedimento de coleta e tratamento de dados nas bases legais de exercício regular do seu direito, execução e/ou preparação contratual e cumprimento de uma obrigação legal ou regulatória em total consonância com a LGPD.

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco”. Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

É importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos da empresa. No quadro a seguir é possível verificar os parâmetros de riscos sobre impactos e probabilidades formuladas pela empresa em estudo:

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	Probabilidade	Impacto	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	15	15	225
R02	Modificação não autorizada.	15	15	225
R03	Perda	15	15	225
R04	Roubo	15	15	225
R05	Remoção não autorizada.	15	15	225
R06	Coleção excessiva.	15	15	225
R07	Informação insuficiente sobre a finalidade do tratamento.	15	15	225
R08	Tratamento sem consentimento do titular dos dados pessoais. (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	15	15	225
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	15	15	225
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	15	15	225
R11	Retenção prolongada de dados pessoais sem necessidade.	15	15	225
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	15	15	225
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	15	15	225
R14	Reidentificação de dados pseudonimizados	10	15	150

Fonte: formulado pela empresa em estudo – Assunção Promotora (2022)

Legenda: P – Probabilidade; I – Impacto

Onde:

- Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
- Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
- Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Com base nestes dados, é possível evidenciar as políticas de governança de dados, que se baseiam nas diretrizes elencadas para a elaboração do relatório de impacto e que podem ser utilizadas para garantir que seus dados e ativos sejam usados adequadamente e gerenciados de forma consistente. No tópico seguinte, será evidenciado a análise dos dados colhidos através do questionário aplicado.

#### 4.3.2 Coleta de dados – Entrevista e análise de dados

Evidencia-se que a referida empresa foi escolhida por se tratar de um grande exemplo no que se refere à adequação aos parâmetros exigidos pela LGPD; nessa perspectiva, os dados aqui colhidos e analisados poderão ajudar de forma relevante o mercado brasileiro, a academia, e até mesmo outras empresas que poderão ter um exemplo a seguir no que se refere à proteção e segurança do tratamento dos dados que são coletados por elas.

Conforme observado ao longo do trabalho, a princípio fora realizada análise da Lei Geral de Proteção de Dados, por meio de pesquisa bibliográfica com doutrinadores que abordam o tema na contemporaneidade, a fim de entender os seus conceitos e pressupostos. Por conseguinte, nesta etapa da pesquisa no que concerne à análise do estudo de caso, aponta-se que foi elaborado um instrumento de pesquisa, qual seja: questionário, o qual será possível identificar as principais informações da empresa em relação aos pontos que são mencionados pela lei.

O referido instrumento de pesquisa consiste em um questionário com nove perguntas relacionadas ao tema da proteção de dados aplicados ao Sr. Raphael Bacellar, membro inscrito na Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) e responsável no qual foram consideradas as principais pontos de tratamento de dados trazidos pela legislação vigente.

O questionário aplicado foi estruturado em 03 (três) blocos temáticos totalizando nove questões:

- 1º bloco: implantação da LGPD na Assunção Promotora; contendo três questões; na sequência os demais blocos trataram da percepção do entrevistado em relação às estratégias utilizadas para a adequação da empresa aos parâmetros exigidos
- 2º bloco: estratégias de adequação à nova legislação e para tanto, foram propostas mais três questões;



- 3º bloco: parâmetro analítico: assunção antes da LGPD e depois, sendo que neste item foram propostas mais três questões

- 

Em relação ao 1º bloco - à implantação da LGPD na assunção promotora:

Foi perguntado ao Sr. Rafael Bacellar, de que forma e porque houve a implantação da LGPD dentro da assunção promotora?

R: “A implantação das regras implementadas pela lei 13.709/18 se deu, inicialmente, quando a Febraban Federação Brasileira de Bancos e a ABBC – Associação Brasileira de Bancos, com objetivo de aperfeiçoar o atendimento aos clientes na oferta de crédito consignado no país, instituíram o Sistema de Autorregulação de Operações de Empréstimo Pessoal e Cartão de Crédito com Pagamento Mediante Consignação, que entrou em vigor no dia 02 de janeiro 2020. Um dos pilares exigidos por este sistema era o de conformidade à LGPD, e a sua inadequação poderia resultar ao correspondente bancário diversas sanções, dentre elas o distrato definitivo com as instituições signatárias à Autorregulação”

Dessa forma, evidencia-se que o informativo enviado asseverou que a inadequação da empresa às exigências poderia, dessa forma, acarretar como uma das consequências o distrato definitivo com as instituições como forma de sanção, de forma que, tal exigência não apontou um problema à empresa, uma vez que esta já sinalizava para a criação de uma cultura de proteção de dados, conforme prelecionado no relatório de impactos.

Em relação ao questionamento nº 2 (segundo), foi em razão de alguma notificação do Banco sobre a obrigatoriedade dessa adequação? R - “Os bancos, contrataram uma empresa de auditoria, Ernst & Young (EY), que nos notificou informando os pilares de avaliação, dentre eles a adequação à LGPD – (comunicação em anexo)”. Tal informativo foi apontado no tópico anterior e consta em anexo ao final do Trabalho.

O 3º (terceiro) questionamento deste primeiro bloco, foi: Quais foram os pontos principais dentro da área de atuação da empresa foram trabalhados para serem modificados?

R: “Inicialmente, foi realizado um levantamento dos fluxos da operação (data mapping) para identificar os dados tratados internamente, após essa primeira etapa, foram identificadas as bases legais para tratamento das informações tratadas pela empresa e realizados os ajustes necessários à adequação”;

Em relação a tal questionamento, apresenta-se a título de exemplo o inventário de dados pessoais, essa guia é um formulário operacional a ser preenchido de acordo com a sua atividade função na empresa, para o levantamento de fluxo mencionado acima:

De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados	
Descrição do Fluxo do tratamento dos dados pessoais	<ul style="list-style-type: none"> <li>o atendimento pelo call center é efetuado, através do software digisac, onde nossos colaboradores entram em contato com os clientes oriundos de uma base de dados fornecida pela if.</li> <li><b>OBSERVAÇÃO ARGUMENTOS:</b> A Argumentação não deve deixar dúvidas sobre o produto que está sendo oferecido. Devemos nos lembrar de colocar a escuta ativa e técnicas de venda em prática. O produto deve ser oferecido de maneira que o cliente possa entender</li> </ul>

Elaborado pelo autor a partir de dados fornecidos pela empresa

Dessa forma, demonstra-se no quadro abaixo quais as informações coletadas, qual o tempo de retenção dessas informações, de modo que as sistematizações destas informações são essenciais para a organização do tratamento de dados e descarte de forma correta com a mitigação de eventuais riscos:

7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal	Nome endereço residência número de telefone fixo residencial e-mail pessoal	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.1.2 - Informações de identificação atribuídas por instituições governamentais	CPF RG número da carteira de motorista	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.1.3 - Dados de identificação eletrônica	Não se aplica			
7.1.4 - Dados de localização eletrônica	Não se aplica			

Posteriormente, no bloco 2, foram realizadas as seguintes perguntas:

- Estratégias de adequação à nova legislação

- Quais mecanismos foram utilizados para modificar a estrutura da empresa?

R: “A empresa adequou os contratos de prestação de serviços, com a inserção de cláusulas acerca da privacidade de dados; estruturou políticas para disciplinar o uso de estações de serviços; realizou ajustes na hierarquia de acessos a informações, conforme a necessidade do cargo, dentre outros pontos”.

- Foi contratado alguma assessoria?

R: “Sim, foi contratada uma empresa de consultoria e um software de implantação – DPOMAX”.

- Como essa situação foi trabalhada junto aos funcionários?

R: “Foram realizadas reuniões e treinamentos com os colaboradores para a conscientização e aplicação das novas diretrizes”.

No que tange ao bloco 3, foram realizadas as seguintes perguntas:

- Parâmetro analítico: assunção antes da LGPD e depois

- Como trabalhava a assunção em relação aos dados e fluxos antes da LGPD?

R: “A empresa, por ser correspondente bancária, sempre teve regras rígidas em sua atuação, contudo, quanto à proteção de dados, conforme previsto pela lei 13.709/18, precisou se ajustar, tendo em vista que antes da legislação os dados de terceiros eram mais facilmente acessados de forma indiscriminada”.

- Após a vigência da norma e implantação da empresa o que mudou?

R: “Após a implantação, novas regras e políticas internas foram criadas para garantir que os acessos aos dados ocorram em conformidade com a legislação, nomeando inclusive um DPO, para contato direto com os titulares de dados, bem como para realizar as comunicações obrigatórias, caso sejam necessárias”.

- Como os funcionários tiveram que se ajustar para cumprimento da lei?

R: “Em razão da empresa ser correspondente bancária, e existir uma exigência de certificação, todos os colaboradores que prestem atendimento ao público, realizaram um curso para obter uma certificação da LGPD, os demais passaram por treinamentos”.

Em suma, ao analisar as respostas obtidas, verifica-se a preocupação dos gestores da empresa com a questão da proteção de dados e seu tratamento de acordo com as exigências da LGPD, uma vez que, é de inteira responsabilidade das empresas obter o máximo de cuidado no que se refere ao tratamento de dados de seus clientes, pois os riscos inerentes à divulgação desses de maneira errônea e, ainda sem o devido consentimento do particular, as consequências serão inevitáveis para fonte que os informou, ou seja, a responsabilização civil dos envolvidos.

## 5 CONCLUSÃO

A tecnologia trouxe incontáveis impactos para a vida das pessoas em geral, sobretudo, para a caracterização de um novo conceito que outrora ainda se mostrava de difícil delimitação e configuração, os dados, que por muito tempo se mantiveram na obscuridade da internet, sendo usados de qualquer maneira, foram objeto de regulamentação legal a nível mundial. A *General Data Protection Regulation (GDPR)*, lei precursora na regulamentação e pontual no início da conformidade de diversos países para com o tratamento correto dos dados, influenciou em diversos aspectos à lei brasileira que versa sobre dados, a LGPD.

Ademais, toda a conscientização para o tratamento e regulamentação dos dados na internet, bem como seu tráfego no comércio internacional, foi impulsionada pela Europa, que impôs como regra para manter relações comerciais a adequação de todos os países que ainda quisessem manter relações comerciais com a União Europeia. O Brasil, iniciou esse processo, e em 2018 promulgou a lei 13.708/18, que somente teria vigência no ano de 2020, tempo suficiente para que tanto a sociedade, quanto quem controla e realiza os tratamento dos dados se adequasse a norma.

Dessa forma, a importância social de seu estudo se demonstra com o entendimento de que o maior motivador na regulamentação de uma lei nesse sentido foi a forma com que os dados eram tratados no ambiente virtual, como não havia regulamentação, existia um mercado que beirava o extremo da ilegalidade. Além do que, havia o compartilhamento de dados por empresas, venda de dados para comercialização de produtos e até mesmo informações que hoje tem um tratamento diferenciado, denominado de “dados sensíveis”, que eram compartilhados de qualquer forma. Com a ocorrência desses dados alarmantes e cada vez mais a evolução para uma era tecnológica, era inevitável a regulamentação desse fato social.

Nesse sentido, para as ciências jurídicas, traçam-se novos desafios que precisam da delimitação doutrinária e de estudo de pesquisa para conseguir delimitar seu real alcance. Com a criação da lei, nasce mais uma problemática legal, que não percorreu ainda seus limites e entendimentos. No Brasil, muito do Código de Defesa do Consumidor, foi abordado na lei e serviu de parâmetro legal, bem como os conceitos de Responsabilidade Civil para auferir responsabilidades à quem infringir os ditames legais.

Nesse sentido, para que esses dados pudessem ser evidenciados foram utilizados o método o método qualitativo de abordagem e uma pesquisa bibliográfica de caráter exploratório, além de estudo de caso com aplicação de questionário. A principal referência é a pesquisa bibliográfica, que com o advento de uma lei nova ainda sem parâmetros consolidados,

necessita-se buscar os conceitos já firmados e ainda o que já se tem de análise feita no âmbito acadêmico. O estudo de caso, com a Empresa Assunção Promotora Eireli, foi salutar para definir quais mudanças acontecem em uma empresa para haver adequação a lei e como ela é realizada, além dos parâmetros de comparação e entendimento de gastos despendidos pelo setor privado para isso.

Nessa esteira, o estudo de caso evidenciou de mesma forma, como está sendo cobrada essa adequação de cima para baixo, visto que, a Assunção Promotora, não é a controladora dos dados, mas tão somente faz o seu tratamento no que se refere as Instituições Financeiras das quais mantém relações comerciais. Por esse viés, verificando que a própria lei já trouxe diferenciação às pequenas empresas, a conclusão e a visibilidade sobre esse estudo poderá ainda trazer mais benefícios as empresas de pequeno porte, por entender todo o gasto sofrido, além da contratação de conhecimento intelectual para realizar este trabalho, o que seria penoso para uma pessoa jurídica de menor faturamento, diferentemente do que se classifica a empresa em estudo.

De mesma forma, foram esclarecidos os objetivos específicos, explanando a legislação presente no Brasil sobre proteção de dados, que além da LGPD, conta com apoio do Código de Defesa do Consumidor, e também da Constituição Federal, após ter se tornando um direito fundamental. Portanto, envolve os mesmos entendimentos constitucionais em que se definem todos os direitos fundamentais, ilustrando mais uma dinâmica na interpretação da lei.

Assim, ainda dentro dos objetivos específicos, trouxe a análise da aplicabilidade da Responsabilidade Civil nos tribunais e como já está funcionando isso aplicado nas ações que tramitam com motivações de coleta e tratamento de dados. Outrossim, como já traz conceitos de aplicabilidade pelo Código de Defesa do Consumidor, defende-se a ideia da utilização de forma mais adequada da teoria objetiva.

Isto posto, a caracterização e apresentação da Tutela Coletiva, mostrou que ainda não há uma definição pelo judiciário nas sentenças já proferidas, que de muitos casos preferiram oportunizar a empresa por ação de fazer a regulamentação da conduta, do que condená-la a importes altos de danos morais. E, nesse caso, verificou-se também que se ampliou os legitimados para propor ações, que podem ser públicas ou privadas, sendo que o judiciário vem ampliando ainda mais esse leque.

Com isso, a hipótese do trabalho de que há previsibilidade legal de Responsabilidade Civil, pelos dispostos nos arts. 54 ao 55 da Lei, trazendo a possibilidade de sanções administrativa e judiciais, mostrou-se verdadeira. A grande questão da pesquisa foi debatida e respondida, quando se verifica que há previsibilidade legal para a Responsabilidade

Civil das empresas privadas, apesar de ainda não haver um critério ainda na utilização das teorias da culpa, ora é objetiva, ora subjetiva, visto que, divergem os autores em diversos pontos, justificando na própria lei a falta de direcionamento correto, trazendo grandes obstáculos em discussões acadêmicas, que posteriormente serão levadas a grandes debates no judiciário.

Sendo assim, as empresas privadas podem e devem ser responsabilizadas quando houver descumprimento legal, pelo trabalho e demonstrado na pesquisa, já existe uma adequação e trabalho realizado por empresas maiores, que de certa forma obrigam os alinhamentos de outras menores. Nesse sentido, os conceitos de Responsabilidade Civil já se encontram presente, apesar de ainda ser discutido a delimitação em Responsabilidade Civil Objetiva ou subjetiva.

Em pesquisas futuras, pode-se por ter dados mais consolidados até mesmo de julgados, definir a teoria usada na responsabilização civil e também trazer um posicionamento mais certo do judiciário, posto que, certamente se terá julgamentos que enfrentaram instâncias superiores e transitaram em julgado, o que ainda não se tem de forma estabilizada para ser mostrado como um modelo determinado.

## REFERÊNCIAS

BASTOS, Athena. **Direito digital**: guia da lei geral de proteção de dados pessoais: LGPD. 2018. Disponível em: <https://blog.sajadv.com.br/direito-digital-lei-de-protecao-de-dados/>. Acesso em: 20 maio 2020.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Campus, 2004.

BAUMAN, Zygmunt. **A modernidade líquida**: o sujeito e a interface com o fantasma. Rio de Janeiro: Jorge Zahar, 2001.

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.

BRASIL. **Lei n. 12.737/12**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Extraído de: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm). Acesso em: 13 de out. de 2021.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm). Acesso em 11 out. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Promulgada em 05 de outubro de 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)> Acesso em: 08 de out. de 2021.

BIONI, Ricardo, B. **De 2010 a 2018**: a discussão brasileira sobre uma lei geral de proteção de dados. Disponível em: <https://www.colegioregistrals.org.br/doutrinas/artigo-de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-por-bruno-r-bioni/> > Acesso em 12 de out. de 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BIONI, Bruno.; 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*, v. 9, n. 3, p. 1-23, 22 dez. 2020. p. 7.

CAPANEMA. Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. *Cadernos Jurídicos*, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020. p. 166.

CAVALCANTE, Márcio André Lopes. **As associações possuem legitimidade para defesa dos direitos difusos, coletivos e individuais homogêneos, independentemente de autorização expressa dos associados**. *Buscador Dizer o Direito*, Manaus. Disponível em:



<<https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/219c507b38ddfc07899fc1f01ff40c44>>. Acesso em: 20/08/2022.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. **Direito à privacidade na lei geral de proteção de dados pessoais**. Revista da ESMESC, Florianópolis, v. 26, n. 32, p. 363-382, ago.2019.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. São Paulo: Atlas, 2019.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

CORRÊA, Leonardo; CHO, Tae. **Responsabilidade civil na LGPD é subjetiva**. Disponível em: [<https://www.conjur.com.br/2021-jan-29/correa-cho-responsabilidade-civil-lgpd-subjetiva>]. Acesso em: 10/11/2022.

**CONSULTOR JURÍDICO**. "Juíza aplica LGPD e condena construtora que não protegeu dados de cliente"; Disponível em: <https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao>. Acesso em 12 de nov. de 2022.

Caio Mário da Silva Pereira, **Responsabilidade Civil**, 12. ed., Rio de Janeiro: Forense, 2018.

DANTAS BISNETO, Cícero. **Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado**. *civilistica.com*, v. 9, n. 3, p. 1-29, 22 dez. 2020. p. 14. Disponível em: [<https://civilistica.emnuvens.com.br/redc/article/view/493>]. Acesso em: 07/03/2021.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica. com*, v. 9, n. 1, p. 1-38, 2020.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: Revista dos Tribunais, 1980. p. 67

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011

COELHO, Fabio Ulhoa. Curso de Direito Civil. São Paulo: Revistas dos Tribunais,2020.

FORTES, V. B. (2016). **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris.

FERREIRA DA SILVA, Edson. **Direito à intimidade**.2.ed. São Paulo: Ed. Juarez de Oliveira, 2003.

FERREIRA, Diogo Ramos. **Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva?** Disponível em: [<https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ouobjetiva-20112019>].

GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. São Paulo: Celso Bastos, 2003.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**, v. 3: responsabilidade civil. 17. Ed. Saraiva Educação SA, 2019.

GODINHO, Adriano Marteleto; QUEIROGA NETO, Genésio Rodrigues de; TOLÊDO, Rita de Cássia de Moraes. **A responsabilidade civil pela violação a dados pessoais**. Revista IBERC, v. 3, n. 1, 3 abr. 2020. p. 15

GONÇALVES, Carlos Roberto. **Responsabilidade civil**. São Paulo: Saraiva Educação SA, 2020.

GOGANI, Ronaldo. **O maior roubo de dados da história do Facebook que ajudou a eleger Donald Trump**. 2018. Disponível em:

<https://meiobit.com/381701/facebookcambridge-analytica-roubo-dados-ajudou-campanha-donald-trump-e-brexit/>>. Acesso em: 5 jun. 2022.

GONDIM, Glenda Gonçalves. **A responsabilidade civil no uso indevido dos dados pessoais**. Revista IBERC, v. 4, n. 1, p. 19-34, 9 mar. 2021. p. 27.

**Julian Assange**: quem é o fundador do Wikileaks, preso em Londres após quase 7 anos de asilo em embaixada do Equador. BBC Brasil, São Paulo, 11 de abr. de 2019. Disponível em: < <https://www.bbc.com/portuguese/internacional-47895584>>. Acesso em: 10 de out. de 2021.

LIMA, Lindamaria. **Os 10 princípios para tratamento de dados da LGPD**. 2020.

Disponível em:< <https://triplait.com/principios-para-tratamento-de-dados-da-lgpd/>>. Acesso em 13 de out. de 2021.

LEAL, Martha. **Accountability e a judicialização da LGPD**. CONJUR, 2021. Disponível em: <https://www.conjur.com.br/2021-jul-21/martha-leal-accountability-judicializacao-lgpd>, Acesso em: 11 nov 2022.

MASSARELLI JR. José Carlos. FREIRE E ALMEIDA. Verônica Scriptorre. **Proteção de dados pessoais como direito fundamental na área da saúde e suas implicações para os profissionais médicos no Brasil cotejando aspectos do direito comparado na União Europeia e na China**. Anais do Encontro Nacional de PósGraduação – VIII ENPG, Vol.3, p. 538-543, 2019. p. 538-539.

MARTINS JÚNIOR, Mauro Roberto. **O que não te contaram sobre ser um DPO**. São Paulo: PK HUB, 2020.

MAZZOTTI, A. J. A. **Usos e abusos dos estudos de caso**. Cadernos de Pesquisa, [S. l.], v. 36, n. 129, set./dez. 2006

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** Disponível em:

[<https://www.migalhas.com.br/coluna/migalhas-deresponsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-dedados-pessoais--culpa-ou-risco>]. Acesso em 11/11/2022.

MARINELI, Marcelo Romão. **Privacidade e redes sociais virtuais**. Rio de Janeiro: Lumen Juris, 2017.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

PACETE, L. G. (21 de Maio de 2018). “**A GDPR terá um efeito viral**”. Disponível em: <https://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeitoviral.html>> Acesso em: 08 de out. de 2021.

ONU. **Pacto Internacional dos Direitos Civis e Políticos**. Assembleia Geral. Resolução n. 2200-A (XXI). 16.12.1966.

PAIM, Bruna Werlang; GONÇALVES, Lukas Ruthes. **A responsabilidade civil no tratamento de dados pessoais pelas aplicações de inteligência artificial**. In: WACHOWICZ, Marcos (org.). **Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado**. Curitiba: Gedai, UFPR, 2020. 628 p. ISBN 978-65-86233-52-0. p. 451-480.

PEIXOTO, Andrea Stefani. **Lei de Proteção de Dados: entenda em 13 pontos!** Disponível em: <https://www.politize.com.br/lei-de-protecao-de-dados/#:~:text=A%20LGPD%20complementa%20o%20escopo,da%20seguran%C3%A7a%20.Acesso em: 11 nov 2022>.

PIOLI, Marília Bugalho. **A LGPD na jurisprudência - Com a entrada em vigor da LGPD, muito se especula sobre a autoridade das ações sobre o tema**. 2022. Disponível em: <https://www.direitoempresarial.com.br/a-lgpd-na-jurisprudencia>. Acesso em: 11 nov 2022.

SOPRANA, Paula. **Justiça já tem 600 decisões envolvendo lei de proteção de dados**. Folha de São Paulo, 2021. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/07/justica-ja-tem-600-decisoes-envolvendo-lei-de-protecao-de-dados.shtml?origin=folha>> Acesso em 9 de out. de 2021

SOUZA, Marcelo Silveira De. **O papel do Ministério Público no enforcement da Lei Geral de Proteção de Dados e demais desdobramentos da aprovação da LGPD no Judiciário brasileiro**. BRASÍLIA. 2021.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais: lei n. 13.709/2018**. 2019.50 f. TCC (Graduação) - Curso de Direito, Centro Universitário de Brasília – Uniceub, Brasília, 2019. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/13802>. Acesso em: 07 de out. de 2021.

SCHREIBER, Anderson. **Responsabilidade civil da Lei Geral de Proteção de Dados Pessoais**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021. p. 319-338. ISBN 978-85-309-9151-7.

STJ. (2017). **RECURSO ESPECIAL**: REsp nº 1348532 / SP (2012/0210805-4). Relator: Min. Luis Felipe Saloão. DJ: 10/10/2017. Disponível em Superior Tribunal de Justiça: <[https://ww2.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=201202108054](https://ww2.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202108054)>. Acesso em 09 de out. de 2021.

STF. (2021). **RECURSO EXTRAORDINÁRIO**: RE 1010606 RJ. Relator Dias Toffoli. DJ: 11/02/2021. Disponível em:<<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755910773>>. Acesso em 12 de out. de 2021.

STJ. (2014). **RECURSO ESPECIAL**: REsp 1397870/MG, Rel. Ministro MAURO CAMPBELL MARQUES, SEGUNDA TURMA, julgado em 02/12/2014, DJe 10/12/2014) Agravo regimental improvido. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tjrn/656670820>. Acesso em 12 de setembro de 2022.

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, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TRT-3. (2018). **RECURSO ORDINÁRIO TRABALHISTA**: RO 0011653-85.2017.5.03.0101. Relator: Min. Sebastião Geraldo de Oliveira. DJ 31/07/2018. Acesso em 1 de Maio de 2019, disponível em Tribunal Regional do Trabalho da 3ª Região:< <https://as1.trt3.jus.br/juris/detalhe.htm?conversationId=3213>>. Acesso em 09 de out. de 2021.

ZANINI, L. E. (2015). **O surgimento e o desenvolvimento do right of privacy nos Estados Unidos**. Revista Brasileira de Direito Civil

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do Tratamento de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 228-229.

**À  
ASSUNÇÃO PROMOTORA EIRELI - CNPJ 18155963000120**

**Ref.: Comunicado de seleção para participar do processo de monitoramento dos Correspondentes no País (“Correspondentes”), o qual está sendo realizado em conjunto com a Ernst & Young Assessoria Empresarial Ltda. (“EY”), Federação Brasileira de Bancos (“FEBRABAN”) e Associação Brasileira de Bancos (“ABBC”) com base nos requerimentos estabelecidos pela Resolução 4.935, de 29 de julho de 2021, divulgada pelo Banco Central do Brasil – BACEN, e pela Autorregulação de Crédito Consignado.**

Prezados Senhores,

Conforme comunicado enviado em abril/maio de 2022 sobre o início do Ciclo de Monitoramento de Correspondentes de 2022, gostaríamos de informar que **sua empresa foi selecionada** para fazer parte da primeira etapa do processo de monitoramento de Correspondentes de Crédito Consignado. Relembre a seguir como foi estruturado o monitoramento e verifique quais são as orientações e o prazo para responder o questionário.

### **Contexto do processo de monitoramento**

O monitoramento contempla um dos critérios previstos no Plano de Qualidade estabelecido pela Autorregulação para avaliação anual da atuação dos Correspondentes por consultoria independente.

O monitoramento será conduzido pela EY e ocorrerá em duas etapas:

- **Primeira etapa:** Consistirá na aplicação de um questionário a ser respondido pelos Correspondentes, estruturado em cinco pilares: (i) Relacionamento com o cliente, (ii) Políticas de Governança, (iii) Tecnologia da Informação, (iv) Aprendizado e Conhecimento e (v) Adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), nos quais estão incluídos os aspectos da Autorregulação. A avaliação do questionário consistirá na análise das respostas fornecidas e dos documentos comprobatórios encaminhados pelo Correspondente. O questionário a ser aplicado levará em consideração a quantidade de contratos ativos até dez/21 (histórico) de cada Correspondentes conforme a seguir: (a) Questionário Completo – a partir de 70 mil contratos; (b) Questionário Reduzido – até 69.999 mil contratos;
- **Segunda etapa:** Consistirá em confirmar as informações providas na primeira etapa através de vídeo inspeção realizada com os Correspondentes selecionados, conforme critérios amostrais definidos para o projeto. Caso sua empresa seja selecionada para a segunda etapa, haverá uma comunicação pela EY para agendamento de vídeo inspeção. É importante que o Correspondente disponibilize o tempo e as pessoas responsáveis para atendimento à equipe da EY.

O resultado da avaliação anual dos Correspondentes será compartilhado com todas as Instituições Financeiras signatárias da Autorregulação que atuam com a sua empresa. Portanto, as informações fornecidas no processo de monitoramento devem contemplar todas as Instituições Financeiras com as quais sua empresa atua como Correspondentes.

### **Prazo e condução do processo**

- **Primeira Etapa**

Nos próximos dias será concedido acesso à plataforma de compartilhamento seguro da EY para o envio do questionário e para a realização de envios e recebimentos de documentos no decorrer do monitoramento. Somente a EY terá acesso aos arquivos incluídos nesta ferramenta, mantendo total sigilo das informações.

#### **Para que sua empresa obtenha acesso à ferramenta da EY:**

Solicitamos que envie o nome completo e o e-mail do profissional da sua empresa que realizará a troca de arquivos com a EY. Os dados devem ser enviados para o e-mail abaixo:

[monitoramento.corbans@br.ey.com](mailto:monitoramento.corbans@br.ey.com)

**O prazo para resposta do questionário será de 2 semanas a contar do seu recebimento.**

Após o recebimento do questionário respondido e dos respectivos documentos suportes, a EY poderá entrar em contato para esclarecer dúvidas e solicitar informações adicionais.

- **Réplica**

Concluídas as análises das respostas e evidências disponibilizadas, a EY compartilhará o resultado apurado com todos os Correspondentes que, através da réplica, terão a oportunidade de avaliar e, se necessário, contestar algum resultado por meio de comentários adicionais e envio de novas documentações comprobatórias. **A réplica deve ser fornecida somente pela ferramenta EY e o prazo para resposta será de 5 dias a contar do seu recebimento.** Após o fim deste prazo, o acesso à réplica será bloqueado.

### **Autorregulação**

Os Correspondentes serão classificados conforme os parâmetros abaixo, previstos na Autorregulação:

<b>Pilar/ Classificação</b>	<b>Não conforme</b>	<b>Em atenção</b>	<b>Parcialmente conforme</b>	<b>Em conformidade</b>
Pontuação Geral	Inferior a 45%	De 45% a 74%	De 75% a 89%	A partir de 90%

**Os Correspondentes selecionados para o monitoramento que não responderem o questionário ou não participarem da vídeo inspeção, serão enquadrados na classificação "Não Conforme" e estarão sujeitos à suspensão definitiva.**

Ressaltamos que, caso os percentuais de adequação constatados no monitoramento estejam compreendidos nas faixas "Não Conforme" ou "Em Atenção", o Correspondente ficará sujeito a aplicação gradual das medidas administrativas previstas no Anexo I do Documento Correlato da Autorregulação, disponível no link a seguir:

[https://cmsarquivos.autorregulacaobancaria.com.br/Arquivos/documentos/PDF/Anexo%20I%20-%20Texto%20Vigente\(1\).pdf](https://cmsarquivos.autorregulacaobancaria.com.br/Arquivos/documentos/PDF/Anexo%20I%20-%20Texto%20Vigente(1).pdf)

### **Confidencialidade e segurança das informações**

A EY e a ASSUNÇÃO PROMOTORA EIRELI deverão adotar todas as medidas necessárias para manter a mais restrita confidencialidade a respeito dos dados e informações estratégicas, comerciais, mercadológicas e quaisquer outras fornecidas durante o processo de monitoramento, sendo desautorizada a sua distribuição, cópia, fornecimento, comercialização ou, por qualquer outra forma ou meio, revelação desses dados e informações a terceiros, incluindo a própria Instituição Financeira contratante, a qualquer título que seja e a qualquer tempo.

**Enfatizamos que as informações solicitadas durante o processo de monitoramento, assim como o questionário disponibilizado, não podem ser compartilhadas conosco e/ou FEBRABAN/ABBC, ou seja, devem ser compartilhadas somente com a EY, a qual está responsável pela condução do processo.**

A obrigação de sigilo perdurará mesmo depois de encerrado ou rescindido o contrato firmado junto a EY.

Atenciosamente,

Bradesco Financiamentos



**R SILVA ASSESSORIA E SERVIÇOS LTDA  
ASSUNÇÃO PROMOTORA EIRELI**

**RELATORIO DE IMPACTO PROTEÇÃO DE DADOS**

**2022**

# SUMÁRIO

- 
- 01** Identificação dos agentes de tratamento e do encarregado
- 
- 02** Necessidade de elaboração do relatório
- 
- 03** Inventários analisados
- 
- 04** Descrição do tratamento
- 
- 05** Partes consultadas
- 
- 06** Necessidade e proporcionalidade
- 
- 07** Identificação e avaliação de riscos
- 
- 08** Medidas para tratar os riscos
- 
- 09** Aprovação



# 01. AGENTES DE TRATAMENTO E O ENCARREGADO

## Controladores:

- Banco Bradesco S/A
- Banco BMG S/A
- Banco Bonsucesso Olé Consignado S/A
- Banco do Estado do Rio Grande do Sul S/A
- Banco Daycoval S/A
- Banco Pan S/A
- Banco Paulista

## Operadores e/ou Co-controladores:

- R Silva Assessoria e Serviços Ltda
- Assunção Promotora Eireli

## Encarregado:

- Panmalla Carneiro Moreira Bacellar  
dpo@assuncaopromotora.com.br  
(98) 9 8304-0010

## 02. NECESSIDADE DE ELABORAÇÃO DO RELATÓRIO

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) visa descrever os 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.

Embora a lei 13.709/18 não determine com clareza quais são os critérios que definem a necessidade de elaboração de um RIPD, elencamos alguns parâmetros que foram utilizados como indicativos de que determinadas ações de tratamento necessitem de avaliações, em razão do maior grau de risco que represente aos seus titulares de dados.

Os preceitos utilizados, seguiram a orientação desenvolvida pelo article 29 Working Party (WP29), considerando apenas os aplicados aos processos realizados pela empresa R Silva Assessoria e Serviços Ltda, quais sejam:

- Monitoramento sistemático
- Dados sensíveis ou de natureza altamente pessoal
- Tratamento de dados em larga escala
- Combinação de conjunto de dados
- Dados de titulares vulneráveis
- Dados tratados com a finalidade de permitir ou negar o acesso do titular a determinado serviço ou realização de um contrato

A empresa no exercício de seu direito atua de forma preventiva no intuito de mitigação de riscos.



## 03. INVENTÁRIOS ANALISADOS

Operacional - Criação de usuários  
Operacional - Suporte  
Operacional - Monitoramento  
Operacional - Cadastro parceiro  
Operacional - Cadastro substabelecido  
Operacional - Mesa de enquadramento  
Operacional - Regularização  
Operacional - Portabilidade / Compra de dívida  
Operacional - Formalização  
Administrativo - Recursos Humanos

## 04. DESCRIÇÃO DO TRATAMENTO

A presente descrição tem o escopo de demonstrar, de forma genérica, sintética e consolidada, os procedimentos adotados e os dados tratados nas operações de empréstimo consignados e demais produtos financeiros, ofertados pelas instituições bancárias controladoras por intermédio da R Silva Assessoria e Serviços Ltda e Assunção Promotora Eireli, seja na condição de Co-Controladora e/ou Operadora que possam gerar riscos aos Titulares de dados.

Por se tratar de uma operação massificada não é possível definir neste relatório a quantidade de titulares afetados pelo tratamento de dados, contudo pode se determinar que os dados são processados em âmbito nacional, e que apenas são coletados os dados exigidos pelas instituições financeiras controladoras, conforme roteiros operacionais e contratos, que em regra são documentos de identificação pessoal com número de RG e CPF, comprovante de endereço, contracheque, número do benefício do INSS e dados bancários, que podem variar dependendo do convênio ou instituição contratada.

O processamento destes dados é fundamental para que possa ser atingida a finalidade pretendida pelo titular do dados, que neste caso será a concessão do empréstimo bancário.

## 05. PARTES CONSULTADAS

Para elaboração deste Relatório foram consultadas a alta gestão, o encarregado de dados, o gestor do departamento jurídico e de Ti.

O ponto de maior relevância tratado refere-se ao procedimentos de segurança que devem ser adotados para a mitigação de incidentes de vazamento de dados, tais como o de revisar a política de segurança da informação, para que possam ser definidos critérios ainda mais rígidos, reduzindo assim os riscos de vazamento, roubo, perda ou outro incidente com os dados dos titulares, bem como exigir das empresas terceirizadas relatórios que comprovem à adoção de procedimentos de backup e segurança de dados.

## 06. NECESSIDADE E PROPORCIONALIDADE

Na operacionalização de empréstimos consignados são observados os critérios estabelecidos pelas instituições financeiras em seus regulamentos e roteiros operacionais, e todas as informações são compartilhadas por meio digital, através das plataformas disponibilizadas pelo bancos e por meio físico, através do envio dos contratos.

O grupo "Assunção Promotora" fundamenta este procedimento de coleta e tratamento de dados nas bases legais de exercício regular do seu direito, execução e/ou preparação contratual e cumprimento de uma obrigação legal ou regulatória em total consonância com a LGPD



## 07. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Figura 1: Matriz Probabilidade x Impacto

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1. Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD.

Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos da empresa.

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	Probabilidade	Impacto	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	15	15	225
R02	Modificação não autorizada.	15	15	225
R03	Perda	15	15	225
R04	Roubo	15	15	225
R05	Remoção não autorizada.	15	15	225
R06	Coleção excessiva.	15	15	225
R07	Informação insuficiente sobre a finalidade do tratamento.	15	15	225
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	15	15	225
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	15	15	225
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	15	15	225
R11	Retenção prolongada de dados pessoais sem necessidade.	15	15	225
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	15	15	225
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	15	15	225
R14	Reidentificação de dados pseudonimizados	10	15	150

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.

## 08. MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
R01 - Acesso não autorizado.	Evitar	Evitar	5	15	75	Sim
R02 - Modificação não autorizada.	Evitar Mitigar	Evitar	5	10	50	Sim
R03 - Perda	Evitar	Evitar	10	10	100	Sim
R04 - Roubo	Evitar Mitigar	Evitar	5	10	50	Sim
R05 - Remoção não autorizada.	Evitar	Evitar	5	10	50	Sim
R06 - Coleção excessiva.	Evitar Mitigar	Evitar	10	5	50	Sim
R07 - informação insuficiente sobre a finalidade do tratamento.	Mitigar	Evitar	5	15	75	Sim
R08 - Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	Mitigar	Evitar	5	10	50	Sim
R09 - Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	Mitigar	Evitar	5	10	50	Sim
R10 - Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	Evitar	Evitar	5	5	25	Sim
R11 - Retenção prolongada de dados pessoais sem necessidade.	Mitigar	Evitar	10	5	50	Sim
R12 - Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	Reduzir	Evitar	5	10	50	Sim
R13 - Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	Mitigar	Reduzir	10	10	100	Sim
R14 - Reidentificação de dados pseudonimizados	Tolerar	Aceitar	5	5	25	Sim

## 09. APROVAÇÃO

Responsável pela elaboração do relatório de impacto:

- Raphael Bacellar Freitas Silva



Encarregado de Dados:

- Panmalla Carneiro Moreira Bacellar



Representante do Co-Controlador e/ou Operador:

R Silva Assessoria e Serviços Ltda - Romildo Assunção Silva





# Inventário de Dados Pessoais

Essa guia é um formulário operacional a ser preenchido de acordo com a sua atividade de tratamento de dados pessoais. São fornecidos comentários adicionais como notas para auxiliar no preenchimento do formulário.

## 1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais

1.1 - Nome do serviço / Processo de negócio	COMERCIAL - CALL CENTER
1.2 - Nº Referência / ID	VENDA DIRETA - 01
1.3 - Data de Criação do Inventário	2021-07-26
1.4 - Data Atualização do Inventário	2021-07-26

## 2 - Agentes de Tratamento e Encarregado

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador	BANCO BRADESCO FINANCIAMENTOS S.A.	NÚCLEO CIDADE DE DEUS, S/N - PRÉDIO PRATA, 4º ANDAR	06029-900	(11) 55037500	LEILA.NASCIMENTO@BRADESCOBBF.COM.BR
2.2 - Encarregado	PANMALLA CARNEIRO MOREIRA BACELLAR	AV COLARES MOREIRA, 1, SALAS 101 A 109, ED. OFFICE TOWER	65075441	98.32226055	JURIDICO@ASSUNCAOPROMOTORA.COM.BR
2.3 - Operador	R SILVA ASSESSORIA E SERVIÇOS	AV COLARES MOREIRA, 1, SALAS 101 A 109, ED. OFFICE TOWER	65075441	98.32226055	DPO@ASSUNCAOPROMOTORA.COM.BR

## 3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua	X		X	X	
3.2 - Base Legal	CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA; EXECUÇÃO OU PREPARAÇÃO CONTRATUAL		CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA; EXECUÇÃO OU PREPARAÇÃO CONTRATUAL	CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA; EXECUÇÃO OU PREPARAÇÃO CONTRATUAL	

#### 4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados

4.1 - Descrição do Fluxo do tratamento dos dados pessoais	<p>O ATENDIMENTO PELO CALL CENTER É EFETUADO, ATRAVÉS DO SOFTWARE DIGISAC, ONDE NOSSOS COLABORADORES ENTRAM EM CONTATO COM OS CLIENTES ORIUNDOS DE UMA BASE DE DADOS FORNECIDA PELA IF, SEGUINDO OS PASSOS ABAIXO: SCRIPT DE VENDA DOS PRODUTOS E SERVIÇOS (Empréstimo Consignado, Refinanciamento, Portabilidade, Empréstimo Pessoal e Cartão Consignado) • PRONTIDÃO AO ATENDER: Bom dia(boa tarde)! Por Gentileza o Sr.(a) (primeiro nome do cliente) por favor. • SAUDAÇÃO INICIAL: Sr. (a) (nome completo do cliente). Meu nome é (nome do operador), eu falo da Assunção Promotora correspondente autorizado do banco XXXXXX, tudo bem com o Sr.(a)? Senhor(a),informamos que para sua segurança essa ligação está sendo gravada. ABORDAGEM: Sr.(a) XXXXX, o motivo do meu contato é para informar que o Banco XXXXX colocou à sua disposição (citar os produtos oferecidos - Ex. uma linha de crédito consignado, etc...) , para sua comodidade e tranquilidade para pagamento. O Sr.(a) XXXXX gostaria de fazer uma simulação agora sobre valores, taxa e prazos de (citar o produto)? Para Resposta SIM: Faça a identificação positiva do Cliente e a confirmação dos dados pessoais. Por favor, qual é o seu nome completo? - Seu CPF inicia com XXX, quais são os outros números? (questionar os OITO últimos dígitos, ouvir e verificar se está correto). - Data de nascimento - Endereço - Telefone de contato - Faça as simulações de Crédito para o cliente. Exemplo para Empréstimo: O senhor tem disponível para empréstimo o valor de R\$ XXX e com prazo máximo de X meses e parcelas de R\$ XXX. O vencimento da primeira parcela será no dia XX. Nessas condições, a taxa mensal desta operação é de X%, a anual de XX%, IOF e R\$ o valor base do Custo Efetivo Total é de R\$ XXX , e o Custo Efetivo Total é N%. A parcela será debitada em conta-corrente. Podemos dar continuidade à proposta nessas condições? Caso o cliente tenha decidido pela contratação da operação. Importante: O prazo para o crédito ficar disponível na C/C do cliente é de até 48hs. É obrigatório que o crédito seja realizado na c/c de recebimento do benefício. Caso o cliente receba por cartão magnético, ele poderá indicar uma conta corrente de sua titularidade. • FINAL O(A) Sr(a) teria alguma dúvida? Posso lhe ajudar em algo mais? O Sr(a) concorda com as informações apresentadas? Importante informar que o Sr. (a) poderá solicitar o cancelamento desta operação através da central de Atendimento (DO BANCO XXXX-XXXX), no prazo de 7 dias a contar do recebimento do crédito. O(A)Sr(a) teria alguma dúvida? Posso lhe ajudar em algo mais? O Sr(a) concorda com as informações apresentadas? Telefone Central de Atendimento: (98) 3222-6055 Assunção Promotora ( atendimento 08h às 18hs) Contato do Banco XXX-XXXX para capitais e Regiões Metropolitanas XXXXX XXX XXXX para demais localidades. Horário de Atendimento - 24 horas • OBSERVAÇÃO ARGUMENTOS: A Argumentação não deve deixar dúvidas sobre o produto que está sendo oferecido. Devemos nos lembrar de colocar a escuta ativa e técnicas de venda em prática. O produto deve ser oferecido de maneira que o cliente possa entender. Finalizado esse processo, o Contrato será digitado seguindo o seguinte processo: DIGITAÇÃO O PROCESSO DE DIGITAÇÃO INICIA APÓS A VALIDAÇÃO DAS INFORMAÇÕES E DOCUMENTAÇÕES COLHIDAS PELO ANALISTA DE CRÉDITO ATRAVÉS DO CONTATO POR TELEFONE, EFETUANDO O CADASTRO DE ACORDO COM A INSTITUIÇÃO FINANCEIRA SOLICITADA. 1 PASSO : ACESSAR O LINK DA IF 2 PASSO : EFETUA O CADASTRO E ENVIO DE DOCUMENTAÇÕES DE ACORDO COM AS EXIGÊNCIAS 3 PASSO: APOS A DIGITAÇÃO É INFORMADO ATRAVÉS DO ERP GERENCIAL CREDITO O NUMERO DA PROPOSTA GERADA. 4 PASSO: AGUARDAR A ANALISE DO BANCO E ACOMPANHAR ATÉ A FINALIZAÇÃO E PAGAMENTO DA OPERAÇÃO. Para Resposta NÃO: Após a negativa do cliente, o atendimento é encerrado.</p>
--	---

#### 5 - Escopo e Natureza dos Dados Pessoais

5.1 - Abrangência da área geográfica do tratamento	OPERAMOS A NÍVEL NACIONAL
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	BASE DE DADOS DAS IF's E CLIENTE FINAL

#### 6 - Finalidade do Tratamento de Dados Pessoais

6.1 - Hipótese de Tratamento	CONTRATAÇÃO DO PRODUTO JUNTO A INSTITUIÇÃO FINANCEIRA
6.2 - Finalidade	EFETIVAR A CONTRATAÇÃO DO PRODUTO

6.3 - Previsão legal	CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA; EXECUÇÃO OU PREPARAÇÃO CONTRATUAL
6.4 - Resultados pretendidos para o titular de dados	CONTRATAÇÃO DO PRODUTO / SERVIÇOS
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo	

## 7 - Categoria de Dados Pessoais

7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal	Nome endereço residência número de telefone fixo residencial e-mail pessoal	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.1.2 - Informações de identificação atribuídas por instituições governamentais	CPF RG número da carteira de motorista	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.1.3 - Dados de identificação eletrônica	Não se aplica			
7.1.4 - Dados de localização eletrônica	Não se aplica			

7.2 -Dados Financeiros	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.2.1 - Dados de identificação financeira	Números de contas bancárias Números de cartões de crédito ou débito	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.2.2 - Recursos financeiros	Renda	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.2.3 - Dívidas e despesas	empréstimos	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA

7.2.4 - Situação financeira (Solvência)	Não se aplica			
7.2.5 - Empréstimos, hipotecas, linhas de crédito	valor emprestado saldo remanescente data de início período do empréstimo taxa de juros	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.2.6 - Assistência financeira	Benefícios	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.2.7 - Detalhes da apólice de seguro	Não se aplica			
7.2.8 - Detalhes do plano de pensão				
7.2.9 - Transações financeiras	Não se aplica			
7.2.10 - Compensação	Não se aplica			
7.2.11 - Atividades profissionais	Atividades profissionais executadas pelo titular dos dados: natureza da atividade	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.2.12 - Acordos e ajustes	Não se aplica			
7.2.13 - Autorizações ou consentimentos	Não se aplica			

7.3 - Características Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.3.1 - Detalhes pessoais	Idade sexo data de nascimento local de nascimento estado civil nacionalidade	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.3.2 - Detalhes militares	Não se aplica			
7.3.3 - Situação de Imigração	Não se aplica			

7.3.4 - Descrição Física				
--------------------------	--	--	--	--

7.4 - Hábitos Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.4.1 - Hábitos	Não se aplica			
7.4.2 - Estilo de vida	Não se aplica			
7.4.3 - Viagens e deslocamentos	Não se aplica			
7.4.4 - Contatos sociais	Não se aplica			
7.4.5 - Posses	Não se aplica			
7.4.6 - Denúncias, incidentes ou acidentes	Não se aplica			
7.4.7 - Distinções	Não se aplica			
7.4.8 - Uso de mídia	Não se aplica			

7.5 - Características Psicológicas	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.5.1 - Descrição Psicológica	Não se aplica			

7.6 - Composição Familiar	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.6.1 - Casamento ou forma atual de coabitação	Nome do cônjuge ou companheiro(a)	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.6.2 - Histórico conjugal				
7.6.3 - Familiares ou membros da família	Não se aplica			

## 7.7 - Interesses de lazer

7.7 - Interesses de lazer	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.7.1 - Atividades e interesses de lazer	Não se aplica			

## 7.8 - Associações

7.8 - Associações	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)	Não se aplica			

7.9 - Processo Judicial/Administrativo /Criminal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.9.1 - Suspeitas	Não se aplica			
7.9.2 - Condenações e sentenças	Não se aplica			
7.9.3 - Ações judiciais	Não se aplica			
7.9.4 - Penalidades Administrativas	Não se aplica			

7.10 - Hábitos de Consumo	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.10.1 - Dados de bens e serviços	Não se aplica			

7.11 - Dados Residenciais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.11.1 - Residência	Não se aplica			

7.12 - Educação e Treinamento	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.12.1 - Dados acadêmicos/escolares	Não se aplica			

7.12.2 Registros financeiros do curso/treinamento	Não se aplica			
7.12.3 - Qualificação e experiência profissional	Não se aplica			

7.13 - Profissão e emprego	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.13.1 - Emprego atual	Empregador	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINANCEIRA
7.13.2 - Recrutamento	Não se aplica			
7.13.3 - Rescisão de trabalho				
7.13.4 - Carreira	Não se aplica			
7.13.5 - Absentismo e disciplina	Não se aplica			
7.13.6 -Avaliação de Desempenho	Não se aplica			

7.14 -Registros/gravações de vídeo, imagem e voz	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.14.1 - Vídeo e imagem	fotos digitais	ATÉ A EFETIVAÇÃO DO CONTRATO E/OU CANCELAMENTO DA PROPOSTA	ERP GERENCIAL CREDITO E IF	INSTITUIÇÃO FINACEIRA
7.14.2 - Imagem de Vigilância	Não se aplica			
7.14.3 - Voz	Não se aplica			

7.15.1 - Outros (Especificar)	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.15 -Outros (Especificar)				

## 8 - Categorias de Dados Pessoais Sensíveis

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
--	-----------	--------------------------	----------------	--------------------



8.1 - Dados que revelam origem racial ou étnica				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências políticaa				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

## 9 - Frequência e totalização das categorias de dados pessoais tratados

9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

## 10 - Categorias dos titulares de dados pessoais

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		

## 11 - Compartilhamento de Dados Pessoais

11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1 BANCO BRADESCO FINANCIAMENTOS S.A.	DADOS INFORMADOS NA ETAPA 3	CONTRATAÇÃO E FINALIZAÇÃO DO PROCESSO
11.2 - Nome da Instituição 2 BANCO BMG S.A.	DADOS INFORMADOS NA ETAPA 3	CONTRATAÇÃO E FINALIZAÇÃO DO PROCESSO
11.3 - Nome da Instituição 3 BANCO PAN S.A.	DADOS INFORMADOS NA ETAPA 3	CONTRATAÇÃO E FINALIZAÇÃO DO PROCESSO

11.3 - Nome da Instituição 4 BANCO OLÉ BONSUCESSO CONSIGNADO S.A.	DADOS INFORMADOS NA ETAPA 3	CONTRATAÇÃO E FINALIZAÇÃO DO PROCESSO
11.5 - Nome da Instituição 5 SABEMI SEGURADORA SA	DADOS INFORMADOS NA ETAPA 3	CONTRATAÇÃO E FINALIZAÇÃO DO PROCESSO

### 13 - Transferência Internacional de Dados Pessoais

13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			

### 14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio

14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Processo Contratação	Objeto do Contrato	E-mail do Gestor do Contrato
14.1 - Contrato nº 1			
14.2 - Contrato nº 2			

## TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

**Título da Pesquisa:** Responsabilidade Civil das Empresas à Luz da Lei Geral de Proteção de Dados: um estudo de caso sobre a adequação da LGPD na empresa Assunção Promotora Eireli em São Luís/MA

**Nome do Pesquisador Principal ou Orientador (a):** Dra. Josanne C. R. Façanha

**Nome do (s) pesquisadores assistentes/alunos:** Kessia Christina Rosa Silva

1. **Natureza da pesquisa:** Esta empresa está sendo convidada a participar desta pesquisa que tem como finalidade buscar informações de como foi sua adequação frente a vigência da LGPD, tentando entender os meios utilizados para readequação e quais estratégias utilizadas, bem como, possíveis gastos que a empresa teve que suportar para isso.
2. **Participantes da pesquisa:** A pesquisa terá como participantes 02 (dois) funcionários da empresa Assunção Promotora. Sendo estes, o Diretor Administrativo, responsável pela reorganização da empresa e montagem dos novos fluxos após a vigência da lei, bem como o DPO (encarregado de proteção de dados), responsável pela proteção de dados dentro da empresa.
3. **Envolvimento na pesquisa:** Ao participar deste estudo a Assunção Promotora permitirá que o (a) pesquisador faça a análise de informações e dados que consigam atingir o objeto da pesquisa, que seria entender de que forma a empresa se adequou à LGPD, tem liberdade de se recusar a participar e ainda se recusar a continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo. Sempre que quiser poderá pedir mais informações sobre a pesquisa através do telefone da pesquisadora da pesquisa.
4. **Sobre as entrevistas:** As entrevistas serão realizadas por meio de conversa junto aos participantes, onde serão feitas perguntas e repasse de dados, que serão gravadas e transcritas, e também poderão ser solicitados via e-mail, para que se possa entender o objeto do estudo de caso.
5. **Riscos e desconforto:** A participação nesta pesquisa não traz complicações legais. Poderão haver perguntas sensíveis, sendo informações específicas da empresa, que podem ocasionar em desconforto e também, podem ser requeridos alguns dados sensíveis, para o entendimento de todo o processo de mudança da empresa. Nenhum dos procedimentos usados oferece riscos à sua dignidade.



6. **Confidencialidade:** todas as informações coletadas neste estudo serão públicas. Sendo assim, a pesquisa ficará disponível ao público que quiser acessá-la, e de mesma forma às informações coletadas na pesquisa.
7. **Benefícios:** Ao participar desta pesquisa a empresa não terá nenhum benefício direto. Entretanto, esperamos que este estudo traga informações importantes sobre, de forma que o conhecimento que será construído a partir desta pesquisa possa, onde pesquisador se compromete a divulgar os resultados obtidos.
8. **Pagamento:** A empresa não terá nenhum tipo de despesa para participar desta pesquisa, bem como nada será pago por sua participação.

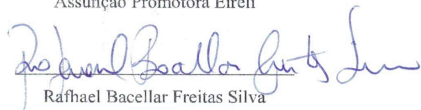
Após estes esclarecimentos, solicitamos o seu consentimento de forma livre para participar desta pesquisa. Portanto preencha, por favor, os itens que se seguem.

#### Consentimento Livre e Esclarecido

Tendo em vista os itens acima apresentados, eu, de forma livre e esclarecida, manifesto meu consentimento em participar da pesquisa. Declaro que recebi cópia deste termo de consentimento, e autorizo a realização da pesquisa e a divulgação dos dados obtidos neste estudo.



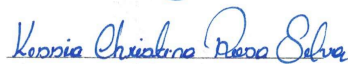
Assunção Promotora Eireli



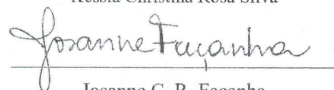
Ráfael Bacellar Freitas Silva



Panmalla Carneiro Moreira Bacellar



Kessia Christina Rosa Silva



Josanne C. R. Façanha

**Pesquisador Principal:** Kessia Christina Rosa Silva; E-mail: [kesschris19@gmail.com](mailto:kesschris19@gmail.com)