UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
CURSO DE MESTRADO

LARISSA ROCHA DE PAULA PESSOA

OS DESAFIOS DA GOVERNANÇA DE DADOS E A REALIDADE CULTURAL BRASILEIRA

FORTALEZA
2021

LARISSA ROCHA DE PAULA PESSOA

OS DESAFIOS DA GOVERNANÇA DE DADOS E A REALIDADE CULTURAL BRASILEIRA

Dissertação apresentada ao Programa de Pós- Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito.
Área de concentração: Constituição, Sociedade e Pensamento Jurídico.
Orientadora: Profa. Dra. Maria Vital da Rocha.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

P567d Pessoa, Larissa Rocha de Paula.
OS DESAFIOS DA GOVERNANÇA DE DADOS E A REALIDADE CULTURAL BRASILEIRA / Larissa Rocha de Paula Pessoa. – 2021.
152 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós-Graduação em Direito, Fortaleza, 2021.
Orientação: Prof. Dr. Maria Vital da Rocha.

1. Dados Pessoais. 2. Transformação Cultural. 3. Sociedade da Informação. 4. Governança de Dados. I. Título.

CDD 340

LARISSA ROCHA DE PAULA PESSOA

OS DESAFIOS DA GOVERNANÇA DE DADOS E A REALIDADE CULTURAL BRASILEIRA

Dissertação apresentada ao Programa de Pós- Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito.
Área de concentração: Constituição, Sociedade e Pensamento Jurídico.
Orientadora: Profa. Dra. Maria Vital da Rocha.

Aprovada em: 28/06/2021.

BANCA EXAMINADORA

_____

Profa. Dra. Maria Vital da Rocha (Orientadora)
Universidade Federal do Ceará (UFC)

_____

Profa. Dra. Dinara de Arruda Oliveira
Universidade Federal de Mato Grosso (UFMT)

_____

Prof. Dr. Paulo Rogério Marques de Carvalho
Centro Universitário 7 de Setembro (UNI7)

Esta dissertação é dedicada a todas as pessoas que disseram "aceito" sem entender as políticas de privacidade e proteção de dados.

Dedico também à minha querida avó.

AGRADECIMENTOS

Durante os intensos anos de mestrado, com o adicional de pandemia, as questões emocionais se afloraram. Enquanto eu estava desenvolvendo esta dissertação, passei por dores emocionais para as quais eu não estava preparada, provocadas pelo vírus, que contaminou pessoas importantes para mim. Mas, com o apoio que eu recebi, consegui chegar até aqui e, finalmente, puder expressar meus sinceros votos de gratidão por conseguir concluir esta dissertação.

Penso, com muita gratidão, nas pessoas maravilhosas, que me apoiaram na realização deste meu sonho, por entenderem minhas ausências, meu esforço, minhas inseguranças e, principalmente, por fazerem desta jornada árdua uma jornada de crescimento pessoal, profissional e acadêmico, a lista não para de crescer.

Agradeço a Deus, em primeiro lugar, por me conceder o livre-arbítrio e a graça de chegar até aqui. Nos momentos díficieis e de angústia que só eu e Deus sabemos, ele me deu forças e me guiou para continuar e realizar este sonho, que é a minha contribuição acadêmica com a produção desta dissertação.

Em seguida, agradeço *in memoriam* ao meu avô e a minha tia Edna, que já não estavam presentes em vida no momento da minha formatura em direito, aprovação no mestrado e defesa desta dissertação, estou segura de que me acompanham nessa jornada ao lado de Deus e que sempre depositaram em mim as melhores felicitações de vida. Amplio meus agradecimentos aos demais familiares, especialmente, a minha avó Francineida por ser uma grande inspiração pra mim e fonte de eterna gratidão; ao meu irmazinho, por quem tenho muito carinho, à minha mãe, por ter me dado vida, e aos meus tios, que sempre estiveram presentes na minha vida.

Agradeço ao meu amor Nykolas, pelo constante carinho, companheirismo, paciência e por estar ao meu lado, em todos os momentos. Agradeço, principalmente, por ter me apoiado de todas as formas e me motivado a prosseguir no meu sonho nesta reta final, fazendo com que eu conseguisse superar a ansiedade e a insegurança, com força de vontade e determinação. Eu te amo e sou muito feliz por tê-lo junto a mim.

Agradeço a minha querida orientadora profa. Maria Vital, pelos ensinamentos, por sua atenção e paciência, não apenas na condução da orientação, mas também nas aulas e no estágio de docência. Sinto-me honrada e privilegiada pela oportunidade de ter sido sua aluna e ter participado de debates tão enriquecedores nas suas disciplinas e que foram

fundamentais para ampliação dos meus horizontes acadêmicos. Além disso, não posso deixar de enaltecer os diversos incentivos que recebi para participar de eventos acadêmicos e de produções cientificas nacionais e internacionais, que me proporcionaram grandes aprendizados e reflexões. Sou imensamente grata por ter uma orientadora que, de fato, me apoiou e me incentivou, assim como também fez correções necessárias e pertinentes, sempre de forma respeitosa, durante toda essa jornada acadêmica. Por isso, faço questão de expressar minha admiração e gratidão.

Agradeço ao querido professor Dr. João Luis pelos ensinamentos na disciplina do Mestrado e na qualificação desta pesquisa, e ao professor Dr. André Dias por suas contribuições valiosas na qualificação da minha dissertação.

Ao professor Dr. Paulo Carvalho e a professora Dra. Dinara de Arruda, agradeço pela disponibilidade e por aceitarem participar da minha banca examinadora, momento único e solene da minha trajetória acadêmica.

Agradeço as minhas amigas Ingrid Eduardo, Gabriela Costa, Jéssica Rodrigues e Mariana Félix pela amizade que começou na preparação para a seleção do mestrado, no nosso grupo de estudos "Quinta-essência" (o nome tem origem em uma nota de rodapé do livro Curso de Direito Constitucional do professor Paulo Bonavides, que menciona um trecho de Aristóteles). Agradeço por ter vivido com vocês uma trajetória intensa de muitos estudos, revisões e dedicação que fez um diferencial na minha aprovação. Vocês são incríveis!

Agradeço aos meus colegas de mestrado, com quem tive a oportunidade de e participar, presencialmente, de aulas, seminários e confraternizações, especialmente, o Breno Silveira e a Fernanda Leontsinis, porque fomos guiados juntos, por nossa orientadora e partilhamos conhecimentos e apoio uns aos outros. Além disso, tenho que agradecer as minhas amigas Mariana Félix e a Sandrelle Jorge, por serem mulheres inteligentes e determinadas. Juntas criamos um projeto incrível, do qual me orgulho muito.

Agradeço a todos os professores do Programa de Pós-Graduação da Universidade Federal do Ceará, na pessoa do coordenador Gustavo Cabral, pelo conhecimento que obtive durante esses anos de mestrado.

Por fim, agradeço à Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (FUNCAP), por investir no conhecimento científico e por ter me concedido uma bolsa de estudo.

Podiam arrancar de você até o último detalhe de tudo que você já tivesse feito, dito ou pensado; mas aquilo que estava no fundo de seu coração, misterioso até para você, isso permaneceria inexpugnável. George Orwell (1984, p.168)

RESUMO

A sociedade da informação surge com a ascensão da tecnologia da informação, ocasionando profundas transformações nas relações sociais, econômicas e políticas, promovendo um crescimento exponencial dos fluxos de informações, devido à sua capacidade de armazenamento, modificação e difusão das informações. Nesse contexto informacional, os dados pessoais e as informações revelaram-se verdadeiros bens de valor econômico, expondo seus titulares aos riscos de violações à liberdade, privacidade, intimidade e outros direitos da personalidade, cabendo a Lei Geral de Proteção de Dados Pessoais (LGPD) a tutela dos dados pessoais. Desse modo, a presente dissertação propõe-se, analisar os desafios e os requisitos de governança de dados para fins de adequação das empresas à Lei Geral de Proteção de Dados, explorando a transformação cultural da sociedade brasileira para cultura da proteção de dados e privacidade, que será analisada sob perspectiva da neurociência visando o desenvolvimento de uma arquitetura de escolhas pautada na privacidade e proteção de dados pessoais. A temática possui relevância social, jurídica, política e econômica, principalmente, no que diz respeito ao fluxo de informação e circulação de dados entre países, revelando a importância da sua proteção no âmbito interno e internacional. Quanto à metodologia, a pesquisa possui uma abordagem metodológica qualitativa, descritiva, exploratória e explicativa, desenvolvida por meio de revisão bibliográfica de obras, análise dos textos legais, revistas, artigos e pesquisas científicas especializadas, nacionais e estrangeiras, jurisprudência, pareceres e documentos (dados secundários). Por fim, conclui-se que o movimento de transformação cultural tornou-se mais forte com a entrada em vigor da Lei Geral de Proteção de Dados, devido à necessidade de adequação das empresas, bem como com a criação da ANPD, que possui um papel importante na promoção da cultura de proteção de dados e privacidade, conscientizando a sociedade sobre a importância dos dados e informações pessoais.

Palavras-chaves: Dados Pessoais. Transformação Cultural. Sociedade da Informação. Governança de Dados.

ABSTRACT

The information society arises with the emergence of information technologies, causing profound changes in social, economic and political relations, promoting an exponential growth of information flows, due to its storage, modification and dissemination capacity of information. In this informative context, personal data and information proved to be true assets of economic value, exposing their holders to the risk of violations of freedom, privacy, intimacy and other rights of the personality, under the General Law for the Protection of Personal Data (LGPD) the protection of personal data. Thus, this dissertation aims to analyze the challenges and requirements of data governance in order to adapt companies to the General Data Protection Law, exploring the cultural transformation of Brazilian society towards a culture of data protection and privacy, which will be analyzed from the perspective of neuroscience aiming at the development of an architecture of choices based on privacy and protection of personal data. The theme has social, legal, political and economic relevance, especially with regard to the flow of information and circulation of data between countries, revealing the importance of its protection at the national and international level. As for the methodology, the research has a qualitative, descriptive, exploratory and explanatory methodological approach, developed through literature review of works, analysis of legal texts, journals, articles and specialized scientific research, national and foreign, jurisprudence, opinions and documents (data secondary). Finally, it is concluded that the cultural transformation movement was strengthened with the entry into force of the General Data Protection Law, due to the need to adapt companies, as well as with the creation of ANPD, which has an important role in promoting a culture of data protection and privacy, making society aware of the importance of personal data and information.

Keywords*: Personal data. Cultural transformation. Information Society. Data management.*

SUMÁRIO

1. INTRODUÇÃO

Os avanços das tecnologias de informação e comunicação provocaram profundas mudanças na dinâmica das relações sociais, governamentais e econômicas. Hoje, é difícil imaginar um mundo inteiro desconectado da tecnologia, sem comunicação e sem informação, isso porque vive-se numa sociedade da informação, imersa no espaço de conexões em rede, que possui um exponencial crescimento dos fluxos de dados, devido à capacidade de armazenamento, modificação e difusão de informações pelos meios eletrônicos.

Nesse contexto informacional, a esfera da privacidade dos indivíduos encontra-se fragmentada, pois, no mundo moderno, tem-se uma "vigilância líquida" [1], uma dimensão-chave, que através da sua fluidez permeou-se ao longo das gerações e com o uso da tecnologia se fez onipresente. Desse modo, as pessoas têm seus movimentos monitorados, acompanhados e observados, bem como seus dados pessoais colhidos para bases de dados com a finalidade de serem processados, tratados, analisados e relacionados com outros dados, para depois serem utilizados, até mesmo sem o consentimento do próprio titular e de forma indevida.

A amplitude das atividades de tratamento de dados pessoais pode repercutir na vida das pessoas e nas suas tomadas de decisões, pois os dados pessoais refletem a personalidade dos seus titulares, tornando-os identificáveis, bem como vulneráveis as violações à autonomia, à privacidade, à intimidade, à liberdade e a própria dignidade da pessoa humana.

Dessa forma, a tutela dos dados pessoais não significa proibir a utilização dos dados, mas impor limites e restrições que visam resguardar a dignidade da pessoa humana, implicando, portanto, na adequação as normas estabelecidas pela Lei Geral de Proteção de Dados. Almejando-se, assim, o desenvolvimento, a consolidação e a funcionalização da proteção de dados pessoais no ordenamento jurídico brasileiro.

Sabe-se que a evolução tecnológica gerou novos desafios para o direito, sendo a proteção de dados pessoais e a privacidade os mais complexos e difícieis no contexto da economia informacional. Por isso, a presente temática possui relevância que transcende ao campo do direito, por refletir em relações não só jurídicas, mas também sociais, políticas e econômicas, principalmente, no que diz respeito ao tratamento de dados

[1] BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Tradução: Carlos Alberto Medeiros. Rido de Janeiro: Zahar, 2013, p.7

pessoais e circulação de informações entre países, revelando, portanto, a sua importância no âmbito interno e internacional.

Além disso, devido à presença das discussões jurídicas sobre tutela de dados pessoais serem recentes no Brasil, em comparação com a União Europeia, faz-se necessário estudar e analisar as diretivas sobre proteção de dados da União Europeia, bem como a doutrina estrangeira, em especial, a desenvolvida por Stefano Rodotá no campo do direito, Manuel Castells no campo da sociologia e as obras dos autores Kahneman, Thaler e Sunstein no âmbito da neurociência, tornando esta pesquisa multidisciplinar.

A presente dissertação propõe-se, inicialmente, realizar uma reflexão sobre a dinâmica das novas tecnologias e a sociedade da informação brasileira, em seguida, analisar os fundamentos da proteção de dados pessoais até a sua concepção como um direito fundamental, que visa resguardar a autodeterminação informacional da pessoa humana, assim como também os princípios que incidem na dinâmica do ciberespaço, para então, investigar os instrumentos de governança de dados e o desenvolvimento da cultura da proteção de dados e privacidade corporativa e, por fim, analisar o papel da Autoridade Nacional na promoção da transformação cultural.

Dessa forma, a problemática abordada se consubstancia nos desafios e na necessidade da proteção de dados pessoais, tendo em vista que a Lei Geral de Proteção de Dados estabelece institutos, princípios e fundamentos que visam resguardar o titular dos dados conciliando com o desenvolvimento tecnológico na era informacional. Assim, a pesquisa tem como problema central: Quais são os desafios e os instrumentos legais de boas práticas e governança para a proteção jurídica dos dados pessoais por agentes privados no Brasil? Como a neurociência pode auxiliar o processo de implementação do programa de privacidade e proteção de dados no desenvolvimento da cultura de proteção de dados e privacidade dentro da empresa?

Sendo o objetivo geral desta pesquisa científica, analisar os desafios e os requisitos de governança de dados para fins de adequação das empresas à Lei Geral de Proteção de Dados, explorando a transformação cultural da sociedade brasileira para cultura da proteção de dados e privacidade, que será analisada sob perspectiva da neurociência visando o desenvolvimento de uma arquitetura de escolhas pautada na privacidade e proteção de dados pessoais.

Nesta pesquisa, foi utilizado o método científico dedutivo na abordagem científica, partindo-se de pressupostos gerais para premissas menores, com o propósito de identificar *standards* relativos à proteção de dados e heuristas para auxiliar o processo

de transformação cultural, já em relação aos métodos de procedimentos, adotou-se o método observacional e comparativo como meios técnicos de investigação.

Quanto a metodologia desta pesquisa, classifica-se como pesquisa básica, pois tem o propósito de gerar conhecimentos novos sobre a temática, em relação aos objetivos, a pesquisa é, predominantemente, exploratória, pois tem como finalidade principal proporcionar mais informações sobre o objeto investigado, é também descritiva, visto que busca descrever os fatos e fenômenos que envolvem a sociedade da informação brasileira e a proteção de dados pessoais e, explicativa, uma vez que visa explicar e analisar os porquês das coisas e as suas causas que requer uma governança de dados, interpretando os problemas relacionados a inobservância da adequação à Lei Geral de Proteção de Dados.

Em relação aos procedimentos técnicos, a pesquisa se classifica, principalmente, em bibliográfica, através de revisão bibliográfica de obras, revistas, artigos e pesquisas científicas especializadas, nacionais e estrangeiras, constituição, jurisprudência e legislação sobre a privacidade e proteção de dados no Brasil, bem como documental, pela utilização de documentos (dados secundários) consistentes e relacionados com a temática. Por fim, quanto à abordagem do problema, trata-se de uma pesquisa qualitativa, pois visa a interpretação dos fenômenos e da legislação pertinente, atribuindo-se um significado interpretativo sobre as informações obtidas e analisadas.

Esta dissertação foi dividida em cinco capítulos, iniciando com esta introdução e finalizando com a conclusão, que abrange desde a noção de sociedade da informação, perpassando sobre o Regulamento Geral de Proteção de Dados (RGPD), a proteção de dados pessoais e os direitos da personalidade, a análise da autodeterminação informacional, os princípios até a governança de dados e o papel da Autoridade de Proteção de Dados.

O Capítulo 2 foi intitulado “A Sociedade da Informação”, possui o seguinte problema específico: Como se desenvolveu a sociedade da informação e qual é a influência do Regulamento Geral de Proteção de Dados da União Europeia sobre a lei de proteção de dados brasileira? Assim, esse capítulo expõe a noção de ciberespaço e sociedade da informação, contextualizando as mudanças sociais com o desenvolvimento das tecnologias da informação, discorrendo sobre a economia da informação e a expansão dos modelos de negócios na internet, abrangendo os reflexos do *Big Data* e da mineração dos dados, até a análise da sociedade da informação brasileira e do contexto social em que ensejou a Lei Geral de Proteção de Dados (LGPD), bem como, a influência do

Regulamento Geral de Proteção de Dados da União Europeia (RGPD) sobre o desenvolvimento da proteção dos dados pessoais no direito brasileiro.

O Capítulo 3 é denominado de "Fundamentos e Princípios da Proteção de Dados Pessoais", propõe-se abordar a questão: Quais são os fundamentos e princípios que conferem proteção dos dados pessoais no ciberespaço? Discorrendo sobre proteção de dados pessoais e os direitos da personalidade, conceituando os dados pessoais e esclarecendo sobre em que consistem os dados pessoais sensíveis e os dados pessoais anonimizados, buscando identificar quais princípios são norteadores da proteção de dados no contexto do ciberespaço, discorrendo sobre os princípios do Marco Civil da Internet, os princípios da proteção dos dados pessoais da LGPD e sobre os princípios da Governança da Internet.

O Capítulo 4 "Tratamento e Governança dos Dados Pessoais", por sua vez, examina a problemática: Quais instrumentos legais de boas práticas e governança para fins de adequação à Lei Geral de Proteção de Dados? Como a neurociência pode auxiliar no desenvolvimento da cultura de proteção de dados e privacidade e promover condutas desejáveis? A partir da compreensão das atividades de tratamento de dados e as funções dos agentes de tratamento e encarregado, busca-se identificar os desafios e analisar os instrumentos de governança de dados, abordando-se a importância da transformação cultural na implementação do programa de privacidade e proteção de dados, além disso, pretende-se analisar as ABNT NBR ISO/IEC 27001: 2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27701:2019 por fornecerem *standards* internacionais capazes de atender o princípio da segurança da informação. Por fim, analisa o papel da Autoridade Nacional na promoção da cultura de proteção de dados e privacidade.

Por fim, no Capítulo 5, refere-se a conclusão desta pesquisa, constatando-se que a sociedade da informação não pode ser concebida sob os moldes das sociedades dos países pertencentes à União Europeia, visto que os problemas existentes no Brasil refletem no processo de virtualização, letramento digital e, principalmente, na transformação e desenvolvimento na cultura de proteção de dados e privacidade. Diante da complexidade e desafios na proteção de dados no país, entende-se a importância da proteção de dados pessoais ser um direito fundamental, mesmo que a PEC n.17 ainda em andamento, além disso, sobre a parte principiológica da LGPD deverá ser concebida como princípios com finalidades, e que uma possível antinomia entre normas deverá ser solucionada pelo diálogo das fontes, sob uma perspectiva sistemática e complementar entre as fontes do direito. Portanto, entende-se que não há como se ter uma governança

de dados sem uma cultura de proteção de dados e privacidade e que a ANPD tem um importante papel na promoção da mudança cultural da sociedade brasileira.

2. A SOCIEDADE DA INFORMAÇÃO

A chave para o poder não é mais o dinheiro ou o petróleo, mas sim os dados pessoais, aqueles que possuem as informações sobre as pessoas apresentam um poder imensurável, isso porque a informação é o que fundamenta a sociedade que se vivência hoje e a nova economia.

Nesse contexto informacional, as pessoas encontram-se inseridas em uma estrutura global de vigilância, que já foi imaginada de certa forma no passado por George Orwell, na obra "1984"[2], onde todos os indivíduos possuem suas informações monitoradas, compartilhadas e, até mesmo, controladas, meticulosamente e de forma onipresente. Veja-se:

> [...] Claro, não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível inclusive que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver — e vivia, em decorrência do hábito transformado em instinto — acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente[3].

O autor aborda temas sensíveis relacionados à privacidade, liberdade, política e outros direitos que são violados pela vigilância do grande irmão, servindo-se para uma reflexão da sociedade atual, que se transformou com o avanço tecnológico, imergindo-se numa vigilância conectada, onde os grandes *players* da tecnologia sabem mais sobre a vida das pessoas do que elas são realmente capazes de imaginar.

Nesse sentido, pode-se mencionar a reflexão de Oliveira e Lopes, ainda sobre o enredo da obra de George Orwell, afirmando-se que as estratégias "[...]iam desde a repressão aos sentimentos, instintos, memória, relações pessoais, até a imposição de uma forma de pensar incoerente – o duplipensar – e o empobrecimento da língua – a novilíngua – a fim de reduzir a capacidade de formulação de ideias"[4].

---

[2] Como observa Rodotá, o modelo de vigilância já foi imaginado até mesmo bem antes do "*big brother*" de George Orwell, pois já era presente no "*Panopticon"* de Jeremy Bentham, um sistema em que permite vigiar sem ser visto. RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.47.

[3] ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009, p.10-11.

[4] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

As ideias colocadas na obra 1984, podem ser percebidas na atualidade. Todavia, também existem aspectos positivos no mundo globalizado, assim, pode-se pontuar que as tecnologias da informação facilitaram exponencialemente a comunicação e a circulação e acesso à informação para as pessoas, eliminando as fronteiras entre os países e impulsionando a fluidez dos dados. Tais dados são extremamente importantes para o desenvolvimento do poder público, das organizações, das empresas privadas e, principalmente, para os *players* da tecnologia, pois as informações desempenham um papel fundamental na economia e na política.

No entanto, muito embora as informações sejam indispensáveis para o desenvolvimento econômico, tecnológico e político, isso não significa um aval para a violação dos direitos dos titulares dos dados. É necessário que haja uma transparência informacional para com o titular do dado, isto é, o cidadão deve ser informado sobre o que será feito com os seus dados pessoais, qual é o tipo de tratamento que será realizado com aqueles dados solicitados.

Isso porque a Lei Geral de Proteção de Dados garante as pessoas direitos que devem ser respeitados pelas empresas e poder público. Todavia, sabe-se que para haver efetivamente a proteção de dados, isso requer uma mudança cultural, um *compliance* de dados e um sistema de segurança da informação. Contudo, ainda que se realize a adequação à LGPD, é possível ocorrer riscos no tratamento de dados por parte dos agentes privados e pelo setor público e, consequentemente, poderá impactar a vida do titular dos dados pessoais.

O presente capítulo, tem como finalidade apresentar os contornos da realidade social, jurídica e econômica da sociedade da informação brasileira, mas para isso, é necessário compreender primeiro a arquitetura do ciberespaço e a sociedade da informação. Em seguida, será abordada a economia da informação e a expansão dos modelos de negócios na internet, visando esclarecer a lógica das transformações da economia e os dados como o principal bem econômico, principalmente, pela utilização do *big data* e a mineração de dados.

Para tratar da sociedade da informação brasileira e, posteriormente, analisar a influência da legislação europeia na construção da Lei Geral de Proteção de Dados do Brasil.

2.1 A Arquitetura do Ciberespaço e a Sociedade da Informação

A concepção sobre ciberespaço é complexa, exige uma análise e percepção que não pode ser feita com uma visão tradicional do direito, aliás, o ciberespaço não foi uma criação do direito. Por isso, é preciso entender as inovações tecnológicas e sociais, até mesmo antes de insistir em criar normas e/ou aplicar leis existentes sem saber como que funciona e sem moldar à realidade social, pois pode acarretar efeitos jurídicos indesejáveis, tais como limitar a evolução tecnológica por uma regulamentação desatualizada ou burocrática, ou mesmo está fadado a ineficácia. Então, conhecer o ciberespaço é trivial para a construção do conhecimento e desenvolvimento da cultura da proteção dos dados e informações no digital.

Buscando explicar o que é o ciberespaço, Lawrence[5] disse que as pessoas estavam lendo o seu livro "Código" usavam a internet e o "ciberespaço". O autor exemplifica que por meio da internet, pelo uso do e-mail, é possível pedir livros na Amazon, verificar horários de filmes, usar o Google, assim como outras páginas da Microsoft. Desse modo, o ciberespaço, embora, criado com base na Internet, é uma experiência mais rica, é algo que tornou possível a comunicação por mensagens instantâneas e jogos onlines, algumas pessoas acreditam pertencer a uma comunidade, outros confundem suas vidas no ciberespaço.

O autor afirma que não há uma linha nítida que separa o ciberespaço da internet, mas há uma diferença entre ambos, para as pessoas com a visão de que a internet são apenas páginas, o ciberespaço é algo obscuro. Existe uma diferença entre as gerações:

> Para a maioria de nós com mais de 40 anos, não existe um "ciberespaço", mesmo que exista uma Internet. A maioria de nós não vive uma vida online que se qualificaria como uma vida no "ciberespaço". Mas para nossos filhos, o ciberespaço é cada vez mais sua segunda vida. Existem milhões que passam centenas de horas, um mês nos mundos alternativos do ciberespaço[6].

---

[5] No original*: "EVERYONE WHO IS READING THIS BOOK HAS USED THE INTERNET. SOME HAVE BEEN in "cyberspace." The Internet is that medium through which your e-mail is delivered and web pages get published. It's what you use to order books on Amazon or to check the times for local movies at Fandango. Google is on the Internet, as are Microsoft "help pages."*
But "cyberspace" is something more. Though built on top of the Internet, cyberspace is a richer experience. Cyberspace is something you get pulled "into," perhaps by the intimacy of instant message chat or the intricacy of "massively multiple online games" ("MMOGs" for short, or if the game is a role-playing game, then "MMORPGs"). Some in cyberspace believe they're in a community; some confuse their lives with their cyberspace existence. Of course, no sharp line divides cyberspace from the Internet. But there is an important difference in experience between the two. Those who see the Internet simply as a kind of Yel-low-Pages-on-steroids won't recognize what citizens of cyberspace speak of. For them, "cyberspace" is simply obscure". LAWRENCE, Lessig. **Código: Versão 2.0**. Aufl. Nova York , 2006, p.9.

[6] No original*: "Some of this difference is generational. For most of us over the age of 40, there is no "cyberspace," even if there is an Internet. Most of us don't live a life online that would qualify as a life in "cyberspace." But for our kids, cyberspace is increasingly their second life. There are millions who spend hundreds of hours a month in the alternative worlds of cyberspace".* LAWRENCE, Lessig. **Código: Versão 2.0**. Aufl. Nova York. 2006, p.9.

Para melhor compreender a interação dinâmica entre a sociedade e o domínio cibernético, Medeiros e Goldoni[7], dizem que houveram mudanças nas relações sociais e desafios nas relações internacionais, em razão do ciberespaço ser um domínio distinto em comparação com os domínios tradicionais de terra, ar e mar que possuem uma concepção territorial e material de fronteiras terrestres, aéreas e marítimas e que se diferem do ciberespaço, que possui parcial imaterialidade, uma vez que apresenta a interconectividade das redes de informação.

Os autores criticam a Doutrina Militar de Defesa Cibernética do Brasil por ter uma visão do ciberespaço como um "'virtual-espaço, constituído por dispositivos computacionais conectados a redes ou não, onde a informação viaja, é processada e / ou armazenada", mas que não explica qual é a natureza, a capacidade de cruzar fronteiras ou status de domínio estratégico do ciberespaço[8]. Desse modo, Medeiros e Goldoni[9], afirmam que é "[...] importante conceituar o ciberespaço como um domínio de interação social", mas que essa definição não é definitiva e precisará ser atualizada com a transformação do ciberespaço.

Sendo assim, entende-se que a "[...] internet e o cyberespaço formam uma estrutura pela qual garantias democráticas se espraiam na conjuntura moderna, de forma transfronteiriça e para além do tempo em que as suas informações são a ela conectadas"[10]. E que, diante disso, o desenvolvimento tecnológico fez com que as relações sociais não fossem mais as mesmas, pois possibilitou que os indivíduos, a sociedade, as empresas e os estados, se relacionassem e se organizassem de forma dinâmica nas redes digitais, dentro do ciberespaço.

---

[7] No original: *The interaction between society and the cyber domain engenders social change, posing practical challenges to international relations, starting where cyberspace becomes a distinct domain compared to the traditional land, air and sea domains.2 While the latter domains are governed by a territorial concept due to the materiality of land borders and conceptions of air and sea space, cyberspace is characterised by its partial immateriality, expressed by the interconnectivity of information networks.* MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace* . **Contexto Internacional** , v. 42, n. 1, pág. 31-54, 2020, p.32.

[8] No original: *In its Military Cyber Defence Doctrine (2014: 18), Brazil views cyberspace as a 'virtual space, consisting of computational devices connected to networks or not, where digital information travels, is processed and/or stored'. The breadth of the definition contained in that document fulfils its doctrinal role, but it does not address the inherent nor the resulting nature of cyberspace, such as its ability to cross borders or its status as a new strategic domain.* MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace*. **Contexto Internacional** , v. 42, n. 1, pág. 31-54, 2020, p.34.

[9] No original: "Therefore, it is important to conceptualise cyberspace as a social interaction domain." MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace*. **Contexto Internacional** , v. 42, n. 1, pág. 31-54, 2020, p.33.

[10] LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito digital: compliance, regulação e governança**. São Paulo: Quartier Latin, 2019, p.17.

Vive-se, atualmente, numa sociedade que na sua organização social se faz indispensável o uso da tecnologia, ou seja, no contexto social contemporâneo os recursos tecnológicos são necessários para desenvolvimento das próprias relações sociais, sobretudo, na difusão da comunicação, do conhecimento, da saúde, do trabalho e de inúmeros outros aspectos.

Em relação ao progresso tecnológico, Castells[11] afirma que o mundo está passando por transformações estruturais, há duas décadas, baseado nas tecnologias da comunicação e informação, tratando-se de um processo multidimensional, mas que se propagou de modo desigual entre os países.

Essas transformações tecnológicas estruturais na organização social deram origem a sociedade em rede[12] que para Castells significa "[...] uma estrutura baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento cumulado" [13] .

Deve-se ressaltar que na sociedade da informação, segundo Bioni a informação constitui "[...] o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-insdutrial" [14].

Desse modo, entende-se a informação como elemento da estrutura social, que se estende pelo conjunto de relações que moldam a própria sociedade e seu arranjo socioeconômico, como a produção, o consumo, o poder e outros, reconfigurando-se com a tecnologia em rede. Assim, pode-se inferir que a sociedade da informação emerge e difunde-se nas redes digitais, formando uma estrutura social que não apenas interage, mas se projeta através da tecnologia da informação, e que apresenta a informação como seu elemento estruturante.

---

[11] CASTELLS, Manuel. A Sociedade em Rede: do Conhecimento à Política. *In:* CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém: Imprensa Nacional, 2005, p.17

[12] Deve-se esclarecer que para fins desta pesquisa será utilizada as expressões "sociedade em rede" e "sociedade da informação" com o mesmo significado, embora o autor Manuel Castells utilize "sociedade em rede".

[13] CASTELLS, Manuel. A Sociedade em Rede: do Conhecimento à Política. In CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém: Imprensa Nacional, 2005, p.17.

[14] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 Reimpressão, Rio de Janeiro: Forense, 2019, p.5.

Nesse aspecto, destaca Castells[15] que a sociedade em rede é baseada em redes globais, uma vez que a comunicação em rede transcende fronteiras, apresentando uma lógica própria de difusão por meio do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia.

As fronteiras se diluem pela virtualização, tornando mais propício a capacidade de criação de uma comunidade virtual. Conforme Lévy[16], a virtualização reinventa uma cultura nômade, pois por meio das interações sociais, uma comunidade virtual poderá ser organizada por afinidade, isto é, pelos mesmos interesses, através de sistemas de comunicação telemáticos, não apresentando um lugar estável. Nesse sentido, Vasconcelos e De Paula alguns benefícios proporcionados pelo desenvolvimento tecnológico:

> O acúmulo de dados e o desenvolvimento de tecnologia para sua agregação, tratamento e uso têm proporcionado uma infinidade de oportunidades de desenvolvimento socioeconômico. Há intensificação e identificação recíproca de grupos de pessoas e suas afinidades, customização e maior eficiência na oferta de produtos e serviços mais adequados à demanda individualizada; tem-se o alcance de prognósticos médicos mais precisos e de diagnósticos mais eficazes, a formulação e a avaliação de políticas públicas direcionadas às necessidades mais prementes da população, a possibilidade de serviços públicos efetivamente prestados conforme a demanda de determinadas localidades[17].

Não há dúvidas de que a internet proporcionou muitos ganhos sociais e econômicos. Destacando-se, recentemente, em tempos de pandemia, que permitiu a continuidade de estudos, serviços e outros negócios por meio da utilização das tecnologias disponíveis, assim como também facilitou a comunicação social e o acesso a informação durante o isolamento em diversos lugares.

Contudo, existem alguns efeitos "negativos", aliás, pode-se perceber que a internet é também utilizada para fins inapropriados e até mesmo criminosos. A utilização de engenharia social e ciberataques acontece de forma bem comum na internet, essas ações de *hackers* pode acontecer de qualquer lugar do mundo, o que dificulta o trabalho

---

[15] CASTELLS, Manuel. A Sociedade em Rede: do Conhecimento à Política. *In:* CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém: Imprensa Nacional, 2005, p.17-18.

[16] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.20-21.

[17] VASCONCELOS, Beto; DE PAULA, Felipe. A Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In:* **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

das investigações dos crimes cometidos na internet, uma vez que não existe fronteiras no ciberespaço.

Além disso, com o fácil acesso as informações dispostas na internet, sobretudo, nas redes sociais, facilitam o "trabalho" do *hacker* que não precisa está próximo da vítima para lhe causar um algo de ruim, assim como também, os *hackers* invadem sistemas de empresas e órgãos públicos, visando obter posse de informações e dados pessoais para fazer ameaças e entre outros crimes possíveis.

Dessa forma, sabe-se que tornar o ciberespaço um ambiente seguro para a utilização das pessoas é desafiador. Essa preocupação reflete na elaboração da Lei Geral de Proteção de Dados quando se refere a segurança da informação e sigilo dos dados, buscando evitar e/ou minimizar os riscos para seus usuários, criando proteção de ataques de *hackers*, vírus, engenharia social entre outras engenhosidades prejudiciais aos titulares pelo uso indevido de seus dados e informações.

Mas, antes de tratar sobre a Lei Geral de Proteção de Dados, deve-se entender que sociedade da informação é, portanto, uma sociedade que tem a sua estrutura social construída em torno de redes de tecnologias de comunicação e de informação processadas digitalmente[18]. Desse modo, observa-se que a tecnologia da informação realizou profundas transformações não apenas no comportamento, na interação e na organização social, mas também na economia. Por isso, faz-se necessário compreender em que consiste a economia da informação e os modelos de negócios na internet.

2.2 A economia da informação e a expansão dos modelos de negócios na internet

As empresas se inseriram nas redes digitais pelo procedimento de virtualização e contribuíram para a formação de uma economia baseada na informação. Isso porque os avanços tecnológicos também inovaram às formas negociais, tornando-se necessário reinventar as formas contratuais como reflexos das mudanças das relações sociais no ciberespaço.

As empresas passaram a utilizar a tecnologia a favor dos seus negócios, seja de forma interna, através de um sistema informático próprio da empresa, seja de forma

[18] CASTELLS, Manuel. **O Poder da Comunicação**. Tradução de Vera Lúcia Mello Joscelyne; Revisão de Tradução de Isabela Machado de Oliveira Fraga. 3ª ed. São Paulo/Rio de Janeir: Paz e Terra, 2019, p.70.

externa, por meio da expansão do seu modelo de negócio na internet e seja por ser, propriamente, uma empresa que trabalha com *Big Data*.

Como foi dito anteriormente, a sociedade passou a se projetar nas redes digitais, consequentemente, as empresas também passaram por um processo de "virtualização" e expansão na internet. Conforme Lévy[19] diferente de uma organização de empresa clássica que reúne os trabalhadores no mesmo prédio, uma empresa virtual se vale, principalmente, do teletrabalho, pois há uma tendência em substituir a presença física por uma participação numa rede de comunicação eletrônica.

A partir do processo de virtualização, pode-se notar uma transformação no modelo organizacional de diversas empresas, que passaram a ser em rede, utilizando recursos e os programas informáticos que contribuem para um desenvolvimento mais colaborativo e coordenado com distribuição de funções no ciberespaço.

O processo de virtualização da empresa impactou as formas de trabalho, visto que os empregados passaram a utilizar programas e recursos informáticos no seu ambiente de trabalho, ou no teletrabalho, de modo que o próprio ambiente de trabalho passou a integrar o espaço privado do trabalhador. Conforme Lévy[20], ao contrário do trabalhador clássico, que tinha seu ambiente e posto de trabalho bem definido, o teletrabalhador transforma seu espaço privado em espaço público e vice-versa, para exercer seu trabalho.

Além da inserção das empresas nas redes digitais, pode-se observar que os indivíduos, a sociedade e os Estados passaram a integrar o ciberespaço. Dessa forma, a interação desses integrantes das redes de tecnologia impulsionou o desenvolvimento da

---

[19] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.18. "A organização clássica reúne seus empregados no mesmo prédio ou num conjunto de departamentos. Cada empregado ocupa um posto de trabalho precisamente situado e seu livro de ponto especifica os horários de trabalho. Uma empresa virtual, em troca, serve-se principalmente do teletrabalho; tende a substituir a presença física de seus empregados nos mesmos locais pela participação numa rede de comunicação eletrônica e pelo uso de recursos e programas que favoreçam a cooperação. Assim, a virtualização da empresa consiste sobretudo em fazer das coordenadas espaçotemporais do trabalho um problema sempre repensando e não uma solução estável. O centro de gravidade da organização não é mais um conjunto de departamentos, de postos de trabalho e de livros de ponto, mas um processo de coordenação que redistribui coordenadas espaçotemporais da coletividade de trabalho e de cada um de seus membros em função de diversas exigências."

[20] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.24-25: "O trabalhador clássico tinha sua mesa de trabalho. Em troca, o participante da empresa virtual compartilha um certo número de recursos imobiliários, mobiliários e programas com outros empregados. O membro da empresa habitual passava do espaço público do lugar de trabalho. Por contraste, o teletrabalhador transforma seu espaço privado em espaço público e vice-versa. Embora o inverso seja geralmente mais verdadeiro, ele consegue às vezes gerir segundo critérios puramente pessoais uma temporalidade pública. Os limites não são mais dados. Os lugares e tempo se misturam. As fronteiras nítidas dão lugar a uma fractalização das repartições.".

economia da informação, isso porque de acordo com Lévy[21] a informação e o conhecimento tornaram-se a principal fonte de produção de riqueza.

Trata-se, portanto, de uma economia informacional e global, conforme Boff, Fortes e Freitas essa economia pode ser definida como a "[...] capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos, e o consumo e a circulação estão organizados em escala global diretamente ou mediante uma rede de conexões entre agentes econômicos" [22].

Sobre esse aspecto, ressalta Lévy[23] que na virtualização da economia, surgiram os novos arranjos socioeconômicos, voltados para informação e conhecimento, como os bancos de dados online, os sistemas especializados e outros instrumentos informáticos capazes de tornar o mercado mais transparente e eficiente, bem como capazes de compreender os "raciocínios do mercado".

A informação e o conhecimento tornaram-se os principais bens econômicos da atualidade, são uma verdadeira fonte de riqueza, valorizados pela existência de uma economia de abundância, em que seu conceito e suas práticas estariam em profunda ruptura com a economia clássica.[24] Por isso, ficou muito famosa a frase dita por Clive Humby de que os "dados são o novo petróleo"[25].

De acordo com Lévy[26], o ciberespaço criou um mercado *on-line* que desconhece a distância geográfica, pois os vendedores e consumidores estão "próximos" pela telecompra, em que o consumo e a demanda são captados em seus mínimos detalhes e os serviços e ofertas se multiplicam, desse modo, afirma-se que o "[...] o cibermercado é mais *transparente* que o mercado clássico.".

Para Lévy[27], essa transparência é crescente no mercado online, sendo cada vez mais diferenciado e personalizado, possibilitando aos atores os ajustes em tempo real para

---

[21] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011 p.55. "As informações e os conhecimentos passaram a constar entre os bens econômicos primordiais, o que nem sempre foi verdade. Ademais, sua posição de infraestrutura – fala-se de infostrutura –, de fonte ou de condição determinante para todas as outras formas de riqueza tornou-se evidente, enquanto antes se mantinha na penumbra."

[22] BOFF, Salete Oro; FORTES, Vinícius Broges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018, p.16.

[23] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.55.

[24] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.55-56

[25] HUMBY, Clive. Data is the new oil. ANA Senior marketer's summit, Kellogg School, 3 Nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html Acesso em: 30.maio.2021

[26] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p. 62

[27] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.63

acompanhar às evoluções e à variedade da demanda. Assim, o autor menciona que a consulta aos bancos de dados online aumentará continuamente, uma vez que os indivíduos questionarão os diagnósticos ou conselhos dados por profissionais com base nas pesquisas e informações dos melhores bancos de dados, sistemas especializados e sistemas feitos para consultas do público[28].

Além disso, a economia da informação desenvolvida no ciberespaço, rompe com a economia clássica, pois segundo Lévy[29], transforma o consumidor em coprodutor. Entretanto, embora o autor visualize o consumidor como coprodutor, atualmente, é notória a possibilidade do indivíduo, ao invés de consumidor, tornar-se o próprio produto, uma vez que suas informações podem ser exploradas pela economia da informação.

No contexto informacional, os dados e informações tornaram-se um bem econômico, principalmente, para os serviços ditos "gratuitos", que dependem das informações ou dados dos usuários, recolhidas para que tais serviços possam ser por eles utilizados, sob perspectiva da economia da informação.

Lévy[30] já ressaltava que os fluxos de consumo se aperfeiçoavam pelo pagamento do "valor de uso", diante dos numerosos serviços oferecidos no ciberespaço, tais como os registros dos usos, das navegações e das avaliações individuais, desempenhando uma cooperação ou orientação personalizada.

Nesse sentido, Bioni[31] afirma que com o desenvolvimento da inteligência mercadológica, sobretudo, em relação a segmentação dos bens de consumo e a sua promoção, os dados pessoais dos indivíduos tornaram-se em um fator vital na engrenagem da economia da informação.

---

[28] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.62-63

[29] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p. 63-64. "Por isso o consumidor de informação, de transação ou de dispositivos de comunicação não cessa, ao mesmo tempo, de produzir uma informação, virtualmente cheia de valor. O consumidor não apenas se torna coprodutor da informação que consume, mas é também produtor cooperativo dos "mundos virtuais" nos quais evolui, bem como agente de visibilidade do mercado para os que exploram os vestígios de seus atos no ciberespaço. Os produtos e serviços mais valorizados no novo mercado são interativos, o que significa, em termos econômicos, que a produção de valor agregado se desloca para o lado do "consumidor, ou melhor, que convém substituir a noção de consumo pela de *coprodução* de mercadorias ou de serviços interativos.".

[30] LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.65-66

[31] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 Reimpressão, Rio de Janeiro: Forense, 2019, p.12-13.

O sistema tecnológico possui uma dinâmica entorno do uso dos dados, fazendo o tratamento destes e colocando o indivíduo numa situação em que é indispensável o fornecimento dos seus dados para obtenção serviços e bens, sejam "gratuitos" ou pagos.

A nova economia de dados provoca uma série de desafios atinentes a proteção dos dados, privacidade, liberdade e outros direitos fundamentais. Sendo necessário que as empresas estejam em conformidade com a Lei Geral de Proteção de Dados, para fins do direito interno, mas se a empresa operar no âmbito internacional deverá se adequar também a outras normas aplicáveis conforme o caso.

Por fim, outros aspectos que devem ser ressaltados é que as empresas devem desenvolver sistemas de segurança da informação e da privacidade, com observância ao *privacy by design* e *privacy by default*, boas práticas e políticas de privacidade, com melhorias contantes, buscando sempre minizar os riscos aos titulares dos dados, e conseguir fazer sua atividade de tratamento de dados de forma mais segura possível. Desse modo, compreender essa dinâmica da economia da informação, se faz necessário diante dos efeitos tecnológicos nas vidas das pessoas.

2.3 O *Big Data* e a mineração dos dados

Neste tópico, apresentar-se-ão os reflexos do *Big Data*, envolvendo a mineração de dados, esclarecendo a sua importância no contexto atual e abordando os problemas relacionados a identificação das pessoas, perfil de usuários ou consumidores, publicidade direcionada e tomada de decisão.

Vivência-se uma era de abundância de informações, isso significa que a todo momento são geradas novas informações no mundo. Essas informações dão origem a um grande volume de dados que necessita do *big data* para serem processados, pois não há como comparar uma análise de dados feita por um humano e uma análise de dado feita pelo *big data*, é muito mais rápido e mais eficiente. Sobre *big data* Mayer-Schonberger e Cujier afirmam que:

> Não há uma definição rigorosa para o termo. A princípio, a ideia era a de que o volume de informação crescera tanto que a quantidade examinada já não cabia na memória de processamento dos computadores, por isso os engenheiros tiveram de aprimorar os instrumentos que utilizavam para a análise.
> [...] big data se refere a trabalhos em grande escala que não podem ser feitos em escala menor, para extrair novas ideias e criar novas formas de valor de maneiras que alterem os mercados, as organizações, a relação entre cidadãos e governos etc.

> Mas isto é apenas o começo. A era do big data desafia a maneira como vivemos e interagimos com o mundo. Mais importante, a sociedade precisará conter um pouco da obsessão pela causalidade e trocá-la por correlações simples: sem saber o *porquê,* apenas *o quê.* Essa mudança subverte séculos de práticas consagradas e desafia nossa compreensão mais básica de como tomamos decisões e compreendemos a realidade.[32]

Um aspecto que foi devidamente observado por empresas que utilizam o *big data* é o fato de que as pessoas estão sempre criando informações sobre elas mesmas dentro do ciberespaço, é uma realidade pode deixar o próprio titular vulnerável por não ter a consciência do valor dos seus dados. Com o advento da Lei Geral de Proteção de Dados tornou-se fundamental desenvolver uma cultura de proteção de dados e privacidade, visando a conscientização sobre medidas a serem tomadas pelos próprios indivíduos na administração e disponibilização de suas informações pessoais, além do conhecimento sobre seus direitos estabelecidos na lei.

A relevância dos dados dos indivíduos para as empresas de tecnologia deve ser vista, ou melhor, compreendida dentro de contextos, funções, finalidades e associações. Isso importa dizer que um dado por si só não possui um valor, mas quando esse dado é tratado passa então a ter valor em determinado contexto, função, finalidade e outras informações associadas a ele, pois desse modo é possível extrair informações relacionadas as vontades e emoções, aliás, comportamentos de forma geral das pessoas.

É assim que os dados possibilitam as empresas a tomarem decisões mais assertivas para com o seu público, pois eles sabem informações importantes para garantir o sucessso de suas ações, tais como opiniões, preferenciais, emoções e outros padrões comportamentais dos indivíduos, conforme Pessoa:

> Dessa forma, o indivíduo passa a ser identificado pelos códigos que os sistemas produzem, como nos casos do número da carteira de identidade no registro geral, do número de CPF, do número do passaporte, do número do cartão de correntista bancário, da chave PIX, ou da combinação de números, letras e signos num *username* em determinada rede social, dentre outros exemplos; mas também passa a ser monitorizado e catalogado pelos dados que, consciente ou inconscientemente, produz. [33]

A identificação ou categorização das pessoas é possível pela mineração dos dados obtidos, que passam a revelar informações sobre as pessoas e facilitar no

---

[32] MAYER-SCHONBERGER, Viktor; CUJIER, Kenneth. **Big Data**: Como extrair volume, variedade e valor da avalanche de informação cotidiana. Tradução de Paulo Polzonoff Junior. Rio de Janeiro:Elsevier, 2013, p. 4

[33] PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede:** cibersegurança, regime global de vigilância social e direito à privacidade no século XXI [recurso eletrônico] / João Pedro Seefeldt Pessoa -- Porto Alegre, RS: Editora Fi, 2020, p.45.

direcionamento de produtos, marketing e outras práticas capazes de induzir as pessoas para fazer algo, atendendo aos interesses das empresas ou político. Precisamente, a mineração de dados pode ser "[...] definida em termos de esforços para descoberta de padrões em bases de dados. A partir dos padrões descobertos, têm-se condições de gerar conhecimento útil para um processo de tomada de decisão"[34].

Rotineiramente, as pessoas cedem seus dados em "troca de descontos" em farmácias, mercantis, lojas. Esses "descontos" são apenas um pretexto das empresas para a captação de dados dos indivíduos, que não possuem conhecimento do que são feitos com esses dados, nem como e onde são utilizados, configurando falta de transparência informacional com o titular. Sendo assim, levando-se em consideração a grande quantidade de pessoas que fornecem seus dados, é plenamente possível essas empresas traçarem, no mínimo, o perfil de seus consumidores.

Já no mundo virtual, observa-se que os softwares ou os provedores de serviços dispõem de uma "Política de Privacidade" ou "Termos de Uso e Serviços" para usuários adquirirem produtos ou serviços online, gratuitos ou não, sendo para tanto necessário concordarem com tais termos e/ou políticas em sua integralidade.

O problema vai além da leitura, por parte do usuário, do texto longo e com letras minúsculas da referida política ou termo de usos e serviços, ele reside no desconhecimento técnico pelo indivíduo em compreender as condições impostas pela empresa, os dados que serão cedidos, bem como nos direitos que serão "renunciados", inclusive, de terceiros, como familiares, amigos e conhecidos.

O "aceito" ou o "concordo" do mundo virtual poderá causar riscos na vida real das pessoas, isso porque os dados que são fornecidos, poderão ser (e de fato são) tratados e/ou minerados com a finalidade de obter informações sobre o usuário ou para além dele, até mesmo categorizando-os. O risco recai, exatamente, na possibilidade de identificação da personalidade, manipulação, discriminação, construção de perfis e seus comportamentos e entre outros.

Nesse aspecto, deve-se mencionar a crítica feita por Doneda[35] sobre as situações de consentimento, ou melhor, do "mito do consentimento" em que não revelação dos dados pelo titular significa a renúncia a determinados bens e serviços, além de pontuar a

---

[34]SILVA, Leandro Augusto da; PERES, Sarajane Marques; Clodis Boscarioli. **Introdução à mineração de dados**: com aplicações em R. Rio de Janeiro: Elsevier, 2016. p. 11

[35] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 Ed. São Paulo: Thomson Reuters Brasil, 2019, p.289-299.

disparidade existente relativas ao meio e poder entre a pessoa que deve dar o consentimento para a utilização de seus dados pessoais e aquele que solicita, sendo um verdadeiro "tudo ou nada".

Sobre esse aspecto, é possível torná-lo mais acessível ao usuário, isso porque não basta ter um documento redigido corretamente, se ele não é compreendido pelo leigo. Assim, os termos de uso e/ou políticas de privacidade quando forem elaborados com *legal design* ou *visual law* poderão facilitar a compreensão do usuário. Pois, conforme Hagan:

> O design oferece uma maneira de repensar e melhorar a experiência jurídica das pessoas. Isso significa que tanto do ponto de vista do leigo - que está tendo que navegar no sistema legal para lidar com um problema ou buscar justiça. E também significa do ponto de vista do profissional jurídico - o advogado, o juiz, o funcionário administrativo do tribunal, o paralegal e muito mais. Nosso sistema jurídico não precisa ser do jeito que é. Pode ser mais claro, mais eficiente, mais utilizável e mais amigável[36].

Mas, o que se pretende abordar neste tópico é que as pessoas geram um grande volume de dados todos os dias, sejam conectadas à internet ou não, sendo o *big data* responsável por estruturar e gerenciar o volume, a velocidade e a variabilidade dos dados humanos, pessoais ou não, produzidos na atualidade [37]. Segundo Santos, Camilo e Mello[38], denomina-se de *Big Data* o grande volume de dados gerados e disponíveis na atualidade, podendo ser compreendido também como um processo que visa trabalhar o gerenciamento e estruturação dos dados humanos e tecnológicos.

Observa-se a importância do *Big Data* dentro do contexto informacional, em que há uma crescente e complexa interação entre sociedade, mercado e tecnologia, baseados e conectados pela informação.

Nesse aspecto, Boff, Fortes e Freitas[39] ressaltam que o conhecimento é utilizado para gerar conhecimento, pois trata-se de uma ferramenta empregada no processo de interação e controle na internet, de modo que a informação passa a ser gerada, armazenada, recuperada, processada e transmitida.

---

[36] HAGAN, Margaret. **Law by Design**. Ebook (*online*). Disponível em: https://www.lawbydesign.co/design-mindsets/#feasibility. Acesso em: 18. abril. 2021.

[37] LANEY, Doug. *3D Data Management: Controlling Data Volume, Velocity and Variety.* **Stanford**, Connecticut: META Group, 2001. Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf Acesso em: 08. Fev.2020

[38] SANTOS, Beatriz Rosa Pinheiro dos; CAMILO, Everton da Silva; MELLO, Mariana Rodrigues Gomes. Big Data e Inteligência Artificial: Aspectos Éticos e Legais Mediante Teoria Crítica. **Complexitas** - Rev. Fil. Tem., Belém, v. 3, n.1 , p. 50-60, jan./jun. 2018, p.52

[39] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018, p.16.

Em outras palavras, na sociedade da informação, destaca-se o aspecto informacional dos dados, que quando são minerados ou tratados, estes revelam acontecimentos, informações, predileções e, sobretudo, a personalidade dos indivíduos.

Desse modo, Silva afirma que os dados pessoais "[...] são as informações que podem ser coletadas e tratadas por meios eletrônicos. São utilizadas por empresas ou órgãos públicos para determinado fim comercial, como o uso para uma publicidade, ou para análise de políticas públicas" [40].

No entanto, existe uma assimetria informacional por empresas e Estado para com o titular, este não possue o conhecimento dos uso e finalidades de seus dados, além disso, percebe-se, inúmeros desafios na proteção dos dados pessoais, relacionados a possibilidade de manipulação das informações, discriminação, vazamento e divulgação indevida de dados, envio de dados para o exterior, comercialização ilegal de dados, bem como outros riscos que acarretam uma vulnerabilidade na segurança da informação e aos direitos da personalidade dos indivíduos.

Desse modo, um grande exemplo da utilização e cruzamento de dados, é caso da "previsão de gravidez" da Target. Trata-se de uma empresa que, em 2002, sua equipe de marketing propôs um desafio ao estatístico Adrew Pole, para descobrir quando uma cliente estava grávida, antes da própria cliente saber. Assim, durante muitos anos, a empresa passou a coletar e mapear informações sobre seus clientes. Diante das informações, começou a promover testes, analisar os dados, até criar os padrões úteis, com a capacidade de atribuir as clientes uma "previsão de gravidez" [41].

O fato curioso e famoso desse caso, foi que após a utilização da "previsão de gravidez", a empresa recebeu uma reclamação de um senhor sobre os cupons de produtos de bebês que fora destinado a sua filha, que era apenas uma estudante e "não estava grávida", o gerente, então, se desculpou pelo ocorrido. Entretanto, pouco tempo depois, o senhor entrou em contato com a Target, para pedir desculpas e informar que descobriu que a filha estava realmente grávida[42].

---

[40] SILVA, Alexandre Ribeiro da. A Proteção de Dados no Brasil: a tutela do direito à privacidade na sociedade de informação. **Dissertação**. Faculdade de Direito da Universidade Federal de Juiz de Fora. Disponível em: <http://bdtd.ibict.br/vufind/Record/UFJF_939b28947f81c4d5a1870fa48a420784> Acesso em: 17.out.2019, p.11.

[41] DUHIGG, Charles. ***How Companies Learn Your Secrets.*** *New York Times*. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping- habits.html?pagewanted=1&_r=1&hp> Acesso em: 14.out.2019

[42] DUHIGG, Charles. ***How Companies Learn Your Secrets.*** *New York Times*. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping- habits.html?pagewanted=1&_r=1&hp> Acesso em: 14.out.2019

Trata-se de uma utilização de dados para publicidade direcionada, conforme Bioni "[...]a publicidade direcionada é uma pratica que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo" [43].

É evidente no caso relatado, que o cruzamento de dados das clientes tornou possível a capacidade de prever uma gravidez, antes mesmo que a grávida tome conhecimento da gravidez, adotando uma política de publicidade direcionada, com envios de cupons para as possíveis clientes grávidas, com a finalidade de aumentar as vendas. Essa previsibilidade, a depender das informações fornecidas e tratadas, podem revelar aspectos muito mais privados dos indivíduos.

Sobre a previsibilidade, destaca-se um estudo realizado por Kosinski, Stillwell e Graepel[44] sobre como as características e atributos privados são previsíveis a partir de registros digitais do comportamento humano. O estudo demonstra que uma enorme variedade de atributos pessoais dos indivíduos, desde a orientação sexual até a inteligência que são extraídas de modo automático e com uma certa precisão por meio dos *likes* do Facebook. A previsão dos atributos e predileções pessoais dos indivíduos, a priori, poderão ser utilizados para contribuir e/ou melhorar diversos produtos e serviços.

Todavia, essa previsibilidade por meio de registros digitais de comportamento humano, levanta inúmeras questões consideráveis, devido à possibilidade de ser utilizada sem que haja o consentimento individual ou mesmo sem sequer as pessoas sejam questionadas a respeito disso. Assim, segundo os referidos autores, as empresas, instituições governamentais, amigos do Facebook e entre outros, "[...] podem usar software para inferir atributos como inteligência, orientação sexual ou opiniões políticas que um indivíduo pode não ter a intenção de compartilhar"[45].

Nesse sentido, pode-se mencionar o escândalo, considerado uma das maiores violações de dados, envolvendo a Cambridge Analytica, empresa que trabalhou na campanha eleitoral de Donald Trump, e na campanha vencedora do Brexit [46]. A empresa

---

[43] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 Reimpressão, Rio de Janeiro: Forense, 2019, p.13.

[44] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. ***Private traits and attributes are predictable from digital records of human behavior***. Disponível em: https://www.pnas.org/content/110/15/5802 Acesso em: 12.out.2019

[45] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. ***Private traits and attributes are predictable from digital records of human behavior***. Disponível em**:** https://www.pnas.org/content/110/15/5802 Acesso em: 12.out.2019

[46] CADWALLADR, Carole; GRAHAM-HARRISON, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* **The Guardian**. Disponível em:

realizava captação de possíveis eleitores online e obteve acesso aos dados a 87 milhões de contas de usuários do Facebook, os dados dos usuários foram repassados para a Cambrigde Analytica pelo Aleksandr Kogan, criador do aplicativo "*This Is Your Digital Life*", semelhante a um "teste de personalidade", que calculava as predileções da personalidade por meio dos dados dos usuários. Nesse aplicativo, era necessário o *login* através da conta do Facebook, no qual solicitava o acesso ao perfil e locais visitados, inclusive, os dados dos amigos, com isso, colheram os dados de 270 mil usuários, presentes em 87 milhões de perfis[47].

O Facebook afirmou que a Cambrigde Analytica havia apagado os dados pessoais e que embora os dados colhidos tivessem o consentimento dos usuários, Aleksandr Kogan não poderia, sem o consentimento dos titulares, compartilhar os dados com a Cambrigde Analytica. Em relação aos dados de terceiros, o pronunciamento do Facebook foi no sentido de que essa prática era permitida quando consentida pelo usuário, mas que foi proibida em 2015[48]. Dessa forma, a Cambrigde Analytica obteve a posse desses dados e os utilizou em estratégias online de identificar eleitores e segmentar publicidade para os perfis, como na campanha eleitoral de Donald Trump realizada em 2016[49].

Observa-se no caso da Cambrigde Analytica, que a principal finalidade era a utilização dos dados para identificar os possíveis eleitores e realizar uma publicidade direcionada. Assim, com o perfil das pessoas delineados, as publicidades direcionadas apresentavam, dentre outras estratégias, um forte apelo emocional. Dessa forma, é possível que a própria validade da tomada de decisão das pessoas seja questionada, uma vez que a cognição política pode ser influenciada emocionalmente, bem como por outros fatores.

A neurociência demonstra ainda que os humanos não sejam irracionais, estes precisam de ajuda para fazerem julgamentos mais precisos e terem tomadas de decisões melhores, pois apresentam a capacidade de tomar decisões rápidas e equivocadas,

---

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election Acesso em: 24.nov.2019

[47] LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito Digital: *Compliance*, Regulação e Governança**. São Paulo: Quartier Latin, 2019, p.86-87.

[48] LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito Digital: *Compliance*, Regulação e Governança**. São Paulo: Quartier Latin, 2019, p.86-87.

[49] Nesse sentido, ver o documentário: PRIVACIDADE HACKEADA. **Documentário**. Direção Karim Amer e Jehane Noujaim. Netflix. 114 min., 2019.

principalmente, quando estereótipos, vieses e diversos outros fatores influenciam a intuição[50].

Nesse contexto, a captação, cruzamento e utilização dos dados das pessoas para obter informações sobre aspectos pessoais e manipular comportamentos, denotam as dificuldades e a importância na proteção dos dados pessoais, visto que é inesgotável a produção de dados pelos indivíduos na era informacional.

Outro caso é o da empresa Google, em 2015, uma pessoa afirmou que o serviço de fotos da empresa Google rotulou as fotos dele com um amigo afrodescendente como "gorilas". A empresa se declarou "horrorizado e genuinamente arrependido", afirmando que o rótulo de gorila não seria mais aplicado as imagens e que estavam trabalhando em correções. Após dois anos, o procedimento adotado foi excluir os gorilas e outros primatas do serviço de reconhecimento de imagem[51].

Nesse aspecto, a inteligência artificial utilizada por empresas como Google, Facebook, Whatsapp, Instagram, entre tantos outros, que são presentes na rotina das pessoas, podem apresentar problemas com dificuldades de soluções a serem adotadas. Além disso, as pessoas desconhecem a utilização e destinação das suas informações, imagens e outros dados pessoais pelo uso de inteligência artificial das empresas, inclusive, pelo Estado.

Segundo Souza[52], existem alguns "desafios" lançados nas redes sociais, como o "#10yearschallenge" que consiste nas pessoas postarem fotos com a diferença de 10 anos, desse modo, o que aparenta ser um simples "desafio", trata-se apenas de um pretexto de que, na realidade, seria um treinamento de técnicas de aprendizado de máquinas para padrões de envelhecimento, pois quando milhões de pessoas, no mundo inteiro, fazem esse desafio, elas fornecem tudo o que uma máquina precisa, ou seja, dados em massa, para começar a treinar os padrões de envelhecimento.

Portanto, "[...] o ciberespaço é por excelência o meio em que os atos podem ser registrados e transformados em dados exploráveis." [53]. Desse modo, na era informacional, as empresas que utilizam o *Big Data* para gerenciar e estruturar o grande volume de dados

---

[50] KAHNEMAN, Daniel. **Rápido e devagar: duas formas de pensar**. Daniel Kahneman; Tradução Cássio de Arantes Leite. 1ª ed. Rio de Janeiro: Objetiva [2012], 26ª reimpressão, 2019, p. 514-522.
[51] SIMONITE, Tom. *When It Comes to Gorillas, Google Photos Remains Blind.* **WIRED.** Disponível em: https://www.wired.com/story/when-it-comes-to-gorillas-google- photos-remains-blind/ Acesso em: 13.out.2019
[52] Ver palestra do TEDx: Souza, Carlos Affonso. Privacidade e Proteção de Dados no Brasil. **TEDx**. Disponível em: https://www.youtube.com/watch?v=Zau-x-j_Uu8 Acesso em: 30. Jan.2020
[53] LÉVY, Pierre. **O que é virtual?**, 2ª Edição, São Paulo, Editora 34, 2011, p.63.

obtidos, ou mesmo que as empresas não utilizem o *Big Data*, mas que tenham acessos aos dados humanos, deverão ter transparência e lealdade com o titular dos dados pessoais informando-os sobre que tipo de tratamento e mineração estão utilizando sobre os dados e qual é a sua finalidade. Sendo assim, é necessário que empresas de *Big Data* adotem internamente boas práticas de transparência com os titulares dos dados e segurança na privacidade dos dados.

Pois, a preocupação que se estabelece com a utilização do *Big Data* diz respeito a própria privacidade das pessoas, com a criação de perfis, dossiês e classificação feitas a partir dos dados pessoais coletados, sem que haja uma transparência do seu uso e até podendo gerar algum tipo de discriminação por consequência de uma decisão automatizada ou por um vazamento de dados, provocando problemas imensuravéis na vida do titular dos dados.

É certo que todo ser humano tem suas predileções, emoções, expressões faciais, posturas corporais e ações físicas que são manifestadas na comunicação, seja presencial ou virtual, uma vez que nesta última pode ser captada a imagem, a biometria ou identificar um padrão comportamental por meio de uma simples curtida em redes sociais. Acontece, que o ato da comunicação na internet gera dados e rastros digitais que dão origem aos dossiês digitais sem um real conhecimento por parte das pessoas sobre quais dados são coletados e tratados, e para que fins são utilizados.

Como já foi dito, os benefícios da internet são inúmeros, mas não se pode desconsiderar a sua complexidade e muito menos deixar de entender os problemas por ela causados de forma pessoal, social, emocional, econômico e político como se relata os grandes acontecimentos de escândalos pelo uso indevido dos dados para fins eleitorais, como o caso da Cambrigde Analytica e o Facebook. Isso porque a internet facilitou a vigilância não somente pelo poder público, mas por quem detém os dados, conforme Machado:

> A vigilância passou a ser utilizada como instrumento de poder pelo Estado, assim como pelas empresas privadas, formando-se uma completa rede de controle em volta da sociedade. Com as inovações tecnológicas, sobretudo na área informacional, as pessoas estão expostas a uma visibilidade permanente, à semelhança do que ocorre nas estruturas panópticas. Além da permanente observação ou sensação de exposição, os indivíduos também estão sendo classificados. Elaboram-se verdadeiros perfis para as pessoas, contendo informações detalhadas acerca das suas características, sem contar que, com a soma destas informações, pode-se construir um perfil falso, revelando-se ainda muito mais grave. Dessa forma, no atual cenário social, político e econômico,

> a informação constitui a matéria prima utilizada pela tecnologia para os indivíduos[54].

Nesse aspecto, sabe-se que os dados são essenciais para a nova economia, mas isso não significa que a mineração possa ser feita de forma irrestrita, e as informações utilizadas inclusive para manipular e controlar as pessoas, retirando-lhe além da privacidade, mas também a própria liberdade, pois as tomadas de decisões de cada individuo deve ser feita por ele próprio, cada pessoa deve ter o controle e responsabilidade sobre sua vida e nome desse direito é liberdade, para ser exercida em conformidade com o ordenamento jurídico.

Desse modo, a proteção de dados se faz necessária para resguardar os titulares dos dados pessoais de violações aos direitos fundamentais, por isso, as empresas devem adotar medidas que minimizem os riscos da atividade de tratamento de dados, bem como façam à adequação a Lei Geral de Proteção de Dados.

2.4 A sociedade da informação brasileira

A sociedade da informação nasce das tecnologias da informação e comunicação, possui uma estrutura social constituída e projetada nas redes digitais, fazendo parte da engrenagem que movimenta a economia da informação. Sob a perspectiva dessa nova realidade social, surge a necessidade de compreendê-la no Brasil, que é caracterizado por grave desigualdade social e por uma assimetria de poder estrutural.

O Brasil apresenta um quadro de problemas de origem histórica e que se perpetua ao longo das gerações, dentre eles pode-se destacar a desigualdade social e a assimetria de poder, que delinearam as dificuldades enfrentadas pela maioria da população em ter acesso ao essencial como saúde, educação, moradia, infraestrutura e entre outros[55].

Diante dessa realidade brasileira, pode-se inferir que o processo de virtualização da sociedade em redes digitais ocorreu de forma desigual, sendo um reflexo da própria estrutura social do país. Nesse sentido, o próprio Livro Verde da Sociedade da Informação

---

[54] MACHADO, Joana de Moraes Souza. Caminhos para tutela da privacidade na sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil / Joana de Moraes Souza Machado. - 2014.185 f. **Tese** (doutorado) – Universidade de Fortaleza, 2014, p.81.

[55] Não é a finalidade deste trabalho propor soluções aos problemas do Brasil, visto que não são soluções fáceis. O intuito, portanto, é constatar que esses problemas existem e que não podem ser ignorados, pois irão interferir no processo de virtualização da sociedade brasileira e, consequentemente, no desenvolvimento da cultura de proteção de dados.

expõe que, desde os debates iniciais, já era claro a dimensão do desafio que necessitava o envolvimento da própria sociedade[56].

> Na era da Internet, o Governo deve promover a universalização do acesso e o uso crescente dos meios eletrônicos de informação para gerar uma administração eficiente e transparente em todos os níveis. A criação e manutenção de serviços eqüitativos e universais de atendimento ao cidadão contam-se entre as iniciativas prioritárias da ação pública. Ao mesmo tempo, cabe ao sistema político promover políticas de inclusão social, para que o salto tecnológico tenha paralelo quantitativo e qualitativo nas dimensões humana, ética e econômica. A chamada "alfabetização digital" é elemento-chave nesse quadro[57].

O Livro Verde da Sociedade da Informação foi publicado no ano 2000, e já destacava a importância da "alfabetização digital". Depois de 21 anos, o desafio persiste, pois o país ainda demonstra dificuldade no que diz respeito a educação e acesso digital, sobretudo, com a pandemia que expôs a necessidade da internet para a continuidade de diversos serviços e atividades.

De acordo com os dados elaborados pelo Núcleo da Informação e Coordenação do Ponto BR, na pesquisa sobre o TIC Domicílios 2018, o Brasil apresentou 46,5 milhões de domicílios com acesso à internet (67% do total), sendo 126,9 milhões de usuários de Internet (70% da população)[58]. Observa-se que, embora a maioria da população brasileira tenha acesso à internet, existe um percentual significativo da população que não possui acesso à rede mundial de computadores, são, portanto, os excluídos digitais.

Nesse aspecto, vale observar o recente estudo elaborado pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) sobre "Revisões da OCDE Sobre a Transformação Digital: A Caminho da Era Digital no Brasil" que examina o acesso e o uso de tecnologias digitais no país.

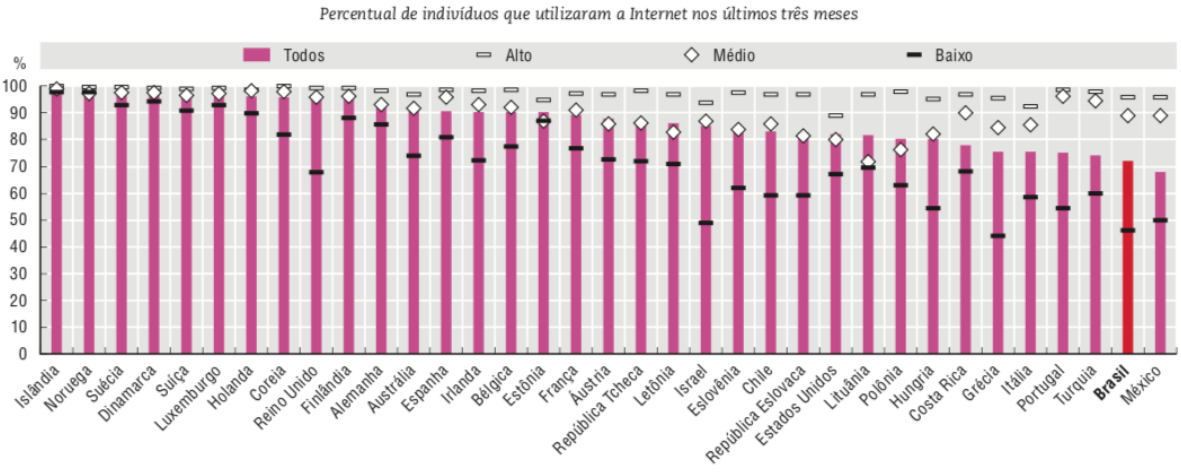
Figura 1- Usuários de Internet no Brasil e na OCDE por nível de escolaridade, 2019 ou mais recente possível.

---

[56] SOCIEDADE da informação no Brasil: **Livro Verde** / organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000, p.XV

[57] SOCIEDADE da informação no Brasil: **Livro Verde**. Organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000, p.V.

[58] Núcleo da Informação e Coordenação do Ponto BR - NIC.br. **Pesquisa sobre o uso das tecnologias de informação e comunicação: pesquisa TIC Domicílios**, ano 2018: Tabelas. Disponível em: http://cetic.br/arquivos/domicilios/2018/domicilios/#tabelas Acesso em: 08.dez.2019



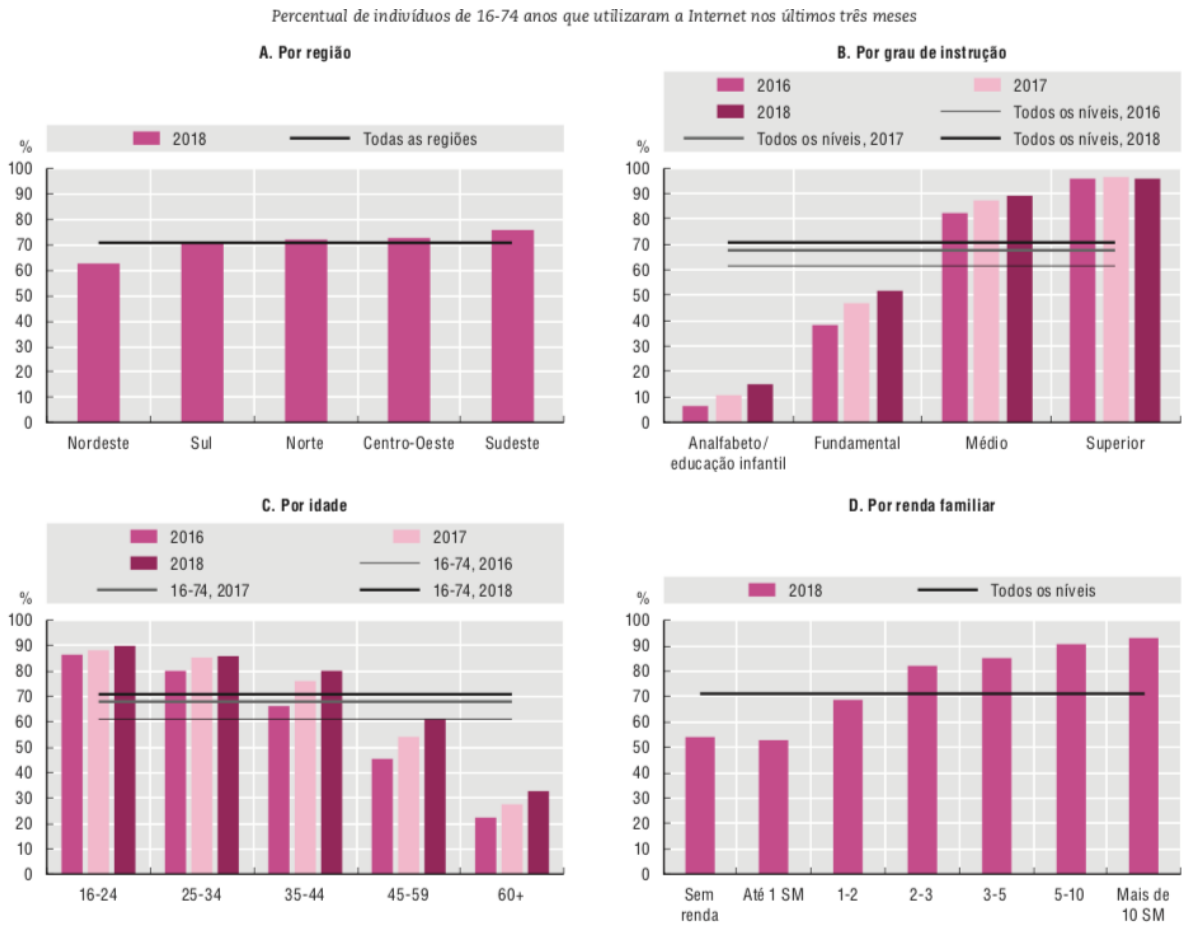
Fonte: OECD (2020), *A Caminho da Era Digital no Brasil* [59].

Nesta imagem gráfica, o estudo realizado demonstra que "as pessoas com alto nível de educação usam a Internet a taxas comparáveis com a maioria dos países da OCDE, enquanto o uso por pessoas com baixo nível de educação está bastante abaixo da média OCDE (73%)"[60].

Assim, pode-se inferir que a educação é um fator que consegue determinar os usuários da internet no Brasil, quanto mais alta se compara com o padrão da maioria dos países da OCDE, mas quando o nível de escolaridade é baixo os usuários da internet ficam abaixo da média dos países da OCDE, o que torna perceptível a necessidade de melhorias educacionais e de acesso à internet no país.

Figura 2- Usuários de Internet no Brasil, por região e grupo sociodemográfico

[59] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.56.
[60] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.56.



Fonte: OECD (2020), *A Caminho da Era Digital no Brasil* [61]

As imagens gráficas acima foram elaboradas com base no aprofundamento dos usuários de internet no Brasil, divididos por região, idade, grau de instrução e renda familiar. Segundo a OCDE, tem-se que a idade é um fator determinante e que evidência uma lacuna existente entre jovens e idosos. Já em relação a renda, a lacuna se refere entre as pessoas de alta renda e os de baixa renda, quanto a análise feita por região, nota-se que as pessoas que vivem no Nordeste, correm o risco de exclusão digital por não conseguir alcançar a média das regiões. O grau de instrução também é um fator de exclusão quando é a escolaridade é baixa[62].

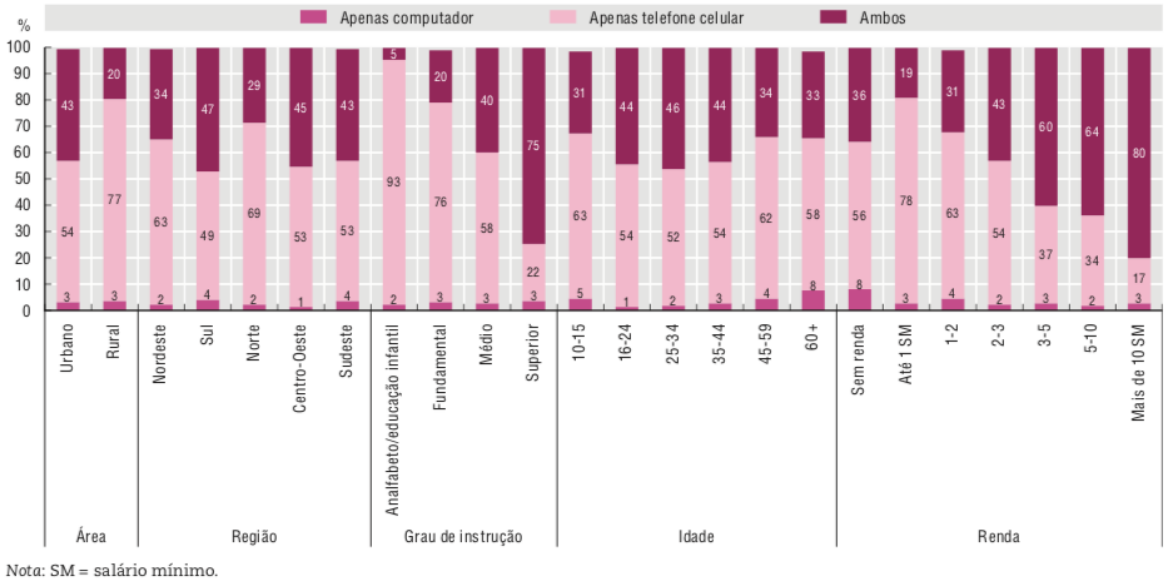
Essa análise sociodemográfica, apresenta os usuários de internet no país e comprova à realidade da sociedade da informação brasileira, com lacunas educacionais, de renda, fator etário e regional.

---

[61] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.56.

[62] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.56.

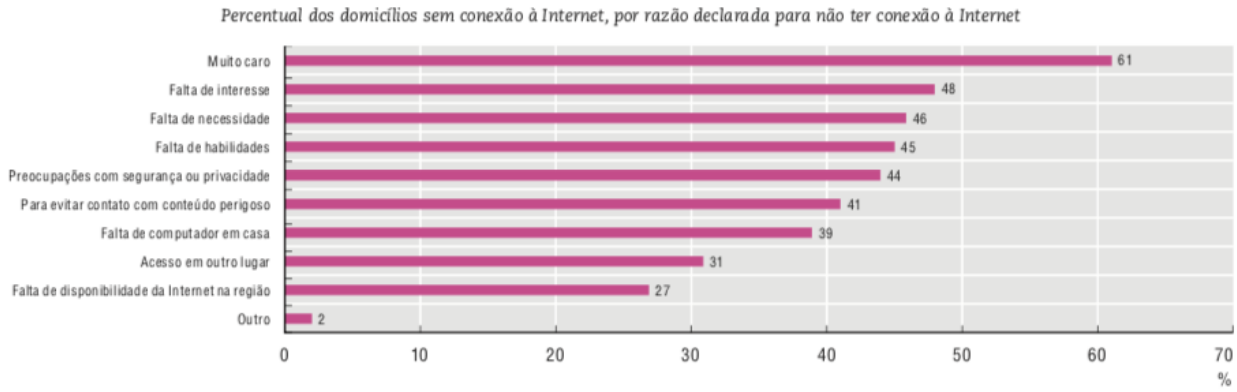
Figura 3- Usuários de Internet no Brasil, por tipo de dispositivo utilizado para acessar a internet (2018)



Fonte: OECD (2020), *A Caminho da Era Digital no Brasil*[63]

Na figura 3, o estudo gráfico aponta que o telefone celular (Cor Rosa Claro) é, cada vez mais, o único dispositivo utilizado no acesso à Internet, principalmente entre a população mais vulnerável (baixa renda e baixo nível de educação), em comparação com o uso de computador (Cor Rosa) ou de ambos (computador e celular – Cor Rosa Escuro), bem como, tem-se que o acesso ao computador é uma realidade limitada e, isso tem reflexos na utilização da internet e seus usuários no Brasil, pois o uso exclusivo do celular ocasiona impede os usuários de realizarem atividades mais complexas[64].

Figura 4 – Barreiras que impedem os domicílios brasileiros de ter internet fixa (2018)



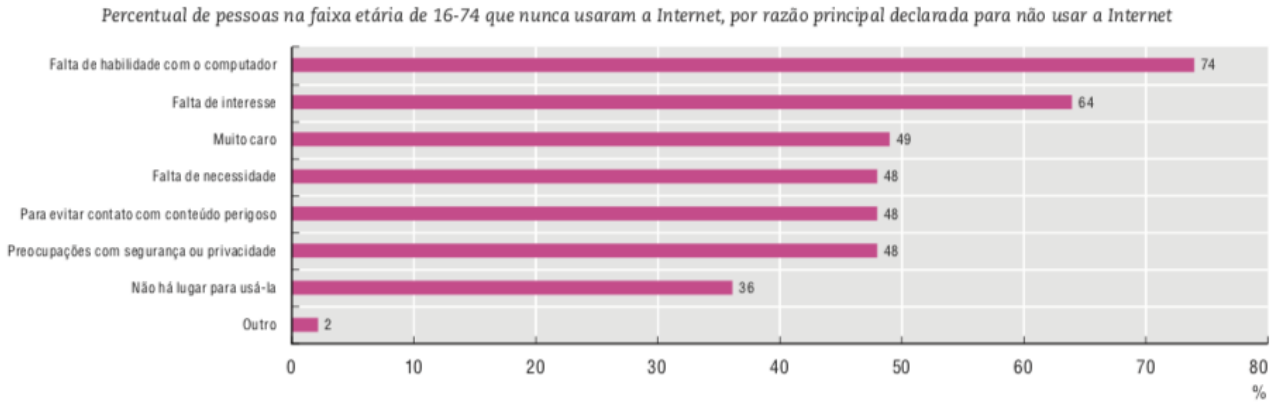
[63] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.57-58

[64] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.57-58

Fonte: OECD (2020), *A Caminho da Era Digital no Brasil*

Nota-se que o principal motivo para os brasileiros não terem conexão à internet é o preço, ou seja, o custo é o maior impeditivo para se ter internet, o que também é um indicativo da necessidade de valores mais acessíveis. Mas, além do valor, a falta de interesse, necessidade e habilidades também são motivos principais para não se ter conexão à internet. Ressalta-se neste gráfico que, existe uma preocupação com segurança e privacidade, encontram-se entre os fatores consideráveis para não se ter acesso à internet no Brasil[65].

Figura 5 – Barreiras que impedem as pessoas de acessarem a Internet no Brasil (2018)



Fonte: OECD (2020), *A Caminho da Era Digital no Brasil*[66]

Em relação a figura 5, gráfico que se refere as pessoas entre a faixa etária de 16-74 anos que nunca utilizaram a internet, tem-se que o principal motivo é a falta de habilidade com o computador com o percentual de 74%, seguido de falta de interesse com o percentual de 64%. Percebe-se que o preço já não está em primeiro motivo, embora continue entre os fatores mais importantes[67].

Todos esses gráficos e análises apresentados acima, demonstram a necessidade de politicas públicas para o letramento digital da população brasileira, bem como a conscientização dos benefícios, conteúdos, serviços e aplicativos[68].

---

[65] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.58

[66] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.58

[67] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.58

[68] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*, p.58-59

Na era da informação, o conhecimento sobre a utilização da internet se faz imprescindível, passa a ser concebido como uma competência. Assim, as pessoas que não foram inseridas nas redes virtuais, por não terem acesso à internet, deverão ser incluídas por meio de políticas públicas, pois de acordo com Lévy[69], a valorização das competências será oposta a desqualificação e ao "acúmulo de detritos humanos", termo utilizado pelo autor para se referir aos excluídos.

Dessa forma, a sociedade da informação, no Brasil, não pode ser concebida do mesmo modo que é estabelecido nos países da Europa, deve-se levar em consideração as peculiaridades do processo de virtualização, bem como os seus problemas internos. É, então, fragmentada em incluídos e excluídos, visto que embora a maioria da população já se encontra inserida nas redes digitais, existe uma parte significativa que sequer utilizaram a internet. Em relação aos excluídos digitais, existe uma tendência de incorporação de forma gradual ao espaço digital por meio de desenvolvimento de políticas públicas.

Em termos de arquitetura global de redes entre os países, segundo Castells, as redes possuem geometrias e geografias diferentes de inclusão e exclusão, pois embora haja a coexistência da sociedade em rede, como estrutura global, com as sociedades industriais, rurais, comunitárias e de subsistência, esta se dará em proporções diferentes.[70] Essas especificidades de cada sociedade da informação derivam das suas características e dos seus componentes principais, tais como valor, trabalho, comunicação, cultura e a sua forma de existência[71].

Então, a necessidade de compreender a sociedade da informação brasileira, significa entender a realidade social e os fatos sociais, para analisar como se desenvolverá a proteção jurídica dos dados pessoais. Pois, o direito como fato social[72] deverá observar

---

[69] LÉVY, Pierre. **O que é virtual?**,Tradução de Paulo Neves 2ª Edição, São Paulo, Editora 34, 2011, p.24. "Assim como a ecologia opôs a reciclagem e as tecnologias adaptadas ao desperdício e à poluição, a ecologia humana deverá opor a aprendizagem permanente e a valorização das competências à desqualificação e ao acúmulo de detritos humanos (aqueles que chamamos de "excluídos")".

[70] CASTELLS, Manuel. **O Poder da Comunicação**. Tradução de Vera Lúcia Mello Joscelyne; Revisão de Tradução de Isabela Machado de Oliveira Fraga. 3ª ed. São Paulo/Rio de Janeiro: Paz e Terra, 2019, p.72

[71] CASTELLS, Manuel. **O Poder da Comunicação**. Tradução de Vera Lúcia Mello Joscelyne; Revisão de Tradução de Isabela Machado de Oliveira Fraga. 3ª ed. São Paulo/Rio de Janeiro: Paz e Terra, 2019, p.73

[72] DURKHEIM, Émile. As Regras do Método Sociológico, 3ª edição. **São Paulo: Martins Fontes**, 2007, p.13. "É fato social toda maneira de fazer, fixada ou não, suscetível de exercer sobre o indivíduo uma coerção exterior; ou ainda, toda maneira de fazer que é geral na extensão de uma sociedade dada e, ao mesmo tempo, possui uma existência própria, independente de suas manifestações individuais."

os fenômenos sociais e buscar um sistema regulatório que melhor se adeque a realidade social.

Embora hajam dificuldades relacionada a própria estrutura da sociedade da informação brasileira percebe-se que, juntamente, com os avanços da tecnologia da informação e comunicação que surgiram os debates e discussões sobre a uso e proteção dos dados no país, mesmo que a temática seja forte na atualidade, deve-se esclarecer que a base fundamentadora desta proteção é bem anterior.

Conforme Instituto Brasileiro de Defesa do Consumidor – IDEC, as iniciativas à respeito do tema começaram aproximadamente em 2010, com consulta e debate público sobre o anteprojeto de lei de dados pessoais, promovida pelo Ministério da Justiça. Em 2011, o IDEC contribuiu na propositura do Marco Civil da Internet e no ano de 2012, foi apresentado o Projeto de Lei n. 4060/2012, que tratava sobre proteção de dados pessoais, na Câmara dos Deputados[73].

Deve-se mencionar que durante o ano de 2011, foi criada a Lei 12.527/11[74], conhecida como a Lei do Acesso à Informação, que disciplina o direito de acesso à informação previsto na Constituição Federal, promovendo a transparência das informações de posse do poder público. Já em 2012, Lei 12.737/12, foi criada com finalidade de tipificação criminial de delitos informáticos, tornando crime a invasão de aparelhos eletrônicos para obtenção de dados pessoais, popularmente conhecida como Lei Carolina Dieckmann[75].

Em 2013, Edward Snowden revelou o programa de espionagem dos Estados Unidos, o que impulsionou a aprovação do Marco Civil da Internet, que foi aprovado em 2014[76].

Segundo o IDEC, a 2ª consulta pública sobre o anteprojeto de lei de proteção de dados pessoais foi realizada em 2015, pelo Ministério da Justiça, mas somente em 2016, o governo federal encaminhou o Projeto de Lei n. 5276 ao Congresso, este projeto foi

---

[73] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021

[74] BRASIL, Lei nº 12.527, DE 18 DE NOVEMBRO DE 2011." **Lei de Acesso à Informação".** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso: 21. Maio.2021.

[75]BRASIL, Lei nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Dispõe sobre a tipificação dos crimes cometidos eletronicamente**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso: 21.maio.2021.

[76] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021.

anexado ao Projeto de Lei n.4060/2012. Nessa conjuntura, Câmara dos Deputados criou uma Comissão Especial para analisar o PL4060/2012 e PL 5276/2016, já no Senado o PL330/2013 é aprovado na Comissão de Ciência, Inovação, Tecnologia, Comunicação e Informática[77].

Em 2018, tornou-se público o escândalo da Cambridge Analytica, envolvendo o mais de 50 milhões de usuários do Facebook, utilizados para fins eleitorais e na saída do Reino Unido da União Europeia. Após esse acontecimento, houve forte pressão pela proteção dos dados, o projeto é sancionado pelo presidente Michel Temer, mas com vetos referentes a Autoridade Nacional de Proteção de Dados e com algumas modificações nas regras sobre tratamento de dados pelo poder público e entre outras regras. Ainda no mesmo ano, o então presidente Michel Temer promulgou a Medida Provisória n. 869, que cria a Autoridade Nacional de Proteção de Dados Pessoais[78].

A Lei n.13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais - LGPD[79], estabelece princípios, direitos e obrigações sobre o tratamento de dados pessoais, protegendo os dados dos titulares sejam estes físicos ou digitais, assegurando assim proteção aos direitos fundamentais de liberdade e privacidade, o livre desenvolvimento da personalidade, a autodeterminação informativa e outros direitos da personalidade. A LGPD é originária do PLC n. 53/2018 que, por sua vez, teve forte influência do Regulamento Geral de Proteção de Dados da União Europeia, buscando colocar o Brasil no nível internacional proteção de dados.

No ano de 2019, foi aprovada a lei que cria a Autoridade Nacional de Proteção de Dados. A sua criação foi aguardada pela sociedade civil e o setor privado, uma vez que a ANPD é responsável por estabelecer as diretrizes sobre a adequação à LGPD.

Em 2020, a pandemia de Covid-19 chega ao Brasil, causando impactos na adequação à LGPD por parte das empresas e do setor público, além do fato de que o país ainda se encontrava sem ANPD. Além das dificuldades com a pandemia, havia um período de incertezas entorno da entrada em vigor da LGPD, que finalmente entrou em

---

[77] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021

[78] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021

[79] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

vigor no dia 18 de setembro de 2020, com exceção das sanções que vão entrar em vigor apenas em agosto de 2021[80].

A efetividade da Lei Geral de Proteção de Dados, que entrou em vigor em 2020, é frequentemente questionada, uma vez que o Brasil por receio de implicações internacionais e buscando se adequar ao Regulamento Geral de Proteção de Dados (RGPD), criou a LGPD e, em seguida, criou a Autoridade Nacional de Proteção de Dados (ANPD), aprovada em maio de 2019, mas que somente foi de fato criada no final de 2020.

Nesse cenário de avanços tecnológicos, o próprio governo brasileiro precisou se adaptar à nova realidade, criando o "Governo Digital" por meio da Lei n. 14.129/2021, que disciplina sobre os princípios, regras e instrumentos para o governo digital, visando o aumento da eficiência pública[81].

A OCDE publicou em 2020, "A Caminho da Era Digital no Brasil" que consiste em analises sobre o desenvolvimento da economia digital, revisões sobre as políticas relativas à digitalização e recomendações visando a melhoria da coerência das políticas sobre o assunto. Em síntese, trata-se de uma revisão que "[...] examina a disponibilidade e a qualidade das redes e serviços de comunicação no Brasil, bem como políticas e regulamentos relacionados", apresenta "[...] as tendências no uso da tecnologia digital entre indivíduos, empresas e o governo, e examina políticas para promover sua difusão", "[...]discute os esforços para aumentar a confiança na economia digital, com foco na segurança digital, privacidade e proteção do consumidor", bem como "[...]analisa políticas para promover a inovação digital e examina as implicações políticas dos modelos de negócios emergentes em setores-chave" [82].

Figura 6 – Marco de Políticas Integradas "A Caminho da Era Digital" da OCDE

---

[80] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021
"Governo edita a MP nº 959 que adia a entrada em vigor da LGPD para 3 de maio de 2021. É aprovado no Senado PL 1.179 nº 2020 que adia as sanções da LGPD para janeiro de 2021, considerando que a Lei entre em vigor em agosto. Após um período de incertezas em relação à MP nº 959 (que poderia caducar se não fosse aprovada pelo Congresso dentro do prazo ou um novo adiamento da LGPD), a Lei entra em vigor no dia 18 de setembro."

[81] BRASIL. **LEI Nº 14.129, DE 29 DE MARÇO DE 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm Acesso: 30.maio.2021

[82] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.3.

Fonte: OECD (2020), *A Caminho da Era Digital no Brasil*[83]

A OCDE apresenta sete políticas integradas para desenvolver o crescimento e bem-estar na era digital no Brasil. Sobre o "Acesso" está relacionado as "infraestruturas e serviços de comunicação confiáveis, sustentam o uso de todas as tecnologias digitais, além de facilitar interações entre pessoas, organizações e máquinas conectadas"[84], ou seja, abrange o acesso aos dados, a infraestrutura, aos serviços de comunicação, aos investimentos, a concorrência e ao desenvolvimento regional[85]. Em relação ao "Uso", significa que "[...] é necessário a fim de que pessoas, governos e empresas colham os benefícios da transformação digital, por meio da participação, inovação, produtividade e bem-estar aprimorados"[86], o que requer investimento.

A "Inovação", por sua vez, "[...] expande os limites do que é possível, levando à criação de empregos, ao crescimento da produtividade, e ao crescimento e desenvolvimento sustentáveis"[87], é importante, pois é capaz de promover transformações

[83] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[84] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[85] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[86] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[87] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.

nas formas como as pessoas interagem, criam, produzem e consomem, pela criação de novos produtos e serviços, bem como gerar novas oportunidades. Desse modo, o elemento "Empregos" é impactado pela transformação digital, pois está associado as alterações na estrutura, natureza e modelo das organizações e mercado, sendo assim, novas oportunidades surgirão e com elas as exigências de novas competências.

A "Sociedade" é afetada pela transformação digital, uma vez que as "[...] tecnologias digitais mudam a forma como as pessoas, empresas e governos interagem entre si"[88], sendo, portanto, necessário o desenvolvimento de políticas públicas que apoiem uma sociedade digital e promova a inclusão social, buscando solucionar os problemas relativos as desigualdades digitais. Já a "Confiança" "[...] é fundamental para a transformação digital; sem ela, as pessoas, empresas e governos não usarão as tecnologias digitais de forma plena, deixando inexplorada uma importante e potencial fonte de crescimento e progresso social"[89]. É destacado nesta política a cooperação internacional em prol de estratégias voltadas para segurança digital e privacidade, visando soluções as questões atinentes a proteção de dados pessoais.

E a "Abertura de Mercado" encontra-se relacionada "[...]a negociações, investimentos, mercados financeiros, concorrência e tributação, têm um papel importante na garantia de que condições favoráveis existam, para a transformação digital prosperar"[90], produção de novos modelos de negócios e novas oportunidades mercadológicas.

Percebe-se que, em alinhamento com essas políticas integradas para o Caminho Digital, é necessário desenvolver no país um cenário seguro para uso dos dados dos titulares, até porque a transformação digital possui a tendência de evoluir e, consequentemente, para proporcionar um desenvolvimento econômico e social na nova economia deve-se garantir a adequação à LGPD.

Além disso, como foi abordado na análise da Figura 4, a preocupação com a segurança e privacidade é uma das barreiras impeditivas aos brasileiros de terem conexão à internet, reforçando a ideia de que não basta promover o acesso à rede mundial de

---

[88] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[89] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.
[90] OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*. p.23.

computadores, é preciso também desenvolver a cultura da privacidade e proteção de dados, por meio da conscientização e educação digital.

Portanto, existe a sociedade da informação brasileira, mas não nos moldes dos países europeus, pois os processos de virtualização das sociedades se deram de formas distintas. Com toda a sua complexidade, desafios e dificuldades o Brasil vem buscando a proteção de dados como foi dito. Para isso, observa-se que o modelo regulatório da proteção de dados do Brasil, busca se adequar aos parâmetros do modelo protetivo do RGPD da União Europeia, o que motiva analisar o Regulamento Geral de Proteção de Dados que inspirou o legislador brasileiro para a criação da Lei Geral de Proteção Dados.

2.5 A influência do Regulamento Geral de Proteção de Dados da União Europeia no Brasil

A economia informacional, como já foi dito, consiste em modelos de negócios que utilizam fluxos de informações e bases de dados, principalmente, desenvolvidos com o uso tecnologias de informação e comunicação, big data e inteligência artificial, tornou necessária a criação de legislações para a proteção dos dados pessoais dos titulares.

O debate entorno da proteção de dados pessoais é bem mais amadurecido na União Europeia, isso significa que a busca pela proteção dos dados tem mais tempo na Europa em comparação com o Brasil, cujo enfrentamento dessas questões é bem mais recente. Segundo Doneda[91], a Lei de Proteção de Dados do Land alemão de Hesse de 1970, é marco do início da disciplina jurídica sobre a proteção de dados pessoais.

Após a Lei criada em Hesse, outras legislações surgiram na europa, como a Lei sueca de proteção de dados – Datalagen, em 1973, a lei francesa de proteção de dados em 1978, a Informatique et libertées, assim apareceram leis semelhantes nos demais países da europa[92]. O demonstra a importância dos dados nos países da europa[93].

---

[91] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021, p.3.

[92] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021, p.9.

[93] Uma decisão que impactou o desenvolvimento deste tema foi o julamento feito em 1983, pelo Tribunal Constitucional Alemão, segundo Doneda "Ao analisar o caso, o Tribunal reconheceu que os avanços tecnológicos tornavam possível o processamento de dados em proporção jamais vista, o que demandava que fosse revisitada a interpretação de alguns direitos fundamentais, em razão do surgimento de ameaças e riscos até então indispensáveis não somente à privacidade, mas também a diversas liberdades e garantias fundamentais, em razão do sugirmento de ameaças e riscos até então impensáveis não somente à privacidade, mas também a diversas liberdades e garantias fundamentais. Assim, a Corte reconheceu a existência de um direito à autodeterminação informacional, formulado a partir do direito geral de

Nesse sentido, a Organização para a Cooperação e Desenvolvimento Econômico OCDE, em 1980 estabeleceu diretrizes relativas à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais e adotou os princípios da limitação da coleta, da qualidade dos dados, da definição da finalidade, da limitação da utilização, da salvaguarda de segurança, da abertura, da participação do indivíduo, da responsabilização, que foram ajustadas em 2013[94].

Já no ano de 1995, foi criada a diretiva 95/46/CE, trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que posteriormente foi substituída pelo Regulamento Geral de Proteção de Dados (RGPD) de 2016, que entrou em vigor em 2018[95]. Mas antes do RGPD, nos anos 2000, a Carta dos Direitos Fundamentais da União Europeia fez previsão sobre a proteção de dados em seu art.8º, garantindo proteção a todas pessoas o direito fundamental a proteção de dados pessoais[96]. Atualmente, com o avanço e desenvolvimento da disciplina de proteção de dados pessoais, as legislações possuem estruturas semelhantes, tais convergências são apontadas de forma geral por Doneda:

> Muito sinteticamente, esses marcos regulatórios reconhecem os dados pessoais e o seu tratamento como fenômenos juridicamente relevantes, estabelecendo direitos e garantiaspara cidadãos, limites para a sua utilização por empresas e organizações e mecanismos que procuram reduzir o risco proporcionado pelo tratamento de dados. Esses elementos são organizados de forma a proporcionar maior controle e proteção ao cidadão sobre seus dados, indo além de uma abordagem vinculada meramente à proteção da privacidade e, ainda, têm como uma de suas consequências mais importantes a consolidação de espaços dentro

---

personalidade e coltado a garantir ao cidadão o direito de controlar a amplitude da divulgação ou utilização de qualquer aspecto relacionado a sua personalidade por meio de seus dados pessoais" DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021, p.9.

[94] OCDE. **Recomendação do Conselho sobre as Diretrizes que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais**.Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188?_ga=2.190186027.1064690390.1621449249-1613775020.1621449249 Acesso em: 30.maio.2021

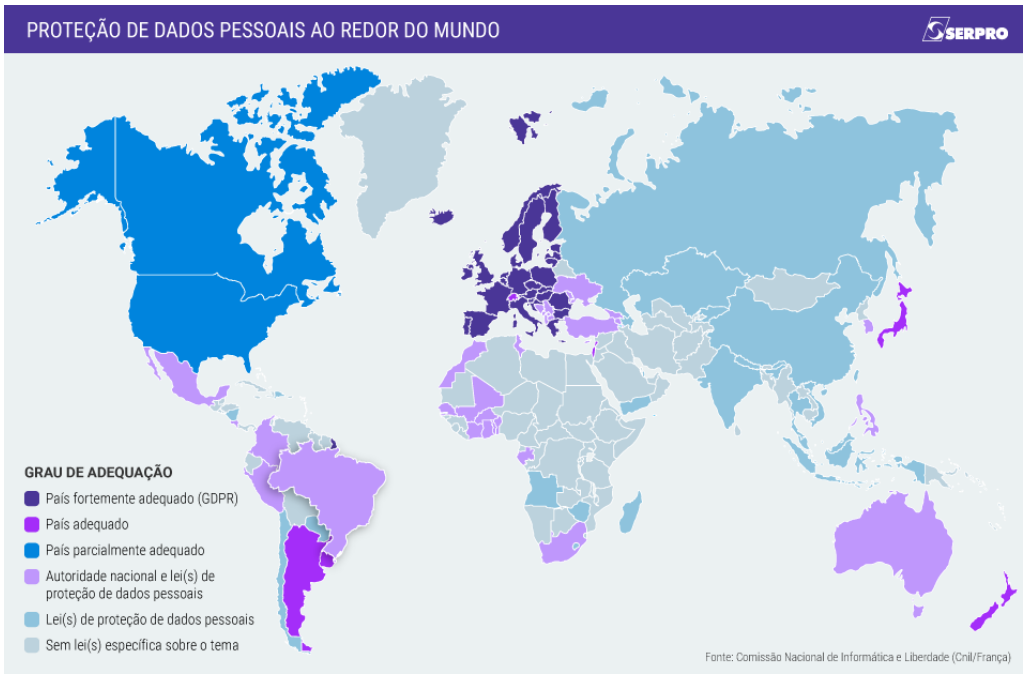
[95] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021

[96] Cf. EUROPEIA, União. Carta dos direitos fundamentais da União Europeia. **DIREITO E DEMOCRACIA**. Disponível em: https://www.researchgate.net/profile/Betania-Alfonsin/publication/43236353_O_Estatuto_da_cidade_e_a_construcao_de_cidades_sustentaveis_justas_e_democraticas/links/5554aff108ae980ca60acf15/O-Estatuto-da-cidade-e-a-construcao-de-cidades-sustentaveis-justas-e-democraticas.pdf#page=205 Acesso: 23.maio.2021. "Artigo 8º Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.".

> dos quais os dados pessoais possam ser tratados licitamente, proporcionando garantias para utilizações legítimas de dados pessoais e fomentando espaços de tratamento e livre fluxo de dados[97].

Nesse aspecto, é perceptível a influência do RGPD na elaboração da Lei Geral de Proteção de Dados, assim como também, observa-se que o regulamento europeu se tornou parâmetro de adequação em metária de proteção de dados pessoais. Veja-se:

Figura 7- Proteção de Dados Pessoais ao Redor do Mundo



Fonte: SERPRO[98]

A imagem trata sobre o nível de proteção de dados no mundo, extraída do SERPRO, na qual percebe-se que o controle do nível de adequação de proteção de dados pessoais de determinado país é feito em analise dos padrões internacionais, principalmente, ao nível de equivalência ao Regulamento Geral de Proteção de Dados.

Assim, é importante observar que a convergência presente nas regulamentações sobre proteção de dados entre os países é um reflexo da necessidade da nova economia de dados, uma vez que buscam proteger e facilitar a circulação de dados entre os países. Isso implica um movimento ao nível internacional de promover e estabelecer padrões internacionais, sob pena de implicações econômicas, politicas, contratuais entre outros

---

[97] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021, p.4.

[98]SERVICO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO. **MAPA DA PROTEÇÃO DE DADOS:** Em que "estágio" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/mapa-sobre-protecao-de-dados-no-mundo/view Acesso: 15.maio.2021

fatores que poderá comprometer negociações internacionais e até provocar medidas de barreiras e isolamentos, o que é alarmante sob o aspecto econômico, mas principalmente sobre a proteção dos dados em circulação transfronteiriças.

Sobre a convergência normativa existente entre a Lei Geral de Proteção de Dados Pessoais e o Regulamento de Proteção de Dados, Bioni e Mendes explicam que:

> Historicamente, a agenda de padronização de normas é um elemento que se confunde com a própria gênese das leis gerais de proteção de dados pessoais. A Organização para Cooperação e Desenvolvimento Socioeconômico/OCDE e o Conselho da Europa/CoE, ao formularem, respectivamente, diretrizes e uma convenção internacional, pautaram toda a produção normativa que lhes é posterior. É, por isso, que se experimentou um alto de grau de convergência das leis de proteção de dados pessoais ao redor do mundo, uma vez que estão estruturadas sobre fundações comuns e fincadas desde o início da década de 1980[99].

Como bem é pontuado pelos autores, o cenário internacional deu origem a uma convergência regulatória sobre a proteção dos dados pessoais, que foi um desdobramento realizado pela própria OCDE.

Todavia, Bioni e Mendes fazem uma advertência, de que embora haja influência do RGPD sobre a LGPD, ambos apresentam diferenças substanciais, principalmente, no que diz respeito a técnica legislativa utilizada por ambas as leis[100].

Como foi já foi explicado, o RGPD, surgiu após a proteção de dados ter um patamar de direito fundamental, é fruto de uma trajetória de proteção de dados desenvolvida na União Europeia, enquanto a lei de proteção de dados brasileira veio de um movimento mais recente no país e após a perplexidade de escândalos envolvendo os dados pessoais, sendo incontestável a influencia do regulamento europeu para a criação da lei brasileira.

A LGPD e o RGPD apresentam convergência em três aspectos importantes, que são destacados por Bioni e Mendes[101], relacionados aos princípios que possuem um

---

[99] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileir de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** [livro eletrônico]/ Ana Frazão Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[100] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileir de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** [livro eletrônico]/ Ana Frazão Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[101] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileir de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** [livro eletrônico]/

"modelo *ex ante* de proteção", a importância do "*accountability"*, bem como o "*enforcement"* em ambas regulamentações.

Existe semelhanças na previsão de proteção de dados pessoais, os referidos autores apontam que a LGPD estabelece os mesmos os princípios presentes no RGPD, e acrescenta ainda outros três princípios: segurança, prevenção e não discriminação. Já em relação aos direitos dos titulares, nota-se uma convergência entre ambos regulamentos, no tocante aos direitos de acesso, notificação, retificação e cancelamento de seus dados, bem como o direito à portabilidade, que se trata uma inovação para ambos.

A importância da análise de equivalência da LGPD ao RGPD, apresenta dois motivos distintos e centrais, conforme Bioni e Mendes:

> Considerando a aprovação da LGPD e o seu sistema de *enforcement* ainda em formação, a discussão sobre o grau de equivalência entre ela e o RGPD adquire importância por dois motivos centrais e, ao mesmo tempo, bastante diversos. Em primeiro lugar, para se saber a probabilidade de o Brasil ser considerado um país "adequado" sob o ponto de vista do sistema europeu de proteção de dados e obter uma decisão da Comissão Europeia favorável a um eventual pleito nesse sentido, o que constituiria uma importante vantagem para as entidades públicas e privadas no Brasil que tratam e transferem dados[102].

Desse modo, percebe-se que as semelhanças entre a LGPD e o RGPD não se trata apenas de uma influência, mas sim de um "movimento" de convergência entre as regulamentações. No mundo globalizado e interconectado, é cada vez mais fácil e fluída a circulação dos dados e informações pessoais, haveria enormes obstáculos se as legislações fossem completamente distintas e/ou sem qualquer parâmetro de proteção de dados pessoais.

Portanto, neste capítulo buscou-se contextualizar e apresentar a complexidade que é o assunto de proteção de dados pessoais, pois mesmo que a legislação brasileira tenha aspectos semelhantes ao RGPD, o que aproxima do cenário de proteção de dados internacional, esta ainda possui desafios internos. Por isso, é relevante compreender as peculiaridades da sociedade brasileira para conseguir traçar perspectivas de mudanças e desenvolver a cultura da proteção de dados para a nova realidade tecnológica econômica.

Ana Frazão Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[102] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileir de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** [livro eletrônico]/ Ana Frazão Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

3. FUNDAMENTOS E PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS

Os direitos da personalidade são intrínsecos à natureza humana, por isso o Código Civil de 2002, estabeleceu um rol exemplificativo desses direitos, possibilitando que haja outros direitos não mencionados expressamente, mas que possam ser tutelados por lei.

De acordo com Orlando Gomes[103] os direitos da personalidade possuem algumas características: são direitos absolutos, ou seja, são oponíveis *erga omnes*, tratando-se, portanto, de uma obrigação negativa; são direitos vitalícios e necessários, permanecem com o seu titular durante toda sua vida; e, por fim, são direitos extrapatrimoniais, intransmissíveis, imprescritíveis e impenhoráveis.

Todavia, é perceptível que o ambiente virtual, sobretudo, as redes sociais, têm relativizado tais características, tornando-se um espaço vulnerável para o titular e para a garantia da direitos de intimidade, privacidade, imagem, principalmente, para os dados pessoais.

Deve-se ressaltar que, embora a proteção dos direitos de liberdade, privacidade e personalidade estejam previstos no ordenamento jurídico, precisamente, amparados na Constituição Federal de 1988 e no Código Civil de 2002, o desenvolvimento tecnológico exponencial e disruptivo provocou a necessidade da criação de uma proteção normativa que tivesse o foco no tratamento dos dados pessoais, incluindo, os meios digitais.

A preocupação com a proteção dos dados pessoais não é restrita ao ciberespaço, abrange também os meios físicos, equipamentos e documentos que não são digitais, mas sem dúvidas, na atualidade, em razão dos avanços tecnológicos os riscos se fazem presentes de forma mais evidente no digital, por isso, a importância de reflexões sobre o tema.

As novas facetas tecnológicas remodelaram as relações sociais e empresariais, bem como desencadearam a era da informação, tornando o acesso ao conteúdo mais fácil e dinâmico, mas, por outro lado, expôs a vulnerabilidade e a necessidade de proteção do

[103] GOMES, Orlando. **Introdução ao direito civil**. 18 ed. Rio de Janeiro: forense, 2001, p.152

titular dos dados pessoais. Sobretudo, pela utilização das redes sociais que possuem um grande volume de informações dos seus usuários e que segundo Doneda "as redes sociais deixam clara, portanto, uma nova vulnerabilidade dos seus usuários que consiste, entre outros fatores, na escassa possibilidade destes conhecerem os efeitos do compartilhamento de suas informações"[104].

Nesse cenário, o ordenamento jurídico brasileiro carecia de uma proteção ao titular dos dados face as novas tecnologias. Conforme Orlando Gomes, "A teoria dos direitos de personalidade somente se liberta de incertezas e imprecisões se sua construção se apoia no Direito Positivo e reconhece o pluralismo desses direitos ante a diversidade dos bens jurídicos em que recaem"[105].

Dessa forma, a Lei do Marco Civil da Internet, promulgada em 2014, estabeleceu os princípios, garantias, direitos e deveres para o uso da internet no Brasil, mas não protegia a privacidade e a proteção de dados de forma completa e estruturada. Posteriormente, a Lei Geral de Proteção de Dados Pessoais foi criada com o propósito de resguardar o titular e proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do indivíduo, disciplinando sobre o tratamento dos dados pessoais, seja ele feito em meios digitais ou não[106].

Ressalta-se, por oportuno, que existe uma Proposta de Emenda à Constituição[107] para inserir o inciso XII-A, ao artigo 5º, e o inciso XXX, ao artigo 22, ambos da Constituição Federal de 1988, para acrescentar a proteção de dados no rol de direitos fundamentais, bem como estabelecer a competência privativa da União Federal para legislar sobre a matéria.

---

[104] DONEDA, Danilo. Reflexões Sobre Proteção de Dados Pessoais em Redes Sociais. **RIPDP – Revista Internacional de Protección de Datos Personales**. Universidad de los Andes. Faculdade de derecho (Bogotá, Colombia). No. 1 Julio – Diciembre de 2012, p.8.

[105] GOMES, Orlando. **Introdução ao direito civil**. 18 ed. Rio de Janeiro: forense, 2001, p.152

[106] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios."

[107] Cf. BRASIL. **Proposta de Emenda à Constituição n. 17/2019**, pelo Senado Federal, que: "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". Senado Federal, Brasília, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais Acesso em: 20.jan.2021.

A busca por incluir a proteção de dados na Constituição ou de criar leis sobre o assunto, decorre do avanço tecnológico, principalmente, no modo veloz de disseminação de conteúdo e informações, as consequências disso é uma fragmentação da esfera da privacidade e intimidade das pessoas, o que no passado não era possível ocorrer na mesma proporção da atualidade.

Além disso, o próprio direito passa por transformações, reagindo diante de novos fatos sociais, pois conforme Grau "[...] o plano do dever-ser é um espelho, um reflexo do plano do ser"[108], ou seja, os riscos de escamoteamento dos direitos da personalidade no ciberespaço provocaram "*inputs*" para criar e/ou alterar leis, visando a proteção dos dados pessoais e o livre desenvolvimento da personalidade.

A transformação jurídica é reflexo da busca por conseguir resguardar as liberdades civis e os direitos fundamentais em jogo. Nesse aspecto, tem-se que a privacidade já não é mais aquela que foi concebida por Samuel D. Warren e Louis D. Brandeis[109] como o direito de ser deixado só. Na atualidade, de acordo com Rodotà[110] a privacidade apresenta uma nova definição, baseada no exercício do próprio titular realizar o controle das suas próprias informações, trata-se do direito à autodeterminação informativa. Isso significa que a autodeterminação informativa é um desdobramento do direito à privacidade, mas no tocante à proteção de dados pessoais, em que cabe ao indivíduo o controle sobre seus dados e informações.

Por isso, diante do contexto atual, ordenamento jurídico deve ser garantir a proteção aos dados pessoais para evitar práticas discriminatórias e outros danos a dignidade da pessoa humana e aos direitos fundamentais do titular. Desse modo, passa-se a analisar os fundamentos da proteção de dados pessoais a seguir.

3.1 Os fundamentos da proteção de dados pessoais

Os fundamentos da proteção de dados pessoais sob o prisma digital, tem como marco legislativo inicial a Lei do Marco Civil da Internet. Em vigor desde 2014, o MCI

---

[108] GRAU, Eros Roberto. **Por que eu tenho medo de juízes**: (a interpretação/aplicação do direito e os princípios), 8ed. refundida do ensaio e discurso sobre interpretação. São Paulo: Malheiros, 2017, p.140

[109] WARREN, Samuel D; BRANDEIS, Louis D. *The Right to Privacy*. **Harvard Law Review**. v. 4, p. 193-196, 1890.

[110] Cf. RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.97-98: "1. Do direito a ser deixado só ao direito de manter controle sobre as informações que me digam respeito; 2. Da privacidade ao direito à autodeterminação informativa; 3. Da privacidade à não-discriminação; 4. Do sigilo ao controle".

disciplina o uso da internet no Brasil, estabelecendo os princípios, garantias, direitos e deveres na utilização da rede mundial de computadores, e diretrizes para União, dos Estados, do Distrito Federal e dos Municípios atuarem em relação à matéria[111].

O Marco Civil da Internet prevê seus fundamentos no art.2º, depreende-se que pelo teor do dispositivo a utilização da internet está baseada no respeito à liberdade de expressão, no reconhecimento da escala mundial da rede, nos direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, na pluralidade e a diversidade, a abertura e a colaboração, na livre iniciativa, a livre concorrência e a defesa do consumidor e, por fim, na finalidade social da rede[112]. Todavia, o MCI não fornece uma proteção suficiente aos dados pessoais, pois não é uma lei geral que visa a proteção dos dados pessoais de forma completa e estruturada.

Já a Lei Geral de Proteção de Dados, por sua vez, tem como fundamentos, o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, e por fim, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[113].

Tais fundamentos apresentam relevância dentro do contexto informacional, pois segundo Castells "[...] a busca da identidade, coletiva ou individual, atribuída ou

---

[111] Cf. BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm> Acesso em: 10. Jan. 2020 "Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria".

[112] BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm> Acesso em: 10. Jan. 2020 "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I - o reconhecimento da escala mundial da rede; II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; III - a pluralidade e a diversidade; IV - a abertura e a colaboração; V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VI - a finalidade social da rede."

[113] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

construída, torna-se a fonte básica de significado social"[114], principalmente, no que diz respeito a autodeterminação informativa e o livre exercício da personalidade, pois o foco da Lei Geral de Proteção de Dados é conferir proteção a pessoa natural[115], por isso, seus dados pessoais são tutelados.

Entende-se, portanto, como dado pessoal a "informação relacionada a pessoa natural identificada ou identificável"[116]. Já o dado pessoal sensível exprime a "[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"[117], deve-se ressaltar a necessidade de proteção do dado mesmo que seja considerado "trivial", pois é possível que um dado pessoal revele informações sensíveis do seu titular[118].

Sobre os dados sensíveis, estes possuem uma proteção maior em razão ao potencial lesivo aos direitos dos titulares. Nesse sentido, Frazão, Oliva e Abilio afirmam que:

> O dado pessoal sensível é objeto de proteção recrudescida tendo em conta o potencial lesivo de sua utilização. Com efeito, por se referir a informações relacionadas aos aspectos mais íntimos da pessoa, pode propiciar discriminações abusivas. Importante atentar que um dado *prima facie* não sensível pode o ser por revelar, indiretamente, aspectos relacionados à origem étnica (ex., com o sobrenome), à orientação sexual (ex., com o nome do companheiro), a convicções religiosas (ex., com os nomes atribuídos aos filhos)[119].

---

[114] CASTELLS, Manuel. **A Sociedade em Rede**. Tradução: Roneide Venacio Majer. 20. Ed. rev. Ampl. São Paulo: Paz e Terra, 2019, p.63.

[115] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º Para os fins desta Lei, considera-se:[...] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;"

[116] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"

[117] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º Para os fins desta Lei, considera-se:[...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;"

[118] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 Reimpressão, Rio de Janeiro: Forense, 2019, p.85.

[119] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020, p.i.

Já em relação ao dado anonimizado, significa que é o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"[120].

Destaca-se que, a proteção de dados pessoais é considerada um direito fundamental, embora ainda esteja em tramitação o Projeto de Emenda Constitucional - PEC 17/2019, que pretende acrescentar ao rol do art.5º da CF/88 o inciso X-A com a seguinte redação: "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais"[121], o próprio Supremo Tribunal Federal- STF[122] no julgamento da ADI n. 6387, n. 6388, n.6389, n.6390 e n. 6393 (Medida Provisória n.954, de 17 de abril de 2020) sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística", tutelou os dados pessoais no âmbito de proteção das cláusulas constitucionais liberdade, privacidade e do livre desenvolvimento da personalidade.

Portanto, embora a proteção de dados pessoais não esteja, até o presente momento, expressamente na Constituição Federal, entende-se que os dados pessoais gozam de uma proteção constitucional, assim como foi dito no voto da Relatora Ministra Rosa Weber, bem como de proteção infraconstitucional.

---

[120] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º Para os fins desta Lei, considera-se: [...] III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;"

[121] Cf. BRASIL. **Proposta de Emenda à Constituição n. 17/2019**, pelo Senado Federal, que: "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". Senado Federal, Brasília, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais Acesso em: 20.jan.2021.

[122] Nesse sentido, ver voto da Relatora Ministra Rosa Weber no STF – julgamento da ADI n. 6387, n. 6388, n.6389, n.6390 e n. 6393 (Medida Provisória n.954, de 17 de abril de 2020) julgamento do IBGE "Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais." (BRASIL, Supremo Tribunal Federal. ADI 6387. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf Acesso: 20.maio.2021)

3.2 O livre desenvolvimento da personalidade e o seu prolongamento por meios dos dados: o direito a autodeterminação informativa

No Brasil, a Constituição Federal de 1988 estabelece como um dos fundamentos da República a dignidade da pessoa humana[123], pode-se entender que o ser humano deve ser respeitado, bem como reconhecido em todas as situações da vida, englobando, desse modo, o ciberespaço.

Assim, a Constituição trata no art. 5º, dos direitos e garantias fundamentais, tais como a inviolabilidade à vida, à intimidade, à privacidade, à liberdade, na livre manifestação do pensamento e no acesso a informação, dentre outros direitos. Sendo esses direitos e garantias previstos em consonância com os tratados internacionais sobre direitos humanos.

Esses direitos também são protegidos pelo Código Civil de 2002, no seu capítulo II que trata dos direitos da personalidade, sob o prisma das relações privadas, aplicáveis entre particulares, ou seja, objetivam a proteção de um particular em face de outro particular.

Dentre os direitos da personalidade, a liberdade de acordo com Bittar[124], é o direito da pessoa poder direcionar suas energias nas relações intersubjetivas, conforme a sua própria vontade, sendo o ordenamento jurídico, que elimina qualquer empecilho à consecução de suas metas, desde que respeitadas as próprias restrições impostas pelo sistema jurídico.

Já o direito à intimidade e à privacidade destinam-se a resguardar a privacidade em seus múltiplos aspectos, pessoais, familiares e negociais, trata-se de um mecanismo de defesa da personalidade humana contra injunções, indiscrições ou intromissões alheias. Ressalta-se que esses direitos vêm adquirindo maior relevância, em decorrência da expansão da virtualização da comunicação e do comércio, como forma de proteção do indivíduo[125].

---

[123] BRASIL. Constituição Federal de 1988. **Constituição da República Federativa do Brasil**, Brasília, DF, Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 27 de julho de 2018. "Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] III - a dignidade da pessoa humana;".

[124] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., rev., aum. e mod. São Paulo: Saraiva, 2015, p.168.

[125] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., rev., aum. e mod. São Paulo: Saraiva, 2015, p.172-173.

Sendo assim, verifica-se que a liberdade, a intimidade e a privacidade são direitos da personalidade, que resguardam a vida e seus elementos particulares da esfera privada do indivíduo, da não exposição e não intromissão a conhecimento de terceiro. De acordo com Rodotà:

> [...] quando os cidadão passam a ser cada vez mais avaliados e classificados apenas a partir de informações a seu respeito, a proteção e o cuidado com estas informações deixa de ser um aspecto que somente diga respeito às esferas da do sigilo ou da privacidade, passando a figurar um componente essencial para determinar o grau de liberdade de autodeterminação individual de cada pessoa.[126]

Isso ocorre, pois, os dados pessoais podem fornecer informações sobre a vida do seu titular, fragmentando a esfera da privacidade e intimidade do individuo, bem como influenciando à sua liberdade de escolha. Nesse sentido, ressalta Bauman que as "[...] informações que fazem as vezes da pessoa são constituídas de "dados pessoais" apenas no sentido de que se originam em seu corpo e podem afetar suas oportunidades e escolhas existenciais."[127].

Além disso, sabe-se que o titular de dados, muitas vezes é também consumidor de determinado produto ou serviço, o que possibilita a aplicação do Código de Defesa do Consumidor - CDC. Sob a perspectiva da proteção de dados, pode-se ressaltar que o CDC dispõe em seu art. 43[128], a necessidade de ter acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo sobre ele, inclusive, sendo comunicado por escrito sobre a abertura de bases de dados, garantindo o direito a acessar e a retificar os seus dados ali registrados.

---

[126] RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.07

[127] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013, p.15.

[128] Cf. BRASIL.**CÓDIGO DE DEFESA DO CONSUMIDOR**. Lei nº 8.078 de 11 de Setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso: 08.jun.2021.
"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.§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor."

Por isso, Doneda afirma que "as modalidades de tutela para os dados pessoais merecem uma atenção particular, seja pela dinamicidade de seu conteúdo como pelo novo cenário que procura regular, marcado pela forte presença da tecnologia."[129]. Nesse sentido, a Lei Geral de Dados Pessoais (LGPD) é criada com a finalidade de conciliar a utilização dos dados pessoais na economia da informação com a proteção dos dados pessoais das pessoas. Segundo Doneda, seria o "[...] estabelecimento de mecanismos capazes de legitimar a inserção de dados pessoais no mercado, nos quais estaria inserida a valoração dos interesses e direitos fundamentais em questão, com os devidos limites e contrapesos"[130].

O direito a autodeterminação informativa, como observa o referido autor[131], surgiu como extensão das liberdades de segunda geração, buscando incluir o consentimento do individuo em fases sucessivas do tratamento e utilização de dados.

É o direito à autodeterminação informativa que assegura aos titulares dos dados pessoais decidirem sobre as informações que lhes respeitam, trata-se de uma liberdade de dispor sobre as suas informações pessoais, para que ela seja correspondente com a própria pessoa e preserve a identidade informática. Sendo assim, a autodeterminação informativa e o livre desenvolvimento da personalidade buscam resguardar a identidade informacional do titular.

Dessa forma, diante da dinamicidade da sociedade da informação e seus contornos jurídicos, sociais, políticos e econômicos, motivaram a necessidade de se buscar conciliar o desenvolvimento da economia informacional com a proteção dos dados pessoais, sem comprometer a autodeterminação informativa e o livre desenvolvimento da personalidade, que buscam resguardar a identidade informacional.

---

[129] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2. Ed. São Paul: Thomson Reuters Brasil, 2019, p.290.

[130] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2. Ed. São Paul: Thomson Reuters Brasil, 2019, p.291

[131] DONEDA, Danilo. Princípios de proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira (coord.). **Direito & Internet III- tomo I: Marco Civil da Internet (Lei nº 12.965/2014)**. São Paulo: Quartier Latin, 2015, p.373 "O direito à autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças especificas neste sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais porém procurava inclui-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros além de compreender algumas garantias, como o dever de informação."

Por isso, a Lei Geral de Proteção de Dados[132] confere ao titular os direitos de confirmação de tratamento de dados, acesso aos dados, correção, anonimização, bloqueio ou eliminação dos dados, portabilidade, revogação do consentimento e revisão das decisões automatizadas, esses direitos devem ser garantidos por empresas públicas e privadas. Tais direitos possibilitam o indivíduo exerça o controle dos seus dados e, consequentemente, o direito a autodeterminação informativa.

Assim, nesse cenário informacional, a Lei Geral de Proteção de Dados busca tutelar os dados pessoais, bem como estabelecer mecanismos capazes de legitimar o tratamento de dados pessoais no mercado, tornando-se, portanto, necessária uma analisar os princípios que norteiam a proteção de dados e o livre desenvolvimento da personalidade no ciberespaço.

3.3 Princípios

Os princípios norteiam a interpretação e a aplicação das normas, nesse cenário tecnológico, eles são importantes por estabelecerem fins a serem promovidos, como a preservação da autodeterminação individual e a proteção da dignidade da pessoa humana. Segundo Humberto Àvila, "os princípios são, portanto, normas que atribuem fundamentos a outras normas, por indicarem fins a serem promovidos, sem, no entanto, preverem o meio para a sua realização"[133].

Observa-se que o legislador optou por criar leis com princípios basilares atinentes aos avanços tecnológicos, possibilitando a funcionalização do direito. Conforme Doneda, uma legislação que fosse feita com menos em princípios em relação as regras, não aparentava ser adequada "[...] pelo risco real de sua obsolescência ser decretada pela

---

[132] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 18. 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: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei".

[133] ÁVILA, Humberto. Teoria dos princípios jurídicos. **Da definição à aplicação dos princípios jurídicos**. 18ª ed. São Paulo: Malheiros, 2018, p.155.

rapidez do progresso tecnológico e pela contínua metamorfose que este produzia na área"[134].

Os princípios que se encontram estabelecidos na Lei do Marco Civil da Internet, na Governança da Internet, no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados, buscam nortear as atividades empresariais e estatais, bem como o interprete da lei, DPO, advogados, juízes e entre outros, para a concretização dos direitos.

Sabe-se que das normas jurídicas decorrem os princípios e regras, embora se pretenda analisar neste tópico apenas os princípios, deve-se esclarecer desde já, que existindo conflitos entre regras, entende-se como possível, diante da complexidade do tema, o diálogo das fontes[135] como uma forma de solução flexível e funcional ao sistema jurídico.

Pois é por meio da teoria do diálogo das fontes que é possível visualizar o diálogo sistemático entre a Constituição Federal de 1988, Código Civil de 2002, o Código do Consumidor, a Lei do Marco Civil da Internet, da Lei Geral de Proteção de Dados entre outras fontes, a depender do caso[136].

Conforme Souza[137], sobre o tratamento do assunto proteção de dados pessoais, a LGPD não possui a exclusividade, existindo em outros diplomas legais (Constituição, Código Civil, Código de Defesa do Consumidor e o Marco Civil da Internet, por

---

[134] DONEDA, Danilo. Um Código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, 2003, p.i. Disponível em: https://www.researchgate.net/profile/Danilo-Doneda/publication/266036287_Um_Codigo_para_a_protecao_de_dados_pessoais_na_Italia/links/5934046b0f7e9beee7bcd261/Um-Codigo-para-a-protecao-de-dados-pessoais-na-Italia.pdf Acesso: 15.jun.2021

[135] A Teoria do Diálogo das fontes foi concebida por Erik Jayme, mas difundida no Brasil por Cláudia Lima Marques que diz: "Aceite-se ou não a pós-modernidade, a verdade é que, na sociedade complexa atual, com a descodificação, a tópica e a microrecodificação (como a do CDC)98 trazendo uma forte pluralidade de leis ou fontes, a doutrina atualizada está à procura de uma harmonia ou coordenação entre estas diversas normas do ordenamento jurídico (concebido como sistema).99 É a denominada "coerência derivada ou restaurada" ("*cohérence dérivée ou restaurée*"),100 que procura uma eficiência não só hierárquica,101 mas funcional102 do sistema plural e complexo de nosso direito contemporâneo.103 Erik Jayme104 alerta-nos que, nos atuais tempos pós-modernos, a pluralidade, a complexidade, a distinção impositiva dos direitos humanos e do „*droit à la différènce*" (direito a ser diferente e ser tratado diferentemente, sem necessidade mais de ser 'igual' aos outros) não mais permitem este tipo de clareza ou de 'mono-solução'. A solução atual ou pós-moderna é sistemática e tópica ao mesmo tempo, pois deve ser mais fluida, mais flexível, a permitir maior mobilidade e fineza de distinções. Hoje, a superação de paradigmas foi substituída pela convivência ou coexistência dos paradigmas" MARQUES, Cláudia Lima, SUPERAÇÃO DAS ANTINOMIAS PELO DIÁLOGO DAS FONTES: O MODELO BRASILEIRO DE COEXISTÊNCIA ENTRE O CÓDIGO DE DEFESA DO CONSUMIDOR E O CÓDIGO CIVIL DE 2002. **REVISTA DA ESMESE**, Nº 07, 2004 – DOUTRINA, p.43 Disponível em: https://core.ac.uk/download/pdf/79073279.pdf Acesso: 08.jun.2021

[136] Lembre-se de que em muitos cenários o titular é também o consumidor.

[137] SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

exemplo), mas o que a diferencia em relação aos demais, é a sua abrangência, com princípios, direitos, responsabilidades e outras normas relativas aos tratamento de dados pessoais.

Desse modo, o fato indicado de que a Lei Geral de Proteção de Dados Pessoais não possui exclusividade temática corrobora com a ideia já explicitada de que é possível a adoção da teoria do diálogo das fontes em detrimento aos critérios da cronológico, hierárquico e da especialidade para resolver os conflitos entre normas[138].

Portanto, sabe-se que os princípios revelam diretrizes finalísticas e servem de fundamento e concretização dos direitos dos titulares, possibilitando a funcionalização do direito face as novas tecnologias, analisar-se-ão os princípios relacionados no ciberespaço, principalmente, a proteção de dados.

3.3.1 Princípios da Lei do Marco Civil da Internet

O Marco Civil da Internet possui uma parte principiológica e outra de regras, os princípios contribuem para o desenvolvimento em rede. Assim, os princípios fundamentais do MCI, encontram-se previstos no art.3º, e visam disciplinar o uso da internet no Brasil, são eles: a liberdade de expressão; privacidade; proteção de dados pessoais; neutralidade da rede; segurança e funcionalidade da rede; responsabilização dos agentes; natureza participativa; liberdade negocial[139].

Acontece que o Marco Civil da Internet não garante de forma satisfatória a proteção de dados pessoais, pois como já foi dito, seu objeto é tratar sobre o uso da internet estabelecendo direitos e deveres dos usuários. De acordo com Machado "[...] na

---

[138] Diante da complexidade do tema, propõe-se afastar os critérios de solução de antinomias e aderir a teoria do diálogo das fontes. Sobre os critérios de solução de antinomias cf. BOBBIO, Noberto. Teoria do Ordenamento jurídico. Tradução de Ari Marcelo Solon; prefácio de Celso Lafer; apresentação de Tercio Sampaio Ferraz Junior. São Paulo, EDIPRO, 2. Ed. 2014, p.94. "As regras fundamentais para a solução das antinomias são três: a) o critério cronológico; b) o critério hierárquico; c) o critério da especialidade".

[139] Cf. BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm> Acesso em: 10. Jan. 2020. "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte".

parte que trata de proteção de dados pessoais, o faz de forma bem tímida, até porque não é este o seu foco principal, deixando ainda uma lacuna muito grande no que se refere a esta temática e, consequentemente merecendo proteção legal especifica"[140].

Contudo, o MCI pode ser considerado o início regulamentação, ainda que tímido, no âmbito digital, o que revela a importância de conhecer seus princípios, até mesmo em razão das informações serem maior no ciberespaço. O primeiro, é o princípio da liberdade de expressão, comunicação e manifestação de pensamento, busca garantir uma internet democrática e livre para todos manifestarem seu pensamento e expressão, sem que haja discriminação e diz expressamente que será nos termos da Constituição Federal. Desse modo, observa-se que o art.5º, caput, e seus incisos IV e XIV e o art. 220, ambos da Constituição[141], resguardam o direito fundamental à manifestação do pensamento.

Além disso, observa-se que o MCI busca a proteção da privacidade no ambiente da internet, pode-se inferir que é um reflexo da proteção constitucional à "vida privada" previsto no art.5º, inciso X, da Constituição Federal de 1988.

Em relação a proteção dos dados pessoais, o MCI diz que será na forma definida em lei. Isso importa observar que durante anos existia essa lacuna, que foi superada com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais.

O princípio da preservação e garantia da neutralidade de rede, busca garantir um tratamento isonômico em rede, sem diferenciação ao tráfego de pacotes de dados, bem como sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação, apresentando apenas duas exceções: "(i) requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações e (ii) priorização de serviços de emergência"[142] elecandos no art.9º, §1º do MCI.

---

[140] MACHADO, Joana de Moraes Souza. Caminhos para tutela da privacidade na sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil / Joana de Moraes Souza Machado. - 2014.185 f. **Tese** (doutorado) – Universidade de Fortaleza, 2014, p.88.

[141] Cf. BRASIL. Constituição Federal de 1988. **Constituição da República Federativa do Brasil**, Brasília, DF, Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 27 de julho de 2018. "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:[...] IV - é livre a manifestação do pensamento, sendo vedado o anonimato; [...] XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;[...] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

[142] Cf. BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm> Acesso em: 10. Jan. 2020. Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica

O princípio da segurança e funcionalização da rede encontra-se previsto no art.3º, inciso V, que disciplina a "preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas"[143]. Observa-se que o princípio da responsabilização dos agentes, está relacionado com o princípio anterior, e diz que os agentes serão responsabilizados de acordo com suas atividades e nos termos da lei, se não houver previsão específica, é cabível responsabilização nos termos do art.927 e art. 944, ambos do Código Civil[144].

O princípio da preservação da natureza participativa da rede, conforme Souza e Lemos, significa que a "internet é, por sua própria natureza, aberta, colaborativa e participativa"[145].

Já o princípio da liberdade negocial, apenas veda as formas que conflitem com outros princípios elencados na Lei do Marco Civil da Internet, tem-se, portanto, o fomento a livre iniciativa e a inovação nos modelos de negócios em rede.

Por fim, o art. 3º, parágrafo único do MCI, diz que: "Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte"[146], observa-se que legislador fez a opção de deixar de forma clara a possibilidade de incidência de outros princípios, mas que não foram previstos por essa lei, embora isso possa ser solucionado através de uma interpretação sistematizada do ordenamento jurídico.

Mas, importa observar que diante de um mundo cada vez mais conectado, os reflexos de tratados e acordos internacionais cada vez mais pelo sistema jurídico pátrio.

---

quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de: I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II - priorização de serviços de emergência.

[143] BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm Acesso: 10. Jan. 2020

[144] Cf. BRASIL. **Código Civil (LEI No 10.406, DE 10 DE JANEIRO DE 2002)**. Brasília, DF, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso: 19. Ago. 2020. "Art.927 Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. [...] Art. 944 A indenização mede-se pela extensão do dano."

[145] SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação** / Carlos Affonso Souza e Ronaldo Lemos, Juiz de Fora: Editar Editora Associada Ltda, 2016, p.56

[146] BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm Acesso: 10. Jan. 2020

É, perceptível quando o assunto se trata de uma proteção de dados pessoais em que se exige um nível mínimo de adequação pelos países cujo parâmetro é a União Europeia[147].

3.3.2 Princípios da Governança da Internet

A internet não é um ambiente sem regulamentações, além do MIC, existe um conjunto de princípios da governança da internet, que segundo a NETmundial "[...] contribuem para uma estrutura de governança da Internet inclusiva, multissetorial, eficaz, legítima e em evolução e reconheceu que a Internet é um recurso global que deve ser gerido no interesse público"[148]. Percebe-se que dentre os valores e princípios que estruturam a governança da internet pode-se mencionar os direitos humanos elencados na Declaração Universal dos Direitos Humanos de 1948, são direitos universais e incidem também na rede mundial de computadores.

Nesse sentido, a NETmundial afirma que as pessoas gozam de proteção em conformidade com "[...] as obrigações legais internacionais de direitos humanos, incluindo os Pactos Internacionais de Direitos Civis e Políticos e Econômicos, Sociais e Culturais, bem como a Convenção sobre os Direitos das Pessoas com Deficiências"[149], definindo-se um rol não exaustivo de direitos formam a base da governança da internet, tais como liberdade de expressão; liberdade de associação; privacidade; acessibilidade; liberdade de informação e de acesso à informação; desenvolvimento; proteção dos intermediários; cultura e diversidade linguística; espaço unificado e não fragmentado; segurança, estabilidade e resiliência da internet; arquitetura aberta e distribuída ambiente favorável para a inovação sustentável e a criatividade.

O primeiro é o princípio da liberdade de expressão, que de acordo com a NETmundial "Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de ter opiniões sem interferências e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras"[150].

---

[147] Vide cap.2.

[148] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF

[149] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p.20.

[150] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ;

Trata-se de um princípio basilar na Constituição Federal de 1988, que reflete também no ambiente virtual, garantindo a livre manifestação de pensamento, expressão e opinião ao indivíduo. No entanto, cabe ressalvar que esse direito não é absoluto, pois não protege o discurso de ódio e, atualmente, ainda se discute acerca das *fakes news* se estaria ou não por ele protegido.

O princípio da liberdade de associação estabelece que: "Toda pessoa tem o direito de reunião e associação pacíficas online, incluindo através de redes e plataformas sociais". É natural de qualquer sociedade a formação de grupos sociais, na internet não é diferente, pois as relações sociais geram grupos sociais que, atualmente, é conhecido por redes sociais. Assim, esse princípio que garante o direito de reunião e associação para fins pacíficos na internet, é também encontrado na CF/88, que engloba o ambiente virtual.

Deve-se dizer que, embora, o direito de reunião seja garantido as pessoas, sabe-se que as redes sociais são viabilizadas por plataformas, estas possuem políticas de uso ou termos de uso, que podem limitar o direito do usuário, desde que descumpra com termos ou politicas da rede social.

O princípio da privacidade diz que "[...] não estar sujeito à fiscalização arbitrária ou ilegal, captura, tratamento e utilização de dados pessoais. Deverá ser garantido o direito à proteção da lei contra tais interferências".

A privacidade é protegida pelo ordenamento jurídico brasileiro, no âmbito constitucional quando se protege a vida privada das pessoas, é também tutelada pelo direito civil e, recentemente, pela lei geral de proteção de dados.

Com o avanço tecnológico, as práticas de tratamento de dados, *profile*, vigilância de comunicações e de geolocalização, bem como outros procedimentos tecnológicos que comprometem a privacidade das pessoas, assim, surgiu a necessidade de uma proteção mais completa e estruturada pela Lei Geral de Proteção de Dados Pessoais, para fins de proteção dos dados, privacidade e, principalmente, a autodeterminação informativa.

Já o princípio da acessibilidade refere-se à promoção de "[...] projeto, desenvolvimento produção e distribuição de informação, tecnologias e sistemas acessíveis na internet"[151], para um ambiente mais inclusivo.

---

traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p.20.

[151] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p.20.

O princípio da liberdade de informação e de acesso à informação estabelece que: "Todos devem ter o direito de acessar, compartilhar, criar e distribuir informação na Internet, de acordo com os direitos dos autores e criadores, conforme estabelecido em lei"[152]. Na era da informação, entende-se que a informação é o que se tem de mais relevante, assim, o direito a liberdade de informação e acesso consiste nos coronários da própria democracia, por isso, é tão importante para o próprio desenvolvimento da sociedade que as informações falsas sejam repelidas.

Já o princípio do desenvolvimento busca que "todas as pessoas têm o direito ao desenvolvimento e a Internet tem um papel vital a desempenhar para ajudar a alcançar a plena realização dos objetivos de desenvolvimento sustentável acordados internacionalmente"[153].

Em consonância com o princípio anterior, existe o princípio da proteção dos intermediários que diz "As limitações de responsabilidade de intermediários devem ser implementadas de uma forma que respeitem e promovam o crescimento económico, a inovação, a criatividade e o fluxo livre de informações"[154].

O princípio da cultura e diversidade linguística determina que "governança da Internet deve respeitar, proteger e promover a diversidade cultural e linguística em todas as suas formas", bem como que este espaço seja unificado, interconectado, estável, não fragmentada, escalável e acessível, em conformidade com o princípio do espaço unificado e não fragmentado.

Outro princípio é o da segurança, estabilidade e resiliência da internet, que estabelece que "[...] a Internet deve ser uma rede segura, estável, resiliente, confiável e fidedigna. A eficácia no tratamento dos riscos e ameaças à segurança e estabilidade da Internet depende de uma forte cooperação entre os diferentes atores"[155], a finalidade é promover um ambiente seguro e repelir os riscos inerentes aos ciberespaço.

---

[152] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p. 21.

[153] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p. 21.

[154] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p. 21.

[155] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ;

O princípio da arquitetura aberta e distribuída busca preservar a internet como um sistema aberto e colaborativo, inovador com tecnologia de ponta-a-ponta. Por fim, o ambiente favorável para inovação sustentável e a criatividade consiste num princípio, relacionado com o anterior, que busca expandir a internet preservando "[...] seu dinamismo, a governança da Internet deve continuar a permitir a inovação livre de barreiras através de um ambiente de Internet favorável"[156].

3.3.3 Princípios do Regulamento Geral de Proteção de Dados da União Europeia

O Regulamento Geral de Proteção de Dados da União Europeia influenciou o desenvolvimento da proteção de dados no Brasil, como foi dito no capítulo 1, trata-se de um regulamento influente e importante no plano internacional. Além disso, deve-se ressaltar que devido a viabilidade transfroteiriça dos dados torna, portanto, indispensável o conhecimento deste regulamento, principalmente, seus princípios.

A regulamentação europeia é principiológica, uma vez que o RGPD estabelece os princípios relativos ao tratamento de dados pessoais em seu artigo 5, quais são: princípio da legalidade, equidade e transparência; princípio da limitação da finalidade; princípio da minimização dos dados; princípio da exatidão; princípio da limitação do armazenamento; princípio da integridade e confidencialidade; e por fim, princípio da responsabilidade.

O princípio da legalidade, equidade e transparência[157] determina que os dados pessoais sejam processados de forma lícita, justa e transparente perante o titular dos dados pessoais.

Isso significa que os dados pessoais deverão ser processados em conformidade com o RGPD, dentro das hipóteses de licitude de tratamento elencadas no art.6º. De

---

traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p. 21.

[156] NETmundial : declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF, p.22.

[157] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN. Acesso em 3 de maio de 2021.

acordo com Vainzof "[...] os responsáveis somente poderão tratar dados dos titulares quando houver uma permissão e fundamentação legal para tal finalidade, notadamente com base no GDPR" [158].

Nesse aspecto, os responsáveis pelo processamento devem possuir a permissão dos titulares, bem como comunicá-los sobre coleta, uso, armazenamento e descarte desses dados, ou seja, estabelecer uma relação transparente com titular dos dados pessoais. Para Vainzof, "[...] a transparência perante o titular, municiando-o com informações apropriadas, ao ponto de empoderá-lo suficientemente para a tomada decisões conscientes."[159].

A transparência também impõe que as informações sejam repassadas para os titulares dos dados pessoais de forma clara, simples e de fácil compreensão, cientificando-os sobre a finalidade do tratamento, duração, armazenamento e descarte, observando as obrigações de transparência previstas no art.13 do RGPD[160].

O princípio da limitação da finalidade[161] estabelece que os dados coletados sejam para fins específicos, explícitos e legítimos, sendo inadmissível, em momento posterior, que os dados sejam processados de forma incompatível com as finalidades iniciais.

Neste princípio, a limitação da finalidade está relacionada com *privacy by design*, segundo Vainzof[162] a proteção é desde a concepção do projeto, a coleta de dados e os propósitos específicos almejados deverão ser analisados pelos *controllers* e informados ao titular de modo transparente, inclusive, utilizarem técnicas organizacional

---

[158]VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018, p.51.

[159] VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018, p.52

[160] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021

[161] Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021 "Art.5- 1 (b) coletados para fins específicos, explícitos e legítimos e não processados de maneira que seja incompatível com esses fins; mais distante em processamento para fins de arquivo de interesse público, os fins de investigação científica ou histórica ou os estatísticos não devem, nos termos do artigo 89.º, n.º 1, ser considerados incompatíveis com os objetivos iniciais («limitação da finalidade»);"

[162] VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018, p.57

para garantir que os dados sejam tratados para cada finalidade específica do tratamento, por *privacy by default*, nos termos do art.25 (2) do RGPD.

Quanto ao princípio da minimização dos dados[163], observa-se que este determina que o tratamento dos dados seja adequado, relevante e limitado ao necessário para alcançar os fins a que se destina o tratamento.

O princípio da exatidão[164] prevê que deve ser tomada todas as medidas razoáveis para que não hajam dados pessoais inexatos, possibilitando que estes sejam atualizados ou mesmo apagados.

Esse princípio fortalece a autodeterminação informativa, uma vez que viabiliza a retificação dos dados pelo titular, para que corresponda com a própria pessoa, por outro lado, impõe aos responsáveis pelo tratamento de dados a adoção de medidas que permitam a atualização ou a remoção das informações inexatas, conforme Vainzof:

> [...] princípio da exatidão nos evidencia de forma bastante cristalina que a proteção de dados pessoais não está apenas preocupada com a privacidade dos titulares, mas também com a sua identidade, pois dados inexatos, imprecisos ou incompletos podem revelar, principalmente perante terceiros, um prolongamento equivocado da identidade da pessoa natural, com resultados potencialmente catastróficos, mormente em casos de *profiling*, *scoring* ou histórico de saúde[165].

Assim, esse princípio busca garantir que as informações obtidas sejam reflexos exatos e precisos da identidade da pessoa titular dos dados, por isso, a possibilidade de retificação, complementação ou até mesmo deletar a informação inexata.

Já o princípio da limitação de armazenamento[166] dispõe que os dados pessoais sejam armazenados de modo que permita a identificação dos seus titulares durante o

---

[163] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.202.

[164] Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021 "Art.5 (1) (d) Exatos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);".

[165] VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018, p. 65.

[166] Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva

período determinado para alcançar os fins os quais se destinam os dados tratados, apenas para fins exclusivamente de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos, é que os dados podem ser armazenados por tempo maior, nos termos do art. 89 (1) do RGPD.

Dessa forma, como alerta Vainzof "[...] quaisquer políticas empresariais baseadas em "reter tudo", possivelmente serão consideradas ilícitas"[167], justamente por não cumprir o disposto no aludido Regulamento.

O princípio da integridade e confidencialidade[168] diz que os dados pessoais deverão ser processados de forma a garantir a sua segurança adequada, resguardando também os dados não autorizados ou ilegais em processamento e contra perda acidental, destruição ou dano, para isso é preciso implementar medidas técnicas e organizacionais para proteger os dados e evitar incidentes.

Esse princípio visa proteger o titular dos dados dos impactos ocasionados pelos incidentes envolvendo o tratamento de dados, bem como impõe a adoção de medidas que sejam capazes de proteger os dados, bem como minimizar os riscos em situações de incidentes.

E, por fim, o princípio da responsabilização que diz: "Art.5º (2). O controlador deve ser responsável e ser capaz de demonstrar o cumprimento do disposto no n.º 1 («responsabilização»)"[169], pode-se inferir que o controlador sempre será

95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021 "Art.5 (1) (e) mantidos de uma forma que permita a identificação dos titulares dos dados por um período não superior ao necessário para os fins para os quais os dados pessoais são tratados; os dados pessoais podem ser armazenados por períodos mais longos, desde que sejam processados exclusivamente para fins de arquivamento de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos, de acordo com o Artigo 89 (1), sujeito à implementação de procedimentos técnicos e organizacionais apropriados medidas exigidas pelo presente regulamento para salvaguardar os direitos e liberdades do titular dos dados («limitação de armazenamento»);"

[167] VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018, p.62

[168] Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021 "Art.5 (1) (f) processado de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra dados não autorizados ou ilegais em processamento e contra perda acidental, destruição ou dano, usando medidas técnicas ou organizacionais apropriadas ('integridade e confidencialidade')."

[169] [169] REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-

responsável pelo cumprimento de todos os princípios estabelecidos no RGPD, supramencionados.

3.3.4 Princípios da Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados é uma regulamentação principiológica, assim como é a regulamentação sobre proteção de dados na União Europeia, ambas inseriram um bojo de princípios que precisam serem observados e atendidos.

Os princípios da Lei Geral de Proteção de Dados e a boa-fé deverão ser observados nas atividades de tratamento de dados pessoais, nos termos do art. 6º[170], estabelecendo dez princípios que devem ser interpretados de forma mais benéfica ao titular dos dados, são eles: o princípio da finalidade; o princípio da adequação; o princípio da necessidade; o princípio do livre acesso; o princípio da qualidade dos dados; o princípio da transparência; o princípio da segurança, o princípio da prevenção; o princípio da não discriminação; e por fim, o princípio responsabilização e prestação de conta.

O princípio da finalidade, estabelecido pela aludida lei, diz que o tratamento precisa ter propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior que seja realizado de forma incompatível com essas

content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021

[170] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "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, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; 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, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; 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 a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

finalidades que foram informadas ao titular[171]. Segundo Belli, "[...] a possibilidade de "reaproveitar" dados previamente coletados deve ser considerada como compatível com a LGPD somente na medida em que o princípio de finalidade, explicitado pelo art.6.I da Lei, seja plenamente respeitado"[172].

Pode-se extrair que o tratamento deve ser realizado de forma compatível com os fins legítimos, específicos, explícitos, bem como de acordo com as informações fornecidas previamente ao titular, isso inibe uma utilização indevida, que ultrapassa a própria finalidade informada, e que impossibilita uma legalidade ao tratamento.

O princípio da adequação determina a compatibilidade do tratamento com as finalidades informadas ao titular, considerando o contexto do tratamento[173], este princípio encontra-se vinculado com o da finalidade.

A adequação refere-se ao tratamento de dados pessoais que é feito de forma compatível com a finalidade, isso significa que o uso deve ser adequado ao que foi informado ao titular, se houver desconformidades, não há que se falar em adequação, visto que a atividade de tratamento tem que possuir um propósito e este deve ser devidamente informado ao titular.

Nesse sentido, o princípio da necessidade estabelece a limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos[174].

Este princípio limita o tratamento de dados ao mínimo necessário para alcançar sua finalidade, consiste numa verdadeira proteção contra o uso excessivo e desproporcionais dos dados pessoais. Assim, pode-se inferir que os três princípios, finalidade, adequação e necessidade, estão interligados.

---

[171] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

[172] BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.399.

[173] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

[174] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

Já o princípio do livre acesso, trata-se de uma garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração sobre o tratamento e a integralidade de seus dados[175].

Esse princípio garante ao titular a possibilidade de acompanhar e obter informações sobre a forma, duração e integridade de seus dados, visa reduzir a assimetria informacional, para que o titular possa ter acesso e conhecimento sobre o uso de seus dados pessoais. O art.9º da LGPD[176], fortalece o princípio do livre acesso, ressaltando que o direito ao acesso deve ser viabilizado de forma clara, adequada e ostensiva, bem como outras informações pertinentes acerca de tratamento e agentes de tratamento.

O princípio da qualidade é também uma garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, levando-se em consideração a necessidade e finalidade para o tratamento.

Assim como o princípio anterior, trata-se de uma garantia ao titular de ter seus dados correspondendo a com a realidade, tendo em vista que as informações contidas nestes dados poderão afetar a vida dos próprios titulares, por expressar aspectos da sua personalidade. Dessa forma, o princípio da qualidade de dados garante ao indivíduo o direito de ter suas informações atualizadas, correspondendo com a personalidade de cada pessoa titular dos dados em tratamento, protegendo, portanto, a autodeterminação informacional.

O princípio da transparência é uma garantia aos titulares, de obterem informações claras, precisas e facilmente acessíveis relativos à realização do tratamento, bem como sobre os agentes de tratamento, resguardados os segredos comercial e industrial[177].

---

[175] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

[176] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020."Art.9º 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 acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: 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. [...] § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

[177] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

O princípio da transparência visa proteger a privacidade e o livre desenvolvimento da personalidade, uma vez que é uma garantia aos titulares de que será informado de forma clara, precisa e facilmente acessível sobre os dados submetidos a tratamento. Chama-se atenção para a possibilidade de utilização do *legal design* e/ou *visual law* como forma de tornar o conteúdo acessível ao leigo, por meio de uma linguagem clara, simples e com uso de elementos do *design*, visando melhorar a experiência do usuário.

Deve-se ressaltar, ainda neste princípio, que tem-se uma proteção do ser humano de ser perfilado por empresas e Estado de forma oculta, inadequada, sem transparência com o titular dos dados pessoais, provocando uma assimetria informacional.

O princípio da segurança estabelece a "[...] utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[178].

Esse princípio busca resguardar o titular dos dados dos riscos presentes nas atividades de tratamento seja no meio físico ou digital, dando primazia a um ambiente seguro, mas caso não ocorra, que haja responsabilização administrativa e civil, conforme o caso. Desse modo, se exige uma adoção de cuidados e medidas por aqueles que realizam atividades de tratamento de dados, inserindo-se, os requisitos de segurança, boas práticas e governança estabelecidos pela LGPD.

O princípio da prevenção, estabelece a "[...]adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"[179]. Este princípio determina a adoção de medidas capazes de prevenir danos aos titulares, como a prevenção de vazamentos de dados, de violação e outras formas que coloquem em risco os dados pessoais. É neste aspecto que o *privacy by design* é extraído da LGPD, tal conceito será analisado no próximo capítulo.

O princípio da não discriminação determina a "[...] impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos"[180]. Este princípio busca

---

[178] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

[179] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

[180] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

inibir o tratamento de dados para fins discriminatórios, ilícitos ou abusivos, isto é, que seja realizado em desconformidade com a legislação, configurando práticas discriminatórias, sobretudo, no que diz respeito aos dados sensíveis, que afeta a própria dignidade da pessoa humana.

Por fim, o princípio da responsabilização e prestação de contas, determina que haja a "[...] 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"[181].

Conhecido como princípio do *accountability*, trata-se da possibilidade de exigir a demonstração dos responsáveis pelo tratamento de dados da adoção de medidas eficazes e que observem o disposto na lei geral de proteção de dados, ou seja, demonstrar que o tratamento é realizado em conformidade com a LGPD.

Portanto, é necessário refletir sobre a proteção dos dados pessoais, privacidade e o livre desenvolvimento da personalidade no contexto de inovações tecnológicas utilizados nas atividades empresariais. Tais princípios desempenham um papel fundamental para a organização das empresas no que diz respeito à adequação às diretrizes previstas na legislação, norteando para a conformidade das atividades com os critérios legais e visando a proteção dos dados pessoais.

Por isso, não se pode falar de tratamento e adequação por *compliance*, sem antes compreender a importância dos princípios na proteção dos dados pessoais, aliás, proteção da vida do indivíduo em se autodeterminar, em ter o controle sobre suas informações e dados pessoais. Sendo assim, passa-se a análise das normas que regem o tratamento de dados, bem como a adequação através da governança de dados.

4. TRATAMENTO E GOVERNANÇA DOS DADOS PESSOAIS

São cada vez mais frequente as notícias sobre os vazamentos de dados, segundo um estudo realizado pelo Massachusetts Institute of Tecnology – MIT indica que os

[181] BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

vazamentos de dados aumentaram em 493% no Brasil, uma estimativa de mais de 205 milhões de dados de brasileiros referentes ao ano de 2019[182].

Em 2021, foram revelados pela mídia mais dois megavazamentos de dados que expôs 220 milhões de brasileiros, com dados sobre telefone, endereço, e-mail, *score* de crédito, foto de rosto, CPF e outros dados pessoais, essas informações estão disponíveis na internet aberta, em relação ao segundo vazamento, consiste em informações de 223,74 milhões de pessoas, mas diferente do outro, este possui um "prévia" disponível, mas o pacote completo de informações são comercializados a depender da quantidade e o pagamento é feito por criptomoeda, ambos vazamentos aparentemente teriam sido compilações realizada em 2019[183].

O que são feitos com esses dados? As evidências que são reportadas pelas mídias sociais apontam que os dados pessoais vazados são comercializados na *dark web* ou mesmo encontram-se disponíveis livremente na internet[184] apresentando inúmeras possibilidades de utilização e facilitação de golpes e outros cibercrimes por quem detém a posse desses dados, violando os direitos fundamentais dos titulares.

São graves os incidentes de segurança da informação envolvendo os dados pessoais noticiados pela mídia, até mesmo depois da entrada em vigor da LGPD. Percebe-se que, o ideal era que durante *vacation legis,* o período fosse utilizado para as organizações se adaptarem antes da entrada em vigor da lei, inclusive, com orientações da própria ANPD, mas não foi esta a realidade.

Uma hipótese que pode ter contribuído para isso, foi a criação "tardia" da Autoridade Nacional de Proteção de Dados, visto que a criação e estruturação ocorreu praticamente junto com a vigência da lei. Desse modo, as tomadas de ações e orientações para uma "preparação" antes da vigência da lei não foi possível e sob este pretexto muitas

---

[182] FOTIOS, Ricardo. Vazamentos de dados aumentaram 493% no Brasil, mostra pesquisa do MIT: Base construída por pesquisador brasileiro identifica mais de 26 bilhões de informações à disposição de criminosos no mundo em dois anos. **Coluna Ricardo Fortios: Cultura. UOL**, online. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-de-dados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html Acesso: 10.jun.2021

[183] VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava**:**Vazamento inclui CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais; Serasa nega ser fonte dos dados. **Tecnoblog**. 2021, online. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/ Acesso: 10.jun.2021

[184] VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava**:**Vazamento inclui CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais; Serasa nega ser fonte dos dados. **Tecnoblog**. 2021, online. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/ Acesso: 10.jun.2021

empresas permaneceram inertes sem realizar a adequação à LGPD durante o *vacation legis*.

Sobre os casos de incidentes frequentemente noticiados, além de evidenciar a ausência da cultura de proteção de dados pessoais, pode-se atribuir um duplo papel, conforme Souza, primeiro demostram que "[...] empresas, governos e entidades da sociedade civil ainda têm muito que fazer em termos de segurança e sigilo de dados. Por outro, a insistente comunicação sobre a ocorrência de vazamentos de dados pode ajudar na conscientização sobre a importância do tema"[185].

Além disso, Medeiros e Goldoni[186] destacam que no Livro Branco 5 da Defesa Nacional 2016, há o reconhecimento de que o ciberespaço possibilita ameaças estatais e não estatais, conforme explicam os autores, uma ameaça cibernética é motivo de preocupação por colocar em risco a própria integridade de infraestruturas sensíveis e, que são mesmo tempo, essenciais para a operação e controle de diversos ourtos sistemas relativos a própria segurança nacional, por isso, afirmam que o ciberespaço é considerado um domínio estratégico.

A segurança da informação e privacidade dos dados é importante para o titular por razões de autodeterminação informativa, privacidade, liberdade e que outros direitos não sejam afetados, é também do interesse das empresas pelo aspecto reputacional da tratativa de dados, pelo receio de sofrer sanções, e não conseguir firmar ou renovar contratos com outras empresas e/ou poder público em decorrência de ausência de adequação à lei geral de proteção de dados pessoais.

Nesse aspecto, Souza afirma que medidas de segurança e de sigilo de dados devem ser incentivadas e seguidas, cabendo a legislação "[...] garantir que as condições para a implantação dessas medidas sejam estimuladas não apenas pelo receio de futuras sanções, mas também como parte essencial de um dever de cuidado que deve instruir toda relação que envolva tratamento de dados"[187].

---

[185] SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[186] MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace*. **Contexto Internacional** , v. 42, n. 1, pág. 31-54, 2020, p.34.

[187] SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

Nesse contexto, em que grande parte das atividades são realizadas no espaço virtual, deve-se identificar os possíveis riscos e aderir mecanismos e sistemas para minimizar as vulnerabilidades existentes e, consequentemente, evitar vazamentos e incidentes de dados pessoais. Por isso, que a Lei Geral de Proteção de Dados estabelece um Capítulo "Da Segurança e das Boas Práticas", que trata da adoção de segurança e sigilo de dados e das boas práticas e governança de dados.

Uma vez que os vazamentos e outros incidentes são problemas ocasionados por falhas na segurança da informação e proteção de dados pessoais, denotam necessidade de adoção de medidas de adequação à Lei Geral de Proteção de Dados Pessoais, lei que já se encontra em vigor. Por isso, para fins desta pesquisa, tem-se como importante identificar e apresentar *standars* para segurança da informação e sigilo dos dados, desenvolver a governança de dados com utilização *nudges* de privacidade e proteção de dados, bem como tratar do papel da Autoridade Nacional na construção da cultura da privacidade e proteção de dados pessoais no Brasil.

5.1 As bases legais para o tratamento de dados pessoais por agente privados

A Lei Geral de Proteção de Dados considera tratamento de dados qualquer atividade que envolva a "[...]coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"[188] nos termos do Art. 5º, X.

Sobre as operações de tratamento dos dados pessoais, conforme Belli existe um "clima" de confiança recíproca estabelecido entres os titulares e os agentes de tratamento, isso acontece porque as leis de proteção de dados buscam favorecer um ambiente juridicamente seguro. Os titulares de dados pessoais passam ter a garantia de que as medidas necessárias serão adotadas para evitar que os dados sejam perdidos, divulgados ou processados, assim, as entidades beneficiam-se desse ambiente juridicamente seguro para realizarem suas atividades de tratamento de dados pessoais [189].

---

[188] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º [...] X - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"

[189] BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.393-394.

O tratamento de dados pessoais deve ser realizado em observância a boa-fé e aos princípios estabelecidos na Lei Geral de Proteção de Dados Pessoais[190], e deve ser de acordo com as hipóteses nela previstas. Pode ser realizado pelo consentimento do titular que deverá atender aos princípios da LGPD e as finalidades específicas e informadas ao titular, mas a lei também possibilita algumas hipóteses em que o tratamento de dados pessoais poderá ocorrer sem que haja o consentimento do seu titular.

São situações que dispensam o consentimento do titular previstas no Art. 7º, tais como para fins de "[...] cumprimento de obrigação legal ou regulatória pelo controlador", nos casos em que for "[...] necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato". Assim como para o "[...]exercício regular de direitos em processo judicial, administrativo ou arbitral", quando forem destinados "para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais". Nas situações que envolvem a "[...] proteção da vida ou da incolumidade física do titular ou de terceiro", nesse sentido, também quando for "[...]para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária". É possível "[...] 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", por fim, "[...] para a proteção do crédito"[191].

---

[190] Como foi dito no capítulo anterior, a LGPD estabelece um bojo de princípios para nortear as atividades de tratamento de dados pessoais, são os princípios: da finalidade, da adequação; da necessidade; do livre acesso; da transparência; da segurança; da responsabilização e da prestação de contas.

[191] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência IX - 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 X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.", algumas das hipóteses são aplicadas ao poder público ou pesquisa, que não serão tratadas nesta dissertação, um vez que a delimitação é para o setor privado."

Nas situações, em que o controlador obteve o consentimento do titular nos termos do art.7º, inciso I da LGPD, e, por conseguinte, necessitar comunicar ou compartilhar dados pessoais com outros controladores, será preciso obter consentimento específico do titular para essa finalidade. A lei deixa claro, que essa exigência não se aplica para os casos em que é dispensado o consentimento do titular, mas que não implica na inobservância dos princípios gerais e direitos do titular, conforme disposto no art. 7º, §6º da LGPD.

Em relação ao consentimento do titular para fins de tratamento, a LGPD exige que seja fornecido de forma escrita ou por outro meio que seja capaz de demonstrar a manifestação da vontade do titular[192]. Uma observação, é que se o consentimento for por escrito, é necessário constar em uma cláusula destacada das demais[193].

Ao controlador recai o ônus probatório de que o consentimento foi obtido em conformidade com a Lei Geral de Proteção de Dados. Nesse aspecto, para obter o consentimento é preciso informar as finalidades determinadas, uma vez que as autorizações genéricas para o tratamento de dados pessoais serão nulas nos termos do Art.7º, §4 da LGPD. Também é vedado o tratamento de dados pessoais que for realizado por vício de consentimento[194], essa norma deve ser interpretada juntamente com os vícios de consentimento do Código Civil.

Além disso, o consentimento do titular pode ser revogado, por manifestação expressa, de forma gratuita e facilitada. Contudo, é importante compreender que o tratamento que foi realizado sob o consentimento dado anteriormente é ratificado enquanto não for solicitada a exclusão, conforme o art. 8º, §5º da LGPD[195].

---

[192] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular."

[193] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 8º [...]§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais."

[194] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 8º [...]§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento."

[195] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.8º [...] § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei".

Ocorrendo alguma mudança nas situações dos incisos I, II, III ou V do 9º da LGPD, que refere-se aos princípio do livre acesso[196], é dever do controlador informar ao titular, destacando as alterações ocorridas de forma específica, podendo o titular, nos casos em que é necessário o consentimento, revogá-lo se entender por discordar, conforme o Art.8º, §6º[197].

O consentimento poderá ser considerado nulo nas situações em que "[...] as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"[198]. Além disso, quando houver mudanças na finalidade do tratamento realizado e que não seja compatível com consentimento original, é dever do controlador informar de forma prévia o titular sobre as modificações na finalidade, para que o titular, caso discorde, possa revogar seu consentimento[199].

Desse modo, quando for necessário o consentimento do titular para a realização do tratamento de dados ou quando for preciso informá-lo sobre alterações da finalidade do tratamento, esse consentimento deverá ser obtido em atenção aos princípios estabelecidos na LGPD, principalmente, o princípio da transparência que impõe a garantia de informações clara, precisas e facilmente acessíveis aos titulares. Para isso, pode-se utilizar do *legal design* e *visual law* para facilitar a compreensão do leigo, transformando a comunicação técnica em uma comunicação mais empática e assertiva, pois o documento idealizado com base na experiência do usuário.

O *legal design* se baseia, conforme Maia, Nybo e Cunha "[...] na ideia de que produtos e processos funcionais e bem projetados devem ser acessíveis e disponibilizados a todos. Podemos e devemos exigir soluções esteticamente mais agradáveis, fáceis de

---

[196] Cf. o capítulo 3, no que se refere aos princípios da LGPD.

[197] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.8º§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração."

[198] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 9º […] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca."

[199] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.9º [...] § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações."

usar e atratativas para nossos problemas jurídicos diários"[200]. Criando, assim, documentos intuitivos e acessíveis ao leigo.

Em relação ao legítimo interesse do controlador para o tratamento de dados pessoais, este somente poderá ser utilizado nos termos do Art. 10 da LGPD, que refere-se as finalidades legítimas e consideradas diante da situação concreta, que inclue e não se limita ao "[...] apoio e promoção de atividades do controlador[...]proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais"[201].

Nesse caso, apenas haverá o tratamento dos dados pessoais necessários para aquela finalidade pretendida, sendo dever do controlador a adoção de medidas visando garantir a transparência do tratamento quando este é realizado baseado em seu legítimo interesse. Ressalta-se que, nos casos de tratamento com base em interesse legítimo do controlador, a ANPD poderá solicitar ao controlador o relatório de impacto à proteção de dados pessoais, devendo-se observar os segredos comercial e industrial.

Sobre esse aspecto, Belli sustenta que a análise de impacto sobre a privacidade deveria ser imprescindível, para as situações em que o controlador fosse implementar um tratamento de dados com base no legítimo interesse. Para o autor a hipótese prevista no no art.7.º, IX, da LGPD, é abrangente e flexível, visto que não há um detalhamento das situações em que poderá ser usado o legítimo interesse, por isso, se pressupõe a elaboração do relatório de impacto à proteção, vez que pode ser solicitado pela ANPD[202].

Em relação ao tratamento de dados pessoais sensíveis, este é mais restrito e somente poderá ocorrer nas hipóteses de consentimento do titular ou de seu responsável legal, feita de forma específica e destacada, constando as finalidades específicas do tratamento, e nas situações em que é dispensado o consentimento do titular, sendo necessário atender algum dos requisitos previsto no art.11 da LGPD[203].

---

[200] MAIA, Ana Carolina; NYBO, Erik Fontenele; CUNHA, Mayara. ***Legal Design***: Criando Documentos que fazem sentido para os usuários. São Paulo, SP: Saraiva Educação, 2020 [Ebook] p.i.

[201] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 10. [...]I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei."

[202] BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.395.

[203] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 11 [...] a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas

A Autoridade Nacional poderá vedar ou regulamentar a comunicação e a utilização compartilhada de dados pessoais sensíveis entre os controladores para fins de vantagem econômica, mas para isso será ouvido os órgãos setoriais do Poder Público[204]. Todavia, em relação os dados sensíveis de saúde a LGPD veda a comunicação ou uso compartilhado entre controladores de dados para fins de obtenção de vantagem econômica, com ressalvas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, os serviços auxiliares de diagnose e terapia, realizados em benefício dos titulares de dados[205].

Nesse aspecto, é interessante observar que a LGPD veda o tratamento de dados de saúde por operadoras de planos privados de assistência à saúde para fins de seleção de riscos na contratação e exclusão de beneficirários[206], protegendo o titular de possíveis discriminações.

Sobre o tratamento de dados pessoais de crianças e de adolescentes[207], impõe dizer que deverá ser realizado em seu melhor interesse, em consonância com a legislação

---

em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

[204] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 11 [...]§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências."

[205] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 11[...]§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.(Incluído pela Lei nº 13.853, de 2019)".

[206] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 11 [...] § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)"

[207] Deve-se esclarescer que não haverá aprofundamento no tratamento de dados de crianças e adolescentes em razão da delimitação do assunto desta dissertação. Mas, convém observar que o tratamento de dados de crianças e adolescentes deve ser analisado não apenas pela LGPD, mas em conjunto com o Estatuto da Criança e do Adoslecente e a Constituição, em atenção a teoria do diálogo das fontes.

pertinente e com a própria LGPD, sendo necessário o consentimento específico e destacado fornecido por um dos pais ou pelo responsável legal pelo menor, cabendo ao controlador utilizar de meios razoáveis para verificar se o consentimento foi dado pelo responsável legal[208].

Um aspecto que deve ser destacado sobre o término do tratamento, a lei disciplina que o fim acontece nas situações em que a finalidade almejada foi alcançada, ou quando os dados não são mais necessários para atingir a finalidade do tratamento,ou quando chega ao fim o período do tratamento, bem como, nas situações em que o titular revoga o consentimento, ressalvado o interesse público e, por fim, quando houver determinação da Autoridade Nacional por ocorrência de violação ao disposto na LGPD[209].

Todavia, é autorizada a conservação dos dados após o término de seu tratamento quando for para o cumprimento de obrigação legal ou regulatória, para fins de estudo por órgão de pesquisa, sendo anonimizados sempre que possível, em situações de transferência a terceiro, e pelo uso exclusivo do controlador, com anonimização dos dados[210], por isso, é importante conhecer a necessidade do dado e o período de sua conservação.

Essa compreensão sobre as bases legais de tratamento de dados pessoais é necessária para que se possa desenvolver o tópico sobre governança de dados, mas antes, será abordado os papéis dos agentes de tratamento e do encarregado (ou DPO).

---

[208] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 14 [...] § 1º 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.[...] § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.".

[209] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ouIV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei."

[210] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

5.2 Os papéis dos agentes de tratamento e do encarregado

Os agentes de tratamento possuem conceitos e funções diferentes em relação ao tratamento de dados, ou seja, o controlador assume uma função distinta do operador, embora ambos sejam considerados agentes de tratamento de dados[211]. Assim, a Lei Geral de Proteção de Dados define o controlador como "[...]pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"[212], é responsável por determinar o tratamento de dados com objetivo de atingir finalidades específicas.

Já o operador é definido como "[...] pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"[213]. Sendo função do operador fazer o tratamento de dados de acordo com as instruções que são estabelecidas pelo controlador, bem como em observância as próprias instruções e as normas sobre a matéria[214].

Ressalta-se que, o encarregado não é considerado agente de tratamento pela LGPD, mas sim uma "[...] pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)"[215], pode ser uma pessoa física ou jurídica[216], esta última, todavia, não pode gerar óbice para o contato do titular, ou seja, mesmo sendo uma pessoa

---

[211] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art.5º [...] IX - agentes de tratamento: o controlador e o operador;"

[212] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art.5º [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;"

[213] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art.5º [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;"

[214] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "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."

[215] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 5º [...] VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);"

[216] Nesse sentido, entendem CARVALHO; MATTIUZZO; PONCE que "[...] o encarregado pode ser pessoa física ou jurídica, interna ou externa. CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.371.

jurídica é necessário que fique claro ao titular quem é o responsável pelo canal de comunicação, ou seja, quem exerce o papel do encarregado.

O encarregado pode ser interno ou externo à empresa, caso o controlador faça a opção por ter um encarregado interno é necessário que seja resguardada a independência e autonomia dentro da empresa. Carvalho, Mattiuzzo e Ponce[217] acrestam que além da indepencia e autonomia, o encarregado tem que ter um financiamento adequado para que possa desenvolver suas atividades de tomada de decisões.

Em relação ao encarregado, este é indicado pelo controlador para ser o canal de comunicação entre o controlador, titular e Autoridade Nacional. Para isso, a identificação e informações de contato do encarregado deverão ser divulgadas, de forma pública, clara e objetiva, constando, preferencialmente, no *site* do controlador[218].

As funções do encarregado consistem em receber as reclamações e comunicações dos titulares, e fornecer esclarecimentos e adotar providências, assim como, receber as comunicações feitas pela Autoridade Nacional e adotar providências solicitadas, deve orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, por fim, executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares[219], ou que sejam estabelecidas pela Autoridade Nacional.

Conforme Carvalho, Mattiuzzo, Ponce[220] para que o encarregado possa executar suas funções, é necessário que existam canais de comunicação acessíveis tanto por titulares de dados pessoais, quanto por funcionários e a própria Autoridade, pois além de ser uma obrigação legal, eles possibilitam a resolução de dúvidas dos funcionários e

---

[217] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.371.

[218] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador."

[219] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020 "Art. 41 [...] § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os 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."

[220] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.371.

colaboradores, comunicação com os titulares e comunicação de possíveis ilícitos para ANPD.

Sobre a função do encarregado, observa-se que a ANPD ainda poderá fazer várias normas complementares, até mesmo definir quando pode ser dispensado a função do encarregado para empresa. De acordo com Carvalho, Mattiuzzo e Ponce[221] mesmo que a Autoridade Nacional indique as hipóteses de dispensa da necessidade do encarregado, levando-se em consideração a própria natureza ou o porte das empresas e também o volume das operações de tratamento de dados, é recomendável que haja o encarregado para fins de estruturação de programas de conformidade da empresa.

Outro aspecto relativo ao encarregado, é que não existe um requisito legal de formação para o exercício da função, mas por razões lógicas e de responsabilidade o encarregado precisa ter o conhecimento da proteção de dados pessoais, até mesmo para que ela possa auxiliar a implementação da proteção de dados e promover o diálogo entre o titular e controlador, controlador e ANPD. Para Carvalho, Mattiuzzo e Ponce, "[...] é interessante que o encarregado tenha formação específica no tange à proteção de dados pessoais, para que possa orientar a implementação do programa de forma adequada"[222].

Devido às incertezas relativas aos agentes de tratamento e encarregado a ANPD publicou o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[223]. De início, já esclarece que os agentes de tratamento devem ser definidos pelo seu caráter institucional, sendo assim, não podem ser considerados controladores ou operadores os indivíduos que sejam subordinados, ou seja, funcionários, os servidores públicos ou as equipes de trabalho de uma organização[224].

Quando se trata de pessoa jurídica, a própria organização é o agente de tratamento, pois estabelece as regras sobre o tratamento de dados pessoais[225]. Um detalhe

---

[221] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.371.

[222] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.371.

[223] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[224] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021, p.5. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021.

[225] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021.

importante é que a mesma organização poderá ser controladora e operadora conforme a sua atuação na operação de tratamento.

As pessoas naturais podem ser consideradas controladoras ou operadoras de dados pessoais. Serão consideradas controladoras quando atuarem por seus próprios interesses, possuírem poder de decisão sobre as finalidades e os elementos essenciais de tratamento. Todavia, serão operadoras quando atuarem conforme os interesses do controlador, sendo assim, o operador deverá ser distinto do controlador, já os funcionários, por sua vez, atuam em subordinação às decisões do controlador e não se confundem com os operadores[226].

A ANPD definiu a controladoria conjunta, pois tal conceito não se encontra explicito na LGPD. Sendo assim, considera-se controladoria conjunta quando existe uma participação conjunta na determinação das finalidades e meios de tratamento de dados, sem a necessidade de que cada controlador determine todos os elementos envolvidos em uma operação de tratamento, só não haverá controladoria conjunta se os objetivos do tratamento forma distintos[227].

Em relação ao operador, este se diferencia do controlador por agir no limite das finalidades determinadas pelo controlador. A ANPD destaca algumas obrigações dos operadores: "(i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador"[228]. Embora a LGPD não determine a existência de contrato entre os agentes de tratamento, esse documento se revela importante para determinar o objeto, duração e finalidades e tratamento de dados pessoais[229].

Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[226] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[227] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[228] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[229] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

Outro aspecto controverso, mas que foi esclarecido pela Autoridade, diz respeito ao suboperador, isso porque não tem previsão legal, mas também não havia proibição da existência de suboperador. Desse modo, é considerado suboperador "aquele que contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador", existindo uma relação direta entre o operador e o suboperador. A ANPD reforça a importância de uma autorização formal do controlador ao operador para que este possa contratar o suboperador[230].

Em relação ao encarregado, este não é um agente de tratamento, deve ser indicado pelo controlador, como regra geral, toda organização deve indicar um encarregado. Nota-se que a ANPD poderá em normativas futuras dizer as hipóteses de dispensa.

A ANPD ressaltou dois aspectos, o primeiro, é sobre a possibilidade do encarregado ter uma equipe de proteção, em atenção as boas práticas e não existir proibição pela LGPD, já a segunda, refere-se a escolha do encarregado, ainda que não exista restrições para ser encarregado de outras organizações concomitantemente, é importante este possa desempenhar suas atribuições com eficiência[231].

Ao controlador cabe a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que se trata de um documento que deve apresentar a descrição dos processos de tratamento de dados pessoais que são capazes de ocasionar riscos às liberdades civis e aos direitos fundamentais, inclusive, deve dispor sobre as medidas, salvaguardas e outros mecanismos para fins de mitigação de risco[232], bem como a metodologia utilizada para coleta dos dados e segurança da informação[233].

---

[230] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[231] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021

[232] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 5º [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;"

[233] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 38 [...]Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a

É função do controlador a elaboração o RIPD, uma vez que a Autoridade Nacional "poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial"[234].

Além disso, quando o titular for afetado em seus interesses, poderá exercer o direito de solicitar as revisões de decisões tomadas unicamente baseadas em tratamento automatizado de dados, cabendo ao controlador fornecer, quando assim for solicitado, as informações claras e adequadas sobre os critérios e procedimentos da decisão automatizada, resguardado o segredo comercial e industrial[235].

Cabe aos agentes de tratamento nos termos da LGPD, "[...] manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse"[236], esse registro refere-se ao *data maping*[237].

Sob a responsabilidade dos agentes de tratamento, a LGPD estabelece que em decorrência do tratamento de dados pessoais, causar danos patrimonial, moral, individual ou coletivo a outrem é obrigado a reparar[238]. O controlador e o operador não serão responsabilizados quando provarem que "[...] não realizaram o tratamento de dados pessoais que lhes é atribuído" "[...]que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;" "ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."

---

garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

[234] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial."

[235] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial."

[236] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "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.

[237] Termo utilizado para se referir ao mapeamento do tratamento de dados."

[238] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "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."

Assim, nas situações em que o tratamento de dados pessoais for irregular[239], o controlador será responsável pelos danos decorrentes da violação da segurança dos dados, já o operador será responsável quando deixar de adotar as medidas de segurança e provocar o dano[240].

Na ocorrência de incidente[241] de segurança que seja capaz de provocar risco ou danos relevantes aos titulares, o controlador tem o dever de comunicar a Autoridade Nacional, ressalta-se que a LGPD não estabeleceu o prazo dessa comunicação deixando para que ANPD estabeleça qual seria o prazo razoável.

Dessa forma, mesmo que a Autoridade Nacional ainda não tenha regulamentado o prazo da comunicação, já se manifestou no sentido de que após a ciência do incidente e havendo risco relevante, a comunicação deverá acontecer com a maior brevidade possível, no prazo de 2 dias úteis, a partir da data do conhecimento do incidente. O prazo foi escolhido levando-se em consideração a necessidade do gerenciamento dos incidentes de segurança por parte da ANPD, bem como as consequências aos titulares[242].

A comunicação sobre a ocorrência do incidente feita do controlador à Autoridade Nacional e ao titular deve conter um conteúdo mínimo de informações relativas ao próprio incidente, como a descrição sobre a natureza dos dados, informações sobre os titulares, a indicação das medidas técnicas e de segurança, os riscos relacionados ao incidente, os motivos da demora, para os casos em que a comunicação não foi feita de forma imediata, bem como as medidas que serão ou já foram adotadas para reverter ou mitigar os efeitos decorrentes do incidente[243].

---

[239] A LGPD considera tratamento irregular quando: Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. (BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 13.out.2020).

[240] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 44 Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano".

[241] Entende-se por incidente um evento adverso e que há risco relevante ao titular dos dados pessoais, conforme consta no site da ANPD. Cf. BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso: 08.jun.2021.

[242] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso: 08.jun.2021.

[243] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em:

Em relação ao conteúdo mínimo que deve ser informado na comunicação sobre o incidente, a ANPD elaborou um "Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à Autoridade Nacional de Proteção de Dados (ANPD)"[244] que deve conter o tipo de comunicação, dados do agente de tratamento, do agente notificante e dados do encarregado, descrição do incidente de segurança com data e hora, o momento em que teve ciência sobre o ocorrido e esclarescimentos sobre a demora da comunicação, e outras informações pertinentes como a natureza dos dados afetados e quantidade e categoria dos titulares afetados, as medidas de segurança utilizadas na prevenção e após o incidente de segurança.

5.3 Da governança de dados pessoais

Uso de dados é o que movimenta a nova economia, mas o tratamento de dados pessoais não pode ser realizado em desconformidade com a Lei Geral de Proteção de Dados, sendo necessário garantir os direitos dos titulares e buscar minimizar os riscos inerentes às atividades de tratamento de dados, por isso, as empresas devem se adequar à LGPD.

A adequação, conforme Frazão, Oliva e Abilio[245] busca conferir efetividade aos direitos e a prevenção de danos, por meio da adoção de mecanismos de *compliance*[246]*,*

13.out.2020. "Art. 48 [...] § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;IV - os riscos relacionados ao incidente;V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo."

[244] Vide Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à Autoridade Nacional de Proteção de Dados (ANPD) – Anexo 1. BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso: 08.jun.2021.

[245] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[246] Entende-se por *compliance* que: "A palavra *compliance* significa, em tradução literal, estar em conformidade. Essa simples tradução, porém, esconde uma das maiores dificuldades da conceituação do termo: trata-se de um conceito relacional, cujo significado só acaba por ser descoberto, assim, por meio de um análise do objeto com o qual se relaciona, dado que, por óbvio, quem está "em conformidade" está "em conformidade" com "algo". *Compliance* estabelece uma relação, portanto, entre um "estado de conformidade" e uma determinada "orientação de comportamento". Se essa "orientação de comportamento" é uma norma jurídica, está-se diante de *compliance* jurídico, cuja designação varia conforme a área do direito, na qual a norma a ser seguida se insere". (SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.729.

como um instrumento operacional, preventivo e capaz de promover condutas compatíveis com os preceitos da LGPD.

Nesse cenário, a implementação de um programa de privacidade e proteção de dados deve atender não apenas a Lei Geral de Proteção de Dados, mas também as outras regulamentações e as particularidades do modelo de negócios, bem como observados os segredos comerciais e industriais. Pois, a LGPD possui "o desenvolvimento econômico e tecnológico e a inovação", "a livre iniciativa", "a livre concorrência" e entre outros como fundamentos[247], ou seja, a lei tenta "equilibrar" os direitos dos titulares com o desenvolvimento econômico. Nesse sentido Frazão, Oliva e Abilio afirmam que:

> A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus *standards* e conceitos abertos. Por se tratar de complemento à regulação estatal, apresenta, ainda, a capacidade de gerar incentivos que agregam e aprofundam controles, adaptando-lhes diante da natureza extremamente dinâmica das evoluções tecnológicas em matéria de dados[248].

Dessa forma, a adequação à LGPD implica adoção de boas práticas e governança nas empresas para fins de efetivação dos direitos dos titulares de dados, para isso são necessárias mudanças na empresa, sem, contudo, fulminar a organização.

Por isso, a governança de dados apresenta um caráter transversal, uma vez que perpassa várias estruturas da empresa, pois segundo Frazão, Oliva e Abilio "[...]não se limita apenas ao relacionamento com consumidores, mas acaba por repercutir em várias esferas da atividade empresarial, a demandar adaptação também de setores que, inicialmente, não estariam diretamente relacionados com a LGPD"[249], havendo, assim, necessidade de adequação em observância ao tratamento de dados que é realizado.

---

[247] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

[248] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[249] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico]

Isso significa que desenvolver um compliance de dados na organização é tornar a empresa em conformidade com a Lei Geral de Proteção de Dados, mas, percebe-se que a lei não impõe um modelo específico para a implementação de um programa de compliance de dados, na realidade, possibilita que os controladores e operadores formulem regras de boas práticas e de governança que contenha as condições de organização, o regime de funcionamento, os procedimentos, como o canal de comunicação para as reclamações e petições de titulares, as normas de segurança, os padrões técnicos, mecanismos de mitigação do risco e de segurança, entre outros[250].

Desse modo, o *compliance* segundo Saavedra pode ser definido como um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica, seja por força de contrato ou lei, possuindo como característica o compromisso com a criação de um sistema complexo de políticas, controles internos e procedimentos, que consiga demonstra que a empresa está buscando "garantir", o estado de *compliance*[251].

O Regulamento Geral de Proteção de Dados da União Europeia estabelece no considerando 78[252], os motivos da necessidade de um *compliance* de dados, diante das

---

/ Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[250] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

[251] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.729.

[252] Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021. "(78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir

atividades de tratamento dos seus dados pessoais exige-se a adoção de medidas técnicas e organizativas adequadas, com a finalidade de assegurar o cumprimento dos requisitos disposto no RGPD, assim, para fins de comprovar esta conformidade, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem os princípios do *privacy by design* e do *privacy by default*.

Observa-se que referido regulamento europeu não apenas exige o *compliance*, mas também indica quais medidas podem ser incluídas para isso, como a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais, a transparência relativa a função e tratamento dos dados, a adoção e melhorias de medidas de segurança.

Nesse aspecto, para a concepção das regras de boas práticas deve-se considerar o tratamento e a natureza dos dados, o escopo, a finalidade, probabilidade e gravidade dos riscos, assim como os benefícios do tratamento para o titular dos dados[253]. Além disso, o controlador deverá observar a estrutura, escala e volume das suas operações, analisar a sensibilidade dos dados que são tratados e a probabilidade e gravidade dados danos aos titulares, em atenção aos princípios segurança e da prevenção[254].

Desse modo, poderá implementar o programa de governança em privacidade e proteção de dados e demonstrar a sua efetividade, nos casos em que houver solicitação pela ANPD ou outra entidade. A LGPD estabeleceu alguns requisitos mínimos para a implementação do programa de governança em privacidade: como a demonstração do comprometimento na adotação de processos e políticas internas; que seja adaptado à estrutura, à escala e ao volume de suas operações e a sensibilidade dos dados; que estabeleça políticas e salvaguardas adequadas com base na avaliação de riscos; atuação transparente, participativa e com base na confiança; mecanismos de supervisão internos e externos; planejamento de resposta a incidentes e remediação; e, por fim, que seja

---

que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos.".

[253] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 50 [...] § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular."

[254] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.50 [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:"

atualizado de forma constante com base no monitoramento contínuo e nas avaliações periódicas[255].

Conforme Frazão, Oliva e Abilio, trata-se de uma autorregulação ou corregulação que busca dar concretude à LGPD "[...]contribuindo para a efetividade da autovigilância, na medida em que permite certa flexibilidade na composição das práticas corporativas para que se amoldem às especificidades de cada atividade, do tamanho da sociedade e dos riscos"[256].

Como já foi dito esse é o conteúdo mínimo dentro de um programa de compliance de dados, a lei possibilita que as organizações coloquem outros requisitos e salvaguardas relativas à proteção de dados. Essas regras de boas práticas e de governança estabelecidas pelas empresas deverão ser publicadas e atualizadas de forma periódica, bem como poderão ser reconhecidas e divulgadas pela ANPD[257].

O desevolvimento de um programa de *compliance* de dados apresenta vantagens, tais como por exemplo atenuação de sanções, mas desde que sejam efetivamente materializados, pois não são suficientes meras "cartas de intenções" ou "programas de fachadas", é preciso ter elementos que caracterizam um programa robusto, pois os "programas de papel" que carece de efeitos na prática possuem a tendência de serem

---

[255] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 50 [...] §2º [...] I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei."

[256] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[257] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 50 [...] § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional."

desconsiderados pelas autoridades regulatórias[258], pois não consistem em mecanismos efetivos de *compliance*[259].

Saavedra ressalta que para a implantação de um Sistema de Gestão de *Compliance* de dados, mesmo que existam diferentes tipos de *data assessments*, deve-se atentar para alguns pontos principais *Risk Assesment* (Análise de riscos), *Data mapping*: Inventário e registro de dados, *Privacy Impact Assement* (PIA) e *Data Protection Impact Assessments* (DPIA)[260].

Nesse aspecto, Carvalho, Mattiuzzo e Ponce afirmam que mesmo que não tenha um modelo rígido de orientação para a implementação de um programa de conformidade, a ANPD poderá expedir orientações sobre a governança em privacidade[261]. Para os autores, os parâmetros estabelecidos na LGPD indicam o que é essencial em qualquer programa de implementação com mecanismos de governança e boas práticas reflita a estrutura, a escala e o volume das operações da empresa ou organização[262].

Sendo assim, dentre os requisitos dispostos na LGPD, existem alguns pontos podem ser destacados e considerados com base na experiência internacional e na doutrina, quais sejam o mapeamento dos dados (ou *data mapping*), identificação de riscos, procedimentos de adequação e adequação de documentos, revisão e implementação de melhorias contínuas.

Sobre o mapeamento de dados (ou *data mapping*), percebe-se que no programa de governança em privacidade é necessário elaborar o mapeamento dos dados, que consiste em mapear os fluxos e processos que sejam relacionados ao tratamento dos dados pessoais, formando um inventário de dados. De acordo com Carvalho, Mattiuzzo e Ponce o mapeamento:

---

[258] Importante destacar que o titular muitas vezes é também consumidor. Dito isso, outras autoridades e órgãos podem atuar em prol dos direitos em jogo. Nesse sentido, convém mencionar o acordo de cooperação feito pela ANPD e o SENACON, para fins de cooperação técnica e operacional referente à proteção de dados pessoais (BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Acesso à Informação**. Convênios e Transferências. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/repasses-e-transferencias-de-recursos-financeiros Acesso: 06.jun.2021).

[259] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[260] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.734.

[261] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.366.

[262] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.366.

> […] é a elaboração de um mapa dos fluxos internos de diferentes classes de dados pessoais tratados pela empresa. Nesse fluxo, é relevante que estejam identificados todos os dados pessoais tratados no âmbito da entidade; como cada dado pessoal é coletado; a finalidade do tratamento de cada categoria; lista de eventuais receptores (internos ou externos) desses dados pessoais – incluindo a informação sobre se o dado é compartilhado com agente localizados no exterior ou atividades de subcontratação de agentes de tratamento; o período de guarda de cada categoria de dado pessoal; eventuais medidas de segurança dos dados adotadas; e identificação de categorias especiais de dados pessoais tratadas (como dados sensíveis e dados de crianças e adolescentes).[263]

É extremamente importante para compreender a situação interna e fazer um inventário dos fluxos e processoas de dados da empresa que irá auxiliar nas tomadas de decisão necessárias para prosseguir com o processo de adequação à LGPD.

A principal função do *data mapping,* que é o inventário e registro de dados, segundo Saavedra é "[...] identificar os dados que transpassam vários sistemas e, em função disso, serve para indicar como os dados estão compartilhados, organizados e onde eles estão localizados"[264]. Assim, após a realização do mapeamento dos dados, deve-se prosseguir para a inicial identificação dos riscos, que não se confunde com o Relatório de Impacto à Proteção de Dados Pessoais – RIPD.

Em relação a identificação dos riscos, sabe-se que toda atividade de tratamento[265] possui riscos e para tentar mitigá-los é preciso primeiro identificá-los por

---

[263] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.367.

[264] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.735.

[265] Vide considerando 75 do RGPD: 75. O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. (REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021).

meio de uma matriz de riscos e a partir dela fazer os desdobramentos da adequação, pois assim será possível saber o que é mais urgente e que necessita de maior atenção dentro da implementação do programa de governança e boas práticas. De acordo com Carvalho, Mattiuzzo e Ponce sobre a matriz de risco deverá apresentar:

> "[...]se o dado pessoal é de uma categoria especial (considerando, por exemplo, a categoria de dados sensíveis da própria LGPD), as finalidades do tratamento, a existência de prazo de retenção legal de dados, eventual risco que o tratamento representa para os direitos e liberdades fundamentais do titular, bem como medidas de segurança ou minimização de riscos já adotadas"[266].

Além disso, os referidos autores destacam que a matriz de risco pode ser útil à medida em que é verificado um maior nível de risco para os direitos fundamentais do titular o que impõe a necessidade das medidas para proteção contra esses riscos[267]. Essa análise inicial dos riscos da empresa é importante para, não somente conhecer as vulnerabilidades, mas também para adoção de medidas preventivas e mitigatórias dos riscos.

Nesse aspecto, Saavedra afirma a importância do *Privacy Impact Assement* (PIA) "[...] serve para reconhecer ou prover medidas mitigatórias necessárias para evitar ou evitar reduzir os riscos identificados. Essa metodologia atua como um facilitador da implementação da "*privacy by design*", exigido pela GDPR"[268]. O PIA deve ser feito logo no início do tratamento, para avaliar a probabilidade ou gravidade do impacto à privacidade, em observância ao *privacy by design.*

A análise de risco deve ser executada de forma adequada, pois caso o contrário, poderá comprometer a efetividade dos mecanismos que serão adotados, seu objetivo consiste em identificar as principais áreas de exposição da organização para que sejam tomadas medidas preventivas proporcionais aos riscos identificados. Destaca-se que, nessa análise, deverá ser feita a partir do contato com todos os setores da empresa, a parte documental, do objeto e local das atividades, para possibilitar o desenvolvimento da governança de dados para aquela determinada empresa, uma vez que pode variar

---

[266] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.367.

[267] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.368.

[268] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.735.

conforme a complexidade, estrutura e tratamento de dados realizados, por isso, a necessidade de uma análise individualizada[269].

Assim, a análise dos riscos é essencial para se ter o conhecimento das fragilidades e conseguir elaborar um programa de *compliance* de dados efetivo, com as diligências necessárias e a adoção de medidas preventivas e mitigatórias dos riscos conforme as peculiaridades da empresa.

A partir da análise dos riscos é possível fazer os procedimentos de adequação e adequação dos documentos. No que se refere aos procedimentos de adequação, estes significam uma adequação internamente da empresa, relaciona-se as atividades e aos controles internos de proteção e seus mecanismos de seguraça e sigilo em observância à Lei Geral de Proteção de Dados Pessoais.

Dessa forma, Carvalho, Mattiuzzo e Ponce afirmam que "[...] o processo de adequação da entidade passará pela adequação de sistemas, processos e procedimentos internos – fruto de colaboração das equipes responsáveis por tecnologia da informação e compliance"[270]. Nesse aspecto, a organização deverá criar internamente mecanismos que possibilitem a efetividade na identificação de incidentes de segurança e as medidas a serem tomadas quando acontecer o incidente, como um protocolo a ser seguido para comunicar os titulares afetados e a ANPD.

Frazão, Oliva e Abilio[271] chamam a atenção que para garantir o efetivo cumprimento das normas nos programas de *compliance*, se faz necessário estabelecer procedimentos e controles internos que seja compatível com a avaliação de riscos, inclusive, criar um setor independente que tenha recursos para exercer a função de vigilância, bem como assegurar o respeito ao programa.

Além disso, é preciso ter um canal de comunicação para que os titulares possam entrar em contato com o encarregado, bem como permita que o titular, faça suas solicitações e, principalmente, exerça seus direitos e confirmar a existência de tratamento

---

[269] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[270] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.368.

[271] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020, p.i.

de dados pessoais, que poderá ser de forma imediata quando o formato for simples ou dentro do prazo de 15 dias[272].

Outro canal é o de denúncias, segundo Saavedra "consiste em um *software* ou linha telefônica ou ambos num mesmo sistema para receber denúncias e críticas à empresa. O canal deverá constar do Código de Ética e Conduta da empresa, juntamente, com dados acerca da composição do Comitê de Ética"[273].

Esse canal é direcionado ao cumprimento do programa de *compliance*, visando prestar esclarecimentos aos funcionários em casos de dúvidas e também receber denúncias para que medidas sejam tomadas e para prevenir o acontecimento de novas práticas semelhantes. Para um bom funcionamento deste canal é preciso que haja confiança, sigilo e que não sejam utilizados para fins distorcidos, capazes de gerar um desistímulo entre os funcionários[274].

Em relação a adequação dos documentos da organização, entende-se que quando se trata de implementação de programa de proteção de dados pessoais, deve-se levar em consideração a necessidade de adequar os documentos internos e documentos com empresas parceiras e documentos que sejam feitos com os titulares, ou seja, todos os documentos da empresa precisam ser analisados e adequados à LGPD.

Isso significa que os documentos internos como a política de segurança, política de privacidade, código de boas práticas, código de ética e outros documentos que regem a empresa devem passar por mudanças para fins de adequação à LGPD. Ainda, no âmbito interno ressalta-se a importância de documentar e registar os protocolos, processos, procedimentos, alterações, anonimização e exclusão relativas aos dados, até mesmo para fins de manter atualizado o mapeamento dos fluxos de dados, sendo necessário uma segurança da informação para resguardar a integridade da cadeia de documentos, como por exemplo pelo uso de critptografia.

---

[272]Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular."

[273] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.739.

[274] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020, p.i.

Um dos documentos é o Código de Ética e Conduta, pois conforme Saavedra[275] é importante que as empresas e corporações tenham seus códigos, com os valores e princípios de proteção de dados e privacidade. Reforçando a necessidade da criação do comitê interno, canal de denúncias da empresa e a política das consequências sobre apuração e penalidades, em casos de descumprimento das normas de *compliance* de dados.

Carvalho, Mattiuzzo e Ponce afirmam que os documentos internos não devem ser simplesmente a letra da lei, é preciso que "[...]os códigos de conduta "estabeleçam de forma clara as obrigações dos funcionários e colaboradores da organização e forneçam instruções sobre o exercício de suas funções para o tratamento e dados pessoais"[276]. Nesse sentido, Frazão, Oliva e Abilio[277] esclarecem que a elaboração do Código de Ética e Conduta consubstanciam os valores, princípios e boas práticas que devem ser observadas por todos, devendo ter uma linguagem clara e direta para ser compreendido por uma simples leitura e que tenha um fácil e constante acesso.

Outro documento que deve ser elaborado ou adequado é a Política de Privacidade e Proteção de Dados. Deve indicar e explicar, de forma simples e clara, a coleta dos dados para fins de tratamento e a sua finalidade, em observância aos princípios da LGPD, sobretudo, os princípios da finalidade, da necessidade e da transparência, apontar os direitos dos titulares, assim como, os procedimentos e medidas preventivas e medidas a serem adotadas em casos de incidentes de dados pessoais e o canal de comunicação com o encarregado. Este documento deve ter uma linguagem acessível, inclusive, com utilização de *legal design* e *visual law*, para torná-lo compreensível ao leigo.

Além da política de privacidade e proteção de dados, é importante revisar os contratos com fornecedores para inserir cláusulas específicas relativas ao tratamento de dados, visando manter os mesmos níveis de segurança e proteção dos dados adotados

---

[275] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.737-739.

[276] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.369.

[277] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

pelo contratante e exigir um comprometimento de conformidade com a LGPD e RGPD[278].

Em relação aos documentos feitos com outras empresas, nos casos em que a empresa tem relação com outra empresa (*Business to Business)*, é preciso adequar aos requisitos da LGPD, quando houver compartilhamento de dados nacionalmente, já nos casos de transferências internacionais, deve-se atentar que outras regulamentações de privacidade e proteção de dados podem incidir sobre o documento, como por exemplo o RGPD, quando a transferência de dados é feita com países da União Europeia.

Já nas situações em que a empresa possui relação direta com o consumidor, os documentos e contratos devem serem adequados à Lei Geral de Proteção de Dados, mas com um cuidado à mais, buscar efetivar os princípios estabelecidos na lei. Dessa forma, chama-se atenção ao fato de que não basta criar cláusulas informando as finalidades do tratamento e outros aspectos nos termos da LGPD se o teor não for acessível e claro para o titular, pois é necessário que as informações sejam ditas de forma clara, precisa e facilmente acessíveis[279] aos titulares, utilizando o *legal design* e *visual law.*

Conforme Carvalho, Mattiuzzo e Ponce[280] os documentos que são utilizados na relação entre a empresa e os titulares de dados pessoais, é importante que seja adotada uma redação que apresente uma linguagem clara e com todas as informações pertinentes ao tratamento de dados e exigidas pelo art.9.º da LGPD[281]. Nesse aspecto, uma das formas de tornar o teor do documento claro e acessível ao titular é utilizar o legal design e o visual law, uma vez que o documento é desenvolvido com foco no ususário.

Ainda sobre documentos, chama-se atenção sobre a necessidade de elaboração do Relatório de Impacto à Proteção de Dados Pessoais – RIPD, uma vez que a lei

---

[278] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.738.

[279] Em atenção ao princípio da transparência, vide capítulo 3.

[280] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.369.

[281] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 9º 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 acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: 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."

determinou não determinou sua obrigatoriedade, mas possibilitou a solicitação pela Autoridade Nacional.

De acordo com Carvalho Mattiuzzo e Ponce, o RIPD é comparado ao *Data Protection Impact Assement* - DPIA, previsto no art. 35 do RGPD[282], mas o regulamento europeu detalhou as hipóteses de requisição do DPIA e o conteúdo mínimo desse documento, já a LGPD não estabelece as hipóteses específicas de requisição do documento, apenas possibilitou que a ANPD regulamente as hipóteses e faça a sua requisição[283].

Belli[284] ressalta que quando o tratamento de dados é feito com base no legítimo interesse (no art.7.º, IX, da LGPD) a análise de impacto sobre privacidade é imprescindível, pois embora o legislador não tenha detalhado as situações em que o RIPD pode ser solicitado, o legítimo interesse por ser abrangente e flexível, nessa hipótesse pressupõe que seja feito o RIPD e que este possa ser solicitado pela ANPD.

O RIPD deve descrever a descrição dos tipos de dados coletados, a metodologia utilizada na coleta e as medidas de segurança da informação para proteção dos dados e

---

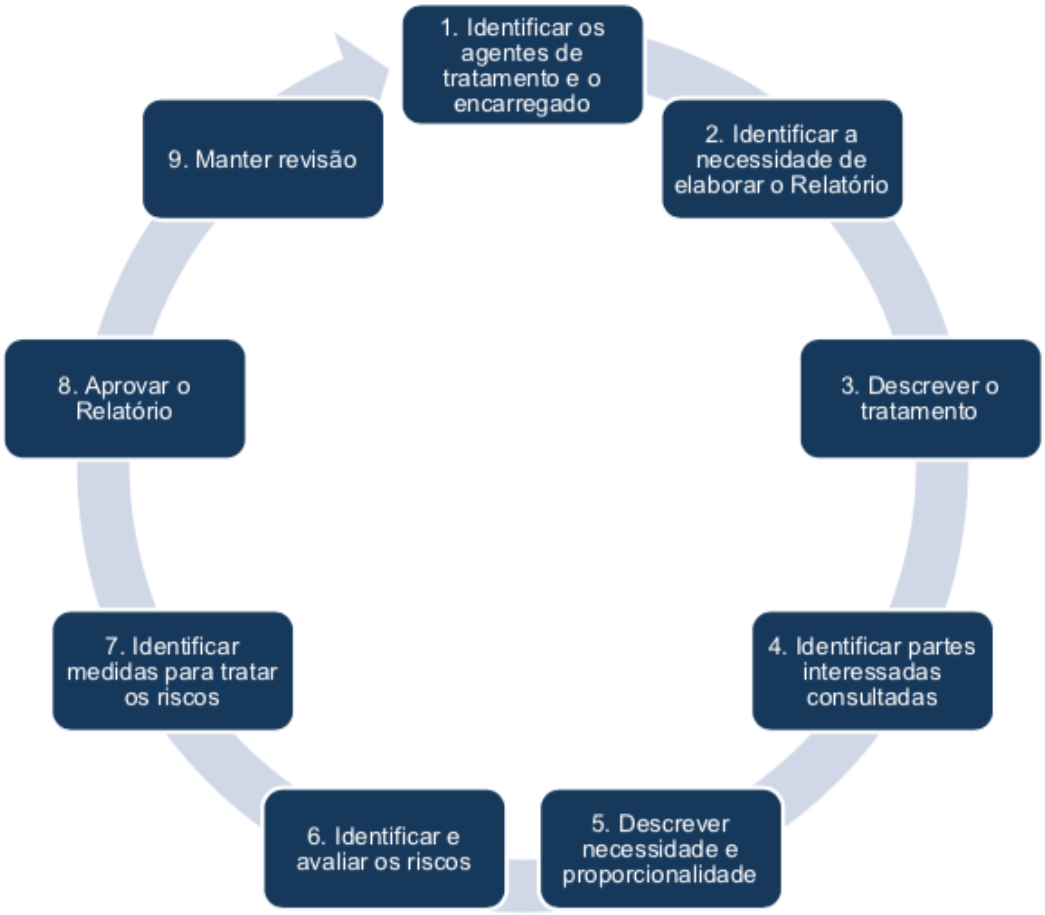
[282]Cf. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021 "Artigo 35.o Avaliação de impacto sobre a proteção de dados 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. 2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala. 4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.o 1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68.o. 5. A autoridade de controlo pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité.".

[283] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.369.

[284] BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.395.

mitigação dos riscos de incidentes, esse documento é elaborado a partir do mapeamento dos dados e da análise de risco inicial e as medidas e procedimentos de implementação do compliance de dados, é feito o RIPD. Especificamente, sobre as etapas de elaboração do RIPD, veja-se:

Figura 8: Etapas de elaboração do RIPD



Fonte: Governo Federal. Oficina Dirigida Relatório de Impacto à Proteção de Dados Pessoais – RIPD, 2020[285].

A estrutura das etapas do RIPD (figura 8), foi elaborada pelo Governo Federal, com inspiração no modelo utilizado pela Inglaterra, indicando o que deve integrar o

[285] GOVERNO FEDERAL. **Oficina Dirigida Relatório de Impacto à Proteção de Dados Pessoais – RIPD**, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/apresentacao-oficina_ripd_v2.pdf Acesso em: 15.jun.2021

relatório. Inclusive, o template editável do RIPD encontra-se disponível em seu *site*[286], ainda que o arquivo tenha sido pensado para o poder público, pode servir de base para as empresas, caso seja necessário a fazer o relatório.

Sobre a comparação entre o RIPD e o DPIA, uma semelhança é que ambos possibilitam as respectivas autoridades de indicar as hipóteses que são obrigatórias elaborar o relatório de impacto da atividade de tratamento de dados, a diferença é que o legislador europeu detalhou as hipóteses em que são necessárias o DPIA, sem contudo engessar a regulamentação também possibilitou que a Autoridade aponte outras hipóteses para fazer o DPIA. Em relação ao RGPD, Saavedra[287] destaca que a empresa que está em desconformidade com as exigências do DPIA pode receber multas pela Autoridade.

Um aspecto que é muito importante na implementação do programa de proteção de dados é a cultura de privacidade e proteção de dados dentro da empresa. Esse ponto não pode ser negligenciado, pois é ele que será o diferencial dentro de uma empresa, isso porque não adianta ter um *data mapping*, as melhores medidas e técnicas de segurança da informação e utilizar as mais avançadas ferramentas de análise de risco para fazer o RIPD, se as pessoas da organização desde a alta gestão até o funcionário de cargo mais simples não estiverem alinhados com o código de ética e conduta e as políticas de privacidade e proteção de dados da empresa, ou seja, se não houver uma cultura de privacidade e proteção de dados pessoais na organização.

Realizar a conformidade da empresa com a Lei Geral de Proteção de Dados Pessoais não é um simples "aplicar à lei", é necessário uma implementação de um compliance de dados, a depender da estrutura da empresa, uma equipe multidisciplinar trabalhando nesse processo de adequação, mas é preciso ir além de procedimentos técnicos, pois exige-se uma mudança cultural dentro da empresa. Nesse sentido, Frazão, Oliva e Abilio dizem que "[...]a sua efetiva implementação exige uma própria mudança de cultura, a fim de reconhecer que a titularidade e o controle dos dados pertencem aos respectivos titulares, de forma que as práticas empresariais deverão ser reestruturadas com esse propósito"[288].

---

[286] GOVERNO FEDERAL. **Relatório de Impacto à Proteção de Dados – RIPD**. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiatemplateRIPD.pdf Acesso: 15.jun.2021.

[287] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.736.

[288] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

Assim, quando se trata de mudança cultural é preciso o compromisso dos funcionários e colaboradores para fins de efetividade do programa de compliance de dados. Desse modo, dois pontos merecem serem analisados: para o primeiro aspecto, será utilizado o método dedutivo, isto é, do geral para o particular, pois devemos compreender e enfrentar à realidade da sociedade brasileira em termos de cultura de privacidade e proteção de dados[289], uma vez que isso reflete dentro da própria cultura de proteção de dados da empresa; já o segundo aspecto, será analisado por meio da neurociência, para tratar a mudança cultural dentro de uma empresa, isso implica necessariamente trabalhar a gestão de pessoas e suas tomadas de decisões em suas funções, desde da alta direção até o funcionário de cargo mais simples.

Os pontos destacados se relacionam pela necessidade da mudança cultural na empresa, o primeiro possui o grande desafio que é realizar o alinhamento dos funcionários com o código de ética e conduta e com a política de privacidade e proteção de dados, isso porque a realidade da sociedade brasileira possui suas peculiaridades e não pode ser percebida da mesma forma da sociedade dos países pertencentes a união europeia, locais em que a cultura da privacidade e proteção de dados já tem um extenso período e com uma construção mais avançada da matéria, enquanto que na sociedade brasileira a cultura de proteção de dados está em construção. Em relação ao segundo aspecto, o desafio é mais "pronfundo", pois requer uma mudança mais efetiva e é inerente ao comportamento do próprio ser humano no ato de suas escolhas.

Desse modo, tem-se que no primeiro aspecto deve-se trabalhar treinamentos, capacitações e conscientização dos funcionários, podendo até fazer eventos abertos ao público em geral, para fins de conscientização da sociedade, e em atenção a função social da empresa.

Sobre a difusão da cultura da privacidade e proteção de dados pessoais, Carvalho, Mattiuzzo e Ponce, pode ser feita por meio da elaboração de cartilhas e outros conteúdos mais interativos, inclusivo, exemplos de casos de violação à proteção de dados divulgados pela mídia, que reiteram as orientações do programa de *compliance* de dados, com a finalidade de conscientizar os funcionários[290]. Os treinamentos devem ser periódicos, conforme Frazão, Oliva e Abilio:

---

[289] Ver o capítulo 02.

[290] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.370.

> Deve-se observar o emprego de expressões claras e didáticas, observando-se o público-alvo do treinamento. É ideal que sejam segregados os funcionários de acordo com as áreas de risco a que estão sujeitos e ao setor a que pertencem – de modo a permitir abordar as especificidades de cada um sem que se deixe de lado a essência do programa. Assim como o programa, para ser efetivo, demanda construção direcionada para as particularidades de cada pessoa jurídica, também os treinamentos podem se revelar mais adequados se adaptados aos funcionários de cada setor e nível de especialidade, em atenção às especificidades de linguagem que, por vezes, caracterizam setores específicos.
> De todo modo, os treinamentos devem ser constantes, tanto para garantir a transmissão de adaptações e alterações no programa como para reiterar suas premissas e contribuir para minimizar o risco de esquecimentos e incompreensões pelo funcionário[291].

Nesse cenário, a própria Lei Geral de Proteção de Dados Pessoais busca estimular a mudança não apenas nas organizações privadas e no setor público, mas principalmente nas pessoas, pois é necessária uma mudança cultural e comportamental em relação aos dados e privacidade. Nesse aspecto, chama-se atenção para a função promocional do direito, buscando-se operar por meio de incentivos as transformações sociais[292].

Sobre o segundo aspecto, deve-se trabalhar por meio de *nudges*, isto é, heurísticas e vieses para que as pessoas tomem as decisões de forma mais assertivas, sob uma perspectiva ética, para fins de privacidade e proteção de dados. Sabe-se que o risco é inerente as atividades de tratamento e a "falha" é algo natural e inerente a própria condição humana, deve-se entender que promover uma cultura de privacidade e proteção de dados não significa que não irá acontecer o vazamento ou outros incidentes de segurança do dados, mas que é possível impulsionar o engajamento dos funcionários e colaboradores a mudanças desejáveis para fins de comprometimento com a proteção de dados e minimização dos riscos.

Desse modo, *nudge* é, conforme Thaler e Sunstein, um estímulo, um empurrãozinho, um cutucão, ou seja, é qualquer aspecto da arquitetura de escolhas que é capaz de mudar o comportamento das pessoas de forma previsível, sem lhes retirar

---

[291] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[292] BOBBIO, Noberto. **Da Estrutura à Função**: novos estudos de teoria do direito. Tradução de Daniela Beccaccia Versiani; revisão técnica de Orlando Seixas Bechara; Renanta Nagamine. Barueri, São Paulo: Manole, 2007, p.72: "Nesse sentido, prêmio e incentivo são, como dizia há pouco, as duas formas típicas pelas quais se manifesta a função promocional do direito. Apenas uma observação mais atenta da frequência e do modo de operar delas pode fazer avançar a análise funcional do direito e promover a adequação da teoria do direito às transformações sociais em curso nos ordenamentos jurídicos das sociedades economicamente mais avançadas, que é desejada pela maioria".

qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos[293]. Ressalta-se que o próprio direito pode ser compreendido como um incentivo de condutas socialmente desejáveis[294].

Nesse sentido, Carmurça diz que os "*Nudges* são soluções levemente paternalistas, constituindo microincentivos que levam a uma mudança de comportamento, podendo serem capazes de condicionar o comportamento à proteção da privacidade"[295].

Desse modo, implementar uma cultura de privacidade e proteção de dados dentro da empresa, significa fazer mudanças necessárias e para isso é preciso compreender alguns aspectos comportamentais dos indivíduos, levando-se em consideração que a neurociência fragilizou a concepção de "*homo economicus*", demonstrando que as pessoas reais possuem dificuldades para fazer decisões complexas, são apenas "*homo sapiens*"[296]. As condutas podem ser transformadas por meio de uma abordagem, "considerada paternalista", em que os arquitetos de escolhas, públicas ou privadas, não apenas identificam as decisões que esperam que as pessoas façam como, na realidade, estão dando um *nugde*, ou seja, conscientemente induzindo as pessoas tomarem determinadas decisões[297] que são desejáveis.

Uma mudança cultura não acontece de um dia para o outro, nem em um mês ou em um ano, é uma construção ao longo do tempo, com conscientização, educação e treinamento dentro da empresa. Mas existe algo que deve ser considerado nesse processo

---

[293] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.14.

[294] Bobbio ao tratar da ideia da função promocional do direito, buscou explicar a importância do encorajamento nas mudanças sociais para obter condutas socialmente desejáveis. Nesse sentido, ver BOBBIO, Noberto. **Da Estrutura à Função**: novos estudos de teoria do direito. Tradução de Daniela Beccaccia Versiani; revisão técnica de Orlando Seixas Bechara; Renanta Nagamine. Barueri, São Paulo: Manole, 2007, p.18: "É notória a impotância que têm, para uma análise funcional da sociedade, as categorias da conservação e da mudança. Considerando agora as medidas de desencorajamento e as de encorajamento de um ponto de vista funcional, o essencial a se destacar é que as primeiras são utilizadas predominantemente com o objetivo da conservação social e as segundas, com o objetivo da mudança".

[295] CAMURÇA, Lia Carolina Vasconcelos. Sociedade de Vigilância, direito à privacidade e proteção de dados pessoais: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor – usuário/ Lia Carolina Vasconcelos Camurça. **Dissertação (mestrado)** – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós- Graduação em Direito, Fortaleza, 2020.

[296] Nesse sentido, explicam Thaler e Sunstein que: "Se você ler livros teóricos de economia, vai descobrir que o Homo economicus pode pensar como Albert Einstein, ter tanta memória quanto um supercomputador e ter tanta força de vontade quanto Mahatma Gandhi. Mas as pessoas que conhecemos não são assim. Pessoas reais têm dificuldade de fazer divisões complexas sem calculadoras, às vezes esquecem o aniversário do parceiro e ficam de ressaca no Ano-Novo. Esses não são Homo economicus, são Homo sapiens" (THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.15.).

[297] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.14.

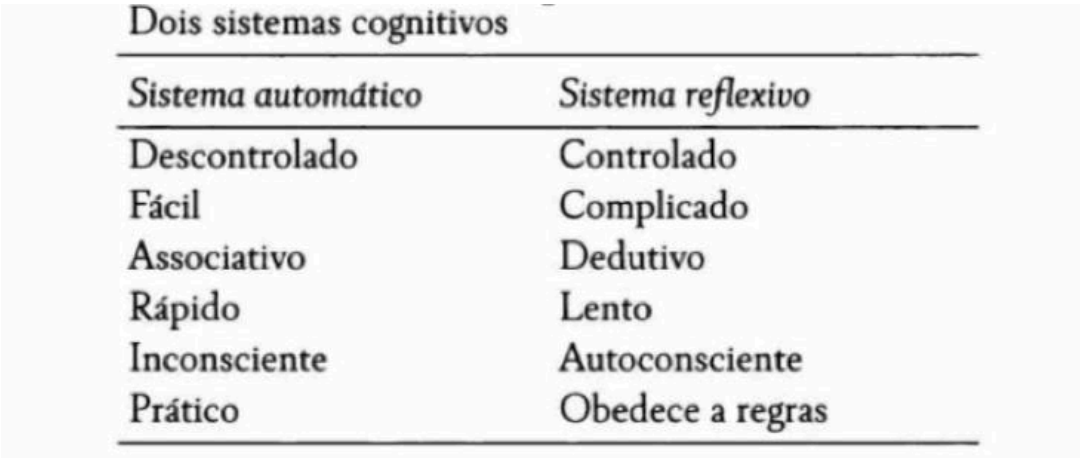
de mudança, os *nudges*. Isso porque, para Thaler e Sunstein, "[...] um nudge é qualquer fator que altere significativamente o comportamento de humanos, mesmo que ignorado por econos"[298].

Segundo os referidos autores, "[...] ao implantar adequadamente tanto os incentivos quanto os *nudges*, aumentamos nossa capacidade de melhorar a vida das pessoas e ajudamos a resolver muitos dos problemas da sociedade. E tudo isso sem impedir a liberdade de escolha de cada indivíduo"[299]. Dito isso, é possível melhorar a tomada de decisão das pessoas dentro da empresa por meio de incentivos e/ou *nudges* em beneficio da proteção de dados, sob uma perspectiva ética capaz de promover mudanças desejáveis em prol da privacidade e proteção de dados pessoais.

Esse aspecto é importante, pois embora haja treinamentos e conscientização sobre a importância da proteção de dados pessoais e sobre as mudanças necessárias, é sabe-se que o indivíduo por si, em seu pensamento possui dois tipos que influenciam suas escolhas e ações. Segundo Kahneman cada pessoa possui dois sistemas de pensamento, "o sistema 1 opera automática e rapidamente, com pouco ou nenhum esforço e nenhuma percepção de controle voluntário. O sistema 2 aloca atenção às atividades mentais laboriosas que o requisitam, incluindo cálculos complexos"[300]. Nesse sentido, Thaler e Sunstein afirmam que "[...] existem dois tipos de pensamento: um intuitivo e automático e outro reflexivo e racional. Chamaremos o primeiro de Sistema Automático e o segundo de Sistema Reflexivo"[301].

Figura 9 – Dois sistemas cognitivos

[298] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.17.
[299] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.17.
[300] Kahneman, Daniel. **Rápido e Devagar**: duas formas de pensar. Tradução Cássio de Arantes Leite. 1ªed. Rio de Janeiro: Objetiva, 2012, p.29.
[301] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.29.



Dois sistemas cognitivos	
Sistema automático	*Sistema reflexivo*
Descontrolado	Controlado
Fácil	Complicado
Associativo	Dedutivo
Rápido	Lento
Inconsciente	Autoconsciente
Prático	Obedece a regras

Fonte: *Nudge*[302]

Sobre a figura acima, os autores Thaler e Sunstein explicam que é preciso considerar "[...] o Sistema Automático sua reação intuitiva e o Sistema Reflexivo seu pensamento consciente. A intuição pode ser bastante precisa, mas muitas vezes cometemos erros exatamente por confiar demais no Sistema Automático"[303], para só, então conseguir incentivar mudanças.

Após entender que o sistema 1 é o operante na maior parte do tempo, é intuitivo e automático, Kahneman diz que o melhor a se fazer "[...] é um acordo: aprender a reconhecer situações em que os enganos são prováveis e se esforçar mais para evitar enganos significativos quando há muita coisa em jogo"[304]. Acontece que esse acordo sugerido por Kahneman requer um grande esforço e também um autoconhecimento e conhecimento sobre o estudo do sistema de pensamento feito pela neurociência. Então, para que haja mudanças comportamentais visando a cultura da privacidade e proteção de dados, pode-se utilizar os *nudges* para melhorar as escolhas feitas pelas pessoas.

Sobre os *nudges*, Thaler e Sunstein afirmam que existem três heurísticas, a ancoragem, a disponibilidade e a representatividade. A ancoragem e ajustes, se manifesta através de uma âncora e que a partir dela que se desencandeiam ajustes na direção que se considera adequada, ou seja, é possível influenciar uma escolha numa situação específica com âncoras[305].

---

[302] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.30.
[303] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.31.
[304] KAHNEMAN, Daniel. **Rápido e Devagar**: duas formas de pensar. Tradução Cássio de Arantes Leite. 1ªed. Rio de Janeiro: Objetiva, 2012, p.39.
[305] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.34-35.

Já a disponibilidade, refere-se a análise de um risco de algo acontecer de acordo com a facilidade em que é possível pensar na situação[306]. Essa heurística, pode ser utilizada sobre os casos que são noticiados pela mídia sobre vazamentos e outros incidentes relativos à proteção de dados pessoais. Todavia, é preciso ter cuidado com a "disponibilidade" para não provocar medos, paralisações e distorções. Sobre a heurística da disponibilidade, Thaler e Sunstein explicam que:

> Quando o "viés da disponibilidade" entra em ação, conduzir a avaliação de volta para o âmbito das possibilidades reais pode causar melhorias tanto nas decisões públicas quanto nas privadas. Uma das melhores formas de aumentar o medo de que aconteça algo ruim é lembrar a população de um incidente semelhante que teve consequências negativas: uma boa forma de aumentar a confiança da população é lembra-la de um incidente semelhante em que tudo correu bem. O problema inevitável é que, quando nos lembramos facilmente de um acontecimento semelhante, distorcemos e inflacionamos nossas estimativas de que volte a acontecer. Por outro lado, quando nada semelhante nos vem à mente, estimamos para baixo[307].

Assim, a cultura da privacidade e proteção de dados dentro da empresa não pode ser concebida a partir do "medo" de que ocorra um vazamento ou outros tipos de violações à proteção de dados, isso poderá provocar comportamentos paralisantes nos funcionários ou mesmo um medo de represálias poderá dificultar a comunicação no tempo hábil de qualquer falha ou incidente para que medidas cabíveis sejam tomadas, bem como possa ser comunicado a Autoridade Nacional e aos titulares afetados.

O medo pode provocar um comportamento indesejável no funcionário, como na situação hipotética de que o funcionário ao apontar um incidente para o "chefe" poderá ter problemas dentro da empresa, deixando com que o medo de represálias e outras emoções influenciem sua na tomada de decisão. Nesse caso, é o medo de ser prejudicado e/ou tentar contornar a situação sozinho que poderá causar um impacto muito maior, como por exemplo afetar o prazo de comunicação à ANPD sobre o incidente e a adoção de medidas cabíveis em tempo hábil para reduzir seus efeitos.

Por outro lado, tem-se a representatividade, compreende-se como a heurística da similaridade, mas esta heurística pode causar graves distorções na percepção de padrões no dia a dia[308]. Pode ser utilizada para as situações de otimismo irreal, em que as pessoas superestismam sua imunidade individual contra danos e deixam de tomar medidas

---

[306] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.34.
[307] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.35-36.
[308] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.38.

sensatas de prevenção, assumindo riscos, assim, pode-se dar esse nugde: "se são lembradas de um evento ruim, as pessoas podem diminuir o nível de otimismo"[309].

Por isso, é preciso saber como e quais nudges utilizar para direcionar as pessoas da empresa a tomarem as melhores decisões comprometidas com a proteção de dados e com o programa de compliance de dados. Nesse aspecto, quando os funcionários encontrarem uma falha ou incidente de segurança, com o *nudge* adequado, eles irão saber lidar com essa situação, bem como a quem devem comunicar nessas situações, como por exemplo comunicar o incidente ao DPO da empresa.

Além disso, um aspecto importante na implementação do programa de proteção de dados é o Compromisso da alta direção na organização, por estimular a cultura da privacidade e proteção de dados dentro da empresa e demonstrar o compromisso com o programa de compliance de dados.

Carvalho, Mattiuzzo e Ponce afirmam que o compromisso explícito e genuíno de agentes da alta direção da organização é capaz de conferir credibilidade ao programa e refletir na tomada de decisões dos membros da organização, bem como serve para desenvolver uma cultura organizacional com valores e práticas em conformidade com os princípios de tratamento de dados pessoais[310]. Até mesmo porque é perceptível que "[...] caso a gerência da pessoa jurídica manifeste-se de forma contraditória com os planos constantes no programa de *compliance*, a mensagem recebida pelos funcionários será de que esse não passa de simples instrumento de fachada"[311]. Esse compromisso da alta direção é um verdadeiro *nudge* de efeito manada[312].

O compromisso da alta direção possui uma função muito influente para mudanças dos funcionários e colaboradores, assim como os outros *nudges* são importantes incentivos de mudanças, pois segundo Thaler e Sunstein "[...]os cientistas sociais chegaram à conlusão de que podem estimular as pessoas a apresentar certos

---

[309] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.44.

[310] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.370.

[311] FRAZÃO, Ana; Oliva, Milena Donato; ABILIO, Vivianne da Silveira. Compliande de dados pessoais. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[312] Nesse sentido, Thaler e Sunstein explicam que "[...] pessoas coerentes e firmes podem influenciar grupos inteiros e mudar suas práticas de acordo com o que elas preferirem". THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.70.

comportamentos apenas oferecendo a elas dicas simples e aparentemente irrelevantes"[313]. Dessa forma, a neurociência demonstra que os humanos são influenciados e que "as vezes, enormes transformações sociais no mercado e na política começam com um simples Nudge"[314]. Assim, entende-se que esse conhecimento sobre os estudos realizados por neurocientistas pode ser utilizado de forma ética e responsável para impulsionar a implementação do programa de privacidade e proteção de dados e desenvolver uma arquitetura de escolhas melhores e alinhadas com o próposito de se proteger os dados pessoais.

Por fim, após a implementação do programa de privacidade e proteção de dados, deve-se manter o monitoramento, revisão e implementação contínua, principalmente, por meio da realização de auditorias internas e externas.

Dessa forma, Carvalho, Mattiuzzo e Ponce ressaltam a importância que sejam realizadas auditorias internas periódicas para analisar o cumprimento de regras por parte de funcionários e colaboradores da empresa e, principalmente, que eventuais pontos fracos do programa sejam identificados por meio de revisões e, consequentemente, alterados e robustecidos, já em relação ao tratamento de dados pessoais sensíveis precisam ser acompanhados de forma mais próxima, em razão dos riscos de danos aos direitos fundamentais serem maiores[315].

O acompanhamento do programa de governança de dados é necessário para que sejam feitos ajustes, melhorias e atualizações e, assim, manter a empresa em conformidade com a Lei Geral de Proteção de dados.

5.3.1 *Da segurança e sigilo dos dados*

A Lei Geral de Proteção de Dados Pessoais estabelece uma seção dedicada a segurança e ao sigilo de dados, destacando que para a implementação de um programa de compliance de dados é preciso além de uma adequação aos princípios e requisitos estabelecidos na lei, sendo necessário adotar medidas e técnicas, nacionais e

---

[313] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.85-86.
[314] THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019, p.65.
[315] CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.372.

internacionais conforme for apropriado para a organização para fins de adoção, para fins de segurança e sigilo dos dados.

A previsão na lei sobre a adoção de medidas e técnicas de segurança da informação é uma decorrente de uma preocupação do legislador com os riscos e vulnerabilidades no desenvolvimento da atividade de tratamento de dados e a possibilidade de afetar liberdades civis e direitos fundamentais do titular. No cenário de constantes avanços tecnológicos, Souza observa que "a preocupação com a segurança e o sigilo dos dados vai aumentar na medida em que a conscientização sobre a relevância dos mesmos dados é disseminada na sociedade"[316].

Desse modo, cabe aos agentes de tratamento o dever de adotar medidas de segurança, técnicas e administrativas que garanta um ambiente seguro e apto para proteger os dados pessoais de acessos não autorizados, destruição e outros incidentes. Inclusive, a ANPD poderá dispor sobre padrões mínimos aplicáveis[317].

Ressalta-se que tais medidas devem ser consideradas desde a própria concepção[318] do produto e/ou serviço até mesmo após fim da execução do tratamento[319]. Pois, assim como no Regulamento Europeu, a LGPD também adota o *privacy by design* e o *privacy by default* para o desenvolvimento de um sistema da informação que assegure a privacidade e a proteção dos dados pessoais do titular.

---

316 SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

317 Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei."

318 Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.46 [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."

319 Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

Todavia, Souza[320] entende que a positivação do conceito *privacy by design* na Lei Geral de Proteção de Dados Pessoais não foi de forma tão explícita como a que ocorreu na legislação europeia, mas que é possível extrair do artigo 46, § 2º.

De toda forma o *compliance* de dados, no que diz respeito a segurança e sigilo dos dados, deverá ser norteado pelos princípios do *Privacy by Design* e *Privacy by Default* desenvolvidos por Ann Cavoukian, em que o primeiro apresenta 7 princípios básicos, incluindo, o *privacy by default*, são eles: 1) Proativo não reativo; Preventivo, não corretivo, que não aguarda o surgimento e materialização dos riscos, busca a prevenção deles, a privacidade é projetada antes do fato; 2) Privacidade como configuração padrão (*privacy by default*), a privacidade é protegida por padrão, ou seja, não é necessária nenhuma ação do individuo para que tenha sua privacidade protegida, pois é feita por padrão; 3) Privacidade incorporada ao design, a privacidade está incorporada no design, sistemas, práticas negociais, é parte integrante de toda a organização, sem lhe reduzir a funcionalidade; 4) Funcionalidade total – soma positiva, não soma zero, busca acomodar todos os interesses legítimos que seja uma soma positiva, evitando-se falsas dicotomias como privacidade x segurança, pois é possível e desejável ter ambos; 5) Segurança de ponta a ponta – Proteção total do ciclo de vida, a privacidade desde o início do projeto até o fim, é incorporada antes do inicio da coleta de dados, deve proteger todo o ciclo de vida dos dados com medidas fortes de segurança até o fim, segurança de ponta a ponta; 6) Visibilidade e transparência – mantenha-o aberto, busca assegurar aos titulares que o tratamento é feito de acordo com os objetivos declarados, conferindo visibilidade e transparência; 7) Respeito pela privacidade do usuário – Mantenha-o centrado no usuário, deve-se manter os interesses dos titulares em primeiro lugar, isto é, conferindo medidas de segurança de privacidade, cominucação e avisos apropriados com opções, tudo centrado no usuário[321].

Assim, o *Privacy by Design* significa que a privacidade e a proteção de dados devem ser incorporadas e protegidas em todo o ciclo de vida dos dados, do início ao fim. Nesse sentido, Saavedra afirma que a empresa "[...] sempre criar produtos e serviços, que,

---

[320] SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[321] CAVOUKIAN, Ann. ***Privacy by design****: The 7 foundation principles Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner of Ontario 2 Bloor Street East, Suite 1400* Toronto, Ontario, CANADÁ. Disponível em: https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf Acesso: 02.jun.2021.

desde o início, estejam de acordo com as diretrizes de um sistema de gestão de *compliance* digital ou de dados, bem como das melhores práticas de *Compliance* de dados"[322].

Nota-se que essa seção da segurança e do sigilo de dados é reflexo do princípio da segurança da informação estabelecido no art.6º, VII da LGPD[323]. Dessa forma, buscando-se fornecer um delineamento jurídico sobre as medidas técnicas e administrativas para a proteção dos dados relativas à segurança da informação, que se propõe analisar as normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 e a ISO/IEC 27701:2019[324] como *standards* a serem implementados pelas organizações.

Enquanto não se tem uma recomendação da Autoridade Nacional sobre quais medidas devem ser adotadas e levando-se em consideração que a própria LGPD já está em vigor em sua grande parte, ficando ressalvada apenas às sanções que entrará em vigor em agosto de 2021, compreende-se que não é interessante que as organizações permaneçam inertes e aguardando o posicionamento da ANPD para que iniciem o processo de adequação à lei e adoção de medidas de segurança da informação.

Dito isso, as ISO/IEC 27001: 2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019 fornecem *standards* internacionais capazes de atender o dispositivo legal e concretizar o princípio da segurança da informação, ou seja, complementam a Lei Geral de Proteção de Dados Pessoais no que diz respeito à segurança e sigilo dos dados.

Sendo assim, quando se trata de proteção de dados, as empresas e instituições precisam implementar um sistema de gestão de segurança da informação internamente, a ISO/IEC 27001 de 2013 é a norma que define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). De modo geral, essa norma busca fornecer requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação.

A própria necessidade e objetivos empresariais atuais reforçam a adoção de um processo organizacional e estruturado de gestão de segurança da informação pautado pelo requisito da segurança. Por isso, é importante implementar um sistema de gestão de

---

[322] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.737.

[323] Ver capítulo anterior que trata sobre o princípio da segurança da informação.

[324] Uma observação que deve ser feita em relação a análise das ISO's, é que estas são consideradas *standards* internacionais que podem servir de base para a segurança da informação. Contudo, não se predente aprofundar na própria ciência da segurança da informação, por limitação de capacidade técnica e formacional desta autora.

segurança da informação na empresa porque segundo dispõe a ISO/IEC 27001 de 2013[325], esse sistema visa preservar a confidencialidade, integridade e disponibilidade de informações, aplicando um processo de gestão de risco e dá confiança às partes interessadas que os riscos são gerenciados de forma adequada.

É necessário um alinhamento da organização e estrutura geral da gestão com a segurança da informação, isso significa que a segurança da informação precisa ser considerada nas etapas dos projetos de processos, sistemas de informação e controle, de uma forma sistêmica e não isolada, pois um incidente em determinado ponto pode repercutir em outro, observando-se as necessidades da empresa. A própria ISO/IEC 27001:2013 afirma que é compatível com outros padrões de sistema de gestão, essa opção por adotar mais sistemas vai depender da própria realidade da empresa e da sua complexidade, mas que a sua implementação e manutenção já melhora a situação da empresa ao nível interno e internacional[326].

São os requisitos previstos na norma para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da informação, incluindo a avaliação e tratamento dos riscos de segurança da informação, sendo cabíveis a todos os tipos de empresas e organizações, pois podem serem adaptadas as realidades, tamanho e natureza das empresas. Todavia, é ressalvado que caso haja exclusão dos requisitos presentes nas cláusulas 4 até a 10, não será possível obter a conformidade da ISO/IEC 27001:2013[327].

De acordo com a norma[328], é preciso conhecer o contexto interno e externo que possuem relevância para o sistema de gerenciamento da segurança da informação, bem como compreender as necessidades e expectativas das partes interessadas, que são relevantes para o sistema de gestão de segurança da informação. Destaca-se que os requisitos das partes interessadas podem incluir outros requisitos legais e regulamentares e obrigações contratuais.

---

[325] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.
[326] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.
[327] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.
[328] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.

Outro aspecto é a determinação do escopo do sistema de gestão de segurança da informação da organização, que levará em consideração os requisitos, bem como as interfaces e dependências entre as atividades realizadas pela organização, e aquelas que são realizadas por outras organizações. A norma exige que o escopo deve estar disponível como informação documentada[329].

Deve-se destacar que sobre a criação da política de segurança da informação, a norma determina alguns critérios que devem serem observados, como o alinhamento da política com o propósito da organização, se possui os objetivos da segurança da informação ou mesmo apresenta uma estrutura para definir tais objetivos, acrescenta-se o compromisso com a melhoria contínua do sistema de gestão da segurança da informação. Ressalta-se que a política de segurança da informação deve estar disponível como informação documentada, haver comunicação sobre a própria política dentro da organização e estar à disposição das partes interessadas.

A alta administração deve atribuir a responsabilidade e relatar o desempenho para garantir que o sistema de gestão de segurança da informação esteja em conformidade com os requisitos deste Padrão internacional e relatar o desempenho do sistema de gestão de segurança da informação para a alta administração.

Esta norma apresenta orientação sobre planejamento, explicando as ações para lidar com riscos e oportunidades, para que seja possível alcançar os resultados pretendidos e prevenir ou reduzir os efeitos indesejáveis, para isso, a organização precisa planejar as ações para lidar com esses riscos e oportunidades, e ações de como integrar e implementar as ações em seu sistema de gestão de segurança da informação processos; e, por fim, avaliar a eficácia dessas ações.

De um modo geral, a norma fornece parâmetros, isto é, requisitos para que a empresa ou organização esteja em conformidade com o sistema de gestão de segurança da informação, visando que estes sejam implementados e melhorados com a necessidade e com o tempo, sendo necessário fazer auditorias, estabelecer métodos e responsabilidades, levando-se em consideração os processos envolvidos e os resultados das auditorias anteriores, o cumprimento dos objetivos, feedback, resultados da avaliação de risco, melhorias contínuas e ações corretivas para o que não está em conformidade.

---

[329] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.

Já a ISO/IEC 27002:2013 surge para complementar a ISO/IEC 27001:2013 que trata sobre o processo de implementação de um Sistema de Gestão de Segurança da Informação. Apresenta, por sua vez, técnicas e código de prática para controles de segurança da informação para que as empresas usem como uma referência para a seleção de controles no processo de implementação de um Sistema de Gestão de Segurança da Informação baseado na ISO/IEC 27001:2013.

A norma é clara em relação a sua aplicação a organizações de todos os tipos e tamanhos (incluindo setor público e privado, comercial e sem fins lucrativos), que realizem atividades de coletar, processar, armazenar e transmitir informações em muitas formas, incluindo eletrônica, física e verbal (por exemplo, conversas e apresentações)[330].

A norma reforça a ideia da informação como um ativo importante, sobretudo, no mundo interconectado, em que "[...]a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos"[331].

Sobre os riscos, a norma diz que os ativos estão sujeitos a ameaças deliberadas e acidentais, enquanto os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Isso porque quando acontece mudanças nos processos e sistemas de negócios ou mesmo porvocadas por leis e regulamentações, podem criar novos riscos à segurança da informação e, consequentemente, causar prejuízos a organização, os riscos de segurança da informação estão sempre presentes. Nesse aspecto, a segurança da informação se mostra eficaz para reduzir esses riscos protegendo a organização contra ameaças e vulnerabilidades e, assim, minimizar os impactos aos seus ativos[332].

Isso por que a segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software, hardware, criptográfia. Esses controles precisam ser estabelecidos, implementado, monitorado, revisado e melhorado, quando

---

[330] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT, 2013.

[331] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT, 2013.

[332] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT, 2013.

necessário, para garantir que os objetivos específicos de segurança e negócios da organização sejam atendidos[333].

Segundo Souza, a norma ISO/IEC 27002:2013 define as características da segurança da informação "(i) a confidencialidade, informações acessíveis apenas a quem seja autorizado; (ii) disponibilidade: informações sempre disponíveis a quem deve acessá-las; e (iii) integridade: informações devem ser fidedignas e autênticas"[334] que necessitam serem preservadas.

O referido autor afirma que a norma da ABNT ISO/IEC 27002, pode servir de subsídio aos agentes de tratamento e mesmo que seja regulamentado por parte da ANPD "não deve se afastar do que já foi previsto pelo Decreto 8.771/16 e pela norma da ISO/IEC 27002 e, se for o caso, deverá conceder prazo para eventual adaptação dos agentes de tratamento às suas disposições"[335].

Já em relação a ABNT NBR ISO/IEC 27701:2019, nota-se que esta norma estabelece requisitos e diretrizes para a proteção dos dados pessoais, levando-se consideração outras ISO's e o Regulamento Geral de Proteção de Dados da União Europeia, mas diz expressamente que pode ser interpretado conforme a legislação local, nesse caso, conforme a Lei Geral de Proteção de Dados[336].

Assim, a ABNT NBR ISO/IEC 27701:2019 apresenta os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) configurando como uma extensão das ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, buscando estabelecer a gestão da privacidade. Ressalta-se que esta norma é aplicável a todos os tipos e tamanhos de organizações, públicas ou privadas[337].

---

[333] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT, 2013.

[334] SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[335]SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[336] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2019 - **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. ABNT, 2019, p.IX.

[337] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2019 - **Técnicas de segurança —Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. ABNT, 2019, p.1

Trata-se de uma verdadeira ampliação aos requisitos previstos na ABNT NBR ISO/IEC 27001:2013, referente à proteção da privacidade dos titulares de dados pessoais, com requisitos e diretrizes, incluindo, expressamente os conceitos de *privacy by design* e o *privacy by default* para "assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado"[338].

Portanto, a segurança da informação tornou-se indispensável para qualquer empresa, organização, instituição, seja pública ou privada, em decorrência do crescente números de utilização dos sistemas operacionais que envolvem o tratamento de dados pessoais. Acrescenta-se a isso, a pandemia do COVID-19 em que o isolamento social foi uma das medidas adotadas para o controle do avanço da contaminação, o que impulsionou o *home office,* o comércio virtual, aulas onlines entre outras práticas no ciberespaço.

Nesse cenário, pretende-se fortalecer que a Lei Geral de Proteção de Dados Pessoais já está em vigor, com ressalva das sanções que entrarão em vigor em agosto de 2021, e que as organizações devem se adequar a LGPD e, consequentemente, buscar implementar tais *standards* estabelecidos nas ISO's capazes de reduzir os riscos e as vulnerabilidades da proteção dos dados e privacidade dos titulares.

5.4 O Papel da Autoridade Nacional de Proteção de Dados na Governança dos Dados Pessoais no Ciberespaço

A Autoriadade Nacional de Proteção de Dados possui um papel fundamental na efetividade da Lei Geral de Proteção de Dados Pessoais, principalmente, para conduzir um delineamento jurídico sobre a privacidade e proteção de dados nos pontos que requer a regulamentação pela autoridade.

A Lei Geral de Proteção de Dados Pessoais sofreu algumas modificações pela Lei nº 13.853/2019, sendo uma delas a criação da Autoridade Nacional de Proteção de Dados, como um órgão da administração pública federal, integrante da Presidência da República, por natureza jurídica transitória, visto que poderá ser transformada em até 2 anos da entrada em vigor da estrutura regimental da ANPD, pelo Poder Executivo em

[338] ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2019 - **Técnicas de segurança —Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. ABNT, 2019, p.51.

entidade da administração pública federal indireta[339]. Assim, mesmo com essa vinculação a Presidência da República, a lei é clara em garantir que a ANPD possua autonomia técnica e decisória[340].

No entanto, Vasconcelos e De Paula[341] fazem algumas ressalvas sobre o desenho legal da ANPD relativa à sua vinculação à Presidência da República que, embora haja a transitoriedade, continuam válidas todas as ressalvas da baixa independência, autonomia técnico-administrativa e orçamentária.

A composição da Autoridade Nacional de Proteção de Dados é feita por um Conselho Diretor que é o órgão máximo de direção, por um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, por uma Corregedoria, por uma Ouvidoria, por órgão de assessoramento jurídico próprio e, por fim, unidades administrativas e unidades especializadas necessárias[342]. Todavia, neste tópico, pretende-se abordar as competências da ANPD estabelecidas no art.55-J da LGPD[343] para contribuir com o desenvolvimento da arquitetura da cultura de privacidade e proteção de dados no Brasil.

---

[339] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.".

[340] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 55-B. É assegurada autonomia técnica e decisória à ANPD."

[341] VASCONCELOS, Beto e DE PAULA, Felipe. A Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020).**

[342] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 55-C. A ANPD é composta de: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; V - órgão de assessoramento jurídico próprio; e VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei".

[343] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 55-J. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para

Deve-se esclarescer que a função da ANPD não se resume a fiscalizar e aplicar multas, existem várias competências listadas no art. 55-J da LGPD, nas quais pode-se classificar de forma macro, em função 1) preventiva, cooperativa e dialógica; 2) fiscalizatória e sacionátoria; 3) regulatória; por fim, 4) gestão e organização, que são competências relativas a sua própria gestão e organização interna.

---

serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. § 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. § 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. § 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. § 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. § 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. § 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada."

As competências preventivas, cooperativas e diaológicas estão relacionadas as atividades de conscientização, estudos, diretrizes, escuta e cooperação, nacional e internacionalmente, sobre a proteção de dados. Por isso, cabe à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, assim como também promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e medidas de segurança. Promover e elaborar estudos sobre as práticas nacionais e internacionais, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis, bem como, promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional e, por fim, ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante.

Sobre a função dialógica, deve-se ressaltar que o art.55-J, § 4º da LGPD[344] estabelece que ANPD irá manter um fórum permanente de comunicação com cooperação técnica com outros órgão e entidades da administração pública, para fins de facilitar as funções regulatória, fiscalizatória e sancionatória.

Quanto as competências fiscalizatória e sancionatória da ANPD, significa que a autoridade pode fiscalizar e sancionar em caso de tratamento de dados realizado em descumprimento à LGPD, desde que seja por processo administrativo assegurado o contraditório, a ampla defesa e o direito de recurso. Pois, deve zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial e observada a proteção de dados pessoais e do sigilo das informações, apreciar petições de titular contra controlador quando não for solucionada no prazo estabelecido. Garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento.

Ainda sobre essas competências, a Autoridade Nacional pode solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, bem como realizar auditorias, ou determinar sua

---

[344] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.55-J [...] § 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.".

realização, no âmbito da atividade de fiscalização. Além disso, poderá celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa. Em relação a infrações de outras leis e regulamentações a ANPD poderá comunicar às autoridades competentes as infrações penais das quais tiver conhecimento e comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal.

A autoridade também poderá articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação, nesse aspecto, pode-se mencionar a acordo de cooperação realizado entre ANPD e a SENACON e o acordo entre ANPD e o CADE. Mas, cabe exclusivamente à ANPD a aplicação de sanções e as demais competências tem prevalência, no que diz respeito à proteção de dados pessoais, em relação as outros órgãos e entidades, mas que poderá articular sua atuação com órgãos e entidades[345].

As funções fiscalizatória e sancionatória da Autoridade Nacional fazem com que assuma um papel de buscar garantir a aplicação e efetividade da Lei Geral de Proteção de Dados seja por agentes privados seja pelo setor público.

Em relação a competência regulatória, tem-se que cabe à ANPD editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação. Além disso, pode dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial. Inclusive, editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais, nesse sentido, pode deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos.

---

[345] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.".

A competência regulatória é importante para que alguns dispositivos da LGPD tenham seu conteúdo e entendimento sedimentado pela Autoridade Nacional, uma vez que se fossem tratados na própria lei poderia ficar obsoletos com o tempo, em razão do avanço tecnológico. De acordo com Lemos e Branco[346], a LGPD assim como RGPD não identifica as medidas de segurança, técnicas e administrativas e isso não poderia ser diferente, pois quando a lei trata de tecnologia, o detalhamento técnico causaria à obsolescência rapidamente.

Nesse aspecto, a ANPD irá identificar e estimular os padrões técnicos mínimos a serem observados por todos os destinatários da LGPD[347], o que conforme Lemos e Branco "[...] permitirá, ao menos em tese, a atualização periódica desses padrões, deixando-os em conformidade com o estado da arte e alinhados às demandas mais recentes de proteção de dados pessoais dos indivíduos"[348].

Uma observação sobre a regulamentação e normas feitas pela ANPD, é que antes de serem elaboradas, estas deverão ser precedidas por consultas e audiências públicas e análises de impacto regulatório[349].

E, para fins de gestão e organização interna a ANPD pode arrecadar e aplicar suas receitas e publicar, no relatório de gestão, o detalhamento de suas receitas e despesas. Ainda deverá elaborar relatórios de gestão anuais acerca de suas atividades, bem como, implementar mecanismos simplificados, inclusive por meio eletrônico, para fins de reclamações sobre o tratamento de dados pessoais.

Sobre a competência de gestão e organização interna, nota-se que a Autoridade Nacional já realizou o seu Regimento Interno, Portaria Nº1, de 8 de março de 2021[350], o que é essencial para estrutrura, organização e atuação da ANPD.

---

[346] LEMOS, Ronaldo; BRANCO, Sérgio. PRIVACY BY DESIGN:CONCEITO, FUNDAMENTOS E APLICABILIDADE NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.457

[347] Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais".

[348] LEMOS, Ronaldo; BRANCO, Sérgio. PRIVACY BY DESIGN:CONCEITO, FUNDAMENTOS E APLICABILIDADE NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021, p.457.

[349]Cf. BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm> Acesso em: 13.out.2020. "Art.55-J […] § 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.".

[350] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Regimento Interno**, Portaria Nº1, de 8 de março de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 Acesso: 30.maio.2021.

Após analisar as competências da ANPD, é preciso fazer algumas considerações pertinentes à criação "tardia" da ANPD e o cenário de pandemia do COVID-19. Como se pode notar a pandemia acelerou o processo de virtualização no Brasil, instaurando-se o trabalho em *home office*, as aulas *online*, a telemedicina e, principalmente, a comunicação *online*, que já existiam mas tiveram maior aderência em decorrecia do isolamento social, que foi uma das principais medidas adotadas no Brasil para conter o avanço vírus, ocorre que juntamente com essa virtualização houve, por consequência, o aumento do fluxos de dados e informações pessoais.

Assim, considerando o impacto da pandemia e ausência da vigência da LGPD e ausência da ANPD, gerava mais dificuldades sobre a proteção de dados no país, principalmente, pela importância que inicio da atuação da ANPD fosse anterior à vigência LGPD, para que se pudesse promover orientações no sentido de adequação e conformidade à lei. Nesse sentido, Vasconcelos e De Paula afirma que o cenário sem ANPD era de "[...] falta de regras e diretrizes claras, de linhas interpretativas e orientações mínimas de cumprimento, bem como de competências bem consolidadas a partir do início dos trabalhos da autoridade"[351].

Surgem os desafios na governança regulatória da ANPD sobre o tema, de acordo Vasconcelos e De Paula "Um cenário como esse tem o condão de aumentar o grau de violações de direitos fundamentais, seja por agentes privados, seja por órgãos ou entidades públicas"[352].

Dessa forma, com as alterações sobre a *vacatio legis* da LGPD, tem-se que boa parte da legislação entrou em vigência no dia 18 de setembro de 2020, mas as sanções somente vão entrar em vigência em agosto de 2021. Em relação à Autoridade Nacional, verifica-se que foi criada em 2020, realizando a nomeação do Conselho Diretor em 06 de novembro de 2020.

Isso significa que a Autoridade Nacional foi criada recentemente, nesse início de atuação tem-se que o foco é criar a própria estrutura organizacional, definir suas

[351] VASCONCELOS, Beto e DE PAULA, Felipe. A Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

[352] VASCONCELOS, Beto e DE PAULA, Felipe. A Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

atribuições e competências de forma efetiva, o que pode ser extraído do próprio planejamento estratégico 2021-2023, que visa nortear as ações da ANPD.

No planejamento estratégico 2021-2023, apresenta a Missão, Visão e Valores da ANPD, bem como as ações e objetivos para o período de 3 anos. A missão, visão e valores foram traduzidos no mapa estratégico e correlacionados com os objetivos estratégicos, veja-se:

Figura 10- Mapa Estratégico da Autoridade Nacional de Proteção de Dados

Fonte: ANPD[353]

A partir desse documento, é possível extrair os rumos que serão adotados pela ANPD, por meio de seus objetivos e ações buscam perquirir sua visão, cumprir sua missão e guiados pelos valores.

Em realação as ações, estas "[...] são orientadas pelos objetivos estratégicos, e contam com um conjunto de ações internas táticas e operacionais para sua execução". E, os objetivos estratégicos, foram divididos em três: "Objetivo Estratégico 1: Promover o fortalecimento da cultura de Proteção de Dados Pessoais"; "Objetivo Estratégico 2:

[353]BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Planejamento estrátegico 2021-2023**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf Acesso: 18. maio.2021

Estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais" e o "Objetivo Estratégico 3: Aprimorar as condições para o cumprimento das competências legais"[354].

Dessa forma, a ANPD tem muitas atividades para realizar e desafios para enfrentar, sobretudo, em desenvolver a cultura de privacidade e proteção de dados no país, fiscalizar e atuar nos casos de incidentes de dados pessoais.

Percebe-se que a Autoridade Nacional tem realizados acordos de cooperação técnica, que irá impulsionar a sua atuação conjunta com outros órgãos. Em março 2021, houve a assinatura do Acordo de Cooperação Técnia[355] com SENACON, com duração de 24 meses, apresentando como objetivo:

> promoção de ações conjuntas nas áreas de proteção de dados pessoais e defesa do consumidor, incluindo intercâmbio de informações, uniformização de entendimentos, cooperação quanto a ações de fiscalização, desenvolvimento de ações de educação, formação e capacitação e elaboração de estudos e pesquisas[356].

Já em junho de 2021, fechou um acordo de cooperação com o CADE, com duração de sessenta meses e tem como objetivo:

> Cooperação técnica entre a Agência Nacional de Proteção de Dados (ANPD) e o Conselho Administrativo de Defesa Econômica (CADE), para o compartilhamento de informações, estudos, pesquisas e experiências nas matérias em que há intersecção das suas respectivas áreas de competências e de suas finalidades, assim como a promoção conjunta e coordenada de eventos de capacitação relacionados à proteção de dados e da livre concorrência[357].

Em atuação cooperativa técnica entre a ANPD, o Ministério Público Federal (MPF), a Secretaria Nacional do Consumidor (Senacon) e o Conselho Administrativo de Defesa Econômica (Cade), ambos emitiram uma recomendação ao Facebook e ao WhatsApp, relativa à nova política de privacidade do aplicativo de mensagens, solicitaram o adiamento da data prevista para a nova política de privacidade do WhatsApp

---

[354] BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Planejamento estrátegico 2021-2023**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf Acesso: 18.maio.2021

[355]ACORDO De Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados, e a Secretária Nacional do Consumidor do Ministério da Justiça e Segurança Pública- MJSP. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/arquivos/acordo_anpd_senacon_assinado.pdf Acesso: 08.jun.2021

[356] ACORDO de Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados, e a Secretária Nacional do Consumidor do Ministério da Justiça e Segurança Pública- MJSP. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/arquivos/acordo_anpd_senacon_assinado.pdf Acesso: 08.jun.2021

[357] ACORDO de Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados – ANPD e o Conselho Administrativo de Defesa Ecnômica – CADE https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf

(15/05/21). Além disso, solicitaram que não houvesse qualquer tipo de tratamento ou compartilhamento de dados obtidos com base na nova política de privacidade[358].

A Autoridade Nacional tem que buscado fazer acordos de cooperação técnica, o que pode lhe proporcionar mais agilidade em determinadas atuações sobre o tema, pois as outras entidades e órgãos já são consolidados e estruturados há mais tempo. E, isso não lhe retira a autonomia, apenas contribui para o desenvolvimento da privacidade e proteção de dados no país.

Entende-se que a atuação da Autoridade Nacional, neste atual momento, deve ser concebida mais nas funções cooperativas, dialógica e preventiva, do que o enfoque sancionatório, pois ainda é necessário sedimentar alguns entendimentos e regulamentações sejam feitas pela própria Autoridade.

Nesse sentido, a ANPD publicou um Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[359], buscando estabelecer diretrizes orientativas e não vinculativas aos agentes de tratamento e o encarregado.

Ressalta-se que, o fato de que a lei possibilita a autoridade realizar a relagumentação e interpretação não exime que as organizações deixem de implementar o compliance de dados, ou seja, de está em conformidade com a Lei Geral de Proteção de Dados, nessa situação, as empresas devem buscar a adequação à LGPD e fazer os ajustes necessários conforme as regulamentações da ANPD.

No cenário brasileiro, o que se entende como desafiador é a própria mudança cultural, por isso, é preciso pensar em medidas eficazes de conscientização para a sociedade, garantindo a construção dessa mudança em passos, pois sabe-se é uma jornada de transformação cultural e que não se realiza de forma rápida.

Sobre a atuação na conscientização da população, tem-se que o ideal é a construção de conteúdos com linguagem simples, clara e precisa, com a utilização de visual law e legal design, pela aplicação de ícones, imagens, cores, que facilitem a compreensão do leigo.

Portanto, nesse momento inicial, pecerbe-se uma postura da ANPD mais preventiva e dialógica do que sancionatória, até mesmo porque as sanções só entrarão em

---

358 https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade

359 BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021.

vigor em agosto de 2021, sendo este espaço de tempo ideal para as empresas destinarem a implementação dos programas de privacidade e proteção de dados. Além disso, nota-se que há um grande objetivo que é desenvolver a cultura de proteção de dados no país, o que é um grande desafio para Autoridade.

5 CONCLUSÃO

O presente trabalho buscou contribuir academicamente para a temática da proteção de dados pessoais no Brasil, contextualizando a dinâmica do novo cenário informacional e a necessidade de proteção de dados no país, bem como os desafios da governança de dados à realidade brasileira.

A partir da compreensão da arquitetura do ciberespaço, buscou-se demonstrar e analisar a expansão dos novos modelos de negócio e a nova economia informacional, conceituando-se o *big data* e os impactos nas relações sociais, jurídicas e politicas para, então, tratar da sociedade da informação na realidade brasileira.

Embora seja perceptível a existência de um "abismo" na tratativa do assunto entre o Brasil e União Europeia, visto que, nos anos 2000, enquanto que no Brasil era publicado o livro verde falando sobre a sociedade de informação e a necessidade do alfabetismo digital, no mesmo ano, a União Europeia já estava reconhecendo os dados pessoais como direito fundamental, essa diferença na realidade não pode ser ignorada, mas sim trabalhada para o desenvolvimento da cultura de proteção de dados e privacidade.

Sendo notória a influência da Regulamento Geral de Proteção de Dados da União Europeia na construção da legislação de proteção de dados no Brasil, fruto de um movimento convergência das regulamentações protetivas frente à circularidade transfronteiriços dos dados.

Em relação aos fundamentos e princípios da proteção de dados pessoais no país, tem-se a concepção de que a proteção de dados implica na autodeterminação informacional do titular e essa proteção se revela como um direito fundamental no ordenamento jurídico brasileiro, levando-se em consideração a decisão proferida pela Relatora Ministra Rosa Weber do STF.

Entende-se que os princípios possibilitam a funcionalização do direito face ao avanço tecnológico. Além disso, no sistema do ordenamento jurídico brasileiro, nas situações em que haja conflitos entre normas propõe-se a aplicação da Teoria do Diálogo das Fontes face os critérios da hierarquia, especialidade e cronológico.

Com a crescente utilização de novas tecnologias, principalmente, por causa da pandemia, que instaurou um cenário de medidas restritivas como o isolamento social, acelerando o processo de virtualização no país, de forma impositiva e sem ser devidamente planejada, tem-se que as tecnologias facilitaram a continuidade e/ou início de muitas atividades de forma *online*, expandindo novas formas de negócios e modificando as relações sociais. Por outro lado, também evidenciou vulnerabilidades na proteção de dados pessoais e privacidade, pelos casos noticiados de grandes vazamentos de dados e ataques cibernéticos aos sistemas de seguranças de empresas e do poder público.

Buscando conciliar a proteção do titular e o desenvolvimento econômico, a Lei Geral de Proteção de Dados Pessoais estabeleceu as bases legais para a realização de tratamento de dados, assim como determina a governança de dados e a segurança da informação e sigilo dos dados.

Quanto à governança de dados, deve-se fazer algumas observações, entende-se como necessária, em certos aspectos, fazer correlação com o Regulamento Geral de Proteção de Dados para melhor implementar o programa de proteção de dados e privacidade, além disso, alguns dispositivos normativos atribuíram a Autoridade Nacional de Proteção de Dados a função de regulamentação, mas que ainda não foram realizados, até mesmo porque a ANPD foi criada recentemente e pelo que se percebe está fazendo consultas e audiências públicas, promovendo o diálogo antes de publicar seus atos normativos.

Foram analisadas as principais perspectivas para implementar um programa de proteção de dados e privacidade, mas sem esgotar o tema, destacando-se os processos e procedimentos internos para o desenvolvimento de governança de dados, tais como a necessidade de uma visão dos fluxos de dados, por isso, a importância de realizar um *data mapping,* em seguida, compreender a situação em que a empresa se encontra, ou seja, realizar uma análise inicial da empresa para se ter um "diagnóstico" dos riscos e vulnerabilidades relativas aos dados e a partir disso realizar o planejamento de medidas que de proteção de dados e privacidade.

Além disso, é necessária uma adequação de documentos e contratos, seja internamente, como o código de ética da empresa e as políticas de privacidade e proteção de dados desenvolvidas para fins internos da empresa, assim como, externamente, como contratos realizados com empresas parceiras e fornecedores, e os contratos e política de privacidade e proteção de dados desenvolvidas para acesso ao cliente e/ou titular.

Ressalta-se que LGPD destina uma seção para segurança e sigilo dos dados, dada à importância da implementação e/ou melhorias no que diz respeito ao *privacy by design* e *privacy by default* e sistema da informação e sigilo de dados. Nesse aspecto, como ainda não se tem um posicionamento oficial da ANPD, e devido à relevância para atender à LGPD, buscou-se *standards* das ABNT NBR ISO/IEC 27001:2013; ABNT NBR ISO/IEC 27002:2013, ABNT NBR ISO/IEC 27701:2019 para servirem de parâmetros a serem adotados pelas organizações, e como é bem observado pelas normativas, servem para todos os tipos de empresas.

Deve-se pontuar, que todos os processos e procedimentos de adequação por melhores que sejam, não são imunes ao fator humano, isso significa que realizar adequação à LGPD não é simplesmente um "basta aplicar a lei" ou "fazer relatórios e colocar um sistema de segurança", existe o fator humana, que não pode ser desprezado, aliás, deve ser dada maior relevância nesse momento de transformação cultural. Principalmente, porque a sociedade brasileira está iniciando uma conscientização sobre a importância da proteção de dados, nesse sentido, percebe-se acertadamente que um dos objetivos da Autoridade Nacional é a promoção da cultura da privacidade e proteção de dados pessoais.

A transformação cultural é, na percepção deste trabalho, o maior desafio, em razão dos fatores apontados no início desta pesquisa. A realidade brasileira é bem diferente da realidade dos países europeus, no Brasil tem-se problemas estruturais e que refletem na sociedade da informação. Por isso, desde dos anos 2000, o livro verde já apontava a necessidade de um letramento digital, hoje precisa ir além de uma educação para as tecnologias digitais, sendo necessária uma mudança cultural para uma cultura da privacidade e proteção de dados, ou seja, não basta saber usar as tecnologias disponíveis é preciso conhecer os direitos estabelecidos na LGPD, para fins de proteção de dados e privacidade e, consequentemente, o livre desenvolvimento da personalidade e a autordeterminação informacional.

A realidade cultural causa impactos na própria implementação do programa de privacidade e proteção de dados das empresas, pois a não compreensão dos funcionários e colaboradores sobre a importância dos dados e informações poderá ocasionar incidentes (evitáveis) e afetar os direitos dos titulares. A partir disso, buscou-se analisar perspectivas que fossem além de uma capacitação e treinamento dos funcionários, claro sem lhe retirar a importância, mas pensou-se ir além, na compreensão do próprio mecanismos de escolhas humanas baseados em estudos da neurociência, em que se destaca a importância

da utilização de *nudges* para fins de melhorias de escolhas e condutas desejáveis, gerando uma arquitetura de escolhas ética e responsável com os propósitos do programa de privacidade e proteção de dados pessoais.

Sabe-se que a Lei Geral de Proteção de Dados por si só não colocou o país ao nível de proteção exigido pela União Europeia, nota-se que mesmo com a criação da Autoridade o país ainda não atingiu tal nível de adequação, o que possibilita diante deste cenário, levando-se em consideração os desafios para adequação como o tempo, o custo e a mudança cultural, cogitar que algumas empresas realizem sua adequação, inclusive, com certificações internacionais e solicite o reconhecimento de adequação no âmbito internacional, para fins de continuação das atividades de tratamento e circulação de dados internacionalmente, já outra empresas façam adequação à LGPD, sem contudo, obter reconhecimento ao nível internacional, e empresas que terão dificuldades e/ou continuarão inertes.

Por isso, entende-se que a ANPD possui um papel importante na governança de dados, pois cabe a autoridade o desempenho de suas funções, que foi dividia em: 1) preventiva, cooperativa e dialógica; 2) fiscalizatória e sacionátoria; 3) regulatória; por fim, 4) gestão e organização, que são competências relativas a sua própria gestão e organização interna. Ressaltando-se que, nesse momento de mudança, percebe-se uma atuação mais preventiva, cooperativa e dialógica e com objetivos estratégicos no sentido de "promover o fortalecimento da cultura de Proteção de Dados Pessoais"; "estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais" e o "aprimorar as condições para o cumprimento das competências legais", são realmente importantes, sobretudo, para a transformação cultural da sociedade e adequação das empresas.

Portanto, em razão dos avanços tecnológicos, aumento e circulação de dados e informações, bem como as vulnerabilidades relativas à proteção dos dados dos titulares, surgem regulamentações protetivas de dados, inclusive, no Brasil. Nesse sentido, é notória a existência de uma convergência das legislações sobre proteções de dados, até mesmo por causa da ausência de fronteiras na circulação dados e informações, que se entende como positivo, pois se fossem completamente diferentes poderia causar problemas jurídicos e econômicos, até mesmo inviabilizar muitos modelos de negócios.

Mas um aspecto que não pode ser ignorado, é que a Lei Geral de Proteção de Dados Pessoais não altera apenas relações jurídicas, impõe-se uma mudança jurídica, econômica, política e social, sendo o maior desafio o aspecto social, pois não existe

mudança cultural rápida, é um processo de produção e mudança de valores sociais, começando pela educação.

Conclui-se que, o movimento de transformação cultural tornou-se mais forte com a entrada em vigor da Lei Geral de Proteção de Dados, devido à necessidade de adequação pelas empresas, bem como com a criação da ANPD que possui um papel importante na promoção da cultura de proteção de dados e privacidade, conscientizando a sociedade sobre a importância dos dados e informações pessoais.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701:2019 - **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. ABNT, 2019.

ACORDO de Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados, e a Secretária Nacional do Consumidor do Ministério da Justiça e Segurança Pública-MJSP. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/arquivos/acordo_anpd_senacon_assinado.pdf Acesso: 08.jun.2021

ACORDO de Cooperação Técnica entre a Autoridade Nacional de Proteção de Dados – ANPD e o Conselho Administrativo de Defesa Ecnômica – CADE https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf Acesso: 08.jun.2021

ÁVILA, Humberto. Teoria dos princípios jurídicos. **Da definição à aplicação dos princípios jurídicos**. 18ª ed. São Paulo: Malheiros, 2018.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Tradução: Carlos Alberto Medeiros. Rido de Janeiro: Zahar, 2013.

BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados (AIPED). *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 Reimpressão, Rio de Janeiro: Forense, 2019.

BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileir de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** [livro eletrônico]/ Ana Frazão Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., rev., aum. e mod. São Paulo: Saraiva, 2015.

BOBBIO, Noberto. **Da Estrutura à Função**: novos estudos de teoria do direito. Tradução de Daniela Beccaccia Versiani; revisão técnica de Orlando Seixas Bechara; Renanta Nagamine. Barueri, São Paulo: Manole, 2007.

BOBBIO, Noberto. **Teoria do Ordenamento jurídico**. Tradução de Ari Marcelo Solon; prefácio de Celso Lafer; apresentação de Tercio Sampaio Ferraz Junior. São Paulo, EDIPRO, 2. Ed. 2014.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.

BRASIL, Lei nº 12.527, DE 18 DE NOVEMBRO DE 2011." **Lei de Acesso à Informação".** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso: 08.jun.2021.

BRASIL, Lei nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Dispõe sobre a tipificação dos crimes cometidos eletronicamente**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso: 21.maio.2021.

BRASIL, Supremo Tribunal Federal. **ADI 6387**. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf Acesso: 20.maio.2021.

BRASIL. **Código Civil (LEI No 10.406, DE 10 DE JANEIRO DE 2002)**. Brasília, DF, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso: 19. Ago. 2020.

BRASIL. Constituição Federal de 1988. **Constituição da República Federativa do Brasil**, Brasília, DF, Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ ConstituicaoCompilado.htm>. Acesso em: 27 de julho de 2018.

BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Peossoais e do Encarregado**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso: 08.jun.2021.

BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Comunicação de incidentes de segurança**. Brasilia- DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso: 08.jun.2021.

BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Regimento Interno**, Portaria Nº1, de 8 de março de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 Acesso: 30.maio.2021.

BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Planejamento estrátegico 2021-2023**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf Acesso: 18.maio.2021.

BRASIL. Governo Federal. Autoridade Nacional de Proteção de Dados. **Acesso à Informação**. Convênios e Transferências. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/repasses-e-transferencias-de-recursos-financeiros Acesso: 06.jun.2021.

BRASIL. **Lei do Marco Civil da Internet (lei no 12.965, de 23 de abril de 2014).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 10. Jan. 2020.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (lei no 13.709, de 14 de agosto de 2018)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 13.out.2020.

BRASIL. **LEI Nº 14.129, DE 29 DE MARÇO DE 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm Acesso: 30.maio.2021

BRASIL. **Proposta de Emenda à Constituição n. 17/2019**, pelo Senado Federal, que: "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". Senado Federal, Brasília, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais Acesso em: 20.jan.2021.

BRASIL.**CÓDIGO DE DEFESA DO CONSUMIDOR**. Lei nº 8.078 de 11 de Setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm Acesso: 08.jun.2021.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* **The Guardian**. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election Acesso em: 24.nov.2019.

CAMURÇA, Lia Carolina Vasconcelos. Sociedade de Vigilância, direito à privacidade e proteção de dados pessoais: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor – usuário/ Lia Carolina Vasconcelos Camurça. **Dissertação (mestrado)** – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós- Graduação em Direito, Fortaleza, 2020.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. BOAS PRÁTICAS E GOVERNANÇA NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.

CASTELLS, Manuel. A Sociedade em Rede: do Conhecimento à Política. *In:* CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém: Imprensa Nacional, 2005.

CASTELLS, Manuel. **A Sociedade em Rede**. Tradução: Roneide Venacio Majer. 20. Ed. rev. Ampl. São Paulo: Paz e Terra, 2019.

CASTELLS, Manuel. **O Poder da Comunicação**. Tradução de Vera Lúcia Mello Joscelyne; Revisão de Tradução de Isabela Machado de Oliveira Fraga. 3ª ed. São Paulo/Rio de Janeir: Paz e Terra, 2019.

CAVOUKIAN, Ann. ***Privacy by design****: The 7 foundation principles Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner of Ontario 2 Bloor Street East, Suite 1400* Toronto, Ontario, CANADÁ. Disponível em: https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf Acesso: 02.jun.2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 Ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [*et al*]. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. Princípios de proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira (coord.). **Direito & Internet III-tomo I: Marco Civil da Internet (Lei nº 12.965/2014)**. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. Reflexões Sobre Proteção de Dados Pessoais em Redes Sociais. **RIPDP – Revista Internacional de Protección de Datos Personales**. Universidad de los Andes. Faculdade de derecho (Bogotá, Colombia). No. 1 Julio – Diciembre de 2012.

DONEDA, Danilo. Um Código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, 2003, p.i. Disponível em: https://www.researchgate.net/profile/Danilo-Doneda/publication/266036287_Um_Codigo_para_a_protecao_de_dados_pessoais_na_Italia/links/5934046b0f7e9beee7bcd261/Um-Codigo-para-a-protecao-de-dados-pessoais-na-Italia.pdf Acesso: 15.jun.2021.

DUHIGG, Charles. ***How Companies Learn Your Secrets.*** *New York Times*. Disponível em: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp> Acesso em: 14.out.2019.

DURKHEIM, Émile. As Regras do Método Sociológico, 3ª edição. **São Paulo: Martins Fontes**, 2007.

EUROPEIA, União. Carta dos direitos fundamentais da União Europeia. **DIREITO E DEMOCRACIA**. Disponível em: https://www.researchgate.net/profile/Betania-Alfonsin/publication/43236353_O_Estatuto_da_cidade_e_a_construcao_de_cidades_sustentaveis_justas_e_democraticas/links/5554aff108ae980ca60acf15/O-Estatuto-da-cidade-e-a-construcao-de-cidades-sustentaveis-justas-e-democraticas.pdf#page=205 Acesso: 23.maio.2021.

FOTIOS, Ricardo. Vazamentos de dados aumentaram 493% no Brasil, mostra pesquisa do MIT: Base construída por pesquisador brasileiro identifica mais de 26 bilhões de informações à disposição de criminosos no mundo em dois anos. **Coluna Ricardo Fotios: Cultura. UOL**, online. Disponível em: https://cultura.uol.com.br/noticias/colunas/ricardofotios/35_vazamentos-de-dados-aumentaram-493-no-brasil-mostra-pesquisa-do-mit.html Acesso: 10.jun.2021

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

GOMES, Orlando. **Introdução ao direito civil**. 18 ed. Rio de Janeiro: forense, 2001.

GOVERNO FEDERAL. **Oficina Dirigida Relatório de Impacto à Proteção de Dados Pessoais – RIPD**, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/apresentacao-oficina_ripd_v2.pdf Acesso em: 15.jun.2021

GOVERNO FEDERAL. **Relatório de Impacto à Proteção de Dados – RIPD**. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiatemplateRIPD.pdf Acesso: 15.jun.2021.

GRAU, Eros Roberto. **Por que eu tenho medo de juízes**: (a interpretação/aplicação do direito e os princípios), 8ed. refundida do ensaio e discurso sobre interpretação. São Paulo: Malheiros, 2017.

HAGAN, Margaret. **Law by Design**. Ebook (*online*). Disponível em: https://www.lawbydesign.co/design-mindsets/#feasibility. Acesso em: 18. abril. 2021.

HUMBY, Clive. Data is the new oil. ANA Senior marketer's summit, **Kellogg School**, 3 Nov. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html Acesso em: 30.maio.2021

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC. **Dados pessoais**: tudo que você precisa saber sobre seus direitos- Linha do tempo. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo Acesso em: 21.maio.2021.

KAHNEMAN, Daniel. **Rápido e Devagar**: duas formas de pensar. Tradução Cássio de Arantes Leite. 1ªed. Rio de Janeiro: Objetiva, 2012.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. ***Private traits and attributes are predictable from digital records of human behavior***. Disponível em: https://www.pnas.org/content/110/15/5802 Acesso em: 12.out.2019.

LANEY, Doug. *3D Data Management: Controlling Data Volume, Velocity and Variety.* **Stanford**, Connecticut: META Group, 2001. Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf Acesso em: 08. Fev.2020.

LAWRENCE, Lessig. **Código: Versão 2.0**. Aufl. Nova York , 2006.

LEMOS, Ronaldo; BRANCO, Sérgio. PRIVACY BY DESIGN:CONCEITO, FUNDAMENTOS E APLICABILIDADE NA LGPD. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.

LÉVY, Pierre. **O que é virtual?** Tradução de Paulo Neves, 2ª Edição, São Paulo, Editora 34, 2011, p.20-21.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **Direito digital: compliance, regulação e governança**. São Paulo: Quartier Latin, 2019.

MACHADO, Joana de Moraes Souza. Caminhos para tutela da privacidade na sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil / Joana de Moraes Souza Machado. - 2014.185 f. **Tese** (doutorado) – Universidade de Fortaleza, 2014.

MAIA, Ana Carolina; NYBO, Erik Fontenele; CUNHA, Mayara. ***Legal Design***: Criando Documentos que fazem sentido para os usuários. São Paulo, SP: Saraiva Educação, 2020 [Ebook] p.i.

MARQUES, Cláudia Lima, SUPERAÇÃO DAS ANTINOMIAS PELO DIÁLOGO DAS FONTES: O MODELO BRASILEIRO DE COEXISTÊNCIA ENTRE O CÓDIGO DE DEFESA DO CONSUMIDOR E O CÓDIGO CIVIL DE 2002. **REVISTA DA ESMESE**, Nº 07, 2004 – DOUTRINA, p.43 Disponível em: https://core.ac.uk/download/pdf/79073279.pdf Acesso: 08.jun.2021

MAYER-SCHONBERGER, Viktor; CUJIER, Kenneth. **Big Data**: Como extrair volume, variedade e valor da avalanche de informação cotidiana. Tradução de Paulo Polzonoff Junior. Rio de Janeiro:Elsevier, 2013, p. 4

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace*. **Contexto Internacional** , v. 42, n. 1, pág. 31-54, 2020.

NETmundial: declaração multisetorial [livro eletrônico] /Núcleo de Informação e Coordenação do Ponto BR ; [Carlos Francisco Cecconi coordenação ; tradução para o português Carlos Alberto Afonso ; traduções para os demais idiomas ICANN Language Services Team]. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2014. 544 Kb ; PDF.

Núcleo da Informação e Coordenação do Ponto BR - NIC.br. **Pesquisa sobre o uso das tecnologias de informação e comunicação: pesquisa TIC Domicílios**, ano 2018: Tabelas. Disponível em: http://cetic.br/arquivos/domicilios/2018/domicilios/#tabelas Acesso em: 08.dez.2019.

OCDE. **Recomendação do Conselho sobre as Diretrizes que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais**.Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188?_ga=2.190186027.1064690390.1621449249-1613775020.1621449249 Acesso em: 30.maio.2021

OECD (2020), *A Caminho da Era Digital no Brasil*, OECD Publishing, Paris, *https://doi.org/10.1787/45a84b29-pt*.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo : Thomson Reuters Brasil, 2020, p.i.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009, p.10-11.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede:** cibersegurança, regime global de vigilância social e direito à privacidade no século XXI [recurso eletrônico] / João Pedro Seefeldt Pessoa -- Porto Alegre, RS: Editora Fi, 2020.

PRIVACIDADE HACKEADA. **Documentário**. Direção Karim Amer e Jehane Noujaim. Netflix. 114 min., 2019.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD). **Regulamento (UE) 2016/679** Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1623285622306&from=EN Acesso: 03.maio.2021

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAAVEDRA, Giovani Agostini. Compliance de Dados. *In*: **Tratado de proteção de dados pessoais**. Coordenadores DONEDA, Danilo [et al.]. Rio de janeiro: Forense, 2021.

SANTOS, Beatriz Rosa Pinheiro dos; CAMILO, Everton da Silva; MELLO, Mariana Rodrigues Gomes. Big Data e Inteligência Artificial: Aspectos Éticos e Legais Mediante Teoria Crítica. **Complexitas** - Rev. Fil. Tem., Belém, v. 3, n.1 , p. 50-60, jan./jun. 2018.

SERVICO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO. **MAPA DA PROTEÇÃO DE DADOS:** Em que "estágio" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/mapa-sobre-protecao-de-dados-no-mundo/view Acesso: 15.maio.2021.

SILVA, Alexandre Ribeiro da. A Proteção de Dados no Brasil: a tutela do direito à privacidade na sociedade de informação. **Dissertação**. Faculdade de Direito da Universidade Federal de Juiz de Fora. Disponível em: <http://bdtd.ibict.br/vufind/Record/UFJF_939b28947f81c4d5a1870fa48a420784> Acesso em: 17.out.2019.

SILVA, Leandro Augusto da; PERES, Sarajane Marques; Clodis Boscarioli. **Introdução à mineração de dados**: com aplicações em R. Rio de Janeiro: Elsevier, 2016.

SIMONITE, Tom. *When It Comes to Gorillas, Google Photos Remains Blind.* **WIRED.** Disponível em: https://www.wired.com/story/when-it-comes-to-gorillas-google- photos-remains-blind/ Acesso em: 13.out.2019.

SOCIEDADE da informação no Brasil: **Livro Verde** / organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000.

SOUZA, Carlos Affonso Pereira de. SEGURAÇA E SIGILO DOS DADOS PESSOAIS: PRIMEIRAS IMPRESSÕES À LUZ DA LEI 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação** / Carlos Affonso Souza e Ronaldo Lemos, Juiz de Fora: Editar Editora Associada Ltda, 2016.

SOUZA, Carlos Affonso. Privacidade e Proteção de Dados no Brasil. **TEDx**. Disponível em: https://www.youtube.com/watch?v=Zau-x-j_Uu8 Acesso em: 30. Jan.2020.

THALER, Richard H; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução: Ângelo Lessa. 1ª ed. Rio de Janeiro: Objetiva, 2019.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In*: **Comentários ao GDPR.** BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (coord.).São Paulo: Thomson Reuters Brasil, 2018.

VASCONCELOS, Beto e DE PAULA, Felipe. A Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro** [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva, coordenação. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.i.

VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava**:**Vazamento inclui CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais; Serasa nega ser fonte dos dados. **Tecnoblog**. 2021, online. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/ Acesso: 10.jun.2021.

WARREN, Samuel D; BRANDEIS, Louis D. *The Right to Privacy*. **Harvard Law Review**. v. 4, p. 193-196, 1890.

ANEXOS

ANEXO 1- Formulário de Comunicação de Incidente de Segurança com Dados Pessoais à Autoridade Nacional de Proteção de Dados (ANPD)

Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)

Comunicação

Tipo de comunicação:

☐Completa.
☐Parcial.

Para comunicação parcial:

☐Preliminar.
☐Complementar.

Critério para a comunicação:

☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
☐Não tenho certeza sobre o nível de risco do incidente de segurança.

Agente de tratamento

O notificante é:

☐Controlador.
☐Operador.
Se operador, informar se já houve comunicação ao controlador: *[Resposta]*

Dados do agente de tratamento:

Número do CPF ou CNPJ: *[●]*
Nome ou Razão Social: *[●]*
Natureza da Organização *(Pública ou Privada)*: *[Resposta]*
Endereço: *[Resposta]*
Cidade: *[Resposta]*
Estado: *[Resposta]*
CEP: *[Resposta]*
Telefone: *[Resposta]*

E-mail: *[Resposta]*

Dados do notificante:

Nome: *[Resposta]*
E-mail: *[Resposta]*
Telefone: *[Resposta]*

Dados do encarregado:

☐Mesmos dados do notificante.
Nome: *[Resposta]*
E-mail: *[Resposta]*
Telefone: *[Resposta]*

Incidente de segurança

Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu.

[Resposta]

Quando o incidente ocorreu?

[Data e hora]
☐Não tenho conhecimento. Justifique: *[Resposta]*
☐Não tenho certeza. Justifique: *[Resposta]*

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descreva como a organização teve ciência do incidente de segurança.

[Resposta]

Se a comunicação inicial do incidente não foi comunicada no prazo sugerido de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos.

[Resposta]

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

[Resposta]

Qual a natureza dos dados afetados?

☐Origem racial ou étnica.
☐Convicção religiosa.
☐Opinião política.
☐Filiação a sindicato.
☐Filiação a organização de caráter religioso, filosófico ou político.
☐Dado referente à saúde.
☐Dado referente à vida sexual.
☐Dado genético ou biométrico.
☐Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).
☐Dado financeiro.
☐Nomes de usuário ou senhas de sistemas de informação.
☐Dado de geolocalização.
Outros: *[Resposta]*

Qual a quantidade de titulares afetados?

[Resposta]

Qual a categoria dos titulares afetados?

☐Funcionários
☐Prestadores de serviço
☐Clientes
☐Consumidores
☐Usuários
☐Pacientes de serviço de saúde
☐Crianças ou adolescentes
Outros: *[Resposta]*

Medidas de segurança utilizadas para a proteção dos dados

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?
[Resposta]

Riscos relacionados ao incidente de segurança

Quais as prováveis consequências do incidente de segurança para os titulares afetados?
[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?
[Resposta]

Comunicação aos titulares de dados

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?
☐Sim
☐Não
☐Não sei

Forneça detalhes.
[Resposta]

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?
[Resposta]