ESCOLA DE DIREITO DE BRASÍLIA - EDB

CURSO DE GRADUAÇÃO EM DIREITO

MAIRON MICAEL SOARES ROCHA

Uma análise da LGPD e a identificação dos agentes de tratamento de dados pessoais e suas responsabilidades, na operação de marketing digital da BB Seguros.

BRASÍLIA, DF,
JUNHO 2021

MAIRON MICAEL SOARES ROCHA

Uma análise da LGPD e a identificação dos agentes de tratamento de dados pessoais e suas responsabilidades, na operação de marketing digital da BB Seguros.

Trabalho de Conclusão de Curso apresentado como requisito da disciplina Metodologia da Pesquisa da graduação em Direito da EDAP.

ORIENTADORA: MIRIAM WIMMER

BRASÍLIA, DF,
JUNHO 2021

MAIRON MICAEL SOARES ROCHA

Uma análise da LGPD e a identificação dos agentes de tratamento de dados pessoais e suas responsabilidades, na operação de marketing digital da BB Seguros.

Trabalho de Conclusão de Curso apresentado como requisito da disciplina Metodologia da Pesquisa da graduação em Direito da EDAP.

Brasília, 21 de junho de 2021.

_____
Prof. Drª Miriam Wimmer
Professor Orientador

_____
[Nome do membro da Banca, titulação e instituição vinculada]

_____
[Nome do membro da Banca, titulação e instituição vinculada]

RESUMO

A privacidade da era da informação deve ser definida pelo sujeito mantendo o controle sobre suas próprias informações. Nesse sentido, a escolha pessoal é valiosa, considerando que as organizações têm novos poderes para processar dados. O direito à proteção de dados está relacionado ao direito da personalidade, não ao direito da propriedade. A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18 - LGPD) visa proteger as liberdades básicas e a privacidade e o livre desenvolvimento da personalidade de uma pessoa natural. Nesse contexto, à luz das definições de agentes de tratamento estabelecidas pela lei brasileira, o presente estudo tem por objetivo identificar os agentes de tratamento de dados pessoais definidos pela LGPD e suas responsabilidades na operação de de marketing digital da BB Seguros.A metodologia do presente estudo se traduz numa pesquisa bibliográfica e documental, de natureza qualitativa, realizada através de livros, artigos acadêmicos, periódicos e sites especializados quanto ao tema escolhido, tendo também por referência a legislação brasileira e europeia sobre proteção de dados pessoais e as manifestações de órgãos públicos sobre o tema.

Palavras-chave: Privacidade. Informação. LGPD. Agentes de tratamento.

ABSTRACT

The privacy of the information age must be defined by the subject maintaining control over his own information. In this sense, personal choice is valuable, as organizations have new powers to process data. The right to data protection is related to the right of personality, not the right to property. The General Law for the Protection of Personal Data (13.709/18 or LGPD) aims to protect the basic freedoms and privacy and free development of a natural person's personality. Thus, in this context, taking into account the provisions of the Brazilian law on data controllers and data processors, this study aims to identify the personal data processing agents defined by the LGPD and their responsibilities in the digital marketing operation of BB Seguros.

The methodology of this study consists of a bibliographical and documental research, of a qualitative nature, carried out through books, academic articles, periodicals and specialized websites regarding the chosen topic, and taking into account the Brazilian and European legislation, as well as information provided by public bodies regarding the chosen theme.

Keywords: Privacy. Information. LGPD. Data processing agents.

Sumário

1 INTRODUÇÃO

A sociedade da informação é uma sociedade pós-industrial com economia fortemente baseada em tecnologia de informação. Portanto, o grande valor gerado nesta economia não vem principalmente na indústria de produtos materiais, mas na produção de produtos não materiais, aqueles que podem ser transmitidos por redes digitais.

Neste cenário, o mundo digital começa a ganhar corpo com páginas *Web* e e-mail, as pessoas passaram a consumir e a buscar informação digital. Atualmente, são várias as formas pelas quais um indivíduo pode se conectar com a Internet: computadores, *notebooks*, *tablets*, *smartphones* e outros equipamentos eletrônicos, o que facilitou o acesso à Rede, aumentando o fluxo de dados, trazendo a necessidade de legislação específica para garantir os direitos e determinar os deveres daqueles que usufruem dessa ferramenta.

Não há dúvida de que os benefícios do avanço tecnológico são numerosos. Segurança da informação, oportunidade e qualidade estão interligados. Com dispositivos móveis e tecnologia de nuvem, pode-se acessar instantaneamente inúmeras informações, pessoas e serviços.

Hoje, as relações no comércio digital, bem como no mundo virtual, são completamente dependentes do fluxo de informações e da troca de dados. Neste processo, a determinação de diretrizes para nortear o uso de dados torna-se essencial, visto que cerca de 30% o PIB mundial de 2019 foi pelo comércio eletrônico, conforme estudo da ONU (2021).

No entanto, esta dependência do fluxo de informações via Rede veio junto com a coleta de dados pessoais e o risco de exposição das informações dos usuários.

No sentindo de regular essa prática, a Europa é precursora e, desde 1970, está à frente no debate e no estabelecimento de regras que visam à proteção de dados e buscam regular as implicações na utilização destes.

No Brasil, antes de 2018, o assunto de proteção de dados era tratado, indiretamente, em legislações diversas, como o Código de Defesa do Consumidor (Lei no 8.078/1990), a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei n° 12 965/2014), mas não existia uma norma geral que abordasse a proteção de dados.

A União Europeia estabeleceu níveis elevados de proteção de dados pessoais, que acabaram por se tornar um padrão adotado em diferentes países do mundo, com vistas a facilitar o fluxo internacional de dados e manter altos índices de proteção.

O Brasil tem buscado alcançar o patamar das normas legais e regulamentares, além das políticas e diretrizes estabelecidas naquele bloco. Faz parte do desafio facilitar o fluxo de informações sem descuidar do respeito aos direitos dos titulares, e garantir proteção e segurança por meio de regulamentação adequada.

No Brasil, essa discussão partiu do Princípio da Dignidade Humana, abordado nos termos do artigo 1º, inciso III da Constituição Federal, sendo fundamento basilar da República. Apesar da existência de distintas gerações de leis de proteção de dados pessoais já a partir da década de 1970 na Europa, a Lei Geral de Proteção de Dados - LGPD - tornou-se realidade apenas em 2018 no país.

Diante desse cenário, este trabalho visa fazer uma análise da origem da Proteção de Dados Pessoais, passando pelo arcabouço jurídico brasileiro e se aprofundando na Lei mais recente, a LGPD, com foco na definição legal dos agentes de tratamento de dados e nas suas responsabilidades. À luz de tal análise, buscar-se-à analisar especificamente a operação de de marketing digital da BB Seguros, de modo a identificar os papeis desempenhados por cada ator. Espera-se, com isso, auxiliar as diversas empresas que têm adotado o modelo de Mesa de Performance a entenderem quais iniciativas precisam tomar para que se resguardem em cada um dos papeis que atuam, e, consequentemente, efetivem a proteção de dados pessoais cada vez mais.

A metodologia do presente estudo se traduz numa pesquisa bibliográfica e documental, de natureza qualitativa, realizada através de livros, artigos acadêmicos, periódicos e sites especializados quanto ao tema escolhido. Será feita referência também às normas brasileiras e europeias sobre o tema, assim como a manifestações expedidas por órgãos públicos, em particular aquelas expedidas pela Autoridade Nacional de Proteção de Dados – ANPD. Mayer-Schönberger e Doneda foram as principais referências para uma análise das diferentes gerações de leis de proteção de dados pessoais, bem como os *papers* da Centre for Information Policy Leadership (CIPL) and Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP) foram as principais referências para o entendimento da

aplicação prática da LGPD nos processos das organizações (neste trabalho, aplicado à BB Seguros).

Dessa forma, o primeiro capítulo se dedicará a examinar a “privacidade e proteção de dados na era digital”, onde será traçado o paralelo do conceito de privacidade como direito fundamental em razão da sua relação com o princípio da dignidade humana. Ainda neste capítulo será demonstrada a evolução histórica do tema, partindo-se de um conceito mais restrito de privacidade em direção a uma compressão mais ampla sobre a proteção de dados pessoais. Após tal análise, o trabalho fará um breve resgate da produção legislativa brasileira, para então analisar a LGPD e os agentes de tratamento de dados, previsto na Lei.

Por fim, será apresentada a estrutura de tratamento de dados da mesa de performance da BB Seguros, identificando-se as principais atividades de tratamento de dados, o papel que a companhia exerce nessas atividades, quais artigos da Lei se aplicam a cada um desses processos e quais medidas a empresa deve tomar para atender à Legislação.

2 PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DIGITAL

2.1 PRIVACIDADE

A noção de privacidade remonta ao século XVII, período em que passaram a ser vistas habitações com quartos privativos, remetendo à vontade de poder ocultar dos olhos de todos alguns comportamentos. A evolução da privacidade ao longo do tempo ganha corpo com o sentimento coletivo da necessidade em preservar a intimidade (SIBILIA, 2008).

O conceito moderno de privacidade vem da expressão "*right to privacy*", que, em sua formulação original, pode ser traduzida como o direito a estar e ficar só, ou como o direito de ser deixado só. Apesar de parecer um conceito muito amplo, essa ideia traduz-se no direito do ser humano viver sem a intromissão do Estado ou de terceiros em suas atividades. Inicialmente a ideia da não intromissão era suficiente para garantir a intimidade, porém com o avanço da sociedade e os adventos tecnológicos esse conceito ganha linhas mais amplas, a fim de proteger os direitos do cidadão. A esfera íntima das pessoas deve ser resguardada dos sentidos alheios, principalmente da vista e dos ouvidos de outrem. Por muitas vezes, o almejado não se resume apenas à não inerferência de terceiros, mas tamb~em ao simples fato da ausência de conhecimento sobre a vida particular. Por muitas vezes, o almejado não se resume apenas à não interferência de terceiros, mas também ao simples fato da ausência de conhecimentos sobre a vida particular.

Atualmente, a datificação das coisas faz aparecer o conceito de que as pessoas possuem duas vidas, uma *on* e outra *off-line*. A existência desse binômio amplia o conceito de privacidade, extendendo-se a toda manifestação da vida, seja ela marcada por atitudes reais ou comportamentos digitais de todo cidadão. Nesse novo cenário digital, surge a noção de manter sob constante guarda e vigilância todos os dados digitais que permeiam a vida *on-line.* Para Paula Sibilia (2016), vive-se a sociedade do espetáculo (redes sociais, *blogs*, *reality shows*), onde as pessoas abdicam espontaneamente de seu direito à privacidade, motivadas pela necessidade de destaque e reconhecimento.

2.2 PRINCÍPIO DA DIGNIDADE HUMANA

A dignidade é componente essencial da pessoa e condição de liberdade, igualdade, respeito ao outro, solidariedade, da não interferência nas escolhas da vida, e da possibilidade de agir livremente na esfera pública.

> A dignidade é um valor espiritual e moral inerente à pessoa que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que somente, excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos e a busca do Direito à Felicidade".(MORAES, 2003 p. 10).

O termo "dignidade" é empregado para exprimir uma forte carga de respeito à autonomia privada da pessoa e seus direitos, e protege o livre desenvolvimento da pessoa, permitindo que ela participe da vida política e social, tendo direito à cidadania.

> A dignidade da pessoa humana trata-se do valor-síntese que reúne os aspectos essenciais de desenvolvimento e realização da pessoa humana. O seu conteúdo não pode ser descrito de modo rígido, devendo ser apreendido por cada sociedade em cada momento histórico, baseado na sua cultura (SCHREIBER, 2014, p. 8).

Para Silva (2015), a dignidade da pessoa humana é um valor supremo que atrai o conteúdo de todos os direitos fundamentais do homem, desde o direito à vida.

O direito à privacidade representa uma dessas condições especiais para a vida com dignidade. A Convenção Americana dos Direitos do Homem, conhecida também como Pacto de São José da Costa Rica, de 1969, traz no seu artigo 11 § 2º: "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio, ou em suas correspondências, nem a ofensas ilegais a sua honra ou reputação."

Durante o processo de construção e modernização do conceito de privacidade, houve momentos em que foi preciso equilibrar o direito à privacidade com outros direitos, como o da liberdade à informação. Neste sentido, a Constituição Federal de 1988, em seu artigo 220, parágrafo 1º, determina que nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5 º , IV, V, X, XIII e XIV. Assim, o legislador pode disciplinar o exercício da liberdade de expressão e informação levando em conta a vedação do anonimato, o direito de resposta e a não violação da vida privada, da intimidade, da honra e da imagem das pessoas.

A positivação dos direitos decorrentes da personalidade não possui a capacidade de limitá-los, vez que são instrumentos de defesa da dignidade humana e podem se deparar com circunstâncias inusitadas, inerentes à complexidade humana, devendo protegê-las. Assim sendo, tanto na Constituição quanto no Código Civil, o rol destes direitos não é taxativo. Todavia, conforme Diniz (2006), a intimidade, como exigência moral da personalidade deve ser respeitada para que, em determinadas situações, seja o indivíduo deixado em paz.

A Constituição brasileira aborda o tema inicialmente através das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

> Os direitos da personalidade são aqueles ínsitos a pessoa e reconhecidos em suas projeções sociais, em função de sua estruturação física, mental e moral. São aqueles que recebem proteção jurídica com intuito de preservar os valores inatos ao indivíduo, como a vida, a intimidade, o segredo, o respeito, a honra, a intelectualidade e outros tantos, daí serem dotados de certas peculiaridades (BITTAR, 2014,p. 29).

Comenta Diniz (2006) que o direito à vida privada da pessoa contém interesses jurídicos, por isso seu titular pode impedir ou fazer cessar invasão em sua esfera íntima, usando para sua defesa: mandado de injunção, *habeas corpus, habeas data*, mandado de segurança, cautelares inominadas e ação de responsabilidade civil por dano moral e/ou patrimonial.

Quanto à intimidade, Pinho (2000) a considera como sendo a qualidade do que é íntimo. Advém do latim, *intimus*, significando o que é interior a cada ser humano. É o direito de estar só, de não ser perturbado em sua vida particular.

A privacidade significa o poder de revelar-se seletivamente ao mundo e não significa apenas o direito de ser deixado em paz, mas de determinar quais atributos de si de sua vida será revelado aos outros (LEONARDI, 2012).

Afirma Guerra (2003) que o direito à privacidade visa manter a dignidade da pessoa humana. E, dentro deste direito, entram outros, como a imagem.

> Está fundamentado no artigo 5º, X, da Constituição Federal que afirma que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material e moral decorrente de sua violação. É considerada nas proibições de publicidade e nas determinações de inviolabilidade não podendo, desta forma, a imprensa a título de informar, devassar o recato privado e íntimo da pessoa (GUERRA, 2003, p.247).

Além de um direito fundamental consagrado na CRFB, a privacidade é um dos direitos da personalidade previstos no Código Civil de 2002.

> Os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis e inexpropriáveis. Direito subjetivo, "erga omnes", sobrepõe-se ao direito de imprensa, ao direito de informação ou ao de ser informado e ao de liberdade de expressão. (DINIZ, 2006, 134).

Conforme Vianna (2004), é necessário deslocar o foco da privacidade como direito da personalidade, restrito ao direito privado, para o direito público, reconhecendo-a como essencial para a dignidade humana e lhe proporcionando proteção jurídica mais efetiva, ligado ao direito constitucional e aos tratados de direitos humanos.

> O direito à privacidade, concebido como uma tríade de direitos – direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido (direito de não ter registros pessoais publicados) – transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar em um dos fundamentos do Estado Democrático de Direito.(VIANNA, 2004, p.84).

A privacidade é direito fundamental tutelado em nossa Constituição de 1988 e deriva do princípio da dignidade da pessoa humana, previsto no artigo 1º, inciso III, da CRFB.

> O direito fundamental à privacidade está inserido nos chamados direitos de personalidade, o qual possuiu sua matriz teórica na dignidade da pessoa humana, objetivando a proteção das garantias dos cidadãos (LIMBERGER, 2007, p. 116).

O direito à privacidade também está previsto no artigo 5º, inciso X, da Constituição Federal*, in verbis*:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes do País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
>
> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

Na Constituição Federal de 1988, o constituinte não utiliza o termo privacidade. O artigo 5º, inciso X, da nossa Carta Magna estabelece o seguinte: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral sofrido decorrente de sua violação". Comenta Farias (2002) que "ninguém parece ter uma ideia clara do que ela é".

Para Costa Júnior (2007), dentro da esfera privada ainda haveria a esfera da intimidade, ou confidencial, a qual somente participam aquelas pessoas que o indivíduo deposita certa confiança e mantém certa intimidade. O art. 21 do Código Civil dispõe: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar o ato contrário a esta norma.”

Assim, é um desafio para a sociedade, e, por conseguinte, para o direito, regular a nova realidade do mundo digital, uma vez que a troca de dados é parte essencial deste novo modelo de relacionamento entre os membros desta sociedade.

2.3 PROTEÇÃO DE DADOS PESSOAIS

O progresso tecnológico acelerado torna cada vez maior a capacidade de adquirir, armazenar e processar dados. Nesse sentido, a falta de uma legislação específica à época, bem como sua formulação tardia, dificultaram o entendimento e relação dos envolvidos nesse novo processo.

A possibilidade de coleta e processamento de dados pessoais tornou-se, para as empresas e para o governo, não só a capacidade de entender o comportamento individual, mas também a possibilidade de influenciar decisões, valendo-se de ações sutis para criar a ilusão de escolha. A existência do chamado "gêmeo digital", que é uma forma de colher dados de um software e copiá-los para outro, faz com que todos os dados estejam disponíveis e, assim, tais entidades usam seu poder de processamento de dados em benefício próprio.

Dados pessoais são componentes-chave para a identificação do indivíduo. Perecebe-se que, atualmente, o maior inimigo da privacidade na internet não é o governo, mas sim, o comércio, que fez do mundo virtual um grande mercado, onde os dados pessoais são produtos. As informações fornecidas na rede possibilitam que empresas tracem perfis de usuários, formando um banco de dados sobre suas condições físicas, psicológicas, econômicas ou suas opiniões sobre política ou religião (RODOTÁ, 2008).

Os consumidores não conhecem claramente a forma de coleta, compartilhamento e o potencial uso de seus dados íntimos e pessoais por terceiros, e possíveis falhas de segurança podem permitir ataques a servidores e a

dispositivos inteligentes, a fim de obter essas informações de forma ilegal, em razão do seu alto valor de mercado.

Desde 1970, a Europa tem discutido a proteção de dados e suas implicações. Inicialmente normas nacionais dispersas foram estabelecidas, até a divulgação das Diretrizes sobre a Proteção da Privacidade e do Fluxo Transnacional de Dados Pessoais, da Organização para a Cooperação e para o Desenvolvimento Econômico (OCDE), em 1980 (Mayer-Schönberger, 1997).

As diretrizes da OCDE tiveram um importante papel na internacionalização do tema "proteção de dados" e na elaboração das normas europeias que vieram depois.

No entanto, apesar da orientação da Organização sobre o assunto, a regulação da proteção de dados se dava predominantemente em âmbito nacional.

> Até recentemente, a maioria dos estudos comparativos sobre as normas de proteção de dados enfatizava as dessemelhanças internacionais, e tentava explicar estas variações como a razão para as distintas percepções, específicas de cada país, do problema da proteção de dados. Ultimamente, a crescente demanda internacional por substanciais fluxos de dados entre as nações e o conseqüente desejo por um regime de proteção de dados europeu mais homogêneo colocaram esse ponto de vista nacional sob forte pressão. (Mayer-Schöenberger; 1997).

Vale notar que pouco tempo após a sua publicação, em 1981 foi celebrado o primeiro tratado internacional vinculante sobre proteção de dados pessoais – a Convenção para a Proteção dos Indivíduos com Relação ao Processamento Automatizado de Dados Pessoais, conhecida como a Convenção 108.

Mayer-Schönberger (1997) propõe um estudo das similaridades entre as diversas leis de proteção de dados, estabelecendo uma cronologia de gerações que marcam cada um dos momentos. O autor foca seu trabalho na Europa, onde o assunto se encontra mais adiantado.

Segundo Mayer-Schönberger, as leis de proteção de dados de primeira geração tinham como alvo os bancos de dados nacionais centralizados, que ficavam sob o poder do governo e de grandes corporações, o foco não era a proteção da privacidade em si, e sim, o controle sobre a tecnologia.

Bancos de dados podem ser descritos como conjuntos de arquivos, relacionados entre si, que agrupam informações e registros sobre coisas e pessoas. São coleções de dados que, relacionados entre si, procuram descrever e caracterizar algo, dar sentido e eficiência às pesquisas relacionadas a um tema (pessoa, fato ou coisa) específico. Os bancos de dados surgiram na década de 70,

e, atualmente, são de vital importância para diversas instituições de todo mundo, sendo a principal peça de informação e segurança.

Esses bancos de dados surgiram com a necessidade de um planejamento adequado às necessidades empresariais e organizacionais. Ao mesmo tempo, as grandes corporações perceberam o potencial que o processamento de dados tinha em melhorar a administração e gerenciamento.

Diversos países começaram a se movimentar para ter bancos de dados robustos. Tais propostas assustaram os cidadãos, que, com medo de uma vigilância total de suas vidas, iniciaram um movimento em favor da proteção de dados.

O progresso tecnológico acelerado torna cada vez maior a capacidade de adquirir, armazenar e processar dados. Nesse sentido, muitas vezes a sociedade não está preparada para lidar com o excesso de informações disponíveis, bem como a modernidade do assunto não encontra bases legais. A própria legislação, devido à morosidade de sua evolução, não tem preparo para prevenir abusos relacionados à perda de privacidade advinda do grande fluxo de informações.

Ainda sobre a primeira geração, as leis editadas à época não tinham como foco a proteção à privacidade individual, elas tinham um teor funcional. Regulavam o processamento de informações em si, as condições sob as quais este processamento poderia ocorrer legalmente, além de apontarem medidas de sigilo e de segurança. O foco era ter um controle sobre a tecnologia, sobre a utilização dos computadores, tanto que havia leis que versavam até sobre a integridade do código fonte (a programação, em linguagem técnica, das informações).

Desde a primeira geração das leis de proteção de dados, o indivíduo tem a possibilidade de acessar e corrigir seus dados, mas, nessa primeira formulação, não cabia a ele decidir se esses dados seriam processados ou não.

No entanto, durante a década de 70 surgiram os computadores pessoais e a descentralização dos dados, sendo estes distribuídos por inúmeros servidores. Com isso, muitos cidadãos sentiram as consequências da coleta e do processamento de dados de forma irrestrita, o que originou uma nova discussão, agora, com foco nos direitos à privacidade individual do cidadão.

A segunda geração, portanto, é marcada por essa nova ênfase, onde é tratado o direito do cidadão de se defender da exposição, que, de forma difusa, poderia violar seu espaço íntimo. Nessa segunda fase, o indivíduo passa a participar do processo e sua anuência é peça chave para o processamento dos dados, como,

por exemplo, determinava a Lei sobre Proteção de Dados da Noruega, que concedia aos indivíduos o direito de recusar o processamento dos seus dados para fins de marketing direto e pesquisa de marketing.

Neste segundo momento, também houve alteração da forma como o governo se relacionava com o tema, sendo esse, até então, o único responsável pela fiscalização e aplicação das normas de proteção de dados. A partir de agora, esse controle, também passaria a ser realizado, igualmente, por entes privados.

Ainda assim, na prática, o indivíduo que limitasse a troca de informações pessoais teria direitos e serviços restringidos, pois para ter acesso aos serviços públicos, bem como a programas assistenciais e até para viajar ou votar, era preciso haver troca de dados.

Com este cenário, atrelado a um momento em que ressurgiam, na Alemanha, movimentos de participação ativa da sociedade, surgiu uma terceira geração de leis de proteção de dados.

Essa nova etapa foi marcada por uma decisão da Corte Constitucional Alemã, que vinculou a garantia do individuo decidir sobre a disponibilidade e utilização de seus dados aos direitos fundamentais. Com isso, passou-se a reconhecer o direito de proteger seus dados contra terceiros, na forma de um direito à autodeterminação informativa. Autodeterminação pode ser descrita como o direito de decidir por si mesmo, o direito à livre escolha. Este direito, por extensão, chega aos dados pessoais, garantindo a todo cidadão o direito de tratar seus dados com liberdade, assegurando proteção e confidencialidade, caso assim deseje.

A corte alemã ainda declarou que os cidadãos deveriam participar de todo o processamento de dados, desde a coleta até sua utilização. Firmou, ainda, que quando o governo solicitasse dados pessoais, ele deveria dizer a finalidade para a qual os dados seriam utilizados (princípio aplicado na lei brasileira de proteção de dados de 2018 - LGPD).

A terceira geração europeia foi marcada pelos debates iniciados na geração anterior que buscavam entrelaçar temas ainda distantes entre si, como as funcionalidades de processamento de dados, a concentração das discussões nos direitos individuais e a participação ativa dos cidadãos no processo de proteção de dados. Como exemplo, surgiram o direito de apagar velhas informações e o de consentir, ou não, com o cruzamento de seus dados.

Entretanto, a efetivação dos direitos na terceira geração traz consigo um custo social. Em vista disso, este pode ser associado à necessidade de recorrer ao sistema judiciário para a efetivação desses direitos. Essa necessidade diminui ou restringe a parcela da população que poderá exercer amplamente as evoluções advindas da lei.

Já a quarta geração tenta corrigir essa vulnerabilidade do indivíduo, citada na terceira geração. As novas leis e normas, a partir de meados de 80, fortalecem o indivíduo frente às grandes instituições, e, ao mesmo tempo, reduzem a discricionariedade do indivíduo em algumas maneiras de proteção de dados, estabelecendo uma proteção legal obrigatória (Mayer-Schönberger, 1997).

> Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição de uma pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito a autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual na autodeterminação informativa. Isto ocorre porque se parte do pressuposto que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser obtida exclusivamente de uma decisão individual (Doneda; 2006; pg 211-212).

Mayer-Schönberger (1997) afirma que, nesta geração, os países da Europa começaram a se movimentar no sentido de suplementar as leis gerais de proteção de dados com leis setoriais. Por essa razão, são instalados órgãos públicos de suporte para investigar, e de decisão para arbitrar sobre o assunto.

Para o amplo desfrute dos direitos e evoluções trazidos pela quarta geração também há um custo social associado. As empresas e instituições se veem obrigadas a realizar investimentos financeiros a fim de se adaptarem à legislação, já que altíssimas multas e penalidades podem ser impostas no caso de não adequação à lei. O retorno desse investimento não se restringe à adequação às normas e no ganho de privacidade da população, mas, também, na possibilidade de manter relações empresariais com países que vinculam a necessidade de legislações equivalentes à manutenção dos vínculos comerciais.

Doneda (2012) leciona que nas interações sociais tradicionais, somos capazes de avaliar as consequências do fornecimento de nossos dados, por exemplo passando informações mais específicas para pessoas mais próximas e informações mais amplas para pessoas não tão próximas. Nas interações humanas também é possível que uma utilização indevida dos dados de alguém leve essa pessoa a se

afastar socialmente de quem usou com má fé as informações que tinha. Já nas redes sociais os usuários fornecem seus dados para poderem se relacionar com outros usuários, mas não são eles que possuem o poder de determinar o tratamento a ser dado às informações, e sim a rede social que intermediou a relação.

A partir deste cenário, analisemos a produção legislativa brasileira.

3 PRODUÇÃO LEGISLATIVA BRASILEIRA

Apesar de vários dos princípios até aqui descritos na evolução das leis europeias também constarem na legislação brasileira, cabe dizer que a primeira lei nacional, tratando especificamente do tema, data apenas de 2018, quase cinco décadas após o início das discussões sobre o tema no velho continente. Contudo, isso não reflete a ausência de tratamento sobre o tema. Conforme mencionado anteriormente, antes de 2018 havia a extrapolação de outras leis e princípios fundamentais a fim de abordar a proteção de dados pessoais. Princípios da Constituição Federal, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet são exemplos de legislações anteriores que ajudaram no embasamento da lei específica de 2018.

O Código de Defesa do Consumidor (Lei n.º 8.078/1990) traz uma série de garantias com o escopo de evitar a utilização ilícita de dados pessoais nas relações de consumo. Exemplo disso é possível observar em seu artigo 43, que, dentre outros comandos, exige a ciência do consumidor no caso de abertura de cadastro.

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> §4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

A Lei do Cadastro Positivo (Lei 12.414/11), por sua vez, disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Em seu artigo 4º, a referida lei, estabelece que “a abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada”.

> A coleta, armazenamento e utilização de dados pessoais por intermédio da internet exige que o consumidor seja informado previamente, devendo constar em contrato de prestação de serviços ou termos de aplicação de uso, elucidando o conteúdo da permissão. Ademais, é direito do titular das informações coletadas solicitar sua exclusão no momento em que cessar a relação entre as partes, e, para isso, devem existir instrumentos próprios ou a forma ou endereço por meio do qual o usuário pode solicitar a exclusão, somente ficando arquivadas aquelas que decorrem de determinação legal (MIRAGEM, 2014, p.63).

Outro passo passo importante foi dado com a promulgação da Lei Federal nº 12.737/2012, conhecida como "Lei Carolna Dieckmann", qe trata dos crimes cibernéticos no Brasil. Até então, não havia algum tipo de regulamentação que responsabilizasse esses tipos de ilícitos, sendo comum, conforme coloca SILVA (2010), a ocorrência de crimes cometidos na internet relacionados à pessoa, como injúrias, calúnia, difamação, ameaças, violação de correspondências, pedofilia entre outros.

Neutralidade da rede, privacidade, retenção de dados, função social da rede e responsabilidade civil de usuários e provedores são temas tratados na Lei nº 12.965, de 23 de abril de 2014, denominada "Marco Civil da Internet"[1]. Além da neutralidade da rede, às empresas que fornecem o acesso à conexão fica o dever da proteção de todos os registros e dados pessoais; do armazenamento dos registros de conexão e dos acessos às aplicações.

O Marco Civil da Internet estabelece que a empresa deve armazenar registros de conexão e de acesso à aplicativos sempre preservando a honra, a vida privada, e a imagem dos usuários. Tais informações somente podem ser disponibilizadas perante uma ordem judicial, observado o disposto no Art. 7º da mesma Lei.

Vale observar, por fim, que o direito à proteção de dados está relacionado ao direito da personalidade, não ao direito da propriedade. Isso ocorre porque os atributos do direito de propriedade estão diretamente relacionados ao propósito de fins econômicos, e os dados pessoais confidenciais não estão (ou pelo menos não deveriam estar) relacionados a fins comerciais (RODOTÁ, 2008).

[1] ¹ O objetivo de criar a neutralidade na rede visa impedir que provedores de internet possam ofertar serviços de conexões diferenciados, como a venda de um pacote que permite apenas o acesso a e-mails ou a rede social. Ou seja, limitando o uso geral de sua conexão. A neutralidade prevê que as empresas que fornecem o serviço de internet, sejam neutras em relação ao tráfego de dados, não podendo criar qualquer impedimento para que este usuário acesse qualquer conteúdo ou utilize qualquer serviço.

Por outro lado, comenta Mendes (2015) que o princípio da privacidade, como qualquer princípio básico, tem suas limitações porque a vida social é naturalmente observada, por interesse coletivo e público.

3.1 LEI 13.709/18 (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD)

Em 65 artigos, a Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais – "LGPD") estabelece uma série de restrições para instituições privadas e públicas que armazenem dados de internautas, consumidores, partes em um contrato, usuários de serviços públicos ou alvos de políticas públicas. Qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, está sujeitos à LGPD[2]. A LGPD regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil.

Nos termos do art. 6º da LGPD, as atividades que envolvem o tratamento dos dados devem observar os seguintes princípios: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Assim, todas as empresas (ou profissionais autônomos) que mantenham bancos de dados, físicos ou digitais, deverão implementar um programa em conformidade com a Lei, cumprindo todos os passos para que se possa garantir a segurança e proteção dos dados em seu poder. Desse modo, toda e qualquer operação que envolva tratamento de dados pessoais no Brasil necessita adaptar-se à LGPD.

Segundo os princípios da finalidade, adequação e necessidade (correspondentes ao "*data minimisation*"[3]), os dados pessoais devem ser adequados, relevantes e limitados em relação aos fins específicos para os quais eles são processados. Vale ressaltar que o princípio da finalidade estavelece a obrigatoriedade do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma diversa dessas finalidades. O princípio da adequação consiste na compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contesto do

[2] A Lei comporta poucas exceções, previstas em seu art. 4º, que dispõe: "Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei".

tratamento. Já o princípio da necessidade se apresenta como a llimitação do tratamento ao mínimo necessário para o atendimento de suas finalidades, com abrandência apenas dos dados pertinentes, proporcionais e não excessivos em relação às finalidades pré-estabelecidas.

Tal garantia busca impedir justamente o uso ilimitado dos dados pessoais coletados, de forma diversa à que os titulares destas informações poderiam esperar. O princípio do "*data minimisation*" está previsto também no artigo 5º, 1, "c", do Regulamento Europeu de Proteção de Dados (*General Data Protection Regulation* – GDPR), exigindo que sejam coletados apenas os dados adequados, relevantes e necessários para a sua respectiva finalidade.

A Lei nº 13.709, já em seu artigo 2º, preocupou-se em destacar os fundamentos que embasam a proteção de dados pessoais. Assim, o princípio de proteção de dados pessoais deve ser baseado no respeito pela privacidade; autodeterminação informativa; liberdade de expressão, informação, comunicação e opinião; intimidade, inviolabilidade da honra e imagem; desenvolvimento econômico e tecnológico e inovação; livre iniciativa, livre concorrência e defesa do consumidor; direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas singulares (BRASIL, 2018).

A lei 13.709/2018 cita, em seu artigo 2º, inciso IV, a inviolabilidade da initimidade, da honra e da imagem como fundamento da proteção de dados pessoais, direitos amparados, também, na Constituição Federal de 1988, em seu artigo 5º.

Os titulares (que são as pessoas naturais identificadas ou identificáveis a quem se referem os dados pessoais) poderão solicitar informações sobre o tratamento desses dados, correção de dados armazenados incorretamente, revogação do consentimento, portabilidade dos dados para outro fornecedor (de produtos e serviços) e até a exclusão de seus dados do cadastro da empresa.

A ANPD (Autoridade Nacional de Proteção de Dados) é o órgão federal responsável por fiscalizar e aplicar a LGPD. A Autoridade foi criada para zelar pela proteção de dados pessoais e possui competências normativas, de fiscalização e de sancionamento.

Com o advento da nova Lei, o titular de dados passa a ter o direito de levar à Autoridade Nacional de Proteção de Dados, ou a outras entidades fiscalizadoras, suas reclamações e solicitações que não sejam atendidas pelas empresas.

No contexto da Lei, o conceito de dado pessoal amplia-se até dimensões além do simples conjunto de dados de pessoa natural identificada, referindo-se também a dados relacionados a pessoas identificáveis. Também são alcançados pela norma outras especificidades de dados. Assim, a lei introduziu também o conceito de dado pessoal sensível, classificação diretamente influenciada pela GDPR e que só havia sido mencionada em legislação brasileira pela Lei do Cadastro Positivo e portanto restrita ao contexto da concessão de crédito. Também é contemplado o conceito de dado anonimizado – relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Cabe observar com especial atenção as informações e orientações sobre o tratamento de dados sensíveis. São assim classificados como os de raça ou etnia, religião, opinião política e ainda informações sobre saúde, genética e biometria. Este grupo, que contém dados mais reveladores sobre o titular, demanda ainda mais cuidado por parte dos agentes de tratamento. Os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, a possibilidade de seu mau uso causar discriminação. Por esse motivo, a LGPD protege ainda mais os dados pessoais sensíveis, pois o dano potencial de sua violação é, em regra, maior que apenas o dano no vazamento dos dados pessoais (BIONI, 2018).

Há ainda a seção III da LGPD, que dispõe sobre dados de crianças e adolescentes. Entre as exigências, o destaque é a questão do consentimento. “O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal”, obriga a lei.

A Lei Geral de Proteção de Dados traz as definições acerca dos atores envolvidas em uma relação de tratamento de dados pessoais, contidas nos incisos V à IX do artigo 5º . São eles o titular, o controlador e o operador, definidos como agentes de tratamento, e o encarregado.

a) Titular é a pessoa natural a quem se referem os dados pessoais.

b) Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais

c) Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais sob orientação e/ou supervisão do responsável pelo tratamento, ou controlador.

d) Encarregado é aquele indicado pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, o detentor dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

e) Agentes de tratamento são aqueles reponsáveis pelo efetivo tratamento dos dados pessoais, são eles o Controlador e o Operador.

De acordo com o inciso X do mesmo artigo, tratamento é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A LGPD apresenta os agentes, ocasiões, ocasiões, formas e finalidades para o tratamento de dados. Em seus artigos 7º e 11, estipula, especificamente, as situações e agentes que podem realizar tal tratamento, de forma que qualquer violação a essas hipóteses implica em violação à Lei de privacidade. O inciso I do artigo 7º aponta o primeiro caso que regula e permite o tratamento de dados: “mediante o fornecimento de consentimento pelo titular”, sendo que este consentimento deve ser, conforme o artigo 8º da mesma lei, “[...] fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular” e, caso seja escrito, o parágrafo 1º diz “[...] esse deverá constar de cláusula destacada das demais cláusulas contratuais”. Também é prevista a utilização para o exercício regular de direitos em processo judicial, administrativo ou arbitral, para a proteção da vida ou da incolumidade física do titular ou de terceiro, para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Além disso, também é permitido o tratamento de dados em diversas outras hipóteses previstas no art. 7º e no art. 11 da LGPD, inclusive, no caso de dados pessoais não sensíveis, quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Ainda, são nulas as autorizações genéricas para o tratamento de dados, devendo o consentimento referir-se às finalidades específicas (art. 8º, §4º),

ressaltando que esse consentimento pode ser revogado a qualquer momento, caso assim se manifeste de forma expressa o titular (art. 8º, §5º).

Ademais, é importante frisar que a LGPD estabelece que mesmo os dados publicamente disponíveis ou tornados manifestamente públicos pelo titular são protegidos, e seu tratamento deve observar os propósitos legítios, os princípios da LGPD e os direitos do titular.

As formas de atendimento ao usuário para que este tenha informação sobre o tratamento dos seus dados deverá ser facilitada, nos termos do art. 9º da LGPD. Assim, o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva. Com isso, o usuário deverá ter a opção de executar os seguintes direitos de forma simplificada: solicitar o acesso aos dados existentes; a anonimização; bloqueio ou eliminação de dados desnecessários; a portabilidade dos dados para outras empresas, bem como a exclusão total dos dados do sistema.

Conforme o relatório “Implementação e regulamentação efetiva sob a nova lei geral de proteção de dados - Prioridades das organizações públicas e privadas implementarem de forma eficaz a nova lei geral brasileira de proteção de dados” (CIPL, 2020), a aplicaçao da LGPD não se restringe apenas às áreas de fins específicos dentro da empresa controladora, mas a todos os departamentos da empresa que, em algum momento, lidam com dados. Dessa forma, dentro do funcionamentos das empresas e instituições, são necessárias adaptações, medidas internas, mudança de cultura, comportamento e práticas a fim de garantir a observância da lei não somente em seu fim específico mas em todas as etapas do processo. É preciso mapear todo o fluxo do tratamento de dados dentro da empresa, desde a coleta até a eliminação. O objetivo principal da LGPD é permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

A LGPD impõe multas para cada infração de até 2% do faturamento, limitadas a R$ 50 milhões (artigo 52, parágrafo II). A alta cifra reflete a preocupação do legislador em dar proteção às informações disponibilizadas e ao tratamento dado a elas.

Com isso, a responsabilização se torna um tema central da LGPD. É necessário que as organizações mapeiem e registrem suas atividades de tratamento

de dados pessoais efetuadas e identifiquem se estão atuando naquela atividade como controladora e/ou operadora.

Uma definição clara de seu papel nos múltiplos cenários de tratamento de dados deve ser registrada por meio de acordos de tratamento de dados ou cláusulas específicas em contratos gerais, por exemplo, de forma que a organização se resguarde de eventuais danos causados aos titulares dos dados.

3.2 OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS NA LGPD

São agentes de tratamento o controlador e o operador de dados pessoais, que serão abordados em mais detalhes em seguida. Inicialmente, porém, cabe registrar que os agentes de tratamento devem ser definidos a partir de seu caráter institucional. O guia orientativo da ANPD sobre agentes de tratamento (2021, p. 5) explica que:

> Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organizção, já que atuam sob o poder diretivo do agente de tratamento.

A Lei Geral de Proteção de Dados traz em seus artigo 5º ,incisos VI e VII e no artigo 39 a possibilidade de as organizações atuarem como controladoras e/ou operadoras de dados pessoais; e, no seu artigo 42, §1º,inciso I ,como co-controladoras. Vide:

> Lei 13.709, de 14 de Agosto de 2018.
>
> Art. 5º Para os fins desta Lei, considera-se:
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados. [...]
>
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. [...]
>
> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.[...]
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipóte-

> se em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Percebemos que o papel de controlador está atrelado ao poder de decisão sobre o uso dos dados. No entanto a utilização prática dos dados pode ocorrer por meio de um terceiro. Conforme relatório da CIPL (2020) explica:

> Como exemplo, um controlador pode utilizar um terceiro para fornecer serviços de folha de pagamento para seus funcionários. Os controladores também podem usar operadores de dentro do seu mesmo grupo econômico. Um exemplo seria quando todas as entidades desse grupo econômico utilizam um help desk de TI administrado por uma entidade específica desse mesmo grupo.

Neste sentido, a ANPD (2021, p.6) ratifica:

> "...serão controladores quando atuarem de acordo com os próprios interesses, com poder de decisão sobre as finalidades e os elementos essenciais de tratamento. Serão operadoras quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento".

O papel de operador, portanto, envolve a ação sob a instrução do controlador. Importante observar que uma organização pode atuar como controladora e operadora. Por exemplo, uma organização seria uma controladora se usasse seus próprios recursos para tratar os dados pessoais de seus próprios clientes, mas também seria uma operadora se fornecesse soluções de TI para outras organizações.

No entanto, em uma mesma atividade de tratamento de dados, "o operador deve ser uma entidade distinta do controlador" (ANPD, 2021, p. 6). Um empregado ou um contratado da empresa controladora nunca será o seu operador, pois, como vimos, apenas instituições assumem este papel.

Por fim, pode haver o papel de co-controlador, caso em que duas ou mais empresas definem em conjunto sobre a utilização dos dados pessoais.

Cada ator terá responsabilidades próprias e deverá adotar medidas para cumpri-las, conforme os princípios da responsabilização e prestação de contas, previstos na legislação.

> Lei 13.709, de 14 de Agosto de 2018.
>
> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A Lei (art. 37) normatiza que tanto os controladores quanto os operadores devem manter registros das atividades de tratamento.

> Lei 13.709, de 14 de Agosto de 2018.
>
> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Afinal, operadores e controladores podem ser responsabilizados conjuntamente, conforme artigo 42, já mencionado. Este é um exemplo em que a Lei reconhece a tenuidade das diferenças e a complexidade na definição de ambos os papeis.

O artigo 18, em seu parágrafo 3, chega a não fazer diferenciação entre os agentes, demonstrando que o legislador compreende a necessidade de comunicação e cooperação entre os agentes em diversas situações de direito do titular dos dados:

> Lei 13.709, de 14 de Agosto de 2018.
>
> Art. 18º O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

Existem, entretanto, exceções para responsabilidade conjunta, como no artigo 43 - mais uma vez reforçando a importância da prestação de contas:

> Lei 13.709, de 14 de Agosto de 2018.
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Além disso, a legislação é mais enfática nas obrigações aplicáveis aos controladores, conforme a tabela a seguir apresentada:

Obrigação	Referência na LGPD	Aplicável aos controladores	Aplicável aos operadores
Definição das bases legais para o tratamento de dados pessoais	Artigo 7	✓ (implícito)	X
Fornecimento de informações aos titulares de dados sobre as atividades de tratamento de dados	Artigo 8, parágrafo 6 Artigo 9 Artigo 14, parágrafo 2	✓	X
Garantia da transparência do tratamento de dados pessoais baseado no legítimo interesse	Artigo 10, parágrafo 2	✓	X
Apresentação dos relatórios de avaliação de proporcionalidade ligada ao interesse legítimo para a ANPD se requisitado	Artigo 10, parágrafo 3	✓	X
Verificação da identidade dos responsáveis legais que fornecem o consentimento em nome das crianças	Artigo 14, parágrafo 5	✓	X
Deletar os dados pessoais ao final da atividade de tratamento de dados	Artigo 16	✓ (implícito)	✓ (implícito)
Receber e responder os pedidos de direitos do titular dos dados e informar os outros controladores e operadores sobre as ações necessárias para cumprir tais pedidos	Artigo 18 Artigo 18, parágrafo 6	✓	X
Instauração de mecanismos e salvaguardas apropriados para transferência de dados	Artigo 33, II	✓	X
Manutenção de registros das atividades de tratamento de dados pessoais	Artigo 37	✓	✓
Elaboração de relatórios de impacto e apresentação dos mesmos para a ANPD se requisitado	Artigo 38	✓	X
Tratamento de dados pessoais de acordo com as instruções dos controladores	Artigo 39	X	✓
Nomeação do encarregado	Artigo 41	✓	X
Indenização pelos danos e prejuízos relacionados às atividades de tratamento de dados pessoais	Artigo 42	✓	✓
Adotação de medidas técnicas e organizacionais para garantir a segurança dos dados pessoais	Artigo 46 Artigo 47	✓	✓
Notificação da ANPD e dos titulares de dados acerca dos incidentes de segurança e adotação de medidas requisitadas pela ANPD	Artigo 48 Artigo 48, parágrafo 2	✓	X
Implementação de programas de conformidade com a LGPD	Artigo 50 Artigo 50, parágrafo 2	✓	✓

Fonte: (CIPL, 2020, p. 26) .

Os artigos relacionados a um ou outro agente na tabela foram assim dispostos pois trazem o termo controlador ou operador explicitamente em seu texto, no entanto, conforme explicado, muitas das responsabilidades do controlador dependem da contribuição do operador.

Portanto, é importante que sejam adotados alguns cuidados nas parcerias realizadas entre controladores e operadores, sendo necessário haver confiança entre eles.

Neste sentido, vale destacar que o controlador tem a prerrogativa e o dever, expressos pela legislação, em seu artigo 39, de verificar se o operador está agindo

de acordo com as suas instruções. Logo, é necessário que haja normativos internos e procedimentos para gerir a relação dos controladores com terceiros, de forma que haja maior proteção dos dados sob seus cuidados em todo o ecossistema ao qual são submetidos, além de políticas para que essas parcerias envolvam operadores que são comprometidos com a proteção de dados pessoais.

Analisados os papeis dos agentes de tratamento de dados, vamos identificar, na operação de mesa de performance da BB Seguros, quem atua em cada um desses papeis e quais iniciativas a BB Seguros deve tomar para se reguardar de eventuais responsabilidades causadas por outros agentes.

4 IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO DE DADOS NA MESA DE PERFORMANCE DA BB SEGUROS

A partir daqui, conforme pretendido no início desta pesquisa, vamos demonstrar o funcionamento da Mesa de Performance da BB Seguros, e, ao final descreveremos as principais atividades e processos, identificando os papeis de cada agente, e quais os normativos que se aplicam a eles, definindo os procedimentos que a organização deve ter para cumprir a LGPD em cada uma de suas responsabilidades.

Inicialmente é importante destacar que a BB Seguros é uma coligada do Banco do Brasil e de outras 5 empresas, conforme a imagem abaixo.

Imagem 1 – Estrutura societária da BB Seguros

Fonte: Banco do Brasil. Disponível em http://www.bbseguridaderi.com.br/pt/conheca-a-bb-seguridade/empresas-do-grupo

A demonstração da estrutura societária é apenas para facilitar o entendimento da relação BB Seguros e cliente. Não há aqui a intenção de discutir a composição econômica/social entre as empresas.

Assim, vale explicar que quando um cliente compra algum seguro, previdência, título de capitalização ou plano odontológico do Banco do Brasil, o cadastro dele ficará sob o domínio do Banco do Brasil.

Entretanto, com base no contrato societário entre as empresas envolvidas, terão acesso completo ao cadastro deste cliente o Banco do Brasil, a BB Seguridade, a BB Seguros e a empresa responsável pelo produto comprado:

a) seguros = Brasilseg

b) previdência = Brasilprev

c) capitalização = Brasilcap

Não entraremos na análise de Brasildental, tampouco da empresa Ciclic, pois seus produtos não são comercializados pela Mesa de Performance, objeto deste estudo.

Importante destacar que apenas os clientes que possuem algum produto de seguridade têm seus dados compartilhados com as coligadas de seguridade (BB Seguros e a coligada do produto). Atualmente, este compartilhamento entre o Banco do Brasil e suas coligadas se dá em razão do contrato societário entre as empresas. Não havendo, por enquanto, termos contratuais entre elas e os titulares autorizando tal compartilhamento. No entanto, inicialmente é possível sugerir que há o legítimo interesse como base legal para este compartilhamento, uma vez que todas as empresas trabalham em conjunto para atender o cliente. O Banco do Brasil fornece atendimento, via agências; a coligada possui toda a operação de pós venda, como central de atendimento, clube de benefícios e processos de sinistros; e a BB Seguros atua como auditora das operações da coligada.

De toda forma, com a vigência da LGPD é importante que a BB Seguros, bem como o Banco do Brasil, documentem qual(is) base(s) legal estão utilizando para compartilhar os dados de seus clientes.

A operação de Mesa de Performance, por sua vez, funciona, resumidamente, conforme a imagem a seguir apresentada.

IMAGEM 2: Agentes de tratamento na mesa de performance da BB Seguros

Fonte: elaboração própria

Atualmente, os dados dos clientes da BB Seguros são carregados pela própria empresa nas ferramentas de mídia. São elas, principalmente – mas não exclusivamente -, o Google e o Facebook. Esses veículos solicitam o nome, sobrenome, e-mail, telefone, CEP, Cidade, Estado, País, Data de Nascimento, Ano de Nascimento, Gênero e Idade. Quanto mais dados forem carregados, maior a possibilidade do cliente ser identificado pelas ferramentas.

A identificação nas ferramentas ocorre por meio de *cookies*. Os *cookies* são pacotes de dados enviados por um site para o computador do usuário. Isso faz com que quando aquele mesmo computador visite outro site, este pacote de dados seja identificado.

Os sites trocam informações entre eles por meio da rede de internet como um todo. Dessa forma, conforme o usuário vai deixando seus dados em um ou outro site, o cruzamento desses dados torna possível relacionar os dados pessoais do usuário com o cookie que está em seu computador.

Portanto, caso os veículos de mídia não recebessem os dados dos clientes da BB Seguros de forma anonimizada, eles conseguiriam identificar de maneira individualizada esses clientes.

Importante mencionar que há discussões sobre a caracterização do *cookie* como dado pessoal; para os fins deste trabalho, no entanto, vamos restringir a discussão à identificação dos papeis de cada agente.

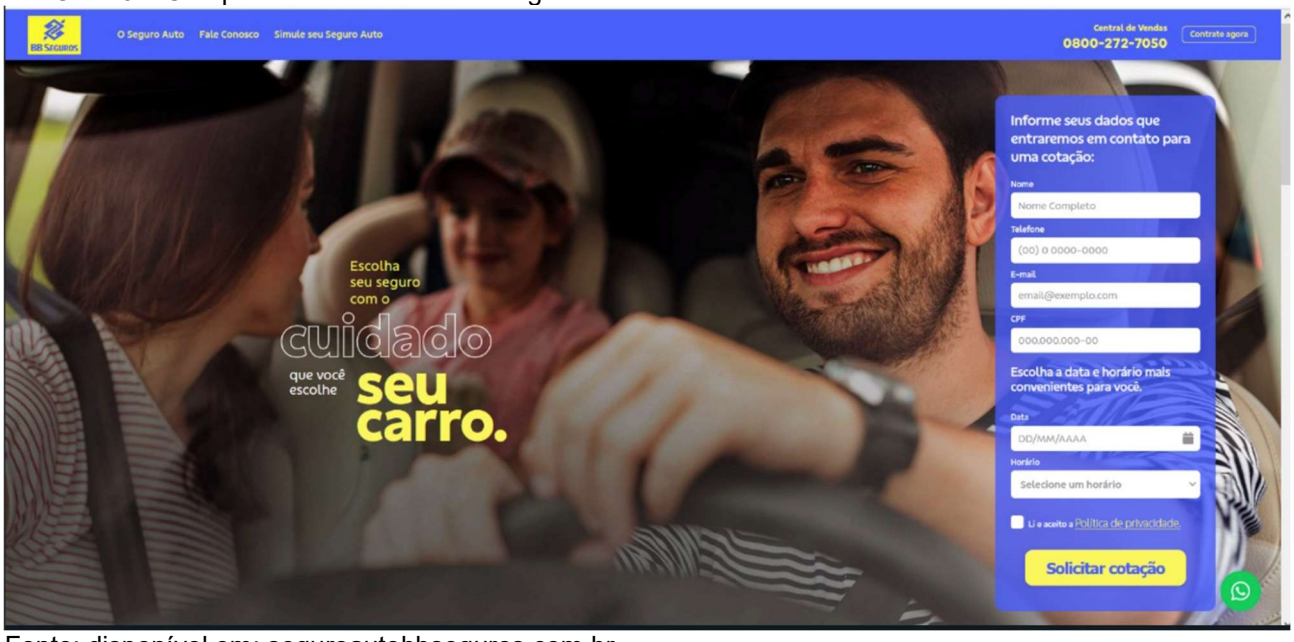
No modelo apresentado, percebemos o papel de controlador das coligadas e do Banco do Brasil, principalmente pelo poder de decisão sobre os dados, conforme art. 5, VI da LGPD. Tal conclusão decorre do fato de que ainda que os contratos possam registrar um papel diferente deste, a ANPD (2021, p. 7) já orientou que:

> o papel do controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento.

O papel da agência de publicidade, por sua vez, é muito sensível. Pois seria possível, e mais lógico, que ela fizesse o carregamento da base de clientes nos veículos de mídia. No entanto, foi uma opção da BB Seguros treinar os próprios funcionários para fazer este carregamento, eliminando a necessidade de troca de arquivos com a agência.

Importante também destacar que nas campanhas digitais em que o cliente fornece dados pessoais (exemplo da oferta que consta da figura abaixo), o controlador deve tomar as devidas precauções, conforme demonstrado até aqui, para que os dados não sejam capturados pela agência de publicidade. Um exemplo é que o site não pode ser hospedado em um Provedor de Hospedagem da agência de publicidade.

IMAGEM 3 – Campanha de oferta de BB Seguro Auto



Fonte: disponível em: seguroautobbseguros.com.br

Considerando esta dinâmica de oferta via mesa de performance, vamos elencar abaixo quais artigos da LGPD se aplicariam nas atividades que envolvem este processo e quais medidas devem ser tomadas pela BB Seguros, para que resguarde sua responsabilidade em cada caso.

TABELA – Tratamento de dados na mesa de performance, obrigações e referências na LGPD.

Tratamento de Dados na Mesa de Performance	**Obrigação**	**Referência na LGPD**
A BB Seguros deve qualificar quais bases legais se aplicam nos diferentes tipos de oferta que ela realiza, bem como: oferta de novos produtos para clientes; oferta de upsell dos produtos que os clientes já possuem; oferta para não clientes.	Definição das bases legais para o tratamento de dados pessoais.	Artigo 7.
Nos casos de oferta com base no consentimento, é preciso que a BB Seguros tenha como provar que o consentimento foi obtido em conformidade com a Lei (vide artigo 9 da Lei). Ressalta-se aqui a importância do consentimento específico para ofertas de Brasilprev Jr., quando houver solicitação de dados do menor, conforme o artigo 14 da Lei.	Fornecimento de informações aos titulares de dados sobre as atividades de tratamento de dados.	Artigo 8, parágrafo 6. Artigo 9. Artigo 14, parágrafo 2 e 5. Artigo 37.
Nos casos de oferta com base no legítimo interesse, é preciso que a BB Seguros tenha relatório de impacto da ação que fundamente seu legítimo interesse. Importante destacar as "avaliações de proporcionalidade, a integração desses relatórios de impacto ao quadro geral de gerenciamento de riscos da organização, a administração dos riscos no âmbito do programa de governança de privacidade e proteção de dados pessoais e nos níveis dos produtos e serviços da organização (através de revisões periódicas,	Garantia de transparência do tratamento de dados pessoais baseado no legítimo interesse. Apresentação dos relatórios de avaliação de proporcionalidade ligada ao legítimo interesse para a ANPD se requisitado.	Artigo 10, parágrafo 2 e 3. Artigo 37. Artigo 38.

por exemplo), e a avaliação dos riscos relacionados especificamente ao uso de fornecedores e terceiros" (CEDIS; 2020)		
Nas ações da mesa de performance que os dados são coletados com finalidade específica de oferta de produtos, é preciso que o controlador garanta a eliminação dos dados após a oferta. Situação perceptível no caso de oferta via central de atendimento para não clientes que solicitam cotação de produtos via formulário de contato nos canais digitais da BB Seguros.	Deletar os dados pessoais ao final da atividade de tratamento dos dados.	Artigo 16. Artigo 18, VI.
Carregamento de dados de clientes nos veículos de midia. Nesse caso, a BB Seguros optou por só deixar que os terceiros tenham acesso aos dados anonimizados, portanto cabe a ela, como controladora, garantir o registro das intruções aos operadores. Portanto, a BB Seguros deve garantir que a agência de publicidade e os veículos de mídia acordam em seguir a política de tratamento de dados da organização. Tal medida pode ser feita por meio de clásulas contratuais, por exemplo. Bem como pela garantia que esses terceiros possuem políticas de tratamento de dados em consonância com as intruções do controlador.	Tratamento de dados pessoais de acordo com as instruções dos controladores.	Artigo 39.

Fonte: Elaboração do autor

Por fim, ressalta-se que todos esses processos podem ser estabelecidos dentro dos documentos de governança da empresa, os quais também são previstos pela LGPD, não havendo, assim, necessidade que cada área tenha o seu documento.

5 CONCLUSÃO

Conforme se debateu nos capítulos anteriores, a privacidade, na era da informação, deve ser definida a partir da ideia de que o sujeito deve dispor de mecanismos para manter o controle sobre suas próprias informações. Isso porque o direito à privacidade representa condição para a vida com dignidade, sem que haja interferência de terceiros em sua vida privada.

Neste sentido, o direito à privacidade e à proteção de dados pessoais passa a ser visto como direito fundamental, pois é essencial para a dignidade humana ligado ao direito constitucional e aos tratados de direitos humanos.

Assim, é preciso que seja ponderado o quanto a liberdade das empresas pode afetar a vida privada das pessoas. De forma parecida, o tema foi enfrentado pela Constituição Federal de 1988, que displina que a liberdade de expressão e informação deve levar em conta a não violação da vida privada, da intimidade, da honra e da imagem das pessoas.

O direito à proteção de dados deve seguir o mesmo caminho. Afinal ele está relacionado ao direito da personalidade, não ao direito da propriedade. Isso ocorre porque os atributos do direito de propriedade estão diretamente relacionados ao propósito de fins econômicos, ao passo que as atividades de tratamento de dados pessoais, por sua possiblidade de expor a intimidade das pessoas, devem levar em consideração a proteção de direitos fundamentais. Prova disso é que seus titulares podem impedir ou fazer cessar invasão em sua esfera íntima, usando para sua defesa: mandado de injunção, *habeas corpus, habeas data*, mandado de segurança, cautelares inominadas e ação de responsabilidade civil por dano moral e/ou patrimonial.

No entanto, no ambiente digital os usuários fornecem seus dados para poderem se relacionar com outros usuários ou com empresas, mas não são eles que possuem o poder de determinar o tratamento a ser dado às informações, e sim quem passou a controlar aqueles dados.

E esses dados são valiosos, pois permitem que as empresas se comuniquem de forma mais assertiva, oferecendo seus produtos para as pessoas cujos dados pessoais revelam um perfil mais propício ao consumo.

Dessa forma, a proteção dos dados pessoais tem sido discutida desde 1970 na Europa, e passou por diferentes momentos, conforme exposto no capítulo 2 deste estudo.

Inicialmente a discussão se concentrava em regular o processamento dos dados. Tratava-se de normas sobre os bancos de dados e sobre a utilização dos computadores, ou seja, sobre o poder sobre as informações. Não havia, de maneira explícita, foco na proteção à privacidade do titular.

Em um segundo momento, os titulares passaram a poder decidir sobre a utilização ou não de seus dados, por parte de quem os controlava. No entanto, quem decidia por não compartilhar o uso dos dados tinha acesso restrito a diversos serviços, inclusive do governo.

O terceiro momento é marcado por uma decisão do Tribunal Constitucional Alemão, que vinculou a garantia do individuo decidir sobre a disponibilidade e utilização de seus dados aos direitos fundamentais, garantindo a todo cidadão o direito de tratar seus dados com liberdade, assegurando proteção e confidencialidade, caso assim deseje. Pela decisão o titular passaria a participar de todo o processamento de dados, desde a coleta até sua utilização.

Por fim, o momento seguinte tem como diferencial uma ampliação do alcance da privacidade e um instrumental mais elaborado de proteção do cidadão reconhecendo o desequilíbrio nas relações dessa natureza. O consentimento do titular, nesta fase, perde um pouco de protagonismo.

O Brasil também tem uma evolução histórica em relação à proteção de dados pessoais, e desde 1990 já tinha algumas garantias previstas no Código de Defesa do Consumidor.

Para crimes cibernéticos, no entanto, a regulamentação não era suficiente para punir os responsáveis, e só em 2012, com a aprovação da Lei conhecida como “Lei Carolina Dieckmann”, que foram dados importantes passos neste sentido.

Então veio o Marco Civil da Internet, estabelecendo que as empresas devem armazenar registros de conexão e de acesso à aplicativos sempre preservando a honra, a vida privada, e a imagem dos usuários.

E a mais recente legislação é a LGPD. Qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, está sujeita à LGPD.

A partir de então, é um desafio para as empresas entenderem a importância da proteção de dados e todos os cuidados que devem tomar para se adequarem à nova legilação, evitando inclusive as altas sanções previstas.

Tais sanções podem ser aplicadas nas atividades de tratamento de dados. Nesses casos a Lei observará qual o papel que organização exerceu, se de controlador ou operador, e cobrará da organização os registros de todos os cuidados que ela deveria ter tomado.

Dessa forma, é importante que as organizações estabeleçam procedimentos, normas internas e políticas de proteção de dados observando os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, minimização da coleta, retenção mínima, responsabilização e prestação de contas.

Diante da análise efetuada, foi possível identificar o papel dos diferentes agentes de tratamento envolvidos nas operações da Mesa de Performance da BB Seguros, delimitando suas responsabilidades à luz da LGPD. Desta forma, o trabalho pôde contribuir para que demais empresas que estão adotando o modelo de mesa de performance observem os tipos de processo que devem ser mapeados e como podem identificar seus papeis nesses processos, com base nos artigos da Lei.

No caso em estudo, a BB Seguros atua como controladora, em todos seus processos da mesa de performance, sendo eles: tratamento dos dados para carregamento nos veículos de mídia, oferta de novos produtos para clientes; oferta de *upsell* (aumento do ticket médio de um produot que o cliente já tem. Por exemplo, aumento do capital segurado do seguro de vida) dos produtos que os clientes já possuem; oferta para não clientes.

Assim, conforme a tabela apresentada no último capítulo deste estudo, os documentos de governança da BB Seguros referentes à proteção de dados pessoais devem incluir os processos da mesa de performance e as iniciativas ali sugeridas, de forma que seja garantida a proteção da responsabilidade da empresa no tratamento de dados, tanto em sua função como controlador, como nas funções dos terceiros contratados (operadores).

6 REFERÊNCIAS

ANPD. **Guia orientativo para definições de agentes de tratamento de dados pessoais e do encarregado.** Brasília, DF. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em 18 jun. 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas – A Função e os Limites do Consentimento**. São Paulo: Editora Forense, 2018.

BITTAR, Carlos Alberto**. Os direitos da personalidade**. 8.ed.,rev. aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2014

BRASIL, LEI Nº 10.406, DE 10 DE JANEIRO DE 2002. Institui o Código Civil. S.i. S.n. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 02 de maio de 2020.

BRASIL, LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. S.i. S.n. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 02 de maio de 2020.

BRASIL, LEI Nº 12.414, DE 09 DE JUNHO DE 2011. Disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. S.i. S.n. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 02 de maio de 2020.

BRASIL, Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 02 de maio de 2020.

BRASIL. Lei N.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Diário Oficial [da] República Federativa do Brasil, Brasília, DF. 15 ago. 2018. Não paginado. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em maio 2021.

BRASIL. Superior Tribunal de Justiça. Recurso Especial (Resp) 1629255 MG 2016/0257036-4. CIVIL E PROCESSUAL CIVIL. RESPONSABILIDADE CIVIL DO PROVEDOR DE APLICAÇÃO. REDE SOCIAL. FACEBOOK. OBRIGAÇÃO DE FAZER. REMOÇÃO DE CONTEÚDO. FORNECIMENTO DE LOCALIZADOR URL. COMANDO JUDICIAL ESPECÍFICO. NECESSIDADE. OBRIGAÇÃO DO REQUERENTE. MULTA DIÁRIA. OBRIGAÇÃO IMPOSSÍVEL. DESCABIMENTO. Relatora: Ministra Nancy Andrighi. Brasília-DF. 22 de agosto de 2017. Diário da Justiça Eletrônico. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/492988772/recurso-especial-resp-1629255-mg-2016-0257036-4/inteiro-teor-492988782?ref=serp. Acesso em: 02 de maio de 2020.

BRASIL**.** Superior Tribunal de Justiça. Recurso Especial (Resp) 1641155 SP 2016/0112378-9. Civil e Processual Civil. RECURSO ESPECIAL. AGRAVO DE INSTRUMENTO. AÇÃO DE OBRIGAÇÃO DE FAZER. FACEBOOK. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. JULGAMENTO *EXTRA PETITA*. AUSÊNCIA. REMOÇÃO DE CONTEÚDO INFRINGENTE DA INTERNET. PREQUESTIONAMENTO. AUSÊNCIA. SÚMULA 211/STJ. MONITORAMENTO PRÉVIO DE PUBLICAÇÕES NA REDE SOCIAL. IMPOSSIBILIDADE. Relatora: Ministra Nancy Andrighi. Brasília-DF. 22 de agosto de 2017. Diário da Justiça Eletrônico. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/492988772/recurso-especial-resp-1629255-mg-2016-0257036-4/inteiro-teor-492988782?ref=serp. Acesso em: 02 de maio de 2020.

CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL); CEDIS. **Implementação e regulamentação rfetiva sob a nova lei geral de proteção de dados - Prioridades das organizações públicas e privadas implementarem de forma eficaz a nova lei geral brasileira de proteção de dados.** 2020. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-idp_white_paper_on_top_priorities_for_public_and_private_organizations_to_effectively_implement_the _lgpd__1_september_2020_.pdf>. Acesso em: 10 jun. 2021.

CORRÊA; Leonardo. **É importante não perder o foco da segurança jurídica no âmbito da LGPD**. 2019. Disponível em: https://www.conjur.com.br/2019-mar-03/leonardo-correa--seguranca-juridica-ambito-lgpd. Acesso em 01 de jun 2021.

COSTA JÚNIOR, Paulo José. **O direito de estar só. Tutela Penal da Intimidade**. 4ª edição. São Paulo: RT, 2007.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: teoria geral do direito civil**, v.1:teoria geral do direito civil.19ª. São Paulo: Saraiva, 2006

DONEDA, Danilo. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. 2006. Disponível em: <Disponível em: http://www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf >. Acesso em: 02 maio 2021.

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

_____. **Reflexões sobre proteção de dados pessoais em redes sociais**. Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia). No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf.pdf. Acesso em: 05 jun. 2021.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito Civil. Teoria Geral**. 7 ed.,Rio de Janeiro: Lumen Juris, 2002.

GUERRA FILHO, Willis Santiago. **Processo Constitucional e direitos fundamentais**. Brasil: C. Bastos, 2003.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012

LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In: SARLET, Ingo Wolfgang (org.). **Direitos, Fundamentais, Informática e Comunicação: algumas aproximações**. Porto Alegre: Livraria do Advogado, 2007a, p. 195-225

MAYER-SCHONBERGER. Generational development of data protection in Europe. In: AGRE, P. E.; ROTENBERG, A.(orgs.). **Technology and privacy: The new landscape**. Cambridge: MIT Press, 1997, pp.219-241.

MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de Direito Constitucional**. 10ª ed. rev. e atual. São Paulo, 2015.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 5. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014.

MORAES, Alexandre de. **Direito Constitucional.** 13ª ed. São Paulo: Atlas. 2003. Diposnível em https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf. Acesso em 10 jun. de 2021.

ONU. **Comércio eletrônico salta para US$ 26,7 trilhões com venda online durante Covid-19.** 2021. Disponível em: https://news.un.org/pt/story/2021/05/1749422. Acessado em 21 de jun. 2021.

PINHO, Luiz Cláudio; BUAIRIDE, Ana Maria Ramos. **Marketing da Comunicação**. São Paulo: Futura, 2000.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014

SILVA, José Afonso da. **Curso de Direito Constitucional positivo**. 18. ed. São Paulo: Malheiros, 2015

SILVA, J. L; MASCARENHAS, S. A. N. **Gestão de bullying e cyberbyllying na universidade – Desafio para a orientação educativa e convivência social e ética no ensino superior – Estudo com estudantes da UFAM** (Brasil. Revista Amazônica). 2010. Disponível em: Dialnet-GestaoDoBullyingECyberbullyingNaUniversidadeDesafi-4028699.pdf. Acesso em 17 jun. 2021.

SIBILIA, Paula. **O show do eu: a intimidade como espetáculo;** Rio de Janeiro: Contraponto, 2016.

VIANNA, C. S. M. **Da privacidade como direito fundamental da pessoa humana**. Revista de Direito Privado, São Paulo, ano 5, p.102-115, jan.-mar. 2004