INSTITUTO BRASILIENSE DE DIREITO PÚBLICO – IDP
ESCOLA DE DIREITO DE BRASÍLIA
CURSO DE GRADUAÇÃO EM DIREITO

LUÍZA RIBEIRO DE MENEZES SOUZA

PROTEÇÃO DE DADOS PESSOAIS: ESTUDO COMPARADO DO REGULAMENTO 2016/679 DO PARLAMENTO EUROPEU E CONSELHO E O PROJETO DE LEI BRASILEIRO N. 5.276/2016

BRASÍLIA
2017

LUÍZA RIBEIRO DE MENEZES SOUZA

PROTEÇÃO DE DADOS PESSOAIS: ESTUDO COMPARADO DO REGULAMENTO 2016/679 DO PARLAMENTO EUROPEU E CONSELHO E O PROJETO DE LEI BRASILEIRO N. 5.276/2016

Trabalho de Conclusão de Curso apresentado ao Instituto Brasiliense de Direito Público, como requisito parcial para à obtenção do título de Bacharel em Direito.

Orientador: Guilherme Pereira Pinheiro

BRASÍLIA

2017

LUÍZA RIBEIRO DE MENEZES SOUZA

PROTEÇÃO DE DADOS PESSOAIS: ESTUDO COMPARADO DO REGULAMENTO 2016/679 DO PARLAMENTO EUROPEU E CONSELHO E O PROJETO DE LEI BRASILEIRO N. 5.276/2016

Trabalho de Conclusão de Curso apresentado ao Instituto Brasiliense de Direito Público, como requisito parcial para à obtenção do título de Bacharel em Direito.

Brasília, 01 de dezembro de 2017.

_____

Prof. Dr. Guilherme Pereira Pinheiro
Instituto Brasiliense de Direito Público
Professor Orientador

_____

Prof. Me. Alexandre Sankievicz
Instituto Brasiliense de Direito Público
Professor

_____

Prof. Ma. Janete Ricken Lopes
Instituto Brasiliense de Direito Público
Professora

Em agradecimento à minha mãe, que com muito carinho, compreensão e paciência, acreditou e me apoiou em todos os momentos.

RESUMO

A sociedade atualmente presencia um avanço tecnológico cada vez mais transformador e a regulação nacional recentemente percebeu que uma nova legislação deve ser formulada para acompanhar as mudanças e, principalmente, resguardar os usuários da internet. Dessa forma, o presente estudo tem por objetivo analisar o Projeto de Lei n. 5.276/2016 que positiva sobre a proteção de dados pessoais a partir da comparação das normas que constituem o recente Regulamento 679/2016 da União Europeia. Busca verificar a aplicabilidade do projeto de lei que deve resguardar princípios fundamentais para que a norma seja plenamente efetiva e legal, além de se ajustar a expectativas internacionais.

Palavras-Chave: Proteção de Dados Pessoais. Responsabilidade civil. Projeto de Lei 5.276/2016. Regulamento 679/2016.

ABSTRACT

The current society witnesses technological advance more and more transformer and the National Regulation recently noticed a new legislation must be formulated to follow changes and, mainly, to protect the internet users. Therefore, the present search has as an object to analyze the Law Project n. 5276/2016 that disposes about the protection of personal data from the comparison of standards wich constitute the recent regulation 679/2016 of the European Union. It quests to verify the applicability of the Law Project that must protect fundamental elements for the standard to be effective and legal, besides to adjust to the international expectations.

Keywords: Protection of personal data. Civil responsibility. Law project 5276/2016. Regulation 679/2016.

SUMÁRIO

INTRODUÇÃO

Os dados pessoais são encontrados em inúmeras situações, sendo até mesmo difícil encontrar um tipo de negócio que esteja completamente apartado da utilização de dados pessoais, tanto na esfera privada como na pública. Devido a isso, não é incomum que a segurança dos dados muitas vezes seja negligenciada, ocasionando riscos ao titular. Logo, o que antes era uma preocupação específica às figuras públicas, de terem sua vida privada protegida, passou a ser generalizada na medida em que os dados pessoais de todos os cidadãos são tratados e utilizados das mais diversas maneiras e muitas vezes sem a devida autorização.

Buscando resguardar os titulares dos dados, vários países já formularam normas para resguardar os titulares dos dados. A lei 12.965/14, popularmente conhecida como Marco Civil da Internet, foi um grande avanço para a normatização dos eventos que ocorrem no meio virtual, ao prever princípios, garantias, deveres e direitos aos usuários da internet, mas apesar de ser um dispositivo que determina de forma expressa a proteção de dados como princípio, não conseguiu abordar todas as questões da matéria integralmente.

Isto posto, o Brasil encontra-se em situação delicada, principalmente após os escândalos de espionagem norte-americana – caso Snowden – quando foi possível constatar que o país está despreparado para lidar com possíveis violações de dados pessoais, mesmo que a jurisprudência já tenha se posicionado acerca de casos sobre dados pessoais e algumas leis já tenham articulado sobre o assunto, as decisões ainda são contraditórias e as leis abordam o tema de forma superficial ou específica para apenas um setor, deixando todos os outros casos desprotegidos.

Observando essa situação e a urgência de uma lei geral, o Poder Executivo por meio do Projeto de Lei n. 5.276/16, formulou o regulamento que busca centralizar as normas de proteção de dados em um único dispositivo. Tendo em vista essa situação do direito brasileiro, o presente trabalho tem por objetivo analisar três dos principais pontos que uma lei de proteção de dados deve aborda e comparar com o regulamento 679/2016 da União Europeia, que entrará em vigor no ano de 2018. A União Europeia retém vários anos de estudo sobre o assunto e aplicação de regulações específicas, portanto, conseguiu apresentar uma lei mais completa e atualizada, servindo de balança para a constatação se o projeto de lei brasileiro está completo e ideal para aplicação.

O Projeto de Lei n. 5.276/2016 claramente se baseou no Regulamento 627/2016 da UE, com diversos artigos que apresentam redação muito próxima a do referido regulamento,

mas alguns pontos importantes aparentam estar mais simplificados na lei brasileira do que na estrangeira, sendo inclusive visível pela diferença do número de artigos. Contudo, será o texto da lei que determinará se todas as questões que causam controvérsias e são necessárias para a proteção de dados foram abordadas no dispositivo.

Antes mesmo de se comparar a letra do projeto de lei brasileiro com a estrangeira, é preciso compreender a trajetória dos dados pessoais e a sua aplicação nos diversos âmbitos sociais e, a partir disso, observar a magnitude dos dados pessoais e a importância da sua proteção. Com base nisso, será analisada a principal lei vigente que trata hoje do assunto, o Marco Civil da internet, para que o trabalho possa contextualizar com o atual cenário e observar, por meio da analise dos artigos, as brechas deixadas pelo dispositivo e que precisam ser definidas de forma mais clara, para que, por fim, seja analisado o projeto de lei de dados pessoais, que será o objeto de estudo do trabalho.

Previamente ao estudo comparado, alguns elementos essenciais serão tratados para que haja a compreensão do objeto do projeto de lei, quais as possibilidades de se ter os dados pessoais processados e, finalmente, a expectativa de ser aplicada a responsabilidade civil nos casos de danos aos titulares.

O segundo capítulo trata dos dados pessoais e seus tipos, pois é a partir desse conceito que o nível de proteção será moldado, respeitando as características de cada dado e principalmente os riscos que o tratamento pode acarretar. Será estudado o conceito geral de dados pessoais e o conceito dos dados pessoais sensíveis e da possibilidade de transformação de dados pessoais em dados anônimos, sendo esse um dos caminhos para a proteção do titular.

Partindo do pressuposto que os dados pessoais são informações que determinam características de um indivíduo, ainda no segundo capítulo, é apresentado o ato do consentimento e seus limites. A importância desse estudo se encontra no fato de que, para que haja a possibilidade do tratamento de dados, a anuência do titular é o meio autorização, pois o indivíduo deve ter o direito de decidir sobre o que será feito com seus dados, salvo exceções. Ademais, pertinente ao assunto, é assimilar quais os limites do consentimento tendo em vista que, de certa forma, o titular abre mão de um direito fundamental expresso no art. 5º da Constituição, ao consentir com o tratamento de seus dados.

Na mesma oportunidade questiona-se se a anuência do titular pode ser equiparada a contrato e, caso resposta afirmativa, que tipo de contrato seria possível respeitando-se todos os princípios para a formação de um consentimento legítimo.

A partir da classificação de dados pessoais, as possíveis consequências de um processamento e a compreensão do consentimento como requisito para o tratamento de dados, a responsabilidade civil é abordada no capítulo seguinte para que os danos causados aos usuários sejam reparados. A futura lei de proteção de dados pessoais deve prezar por um meio de indenizar os titulares que sofrerem danos, além de incentivar que o cumprimento da lei seja eficaz.

O tratamento de dados pessoais dispõe de algumas figuras importantes para a atividade, sendo elas as principais responsáveis pela segurança dos dados após o consentimento do titular, logo, é preciso que se saiba sobre a possibilidade de responsabilização desses agentes e qual tipo será cabível, para isso, é feito um estudo doutrinário e jurisprudencial sobre o assunto, para ser constatado como a jurisprudência se comporta atualmente e qual tipo de responsabilidade, preservando todos os objetivos de uma ei de proteção de dados, deve ser aplicada no caso em concreto.

O último capítulo do trabalho visa o estudo comparado do projeto de lei n. 5.276/2016 e o Regulamento 627/2016 da União Europeia. Esse estudo pretende verificar o nível de adequação do projeto de lei brasileiro aos moldes da moderna legislação sobre o tema. Nesse capítulo será retomado os dois primeiros pontos do trabalho, consentimento e responsabilidade, mas de acordo com o positivado na lei estrangeira e comparando tais elementos com o determinado no PL brasileiro.

Por fim, para que tudo o que foi tratado no trabalho e determinado pelo projeto de lei seja efetivamente cumprido, é preciso que seja constituído um órgão responsável pela fiscalização das atividades de processamento de dados, dessa forma, o último ponto do trabalho finalizará discorrendo sobre as características e responsabilidades trazidas pelo regulamento europeu para determinar o órgão fiscalizador das normas e a comparação com o determinado no PL brasileiro, além das peculiaridades para que a sua formação seja feita de forma legal.

1. INTERNET

A rede mundial de computadores tornou-se o principal meio de troca de informações da atualidade, apesar dos diversos avanços positivos, algumas situações de risco aos usuários surgiram e a necessidade de uma regulamentação passa a ser imprescindível.

1.1 Evolução Histórica dos Dados Pessoais

Os dados pessoais são cumulações de fatos e acontecimentos que formam a personalidade de cada indivíduo, os dados pessoais podem contar de forma precisa a história de vida de cada cidadão. Com o passar dos anos, essas informações tiveram diversos meios de existirem, desde diários, cartas, telegramas e fotos chegando finalmente a internet, por meio de email, blogs, redes sociais. Especificamente no setor Público, o surgimento do processamento eletrônico do Imposto de Renda e, consequentemente, o aprimoramento do Registro de Pessoa Física para o CPF em 1968[1], revolucionou o formato de identificação de cada indivíduo.

Atualmente lidamos com a identificação biométrica que, de acordo com o artigo "History of Privacy" de Jan Holvast, esse tipo de identificação não se resume às digitais, mas é uma análise da estrutura do corpo humano, dos olhos, íris, face, voz[2]. Extremamente revelador são os dados genéticos que, a cada ano, são mais estudados e complexos, ponto interessante abordado por Holvast é que, ao se permitir a análise do dado genético por seu titular, se permite respectivamente a análise dos seus relativos[3].

A busca por obtenção de dados é tão intensa que até mesmo questões neurológicas são levas em consideração, a forma em que o ambiente é percebido pela mulher e pelo homem são diferentes, logo, os consumidores também são alvos diferentes de publicidade, por exemplo[4].

Como é possível concluir, nada na história evoluiu tão significativamente como a tecnologia; foram profundas as mudanças no século XX, contribuindo para revoluções na cultura, na estrutura social da população mundial e principalmente nas formas de economia[5].

---

[1] BRASIL. Ministério da Fazenda. **1968 A 1981 – Começa a Era da Secretaria da Receita Federal**. Disponível em: < http://idg.receita.fazenda.gov.br/sobre/institucional/memoria/imposto-de-renda/historia/1968-a-1981-comeca-a-era-da-secretaria-da-receita-federal > Acesso em: 10 de ago. 2017.

[2] HOLVAST, Jean. **History of Privacy**. 2009. Disponível em: < https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf > Acesso em: 15 de ago. 2017.

[3] Ibidem.

[4] Ibidem.

[5] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 31.

O surgimento da internet em 1960, demonstrou que a busca por projetos de difusão de informações não é recente, a Era da Informação – fase histórica posterior à segunda guerra mundial, propiciou a pesquisa de diversas tecnologias e aparatos que aumentaram a mecanização em diferentes áreas da sociedade, inclusive com grande ênfase nos dados pessoais.

Com o passar dos anos, o número de dados virtuais cresce exponencialmente e de forma astronômica, quatro vezes mais rápido que a economia mundial, em compensação os dados analógicos estão sendo reduzidos a menos de 2% do total de informações no mundo[6].

O termo "*big data*" (megadata, em português) aparece para classificar esse volume de informações armazenada e, inclusive, dá nome a uma nova era. No Livro "Big Data, como extrair volume, variedade e valor", Viktor Mayer- Schönberger e Kenneth Cukier classificam a *big data* como os "(...) trabalhos em grande escala que não podem ser feitos em escala menor, para extrair novas ideias e criar novas formas de valor de maneira que alterem os mercados, as organizações, a relação entre cidadãos e governos etc."[7], mas não é a única definição na literatura.

Mayer- Schönberger e Cukier compara as diversas evoluções que ocorreram durante a história da humanidade e o desenvolvimento da internet e seus objetivos e conclui que

> Os aquedutos permitiram o crescimento das cidades; a imprensa facilitou o Iluminismo, e os jornais permitiram a ascensão do Estado. Mas essas infraestruturas estavam voltadas para o fluxo – de água e de conhecimento, assim como o telefone e a internet. Em contrapartida, a datificação representa um essencial enriquecimento da compreensão humana. Com a ajuda do Big Data, não mais veremos o mundo como uma sequência de acontecimentos explicados como fenômenos naturais ou sociais, e sim como um Universo composto essencialmente por informações.[8]

Dessa maneira, com o advento dos recursos que armazenam informações, a sociedade passa a ser o centro da evolução e todas as dimensões da realidade passam a ser transformadas em dados.

Em 1960, grandes empresas já utilizavam dos mais simples meios de banco de dados e Edgar Codd, pesquisador da IBM, em 1970 publicou o artigo "Relational Model of Data for Large Shared Data Banks" que lançava o modelo de banco de dados compartilhado, o qual usuários não técnicos poderiam armazenar e recuperar grande quantidade de informações.

---

[6] MAYER-SCHÖNBERGER, Victor; CUKIER; Kenneth. **BIG DATA, como extrais volume, variedade e valor**. Tradução: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013. p. 6.
[7] Ibid., p. 5
[8] Ibid., p. 66

Posteriormente foi lançado o primeiro sistema comercial de banco de dados compartilhados e as evoluções dos bancos de dados não pararam até os dias atuais.

Desse modo, pela primeira vez na história, a capacidade de reunir e analisar um número de dados e informações de forma fácil, rápida e barata se torna possível. Danilo Doneda em seu livro "Da privacidade à proteção de dados pessoais" assinala que

> hoje, a exposição indesejada de uma pessoa aos olhos alheios se dá com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação, pela divulgação de notícias a seu respeito na imprensa, pela violação de sua correspondência (...).[9]

Não há dúvida de que as evoluções no âmbito dos dados pessoais são muito úteis para a sociedade. Esse armazenamento permite, por exemplo, que diversas pesquisas importantes sejam embasadas em uma amostra extensa de dados e com maior exatidão. No meio empresarial, é significativo o aumento do número de vendas ao combinar dados e conhecer de forma mais precisa o perfil dos clientes, contudo, a evolução tecnológica também trouxe pontos negativos. Holvast, alega que há uma dupla face na tecnologia, ao mesmo tempo que simplifica a resolução de grandes problemas, também pode caminhar para um lado negativo, o artigo traz o exemplo da identificação por rádio frequência (RFID), em que utilizado para marcapasso é excelente, mas ao mesmo tempo seu chip pode ser utilizado para monitorar todos os passos do usuário[10].

O campo de estudo dos dados pessoais é extenso, complexo e interessante, há autores que consideram que as modificações que a tecnologia está trazendo para a vida humana fará com que o homem do futuro se transforme em um "homem cristal", pois a transparência de seus dados atingirá a sua própria individualidade de estar e ser[11].

1.2 A proteção de dados pessoais pré marco Civil da Internet

Foram os grandes avanços tecnológicos que fizeram com que inúmeros países começassem a se mobilizar para regular as novas situações que surgiam e que poderiam colocar em risco seus cidadãos.

---

[9] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 1

[10] HOLVAST, Jean. **History of Privacy**. 2009. Disponível em: <https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf> Acesso em: 15 set. 2017.

[11] KEEN, Andrew. **The Internet is not the answer**. Disponível em: <https://books.google.com.br/books?id=D3UkBQAAQBAJ&pg=PT135&dq=future+crystal+man+personal+data&hl=pt-BR&sa=X&ved=0ahUKEwjx9srL08bXAhVDI5AKHdIcCnUQ6AEIJzAA#v=onepage&q=crystal%20man&f=false>. Acesso em: 18 set. 2017.

A busca pela proteção dos dados pessoais começa a mostrar resultados em 1970, sendo a primeira Lei de proteção de dados positivada na Alemanha e um ano depois, influenciado por ela, tinha início a primeira Lei Federal de Proteção de Dados Pessoais, que, em 1979, entrou em vigor no Estado de Hesse; atualmente, já existem mais de 100 legislações específicas vigentes no mundo.

Durante muitos anos a discussão se baseou em como haveria uma regulamentação de um espaço virtual que vai além dos limites dos Estados, e a ideia de que não seria possível regulamentar um espaço mundial vigorou por muito tempo[12]. Ana Cristina de Azevedo, em seu livro "Marco Civil da Internet no Brasil" aduz que

> No Brasil, a discussão envolvia 'se' e 'como' o espaço virtual devia ser regulado e, nesse sentido, como a utilização da rede surgiu antes de qualquer previsão legal e rapidamente se expandiu e ocupou lugar de destaque no mundo, a primeira providencia para suprir a lacuna jurídica foi lançar mão da analogia, com o uso de velhas regras criadas tendo em vista outras situações, quando possível encontrar alguma semelhança entre as duas realidades, a prevista na lei e a ocorrente na telemática.[13]

Desta forma, apesar de não haver Lei específica, o Brasil apresentou em sua Constituição Federal de 1988 – como direito fundamental inviolável, a intimidade, a vida privada e a imagem das pessoas, não apenas isso, mas também a inviolabilidade do sigilo de correspondência. Para Laura Mendes, o art. 5º, X da Constituição faz com que seja

> [...] possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentindo excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais", [...]. Assim, não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.[14]

Do abordado por Mendes conclui-se que a Constituição, apesar de ser relacionada sempre à constância e garantia, também deve se adequar às mudanças, isto é, abrir suas possibilidades de interpretação. Peter Häberle, citado por Mendes, entende que a Constituição deve ter como característica principal uma possibilidade de interpretação, deixando espaço para o desenvolvimento da história e de seus cidadãos, denominada como uma sociedade

---

[12] AZEVEDO, Ana Cristina Carvalho. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014, p. 90.
[13] Ibid., p. 91
[14] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 171.

aberta dos intérpretes da Constituição[15]. Com essas características, se faz viável localizar dispositivos que regulem a proteção de dados mesmo em uma constituição formulada anteriormente às grandes mudanças tecnológicas.

Isto posto, a Constituição de 1988 dá inicio às diretrizes das futuras leis de proteção de dados no Brasil, mas não apenas. Danilo Doneda afirma que a legislação brasileira contemplava "o problema da informação inicialmente através das garantias à liberdade de expressão e do direito à informação, que devem ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade."[16], isto é, não havendo uma legislação específica sobre o tema, como já dito, ocasiona o dever de se fazer uma interpretação complexa dos dispositivos espalhados tanto na Constituição Federal, mas também em legislações ordinárias e em diversos códigos, como o Civil, Penal e do Consumidor, com o propósito de sempre ser preservado a privacidade e a personalidade do indivíduo.

A Constituição de 88, influenciada pelo recente fim da Ditadura militar no país, e em resposta aos vários excessos praticados pelo Estado durante este período, lançou o *habeas data*, remédio eficaz utilizado pelo cidadão contra o Estado.

O *Habeas Data,* regulamentado pela Lei 9.507/97, tem como objetivo "assegurar o conhecimento de informação relativa à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de carater público"[17], ou seja, o cidadão tem garantido o direito de obter informações pessoais que estejam em poder unicamente de órgãos governamentais, podendo até mesmo requerer que esses dados sejam corrigidos.

Como já mencionado, não só a Constituição aludiu sobre proteção de dados pessoais. Tal alusão também se encontra na seara dos Códigos Penal, Civil e do Consumidor – este que já atentava para os riscos introduzidos pelo ciberespaço, trazendo dispositivos sobre o assunto. Ainda assim, desde 2010, o Brasil busca aprovar uma Lei de proteção de dados pessoais, haja vista que, apesar de a internet ser de todos e ao mesmo tempo de ninguém, essa característica não justifica a falta de uma regulamentação das atividades que principalmente interferem no Estado. Vinicius Fontes, estudioso do tema, em seu livro "Os direitos de privacidade e a proteção de dados pessoais na internet" demonstra que a carência de uma legislação sobre o assunto faz com que as situações específicas relacionadas à proteção de

---

[15] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 170. apud HÄBERLE, Peter. *Verfassung als öffentlicher Prozeβ,* cit., p. 61 e 62.
[16] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 323
[17] SAENZ, Fabiana Eduardo. **Habeas Data**. Disponível em: <escola.mpu.mp.br/dicionario/tiki-index.php?page=Habeas+data> . Acesso em: 20 ago. 2017.

dados fiquem a "mercê da consciência jurisdicional" de cada juiz, causando uma insegurança jurídica e não alcança uma resposta uniforme e adequada aos problemas[18].

Ademais, a falta de uma regulamentação específica deixa o país em uma conjuntura jurídica delicada, em que desde a garantia dos direitos de seus cidadãos até acordos internacionais são prejudicados pela ausência de regulamentação específica.

1.3 O Marco Civil da Internet

Mesmo a internet tendo começado a ser operada no Brasil nos anos 90, parte de sua regulamentação apenas surgiu em 2014, com o Marco Civil da Internet, nome popular da Lei nº 12.965, de 23 de abril de 2014, depois regulamentada pelo Decreto nº 8.771/2016. O Marco Civil veio amparar a atual sociedade da informação, com a finalidade de estabelecer princípios e garantias para o convívio civil na rede mundial online de computadores, como por exemplo, reafirmando a neutralidade de rede, a liberdade de expressão e a proteção a privacidade dos usuários – evitando que as informações de cada pessoa fossem utilizadas sem sua devida autorização, e constituindo, assim, ponto importante de garantia da privacidade de dados do cidadão.

O Marco Civil pode ser considerado o primeiro avanço significativo sobre o tema da proteção de dados no Brasil. Proporcionou maior clareza à questão, formulando texto sobre a proteção de dados pessoais, tendo como base leis vigentes em outros países e funcionando, em muitos casos, como uma Lei específica do assunto. Pode ser compreendido como um esforço positivo para a regulamentação da Internet, posto que, anteriormente, ressalta Fontes em sua obra que,

> o acesso aos dados e o registro da conduta de seus usuários eram plenamente destituídos de regulação específica, o que também permitiu que a internet se tornasse um ambiente hostil e de cometimento de abusos e violações de direitos. Um exemplo disso está na coleta deliberada de dados sigilosos, tanto em relação às informações quanto ao histórico de navegação em sites da internet, bem como a frequente solicitação de tempo e conteúdo por autoridades públicas sem submissão à prévia análise judicial.[19]

A proteção de dados pessoais na internet foi um dos assuntos principais do Marco Civil da Internet, considerando que sua formulação foi também uma resposta ao Projeto de Lei nº 84/1999, popularmente conhecido como "Lei Azeredo", devido a isso, nesse capítulo iremos analisar alguns artigos fundamentais para fundamentar a necessidade de uma lei

[18] FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p, 12.
[19] Ibid., p. 13.

específica, além de ser possível por meio desse estudo compreender o significado de alguns termos importantes para a regulamentação dos dados pessoais.

O Marco Civil da Internet estabeleceu como princípio a privacidade e a proteção de dados pessoais, como já explanado, mas alguns pontos foram fortemente criticados, apesar da tentativa de detalhar o tema de proteção de dados. Dessa forma, uma Lei específica é imprescindível para que haja uma mensagem clara tanto para as empresas e o próprio governo, como principalmente para o cidadão leigo compreender o funcionamento do espaço virtual.

Analisando seus artigos, diversas normas são voltadas à proteção de dados pessoais e

> Ao proclamar que o acesso à internet é essencial ao exercício da cidadania, o texto assegura ao usuário alguns direitos, como a inviolabilidade da intimidade, do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei, e de suas comunicações privadas armazenadas, salvo por ordem judicial nas duas últimas hipóteses, que vem apenas ratificar o direito já previsto na Constituição Federal, art. 5º , inciso XII, com a diferença de se aplicarem exclusivamente à comunicação pela internet.[20]

Seguindo os princípios básicos encontrados na Carta Magna, logo no início da Lei, em seu art. 3º, inc. II e III, o Marco Civil ratifica a vontade do legislador em proteger a privacidade do usuário da internet e, especificamente no inc. III, aprecia a proteção de dados na medida em que reafirma os princípios constitucionais relacionados ao respeito a privacidade.

O art. 7º expressa a imprescindibilidade do acesso à internet como forma de exercício da cidadania e, para que haja o pleno exercício deste direito, são essenciais o respeito à inviolabilidade dos dados por meio dos princípios de proteção da privacidade, da inviolabilidade e a proteção da intimidade e da vida privada – inclusive havendo a possibilidade de indenização tanto moral como material, do sigilo de suas correspondências virtuais, também as privadas armazenadas, salvo determinação contrária por ordem judicial[21].

Seguindo a leitura do art. 7º, o Marco Civil dispõe sobre a distribuição de dados para terceiros, onde a prática só poderá ser feita quando houver consentimento livre, expresso, informado ou nas hipóteses da Lei. Além disso, para garantir um consentimento esclarecido, a Lei traz a obrigação da informação clara e completa sobre a utilização dos dados. Nas relações contratuais, o referido artigo também determina como indispensável o consentimento expresso sobre a coleta, uso, armazenamento e tratamento de dados pessoais, sempre

---

[20] AZEVEDO, Ana Cristina Carvalho. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014 p. 121

[21] Ibid., p. 128

destacado das demais cláusulas e ainda sobre a possibilidade da exclusão de dados pessoais, salvo hipóteses previstas em Lei.[22]

As evoluções normativas sobre o assunto continuam. O art. 8º reafirma a imprescindibilidade do respeito à inviolabilidade e ao sigilo das comunicações privadas, tornando cláusulas contratuais nulas de pleno direito quando desobedecerem este princípio. Já o inciso II do mencionado dispositivo, de acordo com Vinícius Fortes, determina

> que, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, devem ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, considerando que pelo menos um dos terminais esteja localizado no Brasil, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior. [23]

Este artigo e seus incisos, além de estarem em conformidade com a Constituição Federal, apreciam o CDC ao definir o foro com o objetivo de proteger a parte mais frágil da relação, ou seja, o foro será do consumidor mesmo nos casos de ações virtuais, além disso determina a possibilidade de "ler e interpretar os termos de uso e as políticas de privacidade dos sites da mesma forma como se compreende contratos de adesão nas relações de consumo."[24].

Seguindo a análise do Marco Civil da Internet, a seção II trata especificamente "da proteção aos registros, aos dados pessoais e às comunicações privadas"[25], determinando as formas legais para disponibilização de conteúdos de comunicação privada. O artigo 10 discorre sobre o papel do provedor e esclarece, o que antes era muito conflituoso, sobre o sigilo dos dados pessoais e o conteúdo das comunicações privadas dos usuários na Internet. O artigo judicializa a disponibilização de forma autônoma dos conteúdos que identifique o usuário ao determinar que esta ação só poderá ser feita pelo provedor responsável mediante

---

[22] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 de set. 2017.

[23] FORTES, Vinícius Borges. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Editora Lumen Juris, 2016 p. 129.

[24] KLEE, Antonia Espíndola Longoni. **A regulamentação do uso da internet no Brasil pela Lei n. 12.965/2014 e a proteção dos dados e dos registros pessoais.** Disponível em: < http://revistaseletronicas.pucrs.br/ojs/index.php/fadir/article/view/21427> Acesso em: 02 de set. 2017.

[25] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 de set. 2017.

ordem judicial, respeitando o que já orientado no art. 7º sobre o consentimento livre, expresso e informado do usuário.

O parágrafo 3º do mesmo artigo positiva que

> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

A letra da Lei causou certo incomodo aos defensores da privacidade ao prever que autoridades administrativas possam acessar a dados pessoais sem ordem judicial, o dispositivo permite que haja uma interpretação ampliada e que venha a ferir princípios básicos da proteção de dados que tanto se busca.

A permissão para acessar dados por meio de mero pedido feito por autoridades administrativas, sem determinar quais autoridades seriam e nem a motivação para o haver essa possibilidade de recolhimento de dados, demonstra uma lacuna que espera ser completada por Lei específica, mas o caso em questão é preocupante no ponto em que um projeto de Lei ainda está em tramite e necessita de uma quantidade relativamente longa de tempo para ser concluído, logo, manter essa insegurança jurídica trazida pelo artigo acarreta em possíveis violações de direitos.

Por fim, o parágrafo 4º demonstra novamente a necessidade de um regulamento especial. O artigo delibera que "as medidas e procedimentos de segurança e sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara", os padrões de segurança que serão utilizados serão determinados por meio de regulamento, que atualmente não se tem.

O art. 13 da Lei positiva sobre a guarda de registros de conexão. O artigo apresenta a preocupação de aplicar sanções condizentes com as consequências que a falta de zelo com esses registros pode proporcionar, o parágrafo 6º aborda que as sanções serão determinadas de acordo com a gravidade, os danos e outras consequências decorrentes da infração.

O artigo 15 inicia sua redação determinando que provedor de aplicações é pessoa jurídica, que exerce atividade de forma organizada, profissionalmente e com fins econômicos, a pormenorização é importante para que não haja confusão com a nomenclatura "provedores de internet"[26]. Este provedor deve manter os dados de registro de acesso guardados pelo prazo de 6 (seis) meses, podendo ser alterado por meio de ordem judicial. O parágrafo primeiro positiva sobre aqueles provedores de aplicação de internet que não se enquadram no caput do

[26] Provedores de internet são os que dão acesso ao usuário ao sinal de internet, fazendo a intermediação entre o usuário e a operadora contratada.

artigo mas que o Poder Judiciário pode considerar responsáveis por manter as informações armazenadas, os quais serão obrigados a guardar registros específicos e por período determinado pelo Poder Judiciário.

A necessidade de uma regulamentação especifica também é constatada durante a leitura do art. 15, § 2º, que possibilita que as autoridades previstas no parágrafo possam requerer a conservação dos registros de conexão por prazo superior ao expresso na Lei, há criticas sobre o artigo que se torna de certa forma, contraditório ao não exigir apresentação de ordem judicial para que esse pedido tenha efeito, por isso a necessidade de um maior detalhamento dessas atividades [27].

Assim como determinado nos artigos sobre o registros de conexão, qualquer infração a estas disposições do art. 15, as sanções serão equivalentes a gravidade do feito, é o que traz o parágrafo 4º com redação idêntica a do art. 13, parágrafo 6º.

Acompanhando o determinado no art. 7º, incisos VII e IX, o art. 16 e seus incisos reafirmam a imprescindibilidade do consentimento do titular dos dados e o respeito as finalidades dadas pelo titular para consentir o uso dos dados.

Finalmente o artigo 17, que finaliza a seção II, positiva sobre a responsabilidade sobre os danos decorrentes do uso dos dados por terceiros. É determinado que os provedores que não forem obrigados a guardar os dados, não poderão ser responsabilizados pela utilização dos dados por terceiros, mesmo que de forma fraudulenta.

A justificativa para o armazenamento dessas informações, é devido a busca por ter ferramentas que permitam a identificações de possíveis criminosos cibernéticos, tornando o trabalho de investigação feito pelas autoridades mais célere[28], mas a forma de armazenar os dados ainda não foi determinada, necessitando, novamente, de regulamentação específica.

A Lei não apenas buscou afirmar que sanções são cabíveis para aqueles que cometerem infrações aos artigos, mas também determinou sobre a responsabilização civil daqueles que tem acesso aos dados pessoais.

O tema sobre a responsabilidade civil não é pacificado na jurisprudência brasileira, mas a Seção III da Lei 12.965/14 tenta legislar sobre o assunto ao especificar quem serão os responsáveis civis por danos decorrentes da utilização dos dados pessoais de forma contraria ao determinado na Lei.

---

[27] ACADEMIA BRASILEIRA DE DIREITO DO ESTADO. **Comentários ao Marco Civil da Internet**. Disponível em: < http://abdet.com.br/site/wp-content/uploads/2015/02/MCI-ABDET..pdf >.Acesso em: 19 de set. 2017.

[28] BRASIL. Câmara dos Deputados. **Marco civil da internet**. 2. ed. Brasília: Edições Câmara , 2015. p. 10

O artigo 18 isenta o provedor de conexão da internet de ser "responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros."[29], é afastada a responsabilidade tendo em vista que, como já explicado anteriormente, o provedor de conexão faz o papel de conectar o usuário à internet, são eles os responsáveis apenas pela transmissão da conexão da internet; ademais há uma limitação técnica considerando a imensidão das informações inseridas no espaço cibernético diariamente e também a falta de um controle editorial do conteúdo, uma vez que a liberdade de expressão é princípio que deve ser preservado.

O artigo 19 trata dos provedores de aplicação, aqueles que fornecem atividades online de forma organizada e com fins lucrativos, dispondo que

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

A redação deste artigo divide opiniões, desde uma interpretação positiva, de que as exceções apontadas contribuem para que tenha uma maior segurança jurídica, até o questionamento de sua constitucionalidade, afirmando a impossibilidade do diálogo das fontes com disposições do Código de Defesa do Consumidor ao limitar a responsabilidade dos provedores de aplicação de Internet[30].

Anteriormente ao Marco Civil da Internet, o STJ já possuía precedentes de que a mera notificação da pessoa ofendida, um simples pedido extrajudicial, independentemente de decisão judicial, obrigava o provedor de aplicação a retirar o material alegado impróprio no prazo de 24 horas, como visto no REsp n. 1.323.754 – RJ, a contar do recebimento da notificação[31]. Era a chamada teria do *notice and takedown.* A legislação vigente, por sua vez, determina que os provedores só serão responsabilizados após decisão judicial que não tenha

---

[29]BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 de set. 2017.

[30] CAVALCANTI, Roberto Flávio. **A inconstitucionalidade do artigo 19 do Marco Civil da Internet**. Disponível em: < https://jus.com.br/artigos/30560/a-inconstitucionalidade-do-artigo-19-do-marco-civil-da-internet >. Acesso em 22 de set. 2017.

[31] OLIVEIRA, Carlos Eduardo Elias de. **Aspectos principais da Lei n. 12. 965, de 2014, o Marco Civil da Internet.: subsídios a comunidade jurídica**. Disponível em: < https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica > . Acessado em: 20 set. 2017.

sido acatada, ou seja, é necessário que haja uma decisão judicial específica e que os provedores não cumpram sua determinação para que a responsabilização civil ocorra.

Buscando a celeridade do processo e preocupando-se com a gravidade das possíveis informações que estão sendo disponibilizadas sem a devida autorização, o parágrafo 3º do artigo traz a facilidade de interpor o pedido nos juizados especiais, inclusive podendo o juiz antecipar os efeitos da tutela quando "presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dado irreparável ou de difícil reparação."[32], é o que dispõe o parágrafo 4º do mesmo artigo.

O pedido extrajudicial não é totalmente descartado, o art. 21 da Lei, buscando preservar a intimidade e privacidade do cidadão, mantem a possibilidade de notificação feita pelo ofendido ou seu representante legal, quando o conteúdo for a cerda de "nudez ou de atos sexuais de caráter privado" [33], conhecida como "pornografia de vingança" por ser disponibilizado vídeos e fotos de terceiro sem sua autorização. A responsabilização do provedor ocorrerá apenas após o recebimento da notificação, haja vista que uma pré análise do conteúdo disponibilizado por usuário pode ser considerado censura prévia.

Ambos os artigos, 19 e 21, trazem como requisito de admissibilidade da ordem judicial e da notificação, sob pena de nulidade, nos seus parágrafos 1º e único respectivamente, a obrigatoriedade de evidenciar elementos que permitam identificar a violação da intimidade de forma inequívoca. O problema do dispositivo encontra-se na falta de unanimidade a respeito do que seria a "identificação clara e específica do conteúdo", para Omar Kaminski, advogado e gestor do Observatório do Marco Civil, há dúvidas sobre essa identificação "(...)Bastaria apontar a URL? Serviria uma ata notarial? E na hipótese de não ser possível de obter a URL, ou na falta de conhecimentos tecnicos para tanto, como ficaria a questão?"[34]. São lacunas que a Lei especial também deve se deter e explicar de forma mais objetiva.

A retirada do conteúdo não pode ser feita sem a devida notificação ao usuário responsável pela publicação removida. O art. 20 tenta preservar novamente a liberdade de expressão, ressalvando apenas os casos que tenham previsão legal contrária ou seja expressamente determinado e fundamentado pelo juiz.

---

[32] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 de set. 2017.

[33] Ibidem.

[34] CUBAS, Marina Gama. **Marco Civil da Internet completa um ano com regulamentação pendente**. Disponível em: < https://www.conjur.com.br/2015-abr-23/marco-civil-internet-faz-aniversario-regulamentacao-pendente > .Acessado em: 22 set. 2017.

O art. 22, já mencionado anteriormente, define rol necessário para que haja a admissibilidade do pedido de fornecimento dos registros tanto de conexão como os de acesso. O referido dispositivo se preocupa em permitir que os pedidos de obtenção de dados armazenados pelos provedores sejam feitos apenas quando houver real necessidade de divulgação.

O ultimo artigo do Capítulo III – art. 23, finaliza a listagem dos principais artigos que tratam diretamente sobre o que será abordado no trabalho. Não há dúvidas que o Marco Civil da Internet foi avanço significativo para a regulamentação da internet no Brasil, conclui Fortes que

> Mais do que estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabeleceu que a disciplina do uso da internet no Brasil tem como fundamentos o respeito à liberdade de expressão; o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; a finalidade social da rede.[35]

Apesar de ser composto de alguns artigos que regulam a proteção de dados, a falta de uma Lei geral específica sobre o assunto, causa interpretações abstratas de alguns conceitos essenciais e sem um significado prático e que possa ter uma aplicabilidade imediata. Dessa forma, foi necessária a edição do Decreto nº 8.771/2016, com o desafio de regulamentar, além de outros assuntos, o que significa no contexto do Marco Civil a proteção dos dados pessoais, explicando de maneira mais clara e mais coerente alguns artigos da carta. É o caso, por exemplo, da positivação do art. 10º, §3º, que além de determinar o que é considerado dados cadastrais, limita o acesso ao exigir justificativa e fundamento legal expresso para que seja disponibilizado à administração pública os dados pessoais de um cidadão, mas ainda incorre no erro de não especificar quais autoridades tem essa prerrogativa.

Por fim, ao mesmo tempo que o Marco Civil estipula regras sobre a proteção de dados, é visto de forma clara o cuidado em não adentrar competências que caberiam a uma futura Lei de dados pessoais imprescindível, e que está sendo gestado no âmbito do Poder Legislativo.

---

[35] FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p. 126.

1.4. O Projeto de Lei n. 5.276/2016 sobre proteção de dados pessoais

Como demonstrado no subcapítulo anterior, a Lei 12.965/14 proporcionou os primeiros passos para a redação de Lei específica sobre a proteção de dados pessoais. A partir disso, foram três iniciativas legislativas que buscaram regular de forma objetiva os dados pessoais, a PL nº 4.060/2012, PLS nº 330/2013 e o PL nº 5.276/2016.

O estudo "Proteção de dados pessoais no Brasil – Análise dos projetos de lei em tramitação no Congresso Nacional"[36], feito pela Artigo 19 – organização não governamental, produziu quadro comparativo dos três projetos de Lei, de forma a demonstrar quais pontos estão sendo abordados em cada um e qual o grau de aprofundamento.

ASPECTOS DA LEI	PL 5276/2016	PLS 330/2013	PL 4060/2012
Menção expressa à proteção da liberdade de expressão	🟢	🔴	🟡
Exceção à atividade jornalística e outras formas de expressão	🟢	🟡	🟢
Menção expressa à Lei de Acesso à Informação (LAI)	🟢	🔴	🔴
Evita interpretações que possam ensejar reivindicações do direito ao esquecimento	🔴	🔴	🔴
Órgão regulatório	🟡	🟡	🔴
Mecanismo de participação e controle social	🟡	🟡	🔴
Proteção aos dados sensíveis	🟢	🟢	🟡
Graus de consentimento	🟢	🟢	🔴
Consentimento do titular para compartilhamento a terceiros	🟢	🟢	🔴
Proteção para transferência internacional de dados	🟢	🟢	🔴
Proteção de dados em acesso público	🟡	🔴	🔴
Adoção de medidas de segurança e de manuseio dos dados pessoais	🟢	🟢	🟡
Aplicação ao setor público como um todo, incluindo forças de segurança	🔴	🔴	🔴
Delimitação de pesquisa estatística	🔴	🔴	🔴
PRAZO PARA A LEI ENTRAR EM VIGOR	180 dias	120 dias	90 dias

[36] BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional**. Disponível em: < http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >. Acesso em: 06 de set. 2017.

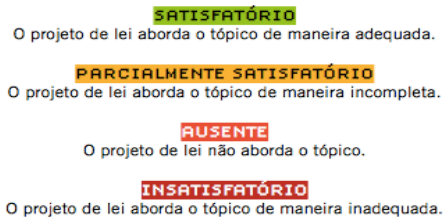

Figura 1. Tabela comparativa entre os projetos de Lei PL nº 5.276/2016, PLS nº 330/2013PL e o PL nº 4.060/2012, organizando quais os pontos abordados e qual o nível de aprofundamento de cada projeto de Lei.[37]

O Projeto de Lei nº 5.276/2016 é o mais recente e, como demonstrado pela tabela, seu teor é mais completo e aborda de maneira satisfatória a maioria dos pontos que são controversos da matéria, deixando apenas as questões sobre as formas de aplicação ao setor público e situações relacionadas ao direito ao esquecimento em aberto. Ademais, diferentemente dos outros projetos de lei, o PL nº 5.276/2016 segue padrão internacional mais sólido, sendo fortemente influenciado por marcos regulatórios de países pioneiros na proteção de dados, como poderemos constatar durante o trabalho.

O anteprojeto de lei do Poder Executivo também foi objeto de amplos debates públicos, "recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições."[38]. Isso demonstra a preocupação em fazer com que diversas áreas da sociedade pudessem participar de sua redação, proporcionando assim um texto com caráter democrático e coeso com a realidade. Por essas e outras razões, e pelas limitações de espaço próprias de um trabalho desse vulto, optamos por concentrar nossa análise no PL nº 5.276/2016.

A votação do projeto foi fixada em regime de tramitação com urgência constitucional – tipo de rito procedimental abreviado, buscando uma análise mais célere do Projeto de Lei, mas apesar do caráter de urgência investido na aprovação da Lei, o trâmite acontece há mais de um ano.

Formular uma lei específica é necessária não apenas para preencher as lacunas deixadas pelo Marco Civil da Internet e proteger melhor o cidadão, mas também deve ter a

---

[37] ARTIGO19. **Proteção de dados pessoais no Brasil – Análise dos projetos de lei em tramitação no Congresso Nacional**. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 06 de set. 2017

[38] BRASIL, **Projeto de Lei n. 5.276,** de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 06 de set. 2017.

intenção de uniformizar o significado dos conceitos essenciais para a proteção de dados e coordenar as políticas internas e externas do Brasil.

O Projeto de Lei que será o foco da análise desse trabalho, como explicado anteriormente, será o PL nº 5.276/2016 que, por meio de 56 artigos, distribuídos em nove capítulos, aborda as regras de tratamento dos dados pessoais, os fundamentos que serão respeitados, e busca garantir a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, é o que o artigo primeiro determina.

O artigo 2º lista o já positivado no artigo primeiro, evidencia que, almejando atender os pontos abordados no primeiro artigo, é preciso que haja o respeito à autodeterminação informativa; à liberdade de expressão, de comunicação e de opinião e a inviolabilidade da intimidade, da vida privada, da honra e da imagem.

A Lei tem a proteção de dados como foco principal, tendo o legislador também se preocupado com o desenvolvimento tecnológico e econômico do país. Logo, as limitações trazidas pela Lei não têm o intuito de impedir que as buscas por novas tecnologias sejam paralisadas, determinando no inciso IV o desenvolvimento econômico e tecnológico.

O artigo 2º demonstra a pretensão da Lei em ser balanceada, uma vez que são várias as atividades que precisam de uma maior liberdade para produção, é o caso das arroladas no art. 4º, mas, apesar de serem exceções, o contido nos incisos II e III, que seriam respectivamente, a utilização dos dados pessoais "para fins jornalísticos, artísticos, literários ou acadêmicos"[39] e "para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais"[40] são limitados por relatórios de impacto à privacidade e por previsões legais.

Retornando ao artigo 3º, este determina o alcance da Lei ao dizer que serão submetidos a ela qualquer tratamento realizado por pessoa natural como por pessoa jurídica de direito público e privado, independentemente do país de origem ou onde estão localizados os dados. A limitação deste artigo encontra-se no alcance das operações, que devem ser realizadas no Brasil e com o objetivo de ofertar e fornecer bens ou serviços, ou tratar dados individuais que se encontram em território nacional.

---

[39] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 06 de set. 2017.

[40] Ibidem.

Conforme já abordado no capítulo sobre o Marco Civil, são vários os termos que devem ser esclarecidos para que haja uma interpretação fiel, compreendendo a finalidade e os objetivos da Lei. O art. 5º apresenta lista com considerações de cada expressão, muitas tendo respaldo com o decreto de regulamentação do Marco Civil da Internet, para os devidos fins desse trabalho as que serão objeto de estudo são:

> I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;
> II – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
> III – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;
> IV – dados anonimizados: dados relativos a um titular que não possa ser identificado;
> V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;
> VI – titular: a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento se seus dados pessoais para uma finalidade determinada;
> VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;
> XII – anonimização: qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;[41]

Além do art. 5º esclarecer as controvérsias com relações alguns termos, o art. 6º incluiu princípios essenciais para a norma, :

> I – finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informado ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;
> II – adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

[41] BRASIL, **Projeto de Lei n. 5.276,** de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 06 de set. 2017.

> III – necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV – livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;
> V – qualidade dos dados: pelo qual devem ser garantidas aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;
> VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
> VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e 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: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX – não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

Os artigos contidos na Seção I da Lei discriminam as formas em que a coleta dos dados pessoais poderá ser feita mas, assim como no Marco Civil, procurando preservar o consentimento livre e a informação clara e inequívoca para que haja essa anuência[42], mas não explicitou a forma que será essa informação, reafirmando as críticas feitas ao Marco Civil que também não especificou como esta informação deverá ser fornecida.

O consentimento para o tratamento de dados é parte importante para que haja o respeito ao direito à liberdade de escolha, isto posto, a anuência tem requisitos para que seja legal, devendo ser livre, informada, inequívoca, específica, determinada e expressa.

O artigo também reafirma a possibilidade da administração pública em tratar os dados respeitando previsão legal ou de regulamento[43], além disso, o titular dos dados deve ser informado em quais circunstancias esse tratamento de dados é possível, é o que determina o parágrafo 1º do artigo 7º e especificamente o artigo 24 da mesma Lei. O descumprimento deste requisito pode fazer acarretar em responsabilização do responsável (art. 7º, §3º).

O consentimento, como já afirmado, é ponto chave para a legalidade do tratamento de dados. O artigo 8º apresenta rol de como as informações devem ser passadas aos titulares dos dados, com a possibilidade de ser nulo o consentimento se não respeitada a forma prevista.

---

[42] BRASIL, **Projeto de Lei n. 5.276,** de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 06 de set. 2017.
[43] Ibidem.

O artigo também afirma que o responsável pelo tratamento não pode ser anônimo, devendo ter todas suas informações para contato disponíveis. Ademais, as ações do responsável durante o tratamento são passíveis de responsabilização.

Seguindo com os requisitos para o consentimento, o artigo 9º determina que quando a anuência for feita de forma expressa, essa deve estar destacada das demais cláusulas contratuais (art. 9º, §1º) e no caso de futura ação processual, cabe ao responsável pelo tratamento dos dados provar que houve o consentimento e que foi obtido conforme admite a Lei.

Neste artigo também é ratificado a necessidade do livre consentimento e da informação clara ao titular sobre o tratamento dos dados, além disso, o parágrafo 6º coloca a vontade do titular claramente como essencial para que o tratamento dos dados seja continuado, ou seja, a qualquer momento o consentimento pode ser revogado necessitando apenas a manifestação de vontade.

No último parágrafo do artigo, é determinado que qualquer mudança dos requisitos para o consentimento poderá ser feita mediante autorização do órgão responsável, levando em consideração o contexto em que foi concedido e a natureza dos dados.

O artigo 10 apresenta outra forma da flexibilização do consentimento, advindo do legítimo interesse do responsável para ter acesso aos dados pessoais, respeitando os direitos e liberdades fundamentais do titular e baseando seu pedido em caso concreto de necessidade.

De acordo com a publicação "XEQUE-MATE, O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil", é preciso que haja certos limites para que essa flexibilização da regra geral de consentimento não seja tão distorcida[44]. Para isso, foi previsto, por meio do art. 10, §2º, medidas para garantir a transparência do tratamento dos dados e com ferramentas visando a possibilidade do titular opinar sobre, além disso, é vedada a utilização de dados que não são cabíveis para a finalidade pretendida (art. 10, §3º) pois, como positiva a Lei, o tratamento dos dados é concluído assim que houver a verificação do alcance da finalidade buscada, não podendo se alongar extrapolando o determinando anteriormente[45].

A Lei neste artigo respeita o principio da necessidade, que de acordo com Fontes esse principio "ressalta que o tratamento deve se limitar ao mínimo necessário para a realização

[44] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 7

[45] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 08 de set. 2017.

das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos (...)"[46].

O artigo 11, no que lhe concerne, manifesta o maior cuidado que deve se ter com o tratamento dos dados pessoais sensíveis, aqueles positivados no art. 5º, III como dados que são diretamente ligados a cada titular, ou seja, são informações pessoais e que caracterizam de forma mais profunda cada cidadão.

Este artigo apresenta primeiramente em seu texto a vedação do tratamento desses dados, sendo possível concluir a partir disso que, em regra, nenhuma pessoa a quem compete as decisões referentes ao tratamento de dados poderá ter acesso a eles e utiliza-los para fins diversos, exceto no rol de possibilidades disponibilizado na Lei.

Os dados pessoais sensíveis poderão ser tratados em situações relevantes como para proteção da vida, quando for necessária para regular direitos em processos judicial ou administrativo – esta situação em específico deve apresentar os motivos da dispensa do consentimento em publicação.

O respeito a liberdade do titular de consentir também é aplicado aos dados sensíveis, ou seja, quando forem fornecido de maneira livre, inequívoca, informado, expresso e específico. Esta situação exige que sejam preenchidos todos os requisitos da anuência, desde o mais básico, como a vontade livre de anuência, até o mais complexo, como a concordância expressa. As demais possibilidades sempre que possíveis devem garantir a anonimização dos dados pessoais. Cabe ressaltar que apesar das possibilidades trazida pela Lei, o tratamento desses dados não poderá ser efetivado causando prejuízos ao titular, exceto se houver determinação legal (art. 11, §2º).

Bem como mencionado, o tratamento de dados pessoais tem prazo definido, será determinado pelo responsável pelo tratamento quando houver concluído o objetivo do tratamento, quando o titular requerer o fim da utilização de seus dados ou, finalmente, quando órgão competente determinar a interrupção do tratamento devido violação da legislação em vigor, é o que determina o art. 15 da Lei.

O capítulo III da Lei aborda os direitos do titular dos dados pessoais. Primeiramente as garantias de todo cidadão a ter seus direitos fundamentais de liberdade, intimidade e privacidade devem ser respeitados nos temos da Lei.

Os demais artigos recapitulam determinações já vistas em artigos anteriores, o art. 18 lista o que o dono dos dados tem direito de obter, é a materialidade da garantia da

[46] FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p. 139.

transparência e da liberdade de expressão, pois o titular tem o direito de saber sobre seus dados que estão sendo tratados, tendo acesso a eles, corrigindo qualquer erro e será atendido quando fizer o pedido de retirada de informações que considere desnecessárias, excessivas ou que estão sendo tratadas em desconformidade com o disposto na Lei[47]. Ademais, o inciso VII não descarta as normas já positivadas no Código de Defesa do Consumidor, que serão aplicadas quando possível.

Os efeitos da determinação neste artigo são imediatos a partir do momento em que o titular fizer o requerimento ao responsável, este deverá prover seu pedido e adotar providencia para o cumprimento[48], além disso, os terceiros que também estejam utilizando os dados devem ser avisados sobre o requerimento do titular. Em caso da não possibilidade de retirada, correção, eliminação, anonimização ou bloqueio dos dados, o responsável deve enviar, no prazo de 7 dias, justificativa motivada.

A Lei aborda no capítulo IV as formas em que ocorrerá o tratamento de dados pessoais pelo Poder Público. Primeiramente faz remissão à Lei nº 12.527/11, popularmente conhecida como a Lei de Acesso à Informação, que positiva quais as pessoas jurídicas de direito público que podem ter acesso ao tratamento de dados pessoais, são elas:

> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Cada pessoa jurídica de direito publico listada tem finalidades diferentes, logo, o tratamento de dados também deverá respeitar a finalidade do órgão que estará utilizando-os, motivado pelo interesse público e para executar competências e cumprir atribuições legais determinadas pelo serviço público.[49]

---

[47] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 08 de set. 2017.

[48] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 08 de set. 2017.

[49] Ibidem.

Fortes, em seu livro, salienta que a Lei de Acesso à informação, apesar de cumprir papel de buscar o direito fundamental à informação, segue princípios administrativos como publicidade dos atos, divulgação das informações de interesse público e entre outros[50].

Visando garantir a transparência determinada em sua própria redação e, procurando respeitar as premissas da Lei que faz remissão, o Projeto de Lei determina que, sempre que for necessário o tratamento de dados pessoais pelo Poder Publico, o agente deve informar de maneira clara as hipóteses que irão ocorrer e, sempre que possível, em seus sítios eletrônicos, centralizando o tratamento em um encarregado, é a clara aplicação do princípio da transparência[51].

O uso compartilhado dos dados fornecidos ao Poder Público ocorrerá unicamente quando obedecer as finalidades específicas, respeitando os princípios elencados anteriormente, como a adequação, a necessidade e a segurança.

O compartilhamento de dados que são originariamente da base de dados do Poder Público só poderá ser feita quando em ação descentralizada de atividade pública e, quando preencher esse requisito, deve respeitar não apenas o determinando na Lei em análise, mas também os disposto da Lei de Acesso à Informação.

São apenas duas as hipóteses de dispensa do consentimento do titular para que possa haver a comunicação e transferência de dados pessoais entre pessoa jurídica de direito público e pessoa jurídica de direito privado, quais sejam: (i) nas hipóteses de dispensa prevista na Lei; ou (ii) quando essa utilização for publicada, garantindo a transparência das ações.

Há grande preocupação do legislador em enfatizar a essencialidade da devida publicação quando realizado tratamentos de dados, não é por acaso que dos sete artigos da Seção I do Capítulo IV da Lei, três falam especificamente sobre o tema. Esta preocupação é legítima principalmente devido ao histórico brasileiro durante a Ditadura e levando em consideração o grande banco de dados que o Estado detém e poderia fazer uso.

A Seção II desse capítulo determina especificamente sobre a responsabilidade quando ação for decorrente de agente ou órgão público. O art. 31 atribui ao órgão competente a faculdade de, quando houver infração decorrente de órgãos públicos, orientar, por meio de medidas cabíveis, a cessação da violação e, na hipótese de violações perpetradas por agente

---

[50] FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p. 115.

[51] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 09 de set. 2017.

público, que as medidas serão aplicadas pessoalmente, respeitando o disposto nas Leis nº 8.112/90 e 8.429/92.

Finalizando a análise do artigo 32, é facultado ao órgão competente exigir aos agentes públicos a publicação de relatórios de impacto de privacidade e recomendar ações para um tratamento de dados corretos.

A relevância do tema dessa pesquisa é clara ao constatar que grande parte da sociedade está conectada e disponibiliza diariamente seus dados pessoais, a sociedade da informação[52] é atual e caminhamos para um grau de interligação absoluta pelas redes, por consequência, a Lei não poderia deixar de legislar sobre as transferências de dados no âmbito internacional.

O artigo 33 apresenta as possibilidades de transferência de dados para países estrangeiros. As possibilidades são, entre elas, quando os países tiverem regulamentação equiparável a Lei – a análise da lei alienígena será feita pelo órgão competente e levará em conta os pontos do parágrafo único do artigo.

Outrossim, será possível a transferência quando em respeito aos compromissos assumidos em acordos de cooperação internacional e, respeitando a publicidade, quando for necessária para executar políticas públicas. Ademais, o órgão responsável também poderá permitir a transferência mas deve considerar as limitações expostas pelo art. 34.

Esta regulamentação aparenta não ser muito viável levando em consideração o grau de conectividade que vivemos atualmente. As relações no âmbito da internet são de constantes trocas de dados no interior e fora do país, barreiras físicas não existem e a limitação dessa troca, na maneira que foi abordada pelo artigo pode ser considerada inviável. Nos comentários feitos ao anteprojeto da Lei, Giovanna Carloni[53] demonstra que o artigo pode ser considerado até mesmo um retrocesso às tecnologias obtidas atualmente, para ela diversos serviços seriam vedados e trazê-los para território brasileiro é extremamente custoso, outro ponto é a utilização que está cada vez maior do dispositivo "nuvem" em que pessoas diferentes e com data centers espalhados no mundo fazem trocas constantes de dados e a sua proibição, atualmente, é impossível, levando em consideração as diversas empresas e pessoas físicas que se beneficiaram com a utilização deste dispositivo.

Como solução, Carloni demonstra que para garantir a segurança na transferência de dados internacionalmente, algumas atitudes são mais viáveis:

---

[52] Conceito desenvolvido pelo economista Fritz Machlup, com origem do termo Globalização.
[53] Advogada especializada em privacidade e proteção de dados.

> Ao invés de focarmos no local onde os dados serão armazenados e processados (ou seja, no país considerado "adequado", o que não dá reais garantias de segurança e iria contra o fluxo de dados que já ocorre cotidianamente), o que os acadêmicos que estudam o assunto sugerem é a transferência do foco para (i) o operador do serviço, para que ele garanta a segurança dos dados com accountability e transparência, e para (ii) as tecnologias capazes de proteger dados como padrão (o chamado "privacy by design"). Ou seja, a ideia é a sempre permissão da transmissão internacional dos dados como regra, independente do país para o qual ocorra a transferência seja considerado adequado ou não (já que não podemos fugir do "status quo" gerado pela internet e computação em nuvem), transferindo assim a responsabilidade pelo respeito às demais regras de proteção de dados aos responsáveis pelo tratamento de dados. [54]

Com relação a responsabilidade dos agentes devido à situação de transferência, o art. 35 que diz que:

> o cedente e o cessionário respondem solidária e objetivamente pelo tratamento dos dados, independentemente do local onde se localizem, em qualquer hipótese.

São chamados de responsável e operador os agentes que tratam os dados, eles devem manter os registros das operações dos dados tratados e o órgão competente irá determinar a forma da guarda deste registro. Como explicado no art. 5º, IX da Lei, o operador está subordinado ao responsável, em que o primeiro só irá realizar o tratamento determinado pelo segundo[55].

A partir dessa premissa, também é encargo do responsável indicar qual será o encarregado pelo tratamento dos dados pessoais, é o que determina o art. 41. O encarregado dos tratamentos é, de acordo com art. 5º, X da Lei, a pessoa física intermediária entre o órgão responsável e os titulares dos dados pessoais. O encarrega tem o papel de auxiliar os titulares por meio de informações e adotar providências, orientar funcionários e até mesmo receber reclamações.

A Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (ABDTIC), durante o debate do ainda anteprojeto para a Proteção de Dados Pessoais fez crítica importante a esse artigo. No seu comentário, a centralização dessas obrigações em uma pessoa acarretaria em mais demora considerando o possível numero de demandas, ou seja, situação oposta a buscada pelo legislador. Mas, assim como afirmado em outras partes do

---

[54] PENSANDO O DIREITO. Consulta Pública do Anteprojeto de Lei de Prote- ção de Dados Pessoais. Disponível em: < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em: 10 set. 2017

[55] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 09 de set. 2017.

dispositivo, o órgão competente poderá estabelecer novas normas direcionadas ao encarregado e hipóteses de dispensa da necessidade da indicação (art. 41, §3º).

A garantia de responsabilidade dos agentes que tratam dos dados pessoais é tema indispensável a ser tratado nessa Lei, tendo em vista que não é apenas a formulação de normas que irão impedir infrações, ademais, é forma de dar segurança jurídica a todos os donos e usuários dos dados e manter sempre os serviços de internet em busca de melhorias em suas ferramentas de segurança com o propósito de evitar qualquer dano ao usuário.

Além dos artigos dispersos neste capítulo, a seção III fala especificamente do assunto. Os artigos 42 a 44 deliberam sobre o tema e positivam que o responsável por tratar os dados pessoais e, em decorrência desse tratamento, causar prejuízos patrimoniais, morais ou mesmo coletivos serão obrigados a repará-lo.

O parágrafo primeiro do art. 42 causa certa confusão ao tornar exceção o ônus da prova invertido a favor do titular apenas nos casos de verossímil alegação ou quando for muito oneroso reunir as provas. Levando em consideração os princípios da proteção, da vulnerabilidade e da facilitação da defesa trazidos pelo Código de Defesa do Consumidor – que também é responsável por regulamentar a proteção de dados, a parte que em sua grande maioria é vista e considerada a mais frágil é justamente a do usuário da internet, logo, determinar que em regra a comprovação dos danos cabe a ele, ignora a vulnerabilidade das partes, tendo em vista que o trabalho com dados virtuais exige, muitas das vezes, um saber técnico que nem todos possuem.

Colaborando para evitar qualquer tipo de responsabilidade, os artigos seguintes – art. 45 a 49, determina medidas que operadores, agentes e o responsável devem adotar para que haja uma maior segurança e sigilo dos dados, desde mesmo sua fase de concepção até execução do tratamento (art. 45, §2º).

Mesmo após o término do tratamento, todos que tiveram contato com as informações são obrigados a manter o sigilo de todos os dados e, caso haja um incidente de segurança e que possa ocasionar danos ao titular, a comunicação ao órgão competente é imprescindível.

Durante o anteprojeto algumas críticas foram feitas a essa determinação, o questionamento apresentado pela Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização (CNseg) é devido a falta de determinação do significado do "incidente de segurança", pois é necessária maior clareza com relação a essa expressão para que não haja interpretações diversas[56], outra questão elaborada

[56] PENSANDO O DIREITO. Consulta Pública do Anteprojeto de Lei de Proteção de Dados Pessoais.

pela BSA The Software Alliance é o fato da Lei exigir que "qualquer incidente" seja notificado, mas não leva em consideração que muitas vezes dados corrompidos que poderiam causar riscos ao titular são qualificados como inutilizáveis, ilegíveis ou indecifráveis, ou seja, impossíveis de serem utilizados de qualquer forma. Logo, a necessidade de comunicar todos os casos, inclusive esse exemplificado, ocasionará um excesso de notificações desnecessárias.

Portanto, como apresentado pela Associação Brasileira de internet (ABRANET), incidentes com menor potencial de danos não podem ser equiparados aos que causam grandes problemas aos titulares e, como o órgão competente será o avaliador da gravidade do incidente, devendo inclusive ter o trabalho de orientar o responsável para tomas providencias para mitigar ou reverter os efeitos do incidente e também deve salvaguardar os direitos dos titulares, este trabalho deve se concentrar nos casos mais relevantes.[57]

Durante toda a leitura da Lei são apresentadas várias responsabilidades e garantias que o órgão competente terá. Tamanho poder discricionário causa certa insegurança jurídica. O penúltimo capítulo do dispositivo legisla sobre a forma que será feita a fiscalização e quais as sanções cabíveis dependendo da pessoa jurídica de direito que cometeu a infração.

O art. 52 define rol de possibilidades de sanções possíveis para infração cometida por pessoa de direito privado, entre elas são a aplicação de multa, bloqueio dos dados pessoais e até mesmo a suspensão de funcionamento de banco de dado. As sanções podem ser cumuladas, dependendo da infração que tenha sido cometida, se houve reincidência, adequando-a aos prejuízos causados e quais os direitos pessoais afetados.

Especificamente sobre o órgão competente, a Seção II estabelece diversas atribuições, entre elas está o dever de zelar pela proteção de dados, elaborar instruções sobre a proteção para políticas públicas, fiscalizar a aplicação das normas, conscientizar a população sobre o tema, estipular e editar normas de proteção de dados, entre outras ações cabíveis.

O Artigo 19 – organização não governamental, defende a ideia de que o órgão competente não deve apenas fiscalizar o tratamento dos dados pessoais "mas se destine

---

Disponível em: < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em: 10 set. 2017

[57] PENSANDO O DIREITO. Consulta Pública do Anteprojeto de Lei de Proteção de Dados Pessoais. Disponível em: < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em: 10 set. 2017

também à regulação de temas mais amplos, relacionados à sociedade da informação como um todo."[58]

O órgão será composto, de acordo com o positivado no art. 54 da Lei, por sete representantes do Poder Executivo federal, um representante indicado pelo Congresso Nacional, um representante indicado pelo Conselho Nacional de Justiça, um representante indicado pelo Conselho Nacional do Ministério Público, um representante indicado pelo Comitê Gestor da Internet no Brasil, um representante da sociedade civil, um representante da academia e dois representantes do setor privado. A inclusão de um representante da sociedade civil e da academia tornam o órgão, além de político, mais democrático e que procura por uma tecnicidade com relação ao tema.

Finalizando a breve análise da Lei, o artigo determina que além das atribuições dadas ao órgão, também haverá a criação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade com objetivo de:

> I – fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> II- elaborar relatórios anuais de avaliação da execução das ações da Politica nacional de Proteção de Dados Pessoais e da Privacidade;
> III- sugerir ações a serem realizadas pelo órgão competente;
> IV – realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e
> V- disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.[59]

Por meio da interpretação da letra da Lei, pode-se acordar que esse Conselho será uma espécie de órgão consultivo, para analisar casos específicos relacionados a matéria e também como um fórum de interação entre governo e sociedade civil que atua no setor. Vislumbramos algo nos moldes de um Conselho Consultivo de Agência Reguladora, como no caso da Agência Nacional de Telecomunicações – Anatel.

A regulamentação que será aprovada no país deve, além de buscar proteger os direitos de cada cidadão, se preocupar com o não engessamento dos avanços tecnológicos que são constantes e impossíveis de serem freados.

---

[58] BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional**. Disponível em: < http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >. Acesso em: 10 de set. 2017.

[59] BRASIL, **Projeto de Lei n. 5.276**, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 08 de set. 2017.

Na análise feita pela professora Jânia Maria Lopes Saldanha, atualmente a sociedade se encontra em uma situação nunca antes vivenciada,

> que não apenas se espalha com uma velocidade fulgurante mas que se sofistica no que diz respeito à desterritorialização e destemporalização das informações, comunicações e registro de dados. Esse cenário de "des" mostra que não estão em jogo e em tensão apenas interesses ligados ao desenvolvimento econômico e às liberdades fundamentais. Emerge um problema geoeconômico diante dos desafios em identificar a legislação aplicável, os atores responsáveis e os graus de responsabilidades.[60]

Assim sendo, o desafio que a regulamentação enfrenta é a procura pelo equilíbrio entre a regulamentação que visa salvaguardar direitos fundamentais sem debilitar o meio tecnológico, o fato de ter sido um projeto que levou em consideração a opinião de diversas áreas da sociedade é ação importante para que a lei seja realista e encontre uma forma de legislar sobre tema tão dinâmico.

No próximo capítulo será analisado alguns aspectos decisivos para a aplicação da lei de proteção de dados, as nomenclaturas utilizadas, os significados e suas característica são essenciais para a melhor compreensão do objeto que a regulamentação trata e quais são seus requisitos.

---

[60] SALDANHA, Jânia Maria Lopes. **Qual direito para os dados pessoais em tempos de Big data?**. Disponível em: < http://justificando.cartacapital.com.br/2015/03/16/qual-direito-para-os-dados-pessoais-em-tempos-de-big-data/ >. Acesso em 28 set. 2017.

2. CLASSIFICAÇÃO DE DADOS E CONSENTIMENTO

O presente capítulo abordará os três tipos de dados pessoais e o conceito de consentimento tratados pelo Projeto de Lei nº 5.276/2016. A classificação de cada espécie de dado pessoal está diretamente ligada à forma como eles serão tratados e também qual será o seu grau de proteção. Diante disso, um estudo abordando suas diferenças é necessário para compreender os objetivos do legislador e qual o alcance jurisdicional da Lei.

Após a constatação de qual tipo de dado pessoal será tratado, é apresentado uma análise aprofundada do conceito jurídico de consentimento como ferramenta principal para disponibilizar ou não esses dados e, dependendo do tipo de dado, quais serão os requisitos necessários para que haja a anuência.

2.1 Dados pessoais

No livro "Privacidade, proteção de dados e defesa do consumidor", Laura Mendes aponta a definição de dados pessoais de Raymond Wacks, que diz ser "informação em potencial, isto é, ele pode se transformar em informação se for comunicado, recebido e compreendido"[61] e podendo essa informação ser oferecida em diferentes formatos.

De acordo com os estudos de Doneda, é importante que haja uma diferenciação entre os vocábulos "informação" e "dados" , para que não sejam utilizadas como sinônimo. Acompanhando a explicação de Wacks, os dados são considerados uma "pré-informação", antes do tratamento e interpretação, já a informação é fase inicial e ampla, podendo ter em seu conteúdo fatos além do ponto principal que poderá será interpretado[62]. Dessa forma, "o vetor que faz a diferença é exatamente o tecnológico", em que se transforma diversas informações em dados organizados e mais específicos. Essa distinção é importante para demonstrar a peculiaridade dos dados pessoais, justificando o empenho em serem protegidos por regulamentação.

O conceito de dados pessoais, levando em consideração que ainda não ocorreu a aprovação de nenhuma regulamentação específica, não está positivado nas leis que se atentaram a legislar sobre o assunto de forma clara nem uniforme entre as legislações.

O art. 5º do Marco Civil da Internet foi reservado para a classificação de alguns termos importantes, mas não contemplou os dados pessoais. A partir da leitura da Lei, a expressão "dados pessoais" aparece repetidas vezes, mas não é feita referencia expressa e específica do

---

[61] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 55

[62] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 152

que seriam, sendo possível apenas deduzir implicitamente devido ao texto do art. 7º, VII, que registros de conexão e de acesso a internet são considerados dados pessoais.

A Lei 12.527/11 traz o conceito de informações pessoais – terminologia usada na para dados pessoais:

> Art. 4º Para os efeitos desta Lei, considera-se:
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

O Instituto Brasileiro de Defesa do Consumidor (Idec), em seu relatório à comissão especial de tratamento e proteção de dados pessoais da Câmara dos Deputados, apresentou o posicionamento das empresas durante a Comissão, é defendido que a redação que define os dados pessoais deve ser restrita, pois, uma redação ampla torna todas as atividades humanas sujeitas à lei. A proposta das empresas é a de definir os dados pessoais como sendo apenas aqueles que identifique de forma precisa o titular[63].

O Idec exibe motivos para a classificação ter em sua redação as expressões "identificada" e "identificável", inclusive nas regulamentações em países estrangeiros e nos Projetos de Lei brasileiro. De acordo com o instituto, os dados identificados são os mais simples. O conhecimento desses dados, apesar de expor o titular consideravelmente, não tem muito proveito por ser um dado menos completo e expressivo, como por exemplo, o número de telefone do titular.

O vocábulo "identificável", de acordo com o Instituto, é a "mina de ouro" dos dados, pois por meio de várias combinações com outros dados é gerado um perfil individual completo e que pode ser utilizado de forma excessiva contra os titulares[64].

Os projetos de lei brasileiros não divergem muito nas redações sobre esse tema. O PL nº 5.276/16, ao menos até o momento, não acatou o requerimento das empresas em mudar a possível classificação dos dados pessoas e no art. 5º, I determina que:

> I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

De acordo com Fortes, o PL 5.276/16 de proteção de dados foi "consideravelmente influenciado pelas normas internacionais que tutelam a proteção de dados pessoais em sentido amplo", dessa maneira não é surpresa que o exposto no artigo 5º, I, é uma definição próxima

---

[63] IDEC. **À Comissão especial de tratamento e proteção de dados pessoais da Câmara dos Deputados**. Disponível em: <https://www.idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf>. Acesso em: 10 set. 2017.
[64] Ibidem.

ao conceito editado pela Convenção de Estrasburgo de 1981, que teve o objetivo de fortalecer a proteção de dados ou seja, a proteção legal das pessoas com relação ao processamento automático de informações pessoais relacionadas a elas[65], no art. 2º, define os dados pessoais como "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação"[66]. A partir desse conhecimento, Doneda conclui que a informação passa a ser considerada dado pessoal quando há um aspecto objetivo que identifique uma pessoa[67].

2.1 Dados pessoais sensíveis e dados anônimos

Os dados sensíveis são categoria dos dados pessoais e indicam, de forma direta e precisa, características, opção sexual, crenças e até mesmo dados genéticos do titular, ou seja, abordam questões estritamente pessoais.

A Constituição Brasileira, em seu art. 5º, X, define como direito fundamental a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e, a partir disso, é compreensível a importância de se buscar uma legislação sobre os dados sensíveis e a necessidade de uma maior rigidez para dispor deles.

O Marco Civil da Internet, assim como no caso dos dados pessoais, não colocou de forma expressa o que seria os dados sensíveis e o que são englobados por eles, apesar de determinar em sua redação a necessidade de uma maior proteção. Essa situação acontece devido a dificuldade em se determinar o que seriam os dados sensíveis, levando em consideração que o momento e a finalidade de cada dado pode ou não violar a intimidade de seu titular.

Na pesquisa realizada por Daniel Piñeiro Rodrigues, conclui-se que

> (...) juristas vêm se apresentando relutantes em definirem um conjunto de informações que possam ser declaradas, *per se*, sensíveis, sem considerar todo o contexto de sua utilização, publicização ou outras formas de tratamento. Nesta mesma linha, podemos verificar a Declaração Internacional sobre Dados Genéticos Humanos da Unesco (DIDGH), salientando que tais dados serão especialmente protegidos em função de seu contexto (HAMMERSCHMIDT, 2008). Em contrapartida, no entanto, a maioria dos Estados membros da União Europeia já apresentam um

[65] ELETRONIC PRIVACY INFORMATION CENTER. **Council of Europe Privacy Covention**. Disponível em: <https://epic.org/privacy/intl/coeconvention/> . Acesso em: 10 set. 2017.
[66] COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS. **Para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Disponível em: < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm> . Acesso em: 10 set. 2017.
[67] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 157

> arraigado pensamento de que existiriam certas categorias de dados que sempre seriam capazes de lesar a esfera íntima da pessoa.[68]

Novamente, cabe à lei específica definir o que será considerado dados sensíveis. Para alguns autores o PL nº 5.276/16 estabeleceu classificação irreal que não leva em consideração a capacidade de armazenamento de informações pelo sofisticado sistema de *big data*. A crítica aponta o que foi concluído anteriormente, em determinadas situações uma informação que não é considerada dado sensível pode ser mais relevante naquele contexto, mas terá uma proteção menor pelo simples fato de não se enquadrar no determinado pela lei[69].

Mas, de acordo com os comentários feitos pela Consultoria Legislativa da Câmara dos Deputados em junho de 2016, a definição de dados sensíveis no PL nº 5.276/16 guarda forte sintonia com a "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais" que faz parte do Conselho da Europa nº 108 e determina em seu art. 6º que:

> "Dados pessoais que revelem a origem racial, opiniões políticas, religiosas ou de outras crenças, bem como dados relativos à saúde pessoal ou à vida sexual não podem ser processados automaticamente ao menos que leis nacionais estabeleçam garantias adequadas. O mesmo se aplica a dados pessoais relativos a condenações criminais."[70]

Outrossim, também buscou se adequar à Diretiva Europeia nº 46, de 1995, que estabelece a proibição de tratar dados que relevem "origem racial ou ética, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual."[71] sem o consentimento expresso do titular. Essa determinação é ratificada pelo Regulamento 2016/679 da União Europeia que revoga a Diretiva Europeia citada, nele os dados pessoais sensíveis

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades

---

[68] RODRIGUEZ, Daniel Piñeiro. **A proteção de dados pessoais sensíveis no contexto do estado democrático de direito**. 2009. Disponível em: < http://www.pucrs.br/edipucrs/IVmostra/IV_MOSTRA_PDF/Direito/72217-DANIEL_PINEIRO_RODRIGUEZ.pdf >. Acesso em 30 set. 2017.

[69] MORAIS, José Luis Bolsan de; NETO, Elias Jacob. **Quem é anônimo no mundo dos metadados? O problema do anteprojeto de lei para a proteção de dados pessoais**. 2015. Disponível em: <http://emporiododireito.com.br/backup/repec-11-quem-e-anonimo-no-mundo-dos-metadados-o-problema-do-anteprojeto-de-lei-para-protecao-de-dados-pessoais-por-jose-luis-bolzan-de-morais-e-elias-jacob-neto/>. Acesso em: 30 set. 2017.

[70] NAZARENO, Claudio. **Comentários ao PL 5.276/16, que dispõe sobre o tratamento de dados pessoais.** 2016. Disponível em: < http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema11/2016_10154_pl5276-2016-tratamento-de-dados-pessoais_claudio-nazareno > . Acesso em: 30 set. 2017.

[71] NAZARENO, Claudio. **Comentários ao PL 5.276/16, que dispõe sobre o tratamento de dados pessoais.** 2016. Disponível em: < http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema11/2016_10154_pl5276-2016-tratamento-de-dados-pessoais_claudio-nazareno > . Acesso em: 30 set. 2017.

> fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas.[72].

Apesar da dificuldade em se determinar de forma específica todos os dados sensíveis, o esforço de se buscar ao menos classificar os dados que, independentemente de seu contexto, são vulneráveis e merecem uma maior proteção é extremamente válido para que os titulares disponham de uma maior segurança jurídica – considerando que a forma de proteção de cada dado é baseada nessa classificação.

Por fim, é necessário que se faça a classificação dos dados anônimos para compreender as propostas de anonimização que a PL nº 5.276/16 aborda em sua redação. Os dados anônimos são considerados contrários ao que os dados pessoais produzem, "são dados que se referem a pessoas que não podem ser identificadas (...). Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), não permite a identificação de seu titular."[73].

A possibilidade de existir um dado absolutamente anônimo, atualmente, está ultrapassada. Devido à quantidade de informações armazenadas no *big data* e à sofisticação das formas de cruzamento deles, afirmar que um dado não tem a capacidade de identificar o titular já se torna quase impossível[74]. Devido a isso o legislador foi prudente ao nomear esses dados como "dados anonimizados" no art. 5º , IV:

> Art. 5º Para os fins desta Lei, considera-se:
> IV – dados anonimizados: dados relativos a um titular que não possa ser identificado;

As práticas de anonimização dos dados é meio eficaz para tratamento dos dados sensíveis, aqueles que identificam objetivamente o titular, sem o expor e mantendo a segurança desses dados. Para que isso ocorra, é necessário eliminar elementos identificadores, por meio da supressão – disponibilizar apenas parcialmente o número do CPF , generalização

---

[72] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 01 out. 2017.

[73] PENSANDO O DIREITO. Dados pessoais, dados anônimos e dados sensíveis. Disponível em: < http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/ > acesso em 01 out. 2017.

[74] PENSANDO O DIREITO. **Você sabe o que são dados anônimos?**. Disponível em: < http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/ > Acesso em 01 out. 2017.

– exibir apenas as iniciais dos nomes ou até mesmo não divulgar a idade exata dos titulares, randomização e pseudoanonimização.[75]

Pode ocorrer dúvida sobre a legalidade dessa prática quando se aprecia a possibilidade de conflito entre a liberdade de expressão contida na Constituição Federal – art. 5º, IV, que veda o anonimato. A resposta deste questionamento é precisa para compreender a possibilidade da existência de dados anonimizados.

Com a leitura do art. 220, também da Constituição Federal, é positivado que não haverá restrição à liberdade de expressão, "observando o disposto no art. 5º, IV, V, X, XIII e XIV"[76], logo, os dados anônimos serão resguardados quando tiverem a intenção de proteger "intimidade, a vida privada, a honra e a imagem das pessoas"[77]. Gilmar Mendes e Paulo Branco ensinam que a liberdade de expressão deve respeitar a dignidade da pessoa humana,

> Respeita-se a dignidade da pessoa quando o indivíduo é tratado como sujeito com valor intrínseco, posto acima de todas as coisas criadas e em patamar de igualdade de direitos com os seus semelhantes. Há o desrespeito ao principio, quando a pessoa é reduzida à singela condição de objeto, apenas como meio para satisfação de algum interesse direto.[78]

Isto posto, também é compreendido em seu texto que "a reclusão periódica à vida privada é uma necessidade de todo homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade."[79].

Apesar da Lei ainda abordar a possibilidade de anonimização dos dados, um exemplo claro da dificuldade em se gerar um dado anônimo é vista no estudo "*Simple Demographics Often Identify People Uniquely*", de Latanya Sweeney. Neste estudo é constatado que 87% da população dos Estados Unidos, baseado em dados simples como o CEP ou seu gênero, faz com que sejam únicas e, consequentemente, identificáveis[80], o fato de algumas pessoas dividirem da mesma característica não impede que com a combinação de outros dados torna as pessoas singulares.

Atualmente, com o grande avanço da tecnologia do *big data*, o desafio de regular esse tema da classificando dos dados fica cada vez mais difícil, tendo em vista que o tratamento

---

[75] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 25

[76] BRASIL. **Constituição, 5 de outubro de 1988**. Constituição da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em: 01 out. 2017.

[77] Ibidem.

[78] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2014. p. 278

[79] Ibid., p. 280

[80] SWEENEY, Latanya. **Simple Demographics Often Identify People Uniquely.** Disponível em: <https://dataprivacylab.org/projects/identifiability/paper1.pdf >. Acesso em: 01 out. 2017

de qualquer informação, dependendo do contexto, pode vir a ter a identificação do titular comprometida, mesmo sendo um simples dado pessoal ou um complexo dado sensível.

Existem estudos que buscam manter a possibilidade de anonimização dos dados, é o caso do trabalho "Not So Unique in the Crowd: a Simple and Effective Algorithm for Anonymizing Location Data" que busca reduzir a possibilidade de localizar pessoas a partir de suas trajetórias diárias. Os pesquisadores demonstram que ao invés de diminuir os dados das informações de localização o melhor método é o de "cortar as trajetórias originais em sub-trajetórias mais curtas e que se espera ter menos singularidades."[81].

Levando em consideração todos esses fatos, a anonimização ainda tem a característica de proporcionar uma maior proteção ao titular, reduzindo os riscos durante o tratamento, dessa forma a PL nº 5.276/16 deliberou que, sempre que possível, preferir a utilização dos dados anonimizados em detrimento dos demais dados pessoais.

2.2 Tipos de consentimento

Após a tentativa de classificar os dados pessoais, surge a necessidade em estabelecer o instituto jurídico do consentimento, visto que todas as informações que poderão ser utilizadas por terceiros relacionam-se a um cidadão que deve ter o seu direito de escolha livre para determinar como serão disponibilizados e tratados seus dados, respeitando assim seu direito à privacidade. Mendes aborda o alto grau de autodeterminação que existe na proteção de dados, pois apenas o titular pode determinar qual o limite para a coleta e processamento de seus dados[82].

Doneda aborda em seu livro a necessidade de se refletir sobre o consentimento pois é por meio dele que o direito fundamental de escolha é afirmado[83], mas também é importante que se compreenda a viabilidade legal de não apenas afirmar o direito fundamental de escolha, mas a possibilidade de dispor do direito fundamental à privacidade.

Mendes e Branco em sua obra, apontam que "os direitos fundamentais não são suscetíveis de renúncia plena, mas podem ser objeto de autolimitações, que não esbarrem no

---

[81] SONG, Yi; DAHLMEIER, Daniel; BRESSAN, Stephane. **Not so unique in the Crowd: a simple and effective algorithm for anonymizing location data**. Disponível em: < http://ceur-ws.org/Vol-1225/pir2014_submission_11.pdf >. Acesso em: 01 out. 2017.

[82] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 60

[83] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** .Rio de Janeiro: Renovar, 2006. p. 375

núcleo essencial da dignidade da pessoa"[84], logo, não existe violação ao direito se houver o consentimento.

No caso dos dados pessoais, de acordo com Doneda, "a legislação sobre a matéria, desde as suas primeiras manifestações, dedicou especial atenção à forma de atuação da proteção de dados, o que determinou a adaptação e criação de instrumentos para a sua tutela."[85].

Há certa dificuldade em se determinar um modelo de tutela que seja cabível devido as constantes mutações dos meios em que os dados pessoais transitam. Doneda determina que o melhor é interpretar os institutos de acordo com o caso em concreto, respeitando os princípios da proteção dos dados pessoais. Sendo assim, o consentimento é instituto básico[86], por meio dele o cidadão poderá autogerir seus dados da melhor forma que lhe convém.

> O consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser verificada a partir dos efeitos da sua concreta aplicação ao caso dos dados pessoais e seus efeitos.[87]

Laura Mendes caminha para o mesmo entendimento, a estudiosa afirma que

> a regulamentação jurídica do tratamento de dados pessoais está amparada no conceito de que o indivíduo deve ter o poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de livre desenvolvimento de sua personalidade. Cabe ao Estado, por meio de legislação, promover os mecanismos necessários para que o cidadão possa exercer o controle do fluxo de informações a seu respeito na sociedade.[88]

A natureza do consentimento ainda não é tema pacificado, Laura Mendes aborda em seu estudo três correntes alemãs que tratam do assunto. A primeira entende que o consentimento tem natureza de declaração de vontade negocial, para a segunda corrente, o consentimento é ato jurídico unilateral e sem natureza negocial, por fim, a terceira corrente defende que o consentimento é ato que se assemelha a negócio jurídico[89].

Doneda, de acordo com seus estudos, é adepto da segunda corrente, acredita que o consentimento não poderia ser comparado a negócio jurídico por dificultar os "atributos da

---

[84] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2014. p. 284
[85] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 361
[86] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 371
[87] Ibid., p. 372
[88] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 60
[89] ibid., p. 62

personalidade que devem ser considerados."[90], isso quer dizer que apesar da anuência para a utilização dos dados por terceiros, o titular não está obrigado aos efeitos vinculantes de uma natureza obrigacional, logo, não seria possível associar o consentimento com um negócio jurídico já que a qualquer momento o titular poderá revogar o consentimento feito, tendo apenas o responsável pelo tratamento que arcar com qualquer consequência desse ato. Doneda conclui que o consentimento é "um ato unilateral, cujo efeito é o de autorizar um determinando tratamento para os dados pessoais, sem estar diretamente vinculado a uma estrutura contratual."[91]

Atualmente o posicionamento mais aceito é o que entende que o consentimento se assemelha ao negócio jurídico. Segundo Mendes, levando em consideração a natureza atípica da permissão dos tratamentos de dados, é constatado que há ao mesmo tempo uma característica negocial e personalíssima, dessa forma a interpretação da natureza do consentimento deverá ser analisada caso a caso e aplicada apenas quando cabível[92]. O estudo feito pela grupo de pesquisa em políticas públicas para o acesso à informação, também chegou a esse entendimento, determinam que o "consentimento é um típico elemento contratual. É por meio dele que que os indivíduos exprimem sua vontade de contratar (...)"[93].

Apesar da divergência, ambos os autores concordam que o consentimento está baseado na autodeterminação do titular, dessa forma não pode ser interpretado como a ausência de interesse do titular com relação ao seus dados, mas como um ato de vontade, que inclusive pode ser revogado no momento em que o titular, de forma justificada, fizer o pedido[94], sendo essa possibilidade princípio fundamental da autodeterminação.

O estudo do tipo de contrato que materializará o ato de consentir, além de relevante para o trabalho, torna possível, a partir da compreensão dos princípios dos contratos, intuir como a doutrina concluiu que o consentimento se assemelha com negócio jurídico.

Caio Mario Pereira define o mundo moderno como o mundo do contrato, a ponto de, caso o contrato não existisse mais, a vida social estagnaria[95]. O contrato além de limitar as partes às suas obrigações também exerce a importante função social de afirmar as vontades

---

[90] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 378
[91] Ibid., p. 378
[92] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. 63
[93] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 43
[94] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 43. p.64
[95] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 10

individuais de cada pessoa. A possibilidade de exercer a ação de contratar ocorre em razão da autonomia da vontade, princípio também importante para o consentimento, pois o tratamento de dados pessoais só ocorre quando o titular manifesta sua vontade livre para disponibilizar seus dados.

O contrato tem o objetivo de projetar as vontades das partes e, de acordo com Pereira, "aquele que contrata projeta na avença algo de sua personalidade. O contratante tem a consciência do seu direito e do direito como concepção abstrata. Por isso, realiza dentro das duas relações privadas um pouco da ordem jurídica total.", trazendo para as questões que envolvem os dados pessoais, no momento em que o titular abre mão de controlar, de forma exclusiva seus dados pessoais, regula uma conduta em seu âmbito privado que não deve ter consequências há terceiros e nem ao ordenamento jurídico como um todo, mas é forma de regular vontades específicas de cada cidadão, singularmente, como melhor o convém.

Apesar da liberdade trazida pela busca de atender aos interesses das partes que formam o contrato, há algumas limitações ao exercício da autonomia da vontade, a função social, por exemplo, é princípio moderno que desafia o entendimento de que dentro de uma esfera contratual tudo é permitido e, ainda de acordo com Pereira, "o reconhecimento da inserção do contrato no meio social e da sua função como instrumento de enorme influência na vida das pessoas possibilita um maior controle da atividade das partes."[96].

A crítica feita ao entendimento de que o consentimento é semelhante a negócio jurídico se fundamenta no princípio da obrigatoriedade advindo da função social. Esse princípio, basicamente, expõe a necessidade de consentimento mútuo para a quebra de um contrato mas, levado em consideração as mudanças em que o próprio instituto do contrato já passou para se adequar aos pressupostos culturais de cada época, como bem exposto por Orlando Gomes,

> Sucede, porém, que o fenômeno da contratação evolui ao ponto de alterar profundamente esse quadro conceitual. O movimento evolutivo não se caracteriza unicamente pelo aparecimento de numerosas *inovações técnicas,* nem pela consagração em princípios jurídicos de suspeitas motivações para justificar a direção e o controle da economia pelo Estado. Dirige-se no sentido de uma reconstrução do próprio sistema contratual orientada no sentido de libertar o conceito de contrato da ideia de autonomia privada e admitir que, além da vontade das partes, outras fontes integram o seu conteúdo. A nova concepção atenta para o dado novo de que, em virtude da política interventiva do Estado hodierno, o contrato, quando instrumenta relações entre pessoas pertencentes a categorias sociais antagônicas, ajusta-se a parâmetros que levam em conta a dimensão coletiva dos conflitos sociais subjacentes. Disciplinados por uma *legislação avulsa* que abandonou

[96] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 13

> a postura tradicional do Código Civil, passam a ser, na explicação de Rodatà, um ponto de referência de interesses diversos, uma estrutura aberta que é preenchida não apenas por disposições resultantes do acordo de vontades, mas também por prescrições da lei, imperativas e dispositivas, e pela equidade.[97]

Pereira ainda cita em sua obra o jurista francês, Louis Josserand, que "conhecido por suas tendências inovadoras, (...) salienta que o conceito contratual procura compensar sua pretensa imobilidade milenar buscando novas tendências."[98]. Logo, a adequação do sistema contratual aos casos de tratamento de dados são cabíveis principalmente quando há a compreensão de que atualmente não é mais possível viver em uma sociedade que não se utiliza dos dados pessoais, mas busca assegurar que os direitos fundamentais e personalíssimos, que são os envolvidos nos tratamentos de dados, sejam protegidos da melhor maneira e principalmente durante sua manipulação.

O princípio da relatividade também se harmoniza ao consentimento, pois determina que a obrigação do contrato só recairá àqueles que tenham compactuado. Da mesma forma, o consentimento não deve ser meio de captura de dados pessoais de outros indivíduos, mesmo que parentes próximos, exemplo claro dessa situação é o cuidado que a regulamentação deve ter com os dados genéticos de cada cidadão, pois, a partir dele todo uma geração pode ser definida.

O princípio do consensualismo, compreende a obrigatoriedade do consentimento para a formação da obrigação, tendo o mesmo conceito do consentimento dos dados pessoais, ao passo que a simples proposta e aceitação não formam negócio jurídico, pois é preciso que o consentimento se iguale ao conteúdo[99], em outras palavras, os princípios do consentimento – finalidade determinada e inequívoca, devem estar presentes para que o contrato seja cabível.

Pereira, aborda em seu livro a necessidade sucedida desse princípio de constituir certas exigências materiais para que o consensualismo não se torne generalizado. Na questão dos dados pessoais, o risco da generalização é iminente, tendo em vista que o número de usuários da internet e os graus de conhecimento de cada cidadão sobre os riscos do tratamento de dados são diversos – desde a ignorância até o domínio completo das possibilidades de proteção. Dessa maneira, o formalismo pode ser ferramenta para que o consentimento,

---

[97] GOMES, Orlando. **Contratos**. 26. ed. Rio de Janeiro: Forense, 2008. p. 18

[98] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 550

[99] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 19

quando se tratar de dados específicos e que possam trazer grandes prejuízos a seus titulares, seja melhor aplicado.

Por último, o Código Civil de 2002 põe fim a críticas ao anterior Código e preenche a lacuna sobre a boa-fé objetiva e a coloca como cláusula geral e, mesmo não aplicando de forma expressa em seu artigo sobre os períodos pré e pós contratual, a interpretação é extensiva. Esse princípio, não apenas nos contratos, mas em todas as relações jurídicas da sociedade deve ser preservado, ainda mais quando se trata de transações que envolvem direitos fundamentais.

Após a análise das características dos contratos, são várias as espécies que encontramos no ordenamento jurídico brasileiro, superficialmente, alguns deles são os contratos de doação, em que uma parte se obriga a transferir de forma gratuita bem para a outra[100], de compra e venda – é o mais utilizado, de caráter bilateral e consensual, tem por finalidade para uma parte a de alienar um bem e para a outra a de adquirir uma propriedade[101], o contrato de locação é aquele em que uma das partes se obriga a fornecer a outra, por tempo determinado, o uso e gozo de bem não-fungível, mediante contraprestação em dinheiro[102], são diversos os contratos e suas novidades não param de aparecer, é o caso do contrato "know-how", em que o inventor usa da sua criatividade para produzir produto e o protege quando o leva ao público, para que outros não o utilizem sem permissão[103].

A doutrina não é unânime sobre a espécie de contrato cabível para os dados pessoais, no livro "Direito, Inovação e Tecnologia", Fabiano Menke elucida questão importante sobre os dados pessoais, de acordo com o estudo da doutrina Alemã, não é possível se falar em uma propriedade dos dados, pois os dados de cada titular representam um retrato da sociedade em que está inserido, não podendo ser reservado exclusivamente a ele, e o próprio indivíduo não pode ser minimizado a mero objeto de obtenção de informação[104], dessa maneira, algumas espécies de contratos podem ser excluídas por perderem seu objeto.

Os contratos também apresentam, apesar da liberdade de contratar e de fixar conteúdo, a figura do contrato de adesão, que recebe críticas fundamentadas na falta da manifestação de vontade de uma das partes[105], mas na doutrina moderna é considerado meio de contratação e,

---

[100] GOMES, Orlando. **Contratos**. 26. ed. Rio de Janeiro: Forense, 2008. p. 253
[101] Ibid., p. 265
[102] GOMES, Orlando. **Contratos**. 26. ed. Rio de Janeiro: Forense, 2008. p. 332.
[103] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 557
[104] MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. Coelho. **Série Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015. 1 v. p. 213.
[105] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014. p. 66.

devido a algumas de suas características, já pode ser constatado atualmente que está sendo aplicado como meio de materializar o consentimento para tratamentos de dados.

Os contratos de adesão surgiram no direito contratual moderno e são, basicamente, a aceitação em bloco de acordo redigido por apenas uma das partes. De acordo com Pereira, este contrato ocorre nos casos de estado de oferta permanente[106], ou seja, o número de ofertas dos serviços ou bens e o número de contratantes é infinita e indeterminada, devido a isso o contrato é feito de forma padronizada e rígida. Além disso, essa espécie de contrato está positivada no art. 54 do Código de Defesa do Consumidor.

Considerando algumas características do contrato de adesão, é possível que se visualize esse tipo como o cabível para o consentimento dos tratamentos de dados. Primeiramente, é preciso que se tenha em mente que o tratamento de dados ocorre em praticamente todas as plataformas da internet, desde redes sociais a sites escolares, e devido a isso, uma das principais características do contrato de adesão, a de ser voltado para um número ilimitado e indeterminando de contratantes, também surge no meio virtual. A formulação de um contrato padrão é a via mais simples para abarcar todas as necessidades das empresas de forma rápida e simples mas, em contrapartida, esse tipo de contrato não respeita um dos principais princípios do consentimento, a vontade livre do titular, limitando as escolhas sobre seus direitos fundamentais e, consequentemente, contrariando o princípio do equilíbrio contratual.

Estudo feito pela USP conclui que

> "o cidadão não deve se submeter à lógica do tudo ou nada dos contratos de adesão, na qual ele deve consentir com o uso de seus dados pessoais sob pena de não ter acesso a um produto ou serviço. Deve-se dar granularidade a tal escolha, de modo que ele possa consentir sobre os diversos usos, por quanto tempo e frequência, sobre o compartilhamento com terceiros e etc. Trata-se de franquear um leque de escolhas ao cidadão, a invés de reduzi-la a uma escolha binária do tudo ou nada."[107].

Outro estudo, feito pela Dra. Cíntia Rosa Pereira de Lima, sobre os contatos de adesão eletrônicos, chegaram em algumas preciosas conclusões. Os usuários, em sua maioria, não leem os contratos e licenças devido a pressa, falta de conhecimento técnico, pela falsa impressão que contratos eletrônicos, pela facilidade e gratuidade, não apresentam cláusulas

[106] Ibid., p. 67
[107] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 7

abusivas e, principalmente, por se depararem com diversas cláusulas, muitas vezes repetidas, que não deixam claro a situação, e com uma linguagem rebuscada[108].

A autora conclui que, em casos de anuência para tratamento de dados, o titular deve estar plenamente consciente sobre a forma de tratamento dos seus dados e as consequência, logo, a manifestação de vontade feita por meio de contrato que não demonstrou claramente essas questões, em cláusulas legíveis e destacadas das demais, torna a manifestação de vontade invalida, aplicando, inclusive, o art. 51 do CDC, que tornam nulas de pleno direito a cláusula contratual[109].

Levando todos esses fatores em consideração, seria o caso da formação de uma nova figura contratual, até mesmo próxima do contrato de adesão pois deve se ter em mente que, devido a utilização diária e constante do tratamento de dados, não é viável transformar a atividade de autorização em algo cansativo e demasiadamente burocrático, pois essa postura poderia acarretar, novamente, em uma automatização por parte dos usuários de sempre autorizarem sem nem mesmo observarem os termos e analisarem as consequências da liberação de seus dados. Para Lima, algumas soluções são possíveis

> A efetiva proteção do consumidor fica debilitada o que preocupa os juristas que propõem algumas soluções. As alternativas são: lege ferenda, considerar uma cláusula abusiva no contexto acima descrito (art. 51 do CDC); pressionar o mercado (os fornecedores que operam online) a estabelecerem cláusulas equitativas e que estejam de acordo com a justa expectativa do consumidor diante da relação jurídica em concreto; e, por fim, a adoção de algumas ferramentas tecnológicas, tais como, ter que descer até ao final a barra de rolagem para poder finalizar a adesão; aparecer um pop up ou outra ferramenta mais eficaz de avisos (warnings) com os termos que fogem à justa expectativa do consumidor; clicar ao lado de cada cláusula manifestando sua expressa anuência.[110]

Superada a questão sobre os contratos, a importância da composição da ideia de consentimento se reflete não apenas nas atuais legislações mas também, por exemplo, foi tratado ao elaborar a Carta dos Direitos Fundamentais da União Europeia, que em seu artigo 8º positiva sobre a proteção de dados pessoais e a necessidade de haver o consentimento[111].

> Proteção de dados pessoais

---

[108] LIMA, Cíntia Rosa Pereira de Lima. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos**. Disponível em: < http://publicadireito.com.br/artigos/?cod=981322808aba8a03 > . Acesso em: 13 de out. 2017.

[109] Ibidem

[110] LIMA, Cíntia Rosa Pereira de Lima. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos**. Disponível em: < http://publicadireito.com.br/artigos/?cod=981322808aba8a03 > . Acesso em: 13 de out. 2017

[111] PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014, p. 16

> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legitimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. [112]

A Diretiva Europeia 95/45/CE também aborda o tema em seu art. 7º, demonstrando mais uma vez a importância do consentimento do tutelar quando houver a necessidade do tratamento de seus dados.

> Artigo 7º
> Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:
> a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento;[113]

Posteriormente, o Regulamento 2016/679 que irá entrar em vigor em 2018, também afirma a necessidade do consentimento.

> (32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral.

O consentimento para dispor dos dados pessoais, no Brasil, é instituído pelo Marco Civil da Internet no art. 7º, que trata sobre os direitos assegurados aos titulares, nele se expressa a vedação do fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, nos outros inciso do mesmo artigo, aborda a necessidade de, informação clara e completa sobre os dados que serão tratados, a possibilidade do consentimento expresso – e que nessa situação, ele esteja em destacado das demais cláusulas contratuais. No art. 16, incisos I e II, reafirma a vedação da utilização de dados de registro de conexão sem o consentimento do titular e a utilização do dado de forma a extrapolar o que foi acordado anteriormente.

---

[112] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Parlamento Europeu, Conselho da União Europeia e Comissão Europeia. 2000 Disponível em: < http://www.fd.uc.pt/CI/CEE/pm/Tratados/Nice/Carta%20Direitos%20Fundamentais.pdf >. Acesso em: 13 set. 2017.

[113] UNIÃO EUROPEIA. **Diretiva1995/46CE, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Diário Oficial das Comunidades Europeias*, Bruxelas, 31 jul.2002. Disponível em: <http://eur-http://eur-lex.europa.eu/pt/index.htm>. Acesso em: 13 set. 2017.

Nesse contexto já se inicia a formulação dos requisitos para o consentimento, deliberando sobre sua forma clara, completa, expressa e destacada. O Projeto de Lei determina os outros requisitos de forma explicita, assim como o encontrado no Regulamento da União Europeia.

O consentimento deve ser feito sempre anteriormente ao tratamento dos dados. O princípio que fundamenta a anuência para que o titular disponibilize seus dados é a ligação entre o que será tratado e a finalidade desse tratamento. A partir disso podemos deduzir os requisitos para o consentimento.

A lei busca por uma gradação do consentimento, desde uma análise básica a máximo[114]. Para que haja o consentimento, primeiramente como análise básica, o titular deve ser informado, ou seja, deve saber quando haverá a coleta, o tratamento ou o compartilhamento de seus dados, sendo esse o passo inicial para que o possuidor possa exercer o seu direito de escolha. Doneda exemplifica o requisito da informação como "uma completa consciência do interessado sobre o destino de seus dados". A segunda parte do consentimento é a ação livre do proprietário, ou seja, após a informação, o consentimento é válido quando não houver nenhum tipo de pressão ou coação sobre o titular dos dados, requisito mínimo para o exercício da autodeterminação.

Ademais, como análise pré-intermediária, o titular deve estar ciente dos objetivos do tratamento feito pelo responsável, a finalidade do uso dos dados. Esse requisito é importante para que a anuência em liberar os dados pessoais para tratamento esteja direcionada e "o consentimento deve ser lido restritamente em relação a sua finalidade: ele serve para um certo tratamento, por um determinado agente, sob determinada ação"[115], não sendo cabível uma finalidade genérica e ampla. De acordo com o estudo "XEQUE-MATE, o tripé da proteção dos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil" – feito pelo grupo de pesquisa em políticas públicas para o acesso à informação da USP, entende-se que

> Não pode o cidadão consentir que seus dados pessoais sejam tratados com base em propósitos totalmente genéricos, emitindo-se uma espécie de verdadeiro "cheque em branco" que esvaziaria qualquer esfera de domínio sobre seus dados.[116]

O consentimento do titular também deve ser feito de forma inequívoca, ou seja, é o consentimento do titular sem nenhum tipo de confusão sobre o tratamento dos seus dados.

---

[114] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 44

[115] DONEDA, Danilo.**Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 383

[116] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 45

Esse consentimento pode não ser expresso tacitamente, mas a partir do seu comportamento no ambiente em que seus dados estão, o responsável poderá concluir sem dúvidas que o titular aprova o tratamento dos dados.

Por fim, o consentimento expresso é necessário quando os dados tratados são mais específicos e revelam a intimidade do titular, necessitando uma anuência mais específica para a utilização. Dessa forma, nesse consentimento:

> Haveria, assim, a carga máxima de participação do cidadão dentro da dinâmica da proteção dos dados pessoais baseada na acepção de que ele deveria seguir seus dados em todos os seus movimentos (Rodotà, 2008:17). Essa adjetivação potencializa ao extremo a concepção da autodeterminação informacional, diferenciando-se, qualitativamente, do qualificador inequívoco e da locução para finalidade determinadas, na medida em que se afasta de qualquer tipo de autorização passiva, tácita ou implícita por parte do titular dos dados pessoais (InternetLAB, 2016: 95)[117]

O consentimento é ferramenta importante para a proteção dos dados pessoais no que tange o direito do titular em determinar quais e como seus dados poderão ser tratados. Todos os requisitos do consentimento são lógicos e caminham para uma maior proteção ao titular que dessa relação assimétrica com o ambiente virtual que está constantemente requerendo seus dados. Mendes conclui que para que haja um consentimento legítimo, além de respeitar os pressupostos narrados, o controlador resguarde "não apenas a liberdade de escolha meramente formal do indivíduo, mas a efetivamente a sua liberdade material."[118].

Apesar da busca pela garantia do direito de expressão e de liberdade do indivíduo, há a possibilidade de utilizar dados pessoais sem a anuência do titular. É o caso trazido pela lei do uso com interesses legítimos, determina o Regulamento 679 de 2016 no seguinte texto:

> Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento.

A terminologia utilizada – interesses legítimos, de acordo com o grupo de pesquisa em políticas públicas para o acesso à informação (GPoPAI/USP), é equivocada, tendo em vista que a hipótese de cabimento para o manuseio desses dados ocorre quando o responsável já tem vínculos com o titular e, após utilizar dados que foram previamente consentidos, apresenta necessidade de utilizá-los novamente, e não necessariamente com o objetivo acordado antes, mas devendo ter conexão com estes. O interesse legítimo será determinado

---

[117] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014.p. 45

[118] Ibid., p.65

"de acordo com a noção de compatibilidade entre o uso adicional e aquele que originou a coleta dos dados pessoais."[119].

Além dessa situação, o consentimento também poderá ser escusado quando o tratamento de dados for indispensável para o cumprimento da finalidade do contrato aceito pelo titular – essa possibilidade ocorre quando, por exemplo, empresa precisa dos dados de cartão de crédito do titular para concluir a compra. Outras possibilidades para a dispensa do consentimento ocorre quando o dado pessoal for necessário para a execução de obrigação legal do fornecedor, para proteção da vida e tutela da saúde, pela administração pública – dentro das suas prerrogativas, e para pesquisa histórica, científica ou estatística.

Como é possível concluir, as exceções da obrigatoriedade do consentimento também seguem regras e não devem ser interpretadas como forma de burlar o determinado em lei sobre a necessidade do consentimento para o tratamento de dados.

2.2.1. *Os limites do consentimento*

O individuo deve ter pleno direito para dispor ou não dos dados que dizem respeito a sua personalidade, mas, alguns princípios devem ser respeitados para que não haja um exagero e que o titular, no futuro, acabe sendo prejudicado devido suas ações que no momento presente não aparentavam ser de risco.

Primeiramente, a privacidade é um conceito relativo, dependendo da geração e cultura que será apreciada. Aqueles que viveram sob ditadura podem ter uma percepção diferente das gerações atuais – embora seja uma falácia dizer que a geração moderna não se importa com a sua privacidade[120]. Dessa maneira, apesar do Código Civil determinar que o direito à privacidade é indisponível, a atualidade demonstra o contrário, o tornando não apenas um direito disponível, mas também com valor econômico.

Desse modo, as trocas de dados pessoais passam a ter por objetivo, muitas vezes, a liberação de um serviços – até mesmo aqueles tidos como não onerosos, como a entrada de um usuário à um rede social gratuita[121], e o consenso passa a ser visto como ação em que o

---

[119] BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. p. 48

[120] HOOFNAGLE, Chris Jay KING, Jennifer LI, Su and TUROW, Joseph. **How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?. Disponível em: <**https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864**>.** Acesso em: 15 set. 2017.

[121] No livro "Direito, Inovação e Tecnologia", em nota de roda pé, os autores transcrevem a frase de autor desconhecido, que contribui com esse entendimento: "não se esqueça, quando um site de mídia social for gratuito, você não é o cliente, você é o produto" (MENDES, 2015. p. 230)

titular abre mão de ser o único processador de seus dados para fornecer a terceiro, é o caso da imagem de uma modelo que é vendida para a promoção de uma marca[122].

Apesar da liberdade dada ao titular, que é o responsável por determinar o que será ou não entregue para o tratamento de dados, o princípio da razoabilidade deve ser aplicado, levando em consideração que o direito à intimidade tem caráter de direito fundamental, merecendo tutela diferenciada, ou seja, da mesma forma que princípios constitucionais são utilizados para delimitar a ação do agente durante o tratamento de dados, o limite para que o titular disponha de seus direitos de personalidade também serão medidos de acordo com esses princípios, pois deve haver um equilíbrio.

O princípio da razoabilidade aparece de forma a limitar tanto o tratamento dos dados como a possibilidade de abrir mão desses dados. Buscando a proteção dos direitos fundamentais, o equilíbrio é necessário para que haja a proteção também dos valores que esses direitos expressam. Isso quer dizer, quando se busca uma nova regulamentação, não se deve buscar apenas os meios corretos de uma produção legislativa, mas também as novas normas devem estar em harmonia com os princípios e valores expressos nos mais altos níveis do sistema jurídico, ou seja, deve haver uma consistência axiológica. Dessa maneira, a liberdade do titular também será limitada pois, ainda que não seja perceptível no primeiro instante, futuramente um direito fundamental pode ser violado.

O princípio da necessidade também deve ser aplicado, e o PL n. 5.276/2016 de proteção de dados o contempla, ele determina que os dados pessoais serão utilizados o mínimo possível, devendo ser substituído sempre que possível por dados anônimos ou optar por recursos que impeçam a identificação do titular.

Menke conclui que toda a pessoa tem o direito ao livre desenvolvimento de sua personalidade, desde que os direitos dos outros não sejam violados e que não atente contra a ordem constitucional ou contra a lei moral, além disso a dignidade da pessoa humana também deve ser observada[123]. Por fim, em citação a Günter Düring, assinala-se que a barreira normativa deve existir para que o ser humano não passe a ser visto como mero objeto de obtenção de informação[124].

A busca por um equilíbrio é o ponto central para a formulação do melhor contrato a que o tratamento de dados será submetido. Nessa linha, não deve seguir nem para o

---

[122] SILVA, Regina Beatriz Tavares da *alii*. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012. p. 35

[123] MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. Coelho. **Série Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015. 1 v. p. 215

[124] idem, p. 230

formalismo extremo, trazendo uma mora num meio que busca justamente a velocidade das ações, nem para uma abertura exagerada de modo que a segurança do titular, que é tanto protegida pelas leis, seja abandonada.

Finalizando, para que se fale em proteção, primeiramente é necessário que se saiba o que são os dados pessoais, os retirando de uma ideia subjetiva e os classificando de forma concreta, inclusive os diferenciando de acordo com seus tipos, já que dependendo dessa classificação, poderão ser considerados mais ou menos invasivos e terão uma proteção diferenciada, dessa maneira, a classificação do dado também será o meio que limitará os responsáveis pelos tratamentos, pois a depender do tipo, regras específicas são impostas e devem ser seguidas para que a coleta seja feita de forma lícita.

O consentimento, por sua vez, apesar do PL 5.276/16 não o colocar como princípio básico para a validação de todos os tratamentos de dados – tendo em vista que há situações em que será dispensado, estabelece regras que devem ser seguidas, para que a autonomia e principalmente a segurança do titular permaneça assegurada, além disso, as variantes do consenso acarretará em consequências processuais diferentes, é o que será tratado no próximo capitulo.

3. RESPONSABILIDADE CIVIL

O tratamento de dados, como já visto, envolve a "invasão" da vida pessoal do titular em vários graus, desde o número de seu CEP até mesmo suas opções sexuais. Atualmente, a captação desses dados é prática necessária nas mais diversas áreas da sociedade, logo, a possibilidade de conflito entre uma ação do responsável e um direito do titular é cada vez maior.[125]

Dessa maneira, a responsabilidade civil é meio que o direito disponibiliza para que aquele que cometeu ato ilícito repare o dano, logo, cabe o estudo dos tipos e desdobramentos da responsabilidade civil existentes no ordenamento jurídico brasileiro para que haja a compreensão de como os agentes de tratamento podem ser responsabilizados.

3.1 Definição da responsabilidade civil e seus elementos

A responsabilidade civil está positivada em capítulo próprio do atual Código Civil, nos artigos 927 a 954, em que é positivada como sendo a situação em que "aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo"[126] e remete aos artigos 186 e 187, também do Código Civil, em que se define o ato ilícito como sendo, *in verbis*, "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito". O art. 187 complementa o artigo anterior, dispondo que "também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes".

A redação do art. 187 do CC expõe uma interpretação próxima ao determinado tanto no MCI como no PL 5.276/2016 ao positivar sobre os limites impostos. No caso da proteção de dados esses limites estão relacionados a concessão dada pelo tutelar, que tem prazo e é clara sobre seus objetivos, exceto nos casos previstos em lei não poderá ultrapassar o que acordado anteriormente.

San Tiago Dantas define que o objetivo da responsabilidade civil é "proteger o lícito e reprimir o ilícito. Vale dizer: ao mesmo tempo em que ela se empenha em tutelar a atividade do homem que se comporta de acordo com o Direito, e reprime a conduta daquele que

---

[125] SILVA, Regina Beatriz Tavares da *alii*. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012. p 26.

[126] BRASIL. **Código Civil. Lei nº. 10.403, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 15 set. 2017.

contraria."[127]. Dessa forma, o legislador, por meio da ordem jurídica, buscou manter o equilíbrio entre as partes, obrigando aquele que cometeu ilícito a fazer com que o lesado retorne à situação mais próxima e possível da que se encontrava anteriormente. Nas palavras de Pablo Stolze Gagliano e Rodolfo Pamplona Filho, a responsabilidade civil

> nada mais é, portanto, que uma obrigação derivada — um dever jurídico sucessivo — de assumir as consequências jurídicas de um fato, consequências essas que podem variar (reparação dos danos e/ou punição pessoal do agente lesionante) de acordo com os interesses lesados.[128]

Além disso, é importante que não haja confusão entre o significado da obrigação e o da responsabilidade. A obrigação ocorre quando o devedor cumpre o prometido de forma livre e espontânea, é um dever jurídico existente desde o início da relação, já há um débito e independe da ação ou omissão do devedor. A responsabilidade, por sua vez, é consequência da falta de cumprimento de uma relação obrigacional, ou seja, ocorre com a inadimplência de obrigação, acarretando indenização cabível de acordo com a situação em concreto. Resumidamente, a obrigação atende dever jurídico anteriormente determinado, enquanto a responsabilidade surge de dever jurídico sucessivo. [129]

Para se configurar responsabilidade civil três são os pressupostos que devem ser preenchidos: a ação, o dano material e/ou moral e o nexo causal entre o ato praticado e o dano. Primeiramente, a ação praticada para ensejar responsabilidade civil deve ser ilícita[130]. A jurisdição brasileira adota o entendimento de que prática ilícita é a "ação ou omissão voluntária, negligencia ou imprudência", determina o art. 186 do CC. Pablo Stolze conclui que apenas o homem pode ser responsabilizado civilmente, pois tem o elemento vontade na sua ação e, logo, "o núcleo fundamental, portanto, da noção de conduta humana é a voluntariedade, que resulta exatamente da liberdade de escolha do agente imputável, com discernimento necessário para ter consciência daquilo que faz."[131]. A voluntariedade é, nesse sentido, a consciência que o agente tem de saber que suas ações irão ou podem provocar evento danoso.

Dessa maneira, em regra, a culpa seria imprescindível para que a conduta do agente seja reprovada, quer dizer, no caso concreto analisado, o agente poderia ter agido de forma

---

[127] DANTAS, San Tiago. **Programa de Direito Civil.** Rio de Janeiro**:** Ed. Rio, 1979. p. 341.
[128] GAGLIANO, Pablo Stolze. **Novo curso de direito civil, volume 3: responsabilidade civil** / Pablo Stolze Gagliano, Rodolfo Pamplona Filho. — 10. ed. rev., atual. e ampl. – São Paulo : Saraiva, 2012. p. 47
[129] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 21.
[130] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 34.
[131] GAGLIANO, Pablo Stolze. **Novo curso de direito civil, volume 3: responsabilidade civil** / Pablo Stolze Gagliano, Rodolfo Pamplona Filho. — 10. ed. rev., atual. e ampl. – São Paulo : Saraiva, 2012. p. 78

diferente, evitando o dano, mas não o fez.

Racionalmente, não há como reparar prejuízo sem que ele exista, sendo o dano, portanto, exigência da responsabilidade civil. Maria Helena Diniz, citando Giorgio Giorgi, doutrinador italiano, determina a impossibilidade de se falar em responsabilidade civil "sem a existência de um dano a um bem jurídico, sendo imprescindível a prova real e concreta da lesão"[132].

Venosa aponta que a alteração feita no art. 186 do atual Código Civil, ao trocar a partícula "ou": "... violar direito ou causar prejuízo a outrem" pela aditiva "e": "... violar direito e dano a outrem...", não significou uma diferença na compreensão do texto anterior, pois, levando em consideração que não são raras as vezes em que o uso de "e" possui o sentido de "ou" e vice-versa, ainda perdurando no ordenamento a indenização quando o caso violar direito e ocasionar dano, ressalvado situações determinadas em lei. A novidade positiva do dispositivo veio ao incluir a indenização pelo dano exclusivamente moral[133], significando que o dano não deve ser interpretado apenas como uma perda material, a violação de direito da personalidade também está prevista.

Isto posto, encontramos a necessidade de compreender especificamente o dano moral que, para o trabalho em particular, é relevante por ter ligação direta com as prováveis consequências que o descumprimento das regras do tratamento de dados pessoais podem acarretar ao titular. O dano moral ocorre quando há "ofensa a um direito da personalidade, sendo que não é qualquer sofrimento ou abalo emocional que equivale a dano moral (..)"[134], ou seja, é a ofensa aos direitos que todo o cidadão tem o poder de controlar, como a vida, integridade física, nome, imagem, liberdade, vida privada, etc., e são protegidos expressamente no Código Civil em seu art. 52. "aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade."[135]. De acordo com o jurista italiano Adriano de Cupis, sem o direito da personalidade "todos os outros direitos subjetivos perderiam o interesse para o indivíduo – o que vale dizer que, se eles não existissem, a pessoa não existiria como tal"[136].

O dano moral não afeta, *a priori*, valores econômicos, mas, mesmo não podendo ser

---

[132] DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2013. p. 77

[133] VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 6 ed. São Paulo: Atlas, 2006. p. 3.

[134] SILVA, Regina Beatriz Tavares da *alii*. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012. p.30

[135] BRASIL. **Código Civil. Lei nº. 10.403, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 15 set. 2017.

[136] DE CUPIS, Adriano. **Os direitos da personalidade.** Tradução: Adriano Vera Jardim e Antonio Caciro. Lisboa: Livr. Moraes, 1961. p. 17.

avaliado de forma quantitativa e concreta a dor e aflição física ou moral de uma pessoa, a reparação é cabível quando se compreende que o ressarcimento é meio de compensação do que foi ocasionado. Sergio Cavalieri também indica que é importante que se evite o abuso dos pedidos relacionados aos danos materiais, dessa forma, a indenização deve ser considerada quando forem danos que causem, em suas palavras,

> dor, vexame, sofrimento ou humilhação que, fugindo à normalidade, interfira intensamente no comportamento psicológico do indivíduo, causando-lhe aflições, angústia e desequilíbrio em seu bem-estar. Mero dissabor, aborrecimento, mágoa, irritação ou sensibilidade exacerbada estão fora da órbita do dano moral, porquanto, além de fazerem parte da normalidade do nosso dia a dia, no trabalho, no trânsito, entre os amigos e até no ambiente familiar, tais situações não são intensas e duradouras, a ponto de romper o equilíbrio psicológico do indivíduo. [137]

Diniz aponta que o direito não tem a intenção de reparar qualquer tipo de padecimento, e sim aqueles que ocorreram apenas devido a privação de um bem jurídico da vítima. O dano moral não é considerado uma lesão abstrata; é, na verdade, a lesão de interesses não patrimoniais e, apesar do direito violado ser imaterial, a violação do direito é concreta e existente[138].

Os danos morais estão além dos dispositivos no Código Civil. A Constituição Federal também prevê expressamente a possibilidade de indenização por danos morais, como determina o art. 5º, nas alíneas V e X:

> 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:
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O código de Defesa do Consumidor também contemplou a responsabilidade civil em seu art. 14, determinando regra geral para o assunto, na linha de que "o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços".

A doutrina diferencia os danos morais em direto e indireto. O dano moral direto, como a própria nomenclatura remete, consiste na violação de um bem jurídico extrapatrimonial

---

[137] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 93
[138] DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2013. p. 113

pertencente ao direto da personalidade – integridade corporal, vida, imagem, ou nas características da pessoa – nome, estado civil, além de incluir as lesões à dignidade humana.

O dano moral indireto acontece quando um bem patrimonial é violado e, por consequência, provoca prejuízos em interesse extrapatrimonial. Antes da entrada em vigor da Constituição de 1988, não era cabível a reparação desse tipo de dano, pois o entendimento jurisprudencial era de que o dano material absorvia o moral, não sendo cabível o pedido de ressarcimento de ambos. Após a atual Constituição, os incisos V e X do art. 5º admitem expressamente a possibilidade, além de também estarem protegidos pelo Código de Defesa do Consumidor em seu art. 6º, VI e VII[139].

Por fim, último requisito necessário para a responsabilização civil é a comprovação da existência de nexo causal entre a ação do agente e o dano, ou seja, é a ligação de determinado comportamento ao dano ocorrido. Nas palavras de Diniz, "bastará que se verifique que o dano não ocorreria se o fato não tivesse acontecido. Este poderá não ser a causa imediata, mas, se for condição para a produção do dano, o agente responderá pela consequência.".[140]

A partir do nexo causal, que deve estar presente em qualquer modalidade de responsabilidade, se identifica o causador do dano e se determina a indenização. Além da função de determinar se será cabível a responsabilidade civil, o nexo causal também delimita a extensão do dano que será indenizado. Anteriormente se achava que a culpabilidade era a responsável por determinar os limites da indenização, mas é possível ter casos em que a culpa é mínima, mas com consequências danosas maiores, como visto anteriormente, podendo configurar casos de danos indiretos.

Após o preenchimento dos requisitos para a configuração de responsabilidade civil, são seis as espécies possíveis de responsabilidade tradicionalmente indicadas pela doutrina. Começaremos pela definição da responsabilidade civil contratual e extracontratual.

A responsabilidade contratual é determinada devido a seu fato gerador, ou seja, diz respeito aquelas obrigações que tiveram como base um contrato entre as partes. O agente nessa situação comete um ilícito contratual ao não adimplir o determinado em contrato ou devido a mora no cumprimento da obrigação.

Venosa tece críticas a essa nomenclatura, no seu entendimento e na doutrina mais moderna, a melhor denominação para essa espécie de responsabilidade seria negocial, em suas palavras, "pois não apenas do contrato emerge essa responsabilidade como também dos

---

[139] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 92
[140] DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2013. p. 129

atos unilaterais de vontade geral, como a gestão de negócios, a promessa de recompensa, o enriquecimento sem causa, entre outros"[141].

A responsabilidade extracontratual – também conhecida como aquiliana, se configura quando não há vínculo contratual entre as partes, a responsabilidade não está prevista em contrato, mas está prevista na lei, pois o dano é causado devido a inobservância da lei, isto é, a lesão causada foi ao direito do ofendido, mesmo que não haja vínculo entre as partes.

Parte minoritária da doutrina compreende que a decomposição da responsabilidade civil é meramente didática, tendo em vista que suas consequências são semelhantes. Venosa ressalta que:

> não existe na realidade uma diferença ontológica, senão meramente didática, entre responsabilidade contratual e aquiliana. Essa dualidade é mais aparente do que real. O fato de existirem princípios próprios dos contratos e da responsabilidade fora deles não altera essa afirmação. Assim, é possível afirmar que existe um paradigma abstrato para o dever de indenizar. O que permite concluir por uma visão unitária acerca da responsabilidade civil. [142]

Aprimorando esse entendimento, Fábio Ulhoa Coelho ensina que a responsabilidade civil não pode estar subordinada a um contrato, expressando que:

> Fico com a solução de classificar a responsabilidade civil como não negocial. Para mim, mesmo quando existe relação contratual entre credor e devedor da obrigação de indenizar, se esta é a própria prestação (e não um simples consectário), estamos diante de uma relação jurídica não negocial, cujo fundamento não é o negócio jurídico, mas ato ilícito ou fato jurídico.[143]

Apesar da divergência doutrinária, o Brasil adota a teoria conhecida como dualista ou clássica, diferenciando uma responsabilidade em que há contrato e a responsabilidade que não teve vínculo prévio. A principal diferenciação dessas responsabilidades ocorre quando se analisa o ônus da prova. Na responsabilidade contratual o ônus da prova é do devedor, tendo o credor apenas a obrigação de afirmar que o dever foi descumprido, já na responsabilidade extracontratual, o autor da ação terá que demonstrar a culpa do agente.

Outra diferenciação está relacionada à origem da responsabilidade. A responsabilidade contratual se origina na inobservância de determinação em convenção, enquanto a extracontratual se origina no descumprimento do dever de não lesar e nem causar dano.[144] Cavalieri conclui que, "em suma: tanto na responsabilidade extracontratual como na

---

[141] VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 6 ed. São Paulo: Atlas, 2006. p. 2.
[142] VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 15 ed. São Paulo: Atlas, 2015. p. 19.
[143] COELHO, Fábio Ulhoa. **Curso de Direito Civil**. Obrigações e Responsabilidade Civil. 5. ed. São Paulo: Saraiva, 2012. p. 210
[144] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 44.

contratual há a violação de um dever jurídico preexistente. A distinção está na sede desse dever."[145].

A compreensão dos requisitos da responsabilidade e seus tipos é importante para que possamos entender como a responsabilidade civil será aplicada aos casos que envolvem processamento de dados. Os dados pessoais, como visto no capítulo anterior, devem ser obtidos por meio do consentimento – que tem semelhança ao negócio jurídico, dessa forma, concluímos que ambas as responsabilidades poderão ser pleiteadas, justamente por estarem resguardadas por normas gerais que devem ser respeitadas.

Todos os tipos de dados pessoais, salvo raras exceções, necessitam de consentimento para que se inicie o seu tratamento, variando apenas o tipo de consentimento que dependerá da espécie de dado – os dados sensíveis, por exemplo, precisam de consentimento expresso por meio de cláusula destacada. Dessa maneira, a responsabilidade contratual ocorrerá quando os pré-requisitos forem atendidos, e após esse consentimento o agente do tratamento cometa ato ilícito, é o caso de informações do titular ser utilizada para outro objetivo que não estava especificado no termo inicial.

A responsabilidade extracontratual, por sua vez, ocorrerá ou a partir das possibilidades de coleta sem o consentimento do titular – como para questões judiciais e administrativas, além dos casos necessários para a proteção da vida e os demais expostos no art. 7º do PL n. 5.276/16 – ou a partir de ato ilícito. Essa questão se torna mais complexa devido à anuência legislativa de liberar dados pessoais sem a necessidade de consentimento em algumas hipóteses, levando em consideração os objetivos da própria lei, que é de justamente proteger o titular.

Outra possibilidade de responsabilidade extracontratual é devido a ato ilícito que ocorre quando há coleta de dados pessoais sem a anuência do titular, neste caso o dano é presumido. No artigo "Responsabilidade civil pela coleta, gestão e armazenamento de dados de outrem" de Leonardo Netto Parentoni, o autor traz posicionamento jurisprudência sólido do STJ sobre o assunto: "No sistema jurídico atual, não se cogita da prova acerca da existência de dano decorrente da violação aos direitos da personalidade, dentre eles a intimidade, imagem, honra e reputação, já que, na espécie, o dano é presumido pela simples violação ao bem jurídico tutelado."[146].

---

[145] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 17

[146] PARENTONI, Leonardo Netto. **Responsabilidade civil pela coleta, gestão e armazenamento de dados de outrem. Disponível em:** <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=7969#_ftnref107> Acesso em: 15 OUT. 2017.

O autor da ação que foi vítima do agente que não teve seu consentimento para processar seus dados, além de ser protegido pela responsabilidade extracontratual, como visto, não terá o ônus de provar que o feito foi ilícito, logo, a responsabilidade do tratamento de dados também encontra outras características que serão apresentadas no próximo tópico.

3.2 Responsabilidade civil na esfera subjetiva e objetiva e a teoria do risco

Continuando com a classificação das responsabilidades, a culpa é identificada, de acordo com teoria adotada desde o Código Civil brasileiro de 1916, como núcleo essencial da responsabilidade, dessa forma o Código Civil de 2002 recepcionou o art. 156 do Código Civil de 1916, mantendo a culpa como condição para a responsabilidade subjetiva mas, de acordo com Cavalieri, é possível afirmar que apesar do Código de 16 ser subjetivista, o atual código prestigia a responsabilidade objetiva[147].

Dessa maneira, quando a responsabilidade se apoia na culpa do agente para conceber o direito de indenização da vítima, a doutrina denomina como responsabilidade subjetiva, também conhecida como teoria da culpa, e é a regra geral do Direito brasileiro. Nesse entendimento, Carlos Roberto Gonçalves determina que "a prova da culpa do agente passa a ser pressuposto necessário do dano indenizável. Nessa concepção, a responsabilidade do causador do dano somente se configura se agiu com dolo ou culpa"[148].

Devido a essa limitação e o cenário atual da sociedade, a responsabilidade objetiva passou a ser fortemente considerada. Essa espécie desprende-se do princípio da culpa e foi alargada pelo Código Civil de 2002 ao associar o risco e a culpa, é o que positiva o art. 927 do Código Civil

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, riscos para os direitos de outrem.

Nesse caso a culpa é irrelevante para configurar a responsabilidade objetiva, bastando apenas o nexo causal entre a ação e o dano. Nos primórdios, a responsabilidade objetiva, de acordo com Augusto Alvim, já se encontrava no Direito Romano, pois a vingança era meio de justiça, sem a necessidade de se encontrar a real culpa[149]. Atualmente o retorno da obrigação

---

[147] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 23
[148] Ibid., p. 46
[149] ALVIM, Agostinho. **Da Inexecução das obrigações** 4.ed. Rio de Janeiro: Saraiva, 1972. p. 238

objetiva não desempenha o mesmo papel dos séculos passados, mas foi resgatada para regular acontecimentos em que a falta de culpa não afasta o dever de indenizar.

O Código de Defesa do Consumidor teve papel importante ao introduzir a responsabilidade nas relações de consumo, e essa nova visão de responsabilidade acarretou em uma interpretação dos contratos de forma que a parte vulnerável é destaque e deve ser protegida[150].

Segundo Venosa, a teoria da responsabilidade civil passa a ter nova formulação quando se admite a existência de uma responsabilidade objetiva, pois nessa situação o ato causador do dano se sobrepõe ao simples ato ilícito, e é por meio de sua análise que há a determinação da responsabilidade do sujeito.[151]

Caio Mário da Silva Pereira, notável civilista, expõe sua opinião sobre a responsabilidade civil e conclui que "insurgir-se contra a ideia tradicional da culpa é criar uma dogmática desafinada de todos os sistemas jurídicos. Ficar somente com ela é entravar o progresso.", principalmente porque o ordenamento brasileiro já aponta uma certa inversão do fundamento da responsabilidade civil, aparecendo nos códigos e nas hipótese concretas a necessidade de indenização sem culpa[152].

Ou seja, de acordo com Gonçalves, a responsabilidade objetiva é de extrema importância para o avanço na matéria de responsabilidade civil, mas a responsabilidade subjetiva subsiste como regra, cabendo a objetiva apenas quando estiver especificado em lei, é o que determina o art. 927 do Código Civil[153]. A ampliação da responsabilidade civil indicada pelo parágrafo único do mesmo artigo é avanço na legislação brasileira pois possibilita ao Poder Judiciário que casos antes considerados não cabíveis de responsabilização passam a ser indenizados.

Dessa maneira, e para o estudo em especial, a possibilidade de ser possível a responsabilização objetiva, é a forma mais eficaz de proteger o titular dos dados pessoais levando em consideração a possível dificuldade em apresentar provas que, no meio virtual, são facilmente comprometidas. É também a opinião de Cavalieri, concluindo que "o desenvolvimento industrial, proporcionado pelo advento do maquinismo e outros inventos

---

[150] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 10
[151] VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 15 ed. São Paulo: Atlas, 2015. p. 7.
[152] PEREIRA, Caio Mario da Silva. **Instituições de Direito Civil**. Vol. III. 18 ed. Rio de Janeiro: Forense, 2014. P. 539-540.
[153] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 48.

tecnológicos, bem como o crescimento populacional geraram novas situações que não podiam ser amparadas pelo conceito tradicional de culpa"[154].

A tendência da jurisprudência é de cada vez mais alargar o entendimento do que se configura a culpa ou até mesmo dispensa-la e, dessa maneira, a noção de uma culpa presumida passa a ser cabível, surgindo a teoria do risco para fundamentar responsabilidade objetiva[155]. A teoria do risco proibe um resultado nocivo advindo do risco criado pela atividade do agente, simplifica a necessidade da causalidade da ação ou omissão para que seja cabível a responsabilidade civil e reduz os meios de defesa do agente, já que não será necessário demonstrar a culpa[156].

Cavalieri resume essa teoria como "todo prejuízo deve ser atribuído ao seu autor e reparado por quem o causou, independentemente de ter ou não agido com culpa."[157]. Além disso, a teoria explica que todo ato praticado pode acarretar em algum tipo de dano à terceiro, devendo ser responsabilizado o sujeito que obteve vantagens ou benefícios devido a essa ação. De acordo com Carlos Roberto Gonçalves,

> A responsabilidade civil desloca-se da noção de culpa para a ideia de risco, ora encarada como "risco-proveito", que se funda no princípio segundo o qual é reparável o dano causado a outrem em consequência de uma atividade realizada em benefício do responsável (*ubi emolumentum, ibi onus*); ora mais genericamente como "risco criado", a que se subordina todo aquele que, sem indagação de culpa, expuser alguém a suportá-lo.[158]

Cavalieri aborda em sua obra cinco subespécies ou modalidades de risco. Para o trabalho em questão, dois tipos de risco podem se enquadrar nas situações que envolvem o tratamento de dados. O primeiro, chamado de risco proveito, determina o responsável como sendo aquele que, obteve vantagens a partir dos danos que causou. A crítica feita a esse modelo é de que o termo "proveito" não conceitua de forma clara o que abrangeria, seria apenas proveitos econômicos? Se a resposta for afirmativa, a responsabilidade objetiva fundada nesse modelo ficaria restrita apenas às situações que envolvem comércio e, ainda, teria a vítima o dever de provar a existência de um lucro[159].

---

[154] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 18
[155] VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 15 ed. São Paulo: Atlas, 2015. p. 5.
[156] SILVA, Regina Beatriz Tavares da *alii*. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012. p 31.
[157] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 152
[158] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 46.
[159] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005. p. 153

O segundo modelo é o do risco criado. Nessa modalidade e diferentemente do risco proveito, não há a necessidade de comprovar vantagens, o dano ocorre devido a imprudência ou negligencia da parte. Para Caio Mário, citado por Cavalieri, essa teoria é a ampliação do risco proveito, aumentando os deveres do agente que terá, nesse caso, o ônus de provar que não cometeu o dano devido a práticas não seguras[160].

As críticas à teoria do risco se baseiam na preocupação de que o agente que exerce atividade de forma segura poderá ser responsabilizado apenas pelo fato dessa atividade ser de risco. Para Cavalieri, as oposições à teoria do risco não procedem, pois o simples fato de haver riscos no exercício de uma atividade não gera responsabilidade, já que, além do requisito de existência de dano, é preciso que um dever jurídico seja violado, no caso o dever de segurança[161].

Além de Cavalieri, José de Aguiar Dias também expõe os motivos para a existência legal da teoria do risco:

> Meditando nisso, hão de concluir os espíritos democráticos que a situação desejável é a do equilíbrio, onde impere a conciliação entre os direitos do homem e seus deveres para com os seus semelhantes. O conflito de interesses não é permanentemente, como quer fazer crer a doutrina extremista, mas ocasional. E quando ele ocorra, então, sem nenhuma dúvida, o que há de prevalecer é o interesse da coletividade. Não hesitamos em consentir na amputação do membro que põe em risco a nossa vida. Não podemos, por qualquer motivo, permitir que o direito do indivíduo todo-poderoso atinja, não outro indivíduo, mas toda a coletividade. Na doutrina do risco nitidamente democrática, não se chega jamais à consequência de afirmar o princípio, aparentemente individualista, mas, em essência, de sentido oposto, nitidamente autocrático, de que o direito de um pode prejudicar a outro, pode ultrapassar as raias da normalidade e fazer do seu titular um pequeno monarca absoluto.

O tratamento de dados feito de forma não segura pode acarretar, em diversas situações, desde propagandas indesejadas à fraudes. Doneda, em seu estudo sobre a proteção de dados pessoais na Itália, constata que o tratamento de dados é apresentado como um "mal necessário", que deve ser evitado sempre que possível, concluindo que a atividade de tratamento é de risco e enseja indenização caso não seja comprovado que todas as medidas de segurança foram tomadas[162].

A manipulação de dados pessoais é considerada uma atividade de risco muito devido aos processos de automatização, pois os dados em si, espalhados, possuem um grau danoso

---

[160] Ibid., p. 153
[161] Ibid., p. 155
[162] DONEDA, Danilo. **Um código para a proteção de dados na Itália**. Disponível em: < http://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf >. Acesso em: 30 out. 2017.

muito menor quando comparado ao agrupamento e as ligações que podem ser feitas entre eles, podendo gerar até mesmo informações minuciosas sobre o titular. Klee explica que "a tecnologia da informação permite transformar dados parciais e dispersos em informações em massa e organizadas. Nesse contexto, os riscos ao direito da personalidade das pessoas aumentam"[163].

Laura Mendes também explica essa situação, determinando que

> em um mundo em que os sistemas informáticos estão conectados em rede e são caracterizados pela sua ubiquidade, não há como garantir a proteção da privacidade e dos dados pessoais sem uma politica adequada de segurança da informação e uma gestão de riscos de incidentes de informação[164].

Dessa forma, a aplicação da teoria de risco é apropriada ao constatar que os riscos causados pelo agente que não se utiliza do mínimo de segurança necessária para o processamento de dados podem produzir danos até mesmo irreparáveis ao titular.

A aplicação da responsabilidade civil nos casos de violação da proteção de dados ainda é controvérsia, tendo em vista que o Brasil não detém lei específica para o assunto. É preciso que a jurisprudência seja analisada, dessa forma, pois são os julgados que atualmente determinam se a responsabilidade civil será aplicada e qual o tipo cabível.

O processo n. 70073667537 de junho de 2017, do Tribunal de Justiça do Rio Grande do Sul – TJRS, negou provimento à apelação que pedia o pagamento de indenização por danos morais, após a autora ter seus dados vendidos pela empresa PROCOB S.A.[165], o acórdão determinou que as informações pessoais de fácil e ampla circulação no mercado de consumo – como CPF, nome, endereço, não configuram violação à vida privada, por serem apenas "informações capazes de proporcionar melhor posicionamento do produto/serviço no mercado, bem assim facilitar a oferta de serviços a potenciais consumidores"[166] e, sem provas concretas de que a divulgação e o uso dos dados acarretou em dano, não é cabível a responsabilização do agente.

A doutrina moderna não compartilha desse posicionamento, os dados de fácil acesso não devem ser confundidos com dados livres de qualquer regra, além disso, ao aplicar o significado dos dados pessoais no caso em tela, é de fácil constatação que os dados fornecidos

---

[163] KLEE, Antonia Espíndola Longoni. **A regulamentação do uso da internet no Brasil pela Lei n. 12.965/2014 e a proteção dos dados e dos registros pessoais.** Disponível em: < http://revistaseletronicas.pucrs.br/ojs/index.php/fadir/article/view/21427 > Acesso em: 30 de out. 2017.

[164] MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. **Revista de Direito do Consumidor**, São Paulo, ano 22, n. 90, p. 245-260, nov. – dez. 2013.

[165] Empresa que exerce a atividade de comercializar informações para outras empresas, consumidores e fornecedores.

[166] BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. Processo Civil. Apelação Civil. n. 70063665228, Rio Grande do Sul, RS, 26 de março de 2015.

pela empresa são dados sensíveis por indicarem de forma direta o titular. A sentença também tornou a responsabilidade civil em subjetiva, ao admitir que a disponibilização dos dados não acarreta em riscos aos titulares, e não considera as possibilidades de fraude que são facilitadas devido ao acesso a esses dados.

Avesso a essa jurisprudência, no mesmo Tribunal e com data anterior a essa decisão, foi interposto a Ação Coletiva n. 001/11401789987[167] em face da Confederação Nacional de Dirigentes Lojistas – SPC Brasil, alegando que a confederação comercializava informações pessoais dos consumidores sem o consentimento prévio e expresso dos titulares. O SPC alegou que os dados, praticamente iguais aos do caso anterior, eram públicos, retirados da base de dados de cadastro de inadimplentes e sendo de mera identificação social, logo, não precisavam de autorização prévia dos consumidores. No voto o juiz alegou o artigo 5º, X da CF, o art. 21 do CC e os artigos 4º e 6º do CDC, em que todos positivam sobre a inviolabilidade da intimidade e privacidade e afirmou que os dados fornecidos eram sensíveis e atingiam direitos inerentes a personalidade dos consumidores por meio dessa divulgação.

A sentença determinou o pagamento de danos morais coletivos no valor de 70 mil reais e mateias no valor de 4.500,00 reais para cada consumidor lesado, obrigou a companhia retirar todos os registros dos titulares que não autorizaram expressamente a utilização de seus dados, além de proibir a venda de informações pessoais de consumidores sem o seu consentimento.

O processo n. 20150710135904APC, no Tribunal de Justiça do Distrito Federal e Territórios – TJDFT, também responsabilizou o agente, neste caso um hospital, por não zelar pelos dados pessoais de paciente que foi vítima de fraude. A sentença afirma que

> "o simples fato de a autora ter seus dados pessoais indevidamente utilizados por terceiros, em virtude de negligencia do hospital em não preservar as informações pessoais de seus pacientes, ofende aos direitos inerentes à sua personalidade, sendo suficiente para lhe causar constrangimento, dor e sofrimento suficientes a caracterizar dano moral."

Ademais, assegura que a concepção doutrinária e jurisprudencial consolidada nos Tribunais é a de que a responsabilidade é cabível com a constatação do simples fato da violação, ou seja, a configuração de possível dano já impõe a obrigação de reparar a vítima, não necessitando de demonstração do prejuízo, caracterizando uma responsabilidade objetiva e aplicando a teoria do risco.

---

[167] BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. Ação Coletiva. n. 001/11401789987, Rio Grande do Sul, RS, 28 de agosto de 2015.

A diferenciação dos casos que admitiram a responsabilidade do agente e do que não admitiu, está no fato de se determinar de forma clara quais dados precisam de proteção e, principalmente, consentir que a violação é dano. Isso quer dizer que, caso a violação cometida pelo agente não seja considerada dano, não haverá nexo causal e, por consequência, mesmo que se determine que a responsabilidade para tratamentos de dados seja objetiva ou subjetiva, não será possível a responsabilização de nenhuma empresa ou ente público.

3.3 Responsabilidade solidária

A responsabilidade civil é em princípio individual e, como já esclarecido, o responsável é aquele que cometeu o dano a partir ação ou omissão voluntária[168], apesar disso, a possibilidade da configuração da responsabilidade devido a ação ou omissão de terceiro não é afastada, configurando a responsabilidade solidária.

Venosa explica que "se unicamente os causadores dos danos fossem responsáveis pela indenização, muitas situações de prejuízo ficariam irressarcidas"[169]. A responsabilidade solidária, dessa forma, é mais uma das formas de responsabilidade, junto com a responsabilidade objetiva e a teoria do risco, que buscam que a vítima não seja prejudicada.[170]

Como estudado, o Código Civil de 2002 se posiciona de forma a prestigiar a responsabilidade objetiva, afastando a culpa e, consequentemente, a responsabilidade solidária também não está mais baseada na prova de que o responsável que deveria prezar pelo bem não o fez. O Código de defesa do consumidor contempla a responsabilidade no art. 14, determinando que "o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos."[171], nos casos de danos devido a tratamento de dados pessoais, o defeito referido no artigo deve ser compreendido como a falta de segurança que deveria ser prestada durante o tratamento[172].

---

[168] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 103

[169] VENOSA, Silvio de Salvo. **Direito Civil: responsabilidade civil**, 6 ed., São Paulo: Atlas, 2006, p.63

[170] Ibid., p. 63-64

[171] 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/L8078.htm>. Acesso em: 01 set. 2017.

[172] IDEC. **À Comissão especial de tratamento e proteção de dados pessoais da Câmara dos Deputados**. Disponível em: <https://www.idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf>. Acesso em: 10 set. 2017.

O Marco Civil e o PL n. 5.276/16 se posicionam positivamente, admitindo a configuração de responsabilidade solidária nos casos de tratamento de dados. O Marco Civil estabelece como princípio que os agentes de tratamento serão responsabilizados de acordo com as atividades que exercem[173], mas em determinados tipos de fornecimento de dados envolvendo empresas estrangeiras, a responsabilidade será solidária[174]. O PL, em seção especial sobre o assunto, positiva que quando houver transferência de dados pessoais, o cedente e o cessionário ficarão sujeitos às mesmas obrigações legais, determinando expressamente a responsabilidade solidária.

A preocupação do legislador em moldar a responsabilidade civil de acordo com os avanços da sociedade é importantíssima, principalmente quando os atos ilícitos ocorrem no meio virtual que desafia o Direito devido suas constantes mudanças, demonstrando assim que as regras gerais sobre a responsabilidade civil não terão sua aplicação impedida pois também buscam acompanhar as variantes.

Manuel A. Carneiro da Frada entende que a utilização da responsabilidade civil é meio para manter uma certa estabilidade apesar das contínuas mudanças acarretadas pela evolução da Internet, rematando que "apenas amparados na provada estabilidade daquele corpo de doutrina lograremos escapar à vertigem da contínua evolução, perspectivar devidamente os seus sinais, averiguar-lhe o peso, medir-lhe corretamente o alcance"[175].

Dessa forma, mesmo que a doutrina geral da responsabilidade não consiga abarcar todas as novidades trazidas pela evolução da tecnologia, ela não deve ser negligenciada, pois a aplicação dos instrumentos jurídicos comprovadamente testados pelo operador do Direito ainda traz segurança jurídica aos usuários.

O trabalho procurou nos primeiros capítulos, apresentar a principal lei que já está em vigência no Brasil – Lei do Marco Civil da Internet, n. 12.965/14, e o Projeto de Lei 5.276/16 que tratará especificamente sobre a proteção dos dados pessoais, caso aprovado. Os dois capítulos seguintes conceituaram expressões importantes que surgiram nas leis de proteção de dados e, por fim, o capítulo presente buscou demonstrar que há consequências para os

---

[173] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 de set. 2017.

[174] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 de set. 2017.

[175] FRADA, Manuel A. Carneiro da. **Vinho novo em odres velhos?**. Disponível em: <http://www.oa.pt/upl/%7Bedbdd555-eea1-4f73-bd2d-5808411e4a31%7D.pdf >. Acesso em: 15 de ago. 2017.

agentes que não observam as normas, eliminando o falso sentimento de que o que ocorre no meio virtual não origina consequências jurídicas. O próximo, e ultimo, capítulo tratará sobre o Regulamento Europeu, principais alterações da Diretiva 95/46/CE, e por meio de comparações com o Projeto de Lei n. 5.276/16, será possível analisar os aspectos importantes que o PL também deverá se ater na sua redação.

4. ESTUDO COMPARADO DO REGULAMENTO 2016/679 DO PARLAMENTO EUROPEU E CONSELHO E O PROJETO DE LEI BRASILEIRO N. 5.276/2016

A busca por regulamentar a proteção de dados acontece por todo o mundo. Centenas de países já positivaram suas regras e trouxeram uma maior segurança tanto para o titular dos dados como para o responsável pelo tratamento. O Brasil, por meio do Marco Civil da internet, teve uma evolução significativa com relação a proteção de dados, mas também demonstrou que há a necessidade de se regulamentar por meio de dispositivo legislativo específico pontos críticos que não foram sanados de forma satisfatória.

Considerando a experiência cumulada no âmbito de proteção de dados pessoais que a União Europeia adquiriu devido a pesquisas extensas e de muitos anos de aplicação de diversas regras, é proveitoso que haja um intercâmbio de ideias e de soluções encontradas fora do âmbito nacional. O estudo comparado vem, dessa forma, continuar o estudo feito nos capítulos anteriores mas agora voltado ao regulamento europeu e o determinado pelo PL brasileiro.

Curiosamente, apesar dos esforços pela proteção de dados já ocorrer há anos na União Europeia, apenas no ano de 2016 foi aprovado o texto final da "*General Data Protection Regulation*" ("GDPR") – regulamento n. 2016/679, no qual houve a concentração das normas de proteção de dados em um único dispositivo legal, criando um regime jurídico único para todos os integrantes da União Europeia[176].

O regulamento n. 679 de 2016 revoga a Diretiva n. 95/46/CE, formulada em outubro de 1995, que não previa em seus artigos todas as evoluções tecnológicas que o mundo iria sofrer. Ele entrará em vigor em maio de 2018 e apresentará novos conceitos que se tornaram indispensáveis nos últimos anos, como o tratamento da pseudoanonimização e a figura do encarregado para a fiscalização do tratamento dos dados pessoais.

Desde 2012, a União Europeia reúne esforços para aprovar o texto que regulamenta a proteção dos dados pessoais, e, devido a isso, o Brasil teve grandes influências no PL 5.276/2016, inclusive apresentando artigos que apenas no ano passado foram vistos no texto final do regulamento[177]. Por isso, a Diretiva n. 95/46/CE, além de perder sua validade em breve, para o estudo em questão, não terá grande proveito. Logo, serão concentradas as

---

[176] COMISSÃO EUROPEIA. **Reform of EU data protection rules**. Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> Acesso em: 30 out. 2017.

[177] MONTEIRO, Renato Leite. **A nova regulação de dados pessoais aprovada na União Europeia e sua influência no Brasil**. Disponível em: < http://renatoleitemonteiro.com.br/analises-juridicas/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil/ >. Acesso em 30 out. 2017.

análises no Regulamento n. 679/2016 e que serviu de base para a, também futura, regulamentação de dados pessoais no Brasil. Evidentemente, por ser recente, não há estudos profundos e específicos sobre a regulamentação na doutrina brasileira, mas a análise seca dos dispositivos é meio para extrair o que de melhor pode ser aplicado no território nacional.

O regulamento apresentou três alterações mais importantes, são elas as alterações da forma de consentir dos titulares, alterações para induzir certos comportamentos por parte dos responsáveis pelo tratamento e as alterações para reformar as competências das Autoridades de Proteção de dados[178]. Devido a isso, esses três pontos em específico serão tratados no trabalho com o objetivo de analisar se o PL brasileiro também está condizente com as inovações trazidas pela União Europeia.

4.1 O consentimento para dados pessoais e dados pessoais sensíveis

Para que haja o estudo do consentimento, é necessário que o conceito de dados pessoais seja compreendido. Na legislação Europeia, os dados pessoais, são compreendidos como qualquer dado referente a uma pessoa singular identificada ou identificável, Doneda explica que a definição foi formulada pelo Conselho Europeu, através da Convenção de Strasbourg, e condiz com a ordem conceitual de dado, como sendo aquele que é atributo da personalidade de um indivíduo[179].

O regulamento traz a conceituação de forma mais ampla ainda, no artigo 4º, dispondo que o dado pessoal não apenas determina o indivíduo de forma direta, mas também indiretamente, além de incluir rol de possibilidades de identificação, sendo até mesmo as características mentais, definições de perfis, endereços de IP, testemunho de conexão – *cookie*, e etiquetas de identificação por radiofrequência e os dados anonimizados, que serão melhor explicados à frente. O PL 5.276/2016 apresentou texto mais simplório, como visto anteriormente; nele, o dado pessoal na Lei é considerado "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa"[180].

---

[178] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf > . Acesso em: 20 out. 2017

[179] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 157

[180] BRASIL, Projeto de Lei n. 5.276, de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 18 de out. 2017

Outro ponto importante para se determinar o consentimento, é conceituar o que seriam dados sensíveis e os limites do seu tratamento. No dispositivo europeu não foi aglomerado a classificação dos dados sensíveis em um único artigo; na realidade, ele está tanto nos preâmbulos de n. 10, 34, 35, 51, como no art. 9[181].

O regulamento determina que os dados pessoais sensíveis – nomeados como categorias especiais de dados, são aqueles em que o tratamento pode ter como consequência riscos significativos aos direitos e liberdades fundamentais do titular. Além de classificar os dados relacionados a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, associação sindical, dados sobre saúde ou vida sexual e orientação sexual, incluiu os dados genéticos e dados biométricos[182], em resposta aos grandes avanços tecnológicos e que atualmente já estão sendo empregados facilmente – é o caso da leitura digital em diversos aparelhos celulares. Os dados sensíveis, assim como no PL brasileira, terão uma proteção adicional, além de aplicar a eles os princípios gerais e outras disposições expostas no regulamento. Esse tipo de dado não poderá ser tratado sem a autorização expressa do titular, apenas em casos específicos e que estão determinados, e para que a dispensa do consentimento ocorra são requeridos motivos robustos.

A inclusão dos dados genéticos e biométricos foram uma inovação do novo regulamento, agentes de áreas da ciência, que tem como principal objeto de tratamento os dados genéticos, concluem que a regulamentação não é exaustiva, e foi redigida dessa forma propositalmente, pois deixa amplo espaço para decisões concretas feitas pelas autoridades nacionais e para o Conselho Europeu. Dessa forma, o que irá moldar o regulamento será justamente a produção jurisprudencial de cada país membro. Esse alargamento das possibilidades tem em vista responder de forma mais célere às mudanças que ainda não são possíveis de ser mensuradas[183] e evitar que as evoluções da ciência sejam impedidas.

Por fim, os dados anônimos não foram contemplados[184], logo, apesar de ser tarefa tecnicamente complexa tratar dados de forma que o titular não seja identificado, o

---

[181] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

[182] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[183] PREITE, Francesca *alii*. **The new european regulation on personal data protection: significant aspects for data processing for scientific research purposes**. 2017. Disponível em: <http://ebph.it/article/viewFile/12286/11354>. Acesso em: 17 out. 2017.

[184] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

regulamento não é aplicado a eles por não terem as consequências do tratamento de um dado pessoal de pessoa singular, é o que determina o preâmbulo n. 26.

O que a Diretiva vigente não abordou, muito também pela época em que foi redigida e a impossibilidade de saber sobre as diversas tecnologias de bancos de dados que iriam surgir, o novo regulamento o fez, ao admitir a existência de dados anonimizados, tratados como dados pessoais – assim como no PL brasileiro n. 5.276/16, pois, apesar da anonimização, o titular ainda pode ser identificado por meio de informações suplementares, mas, se as mantiverem separadas e em segurança, os riscos associados a esse tipo de dado é consideravelmente menor comparado com os demais.

O regulamento incentiva de forma explicita – nos preâmbulos n. 29 e n. 78 e o art. 6º, (4), (e) – às organizações à tratar os dados aplicando a pseudonimização como medida de segurança, mas não afasta a busca por outros meios de segurança – atitudes conhecidas como "*privacy by design*"[185]. É possível fazer um paralelo entre a "*privacy by design*" com o princípio da necessidade previsto no PL 5.276/2016, que também limita a utilização dos dados pessoais ao mínimo necessário, e busca a utilização dos dados anônimos sempre que for igualmente cabíveis.

Como visto nos capítulos anteriores, o consentimento tem papel importante no tratamento de dados pessoais, é por meio dele que o titular poderá anuir sobre a utilização de suas informações e quais os limites de acesso e na diretiva é obrigatório para o tratamento de qualquer dado pessoal.

Ainda na Diretiva 95/46/CE, de acordo com os estudo de Fontes, o conceito de "privacidade dos dados" ou "privacidade da informação" (originalmente denominado 'data privacy') surgiu e o critério utilizado durante todo a diretiva foi a "reinvindicação do indivíduo para controlar a circulação de dados sobre si mesmo". O conceito trazido pela Diretiva não foi retirado do regulamento, e o consentimento ainda é base para o tratamento de dados no novo regulamento, o art. 6º, 1, demonstra que o tratamento de dados só será valido se houver o consentimento, salvo as exceções dispostas em lei e o art. 7º positiva as condições aplicáveis para o consentimento.

Logo no preâmbulo, o consentimento e suas regras são exibidas no n. 32, determinando que para que haja a anuência do titular sobre o tratamento de seus dados, o consentimento deve ser, assim como o determinado no PL brasileiro, livre, específico,

[185] A "*privacy for design"* é um conceito que existe há anos, mas apenas surgiu nas normas jurídicas pelo texto do GDPR. A "*privacy for design"* é a busca pela segurança do titular desde a inclusão de seus dados em um sistema até a encerramento do processamento.

informado e inequívoco, e para se constatar consentimento é preciso de uma ação concreta do titular, ou seja, "o silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento"[186].

As regras para consentir foram reforçadas, a relevância do adjetivo "informado", exige dos agentes de tratamento que os titulares tenham acesso as suas informações utilizadas para o processamento de forma facilitada, afastando uma linguagem complexa e as condições de termos longas e cheias de termos jurídicos que podem impedir o usuário de ter plena consciência do que está sendo feito com suas informações[187]. O posicionamento do regulamento em obrigar os agentes a tomarem providencias com relação ao texto de seus contratos é meio importante para que não perpetue os acontecimentos atuais, do titular não ler os termos de aceite devido a extensão e a linguagem rebuscada.

Essa exigência tem impacto também nas demais características do consentimento. Da mesma forma que o consentimento deve ser dado de forma simples, por utilizar linguagem clara e, consequentemente, o titular ter o conhecimento exato do tratamento de seus dados, a retirada do direito do agente de tratar os dados também deve ser simplificada.

As mudanças feitas pelo regulamento aumentaram a segurança jurídica tanto para o titular como para o agente de tratamento, isso ocorre porque de acordo com os artigos 6º e 7º do regulamento, em breve o consentimento, além de ser obrigatório para todos os tratamentos de dados, deverá, quando a situação exigir declaração escrita, estar totalmente desagregado dos outros termos e condições de uso. Essa exigência faz com que, além do titular declarar conscientemente a sua vontade em deixar que seus dados sejam processados, o agente terá mais facilidade quando precisar comprovar que suas ações são lícitas.

O consentimento não apenas demonstra a vontade do titular em liberar seus dados, mas todo o tratamento deverá ser baseado nesse consentimento, que irá delimitar o alcance dos agentes durante o tratamento. Ademais o novo regulamento também diminui as possibilidades de tratamento sem a anuência do titular e em legítimo interesse do agente, é o caso inclusive quando de interesse público, devendo o tratamento ser "objeto de medidas

---

[186] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.
[187] Ibidem.

adequadas e específicas"[188] ainda devendo sempre prevalecer "os interesses ou direitos e liberdades fundamentais titular"[189].

Assim como no PL brasileiro, o regulamento também autoriza o afastamento do consentimento em algumas situações, que ocorrerá quando os dados forem necessários para o cumprimento de uma obrigação legal; para proteger os interesses vitais do titular ou outra pessoa que seja incapaz de dar o seu consentimento; para o desempenho de uma tarefa de interesse público no exercício da autoridade oficial conferida ao controlador e quando necessário para a defesa de um direito, independentemente de se tratar de um processos judiciais, administrativos ou extrajudiciais[190].

O consentimento, como visto, é alicerce para o tratamento de dados, e ainda principal critério para "medir" a legitimidade do tratamento, salvo as exceções previstas na lei. O regulamento ainda prevê expressamente que para que o consentimento seja legítimo, a escolha de não assentir com o tratamento de seus dados não pode acarretar em prejuízos ao titular, esse ponto é importante levando em consideração que o acesso à diversos sites tem uma considerável quantidade de pedidos de análise de dados, e muitas vezes, aqueles que não concordam com o tratamento, são limitados ao acesso de algumas plataformas.

Para o consentimento da categoria especial de dados, o art. 9º foi exclusivamente editado. Como já dito, os dados sensíveis são únicos e que dizem respeito a características individuais e que, caso utilizados de forma indevida, podem causar graves danos aos titulares. Dessa forma, o regulamento em primeiro lugar proibe o tratamento, dando apenas algumas possibilidades nos termos seguintes, entre ela se o consentimento para o tratamento tenha sido dado de forma explicita. O consentimento no PL brasileiro aparenta ser mais flexível do que o determinado no regulamento europeu, até mesmo por determinar que o consentimento deve ser fornecido na forma escrita "ou por qualquer outro meio que o certifique", abrindo o leque de possibilidade de se obter um consentimento legal.

4.2 A responsabilidade civil na proteção dos dados pessoais

O tratamento de dados pessoais na União Europeia, assim como já constatamos no direito brasileiro, é uma questão de tutela de direitos e liberdades fundamentais, previsto na Convenção Europeia de Direitos do Homem, no art. 8º, 1, que positiva sobre a inviolabilidade

[188] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.
[189] Ibidem.
[190] Ibidem.

da vida privada e familiar, domicílio e da correspondência do individuo e na Carta de Direitos Fundamentais da União Europeia, nos artigos 7º e 8º, que determinam sobre a vida privada e familiar e sobre o direito à proteção de dados pessoais, além de também ser encontrado nas diretivas específicas sobre o assunto.

Devido a constante evolução da tecnologia e dos bancos de dados, a proteção à privacidade foi ampliada e, o que antes surgiu como um direito negativo teve que ser positivado, sendo desafiado a abarcar da melhor maneira todas as novidades da matéria. Dessa forma, a responsabilidade civil aparece na regulamentação Europeia e o próprio regulamento explica que por meio da responsabilização as normas de proteção de dados devem ser respeitadas.

Primeiramente, para que se fale de reponsabilidade, é preciso que algum dano seja cometido contra o titular, a falta de consentimento já acarreta no ilícito do tratamento, como vimos no capítulo anterior, mas outras questões também devem ser observadas pelos agentes, principalmente os princípios da proteção de dados que se encontram espaçadamente no regulamento e sobretudo no art. 5º, 1, que determina os princípios relativos ao tratamento de dados pessoais.

Os princípios da proteção de dados no regulamento são próximos aos determinados no PL n. 5.276/16 brasileiro, estão reunidos no capítulo dois, específico do tema e são eles: o processamento justo, leal e transparente – princípio amplo e que trouxe a transparência como novidade; a limitação da finalidade – impõe que os dados sejam utilizados apenas para os objetivos determinados, respeitando a finalidade inicial; minimização dos dados – equipara-se ao princípio da necessidade, em que apenas será tratado aqueles dados que tenham ligação com finalidades específicas; exatidão – busca a qualidade dos dados, inclusive impondo que os dados que não estejam corretos sejam eliminados rapidamente; a limitação temporal para o processamento dos dados – o titular dos dados só poderá ser identificados pelo tempo em que seus dados estão sendo tratados e, por fim, a segurança – os agentes são responsáveis por manter os dados seguros e aplicar as devidas técnicas para isso.

A diferença mais relevante entre o PL brasileiro e o Regulamento Europeu está na responsabilidade civil inserida como um dos princípios. O art. 5º, 2, requer que os responsáveis pelo tratamento demonstrem que seguiram os princípios, determinando como regra o ônus de provar que a violação não ocorreu sendo do responsável pelo tratamento e, caso não o faça, poderá ser responsabilizado.

Como dito, ao contrário do regulamento, o projeto de Lei brasileiro n. 5.276/16 não impõe como regra o ônus da prova do responsável pelo tratamento, indo contra a jurisprudência do STJ, como já estudado anteriormente. Fica bastante claro que nessa relação a parte que detém maiores poderes e tecnicidade sobre o objeto a ser zelado, e que poderia mais facilmente demonstrar que cumpriu as medidas impostas, seria o agente de tratamento, mas o art. 42, parágrafo único do PL, determina que a inversão do ônus da prova só ocorrerá quando o juiz observar que é excessivamente onerosa a produção das provas pelo titular. Na norma brasileira o agente fica apenas obrigado a demonstrar que o consentimento foi feito respeitando todos os princípios, é o que positiva o artigo 7º, §8º.

O preâmbulo do regulamento também se posiciona sobre o assunto em mais de um ponto, definindo a responsabilização de forma bastante ampla. Afirma, o preâmbulo n. 146, que o responsável pelo tratamento ou o subcontratante, deverão reparar qualquer dano causado ao titular decorrente de atividade que viole as normas, figurando uma responsabilidade objetiva. O significado de dano no dispositivo é interpretado em sentido lato, de forma que abarque todos os objetivos do regulamento e assegure ao titular a indenização integral e efetiva. O PL brasileiro, apesar de não empregar o pronome "qualquer", também não limita a responsabilidade, listando o dano patrimonial, moral, individual ou coletivo como viáveis de responsabilização.

O posicionamento do regulamento, abarcando todos os tipos de danos possíveis e deixando bastante claro essa intensão, auxilia a findar o problema que a jurisprudência brasileira vem enfrentando ao não entrar em consenso sobre o que pode ser classificado como dano. Em todo o regulamento a proteção de dados pessoais é reafirmada como sendo o meio de defesa de direitos e liberdades fundamentais do indivíduo, principalmente quando se trata de dados sensíveis. Essa apreciação torna mais evidente a necessidade de abranger os diversos danos que um mal tratamento de dados pessoais pode acarretar, tornando a responsabilização do agente objetiva e, consequentemente, mais facilmente de ser cobrada, além de estimular que as empresas estejam constantemente promovendo meios mais eficazes de segurança.

Sobre a teoria do risco aplicada na responsabilidade objetiva, o regulamento não apenas baseia a proteção de dados no risco do tratamento, incluindo o risco em diversos artigos como fator a ser considerado para o tratamento, mas amplia as consequências, impactando nas obrigações que, quanto maiores os riscos, mais complexas serão.

O regulamento classifica os risco de forma não exaustiva[191] no preâmbulo 75 e dá ênfase aos dados sensíveis, que podem acarretar em danos maiores

> (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[192].

De acordo com o estudo feito pelo Centro de Liderança de Política de Informação da Hunton & Williams LLP – CIPL, a noção de "escalabilidade" é aplicada no regulamento ao prever que as medidas para a responsabilização dos agentes serão exigidas de acordo com a natureza, o escopo, o contexto e os objetivos do processamento, como está expresso no preâmbulo 76 do regulamento. A escalabilidade e a abordagem baseada em risco são mecanismos que incentivam a responsabilização, com base nas especificidades de uma determinada operação de processamento[193].

Não há um conceito legal do que seria o risco, e para que não aconteça injustiças, é preciso que haja cautela na interpretação, principalmente porque todas as atividades humanas

---

[191] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

[192] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[193] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

têm certa quantidade de risco e o objetivo não deve ser de eliminar totalmente os possíveis danos, até mesmo pela impossibilidade desse feito, mas mitigá-los o máximo possível[194].

Assim sendo, o preâmbulo 76 impõe que haja uma avaliação dos riscos de cada tratamento e ainda a qual grau de risco os dados estão sujeitos. De acordo com o CIPL essa gestão de risco, com o passar dos anos, se torna cada vez mais importante para a proteção de dados e para a regulamentação. Isso ocorre porque ao saber onde o tratamento de dados é mais perigoso, espera-se que todas as partes interessadas no processamento dediquem recursos para diminuir o risco, além de tornar conceitos abstratos em riscos concretos[195]. O art. 39 complementa ao impor que o responsável pela proteção de dados leve em consideração os riscos do tratamento de dados para os direitos e liberdades fundamentais dos titulares, priorizando o cuidado com o processamento de dados sensíveis.

O regulamento, no art. 35, 4, impõe como papel da autoridade de controle de tornar público lista com os tipos de operação que são consideradas de alto risco e, consequentemente, o agente de tratamento terá que seguir os requisitos das avaliações de impacto de proteção de dados.

Embora o PL n. 5.276/16 não dispense tantos esforços nessa questão, o art. 39 determina que o órgão competente poderá cobrar do responsável a elaboração de relatório de impacto nos termos do regulamento, e no capítulo específico sobre segurança, também impõe que os agentes de tratamento utilizem de meios de segurança para a proteção dos dados, evitando eventuais danos e obrigando que as medidas sejam tomadas desde o inicio da concepção do processamento até a sua finalização.

A responsabilidade solidária também é contemplada no regulamento. Assim como no PL n. 5.276/2016, a norma da União Europeia faz distinção entre o Responsável pelo armazenamento dos dados e o operador dos dados, que são chamados, respectivamente, de Responsável pelo Tratamento e Subcontratante. De acordo com o regulamento, para que as normas sejam plenamente respeitadas, é distinta as obrigações do responsável e do subcontratante, mas a responsabilização poderá ser cobrada de ambos, ou seja, o titular poderá responsabilizar diretamente o subcontratante ao ter sofrido danos materiais ou imateriais decorrentes de imperícia ou violação das obrigações, essa possibilidade estimula o

---

[194] SILVA, Regina Beatriz Tavares da *alii*. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012. p. 86.

[195] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

subcontratante a se proteger das possíveis responsabilidades firmando acordos mais específicos com o responsável.

O responsável, por sua vez, terá o cuidado de firmar acordos com contratantes que ofereçam garantias suficientes para o cumprimento do regulamento, inclusive, ao contratar um subcontratante que respeite as normas do regulamento e cumpra código de conduta, essa informação pode ser usada como prova para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

Em um outro momento, o preâmbulo n. 79 do regulamento apresenta a situação em que a responsabilidade dos responsáveis pelo tratamento e dos subcontratantes será compartilhada, isso acontece devido a possibilidade de haver uma controladoria conjunta, ou seja, o responsável pelo tratamento e o subcontratante firmam acordo de como será tratado os dados, dessa forma, nada mais lógico que ambos respondam igualmente.

A isenção da responsabilidade, de acordo com o art. 82 do regulamento, ocorrerá apenas quando o responsável e o subcontratante demonstrarem que suas ações não tiveram nenhuma relação com os danos causados, respeitando o nexo de causalidade necessária. A lei de proteção de dados da UE teve a intenção de proteger o titular da melhor forma possível, deixando a segurança das empresas em segundo plano[196], pois garante que uma violação não fique sem reparação, assim o titular pode fazer pedido de indenização contra cada um dos responsáveis[197].

Durante o debate público do PL n. 5.276/16, várias foram as críticas com relação a responsabilização de ambos os agentes de forma solidária. As empresas alegaram a impossibilidade de controlar e fiscalizar todos os atos do operador, sendo assim prejudicados pela imperícia de terceiros. O regulamento derruba a alegação de forma simples ao impor que ambos sigam as normas e garantindo que, o cuidado tomado por parte do responsável, seja revertido em prova caso necessário. Para o consumidor, a possibilidade de uma responsabilização solidária obriga que os agentes de tratamento se resguardem e façam todo o possível para não serem responsabilizados, logo, protegendo melhor os dados processados.

Durante a leitura do regulamento fica claro o objetivo da norma em proteger o titular ao interpretar o dano de forma ampla, impondo obrigações condizentes aos tipos de

---

[196] GABEL, Detlev; HICKMAN, Tim. **GDPR Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >. Acesso em: 15 out. 2017.

[197] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

tratamento de dados e ainda tornando a responsabilização dos agentes em ação simplificada para o indivíduo. O PL n. 5.276/16, ainda que tenha copiado diversos dispositivos e até utilizado a mesma redação, não adentrou na matéria de forma satisfatória, ao ponto de evitar interpretações que possam colocar o indivíduo em situação difícil de ser reparada.

4.3 Órgãos responsáveis pela fiscalização dos dados pessoais

O Projeto de Lei 5.276 de 2016 apresentou, nos artigos 53 e 54 do Capítulo VIII que trata sobre a fiscalização, o Órgão Competente e o Conselho Nacional de Proteção de dados e Privacidade, que tem o objetivo de fiscalizar e zelar pela prática da Lei de proteção de dados pessoais, atribuindo a eles diversas obrigações. Apesar da iniciativa, deixou algumas lacunas importantes para o funcionamento do órgão, entre elas, qual o formato e se será um novo órgão ou se uma autoridade já existente receberá essa competência.

Doneda explica que o recurso de se ter uma autoridade administrativa com papel de fiscalizar a prática das normas relacionadas a proteção de dados pessoais foi adotada em nos países europeus, se tornando uma das características do "modelo europeu" de proteção de dados e posteriormente sendo difundido em diversos outros países, como Japão, Argentina e alguns estados norte-americanos, conclui que

> Estes órgãos são hoje parte fundamental da estrutura administrativa e jurídica estatal, realizando a aproximação entre as esferas do Estado, do mercado e da pessoa em contextos por demais complexos e especializados para serem efetivamente regulados pelas instituições tradicionais. [198]

Doneda também explica que "a busca por eficiência, redução de custos para o Estado, a estabilização dos mercados, a especialização dos órgãos decisionais do Estado"[199], entre outros, são os principais motivos para a criação do órgão.

As autoridades que fiscalizam, desenvolvem atividade de controle do mercado e das atividades privadas, devido a isso, Doneda explica o discurso de *regulation* e *deregulation*. A *deregulation* é a escolha do Estado em proporcionar ao mercado a regulação de uma atividade, a autoridade reguladora diminui as restrições e possibilita que o próprio mercado delimite a atividade. A *regulation*, em sentido amplo, é papel exercido tipicamente por uma agência reguladora que promulga normas que deverão ser seguidas para corrigir uma atividade do mercado. Doneda aponta que a criação dessa agência ocorreu devido a preocupação com as garantias aos direitos fundamentais, e devido suas técnicas não-

[198] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 385 - 387
[199] Ibid., p.390

legislativas, conseguiu regular situações extremamente dinâmicas, exatamente como as que presenciamos atualmente em razão dos avanços da tecnologia[200].

O modelo europeu, reafirmado pelo Regulamento 679/2016, pode orientar na deliberação de como o órgão de fiscalização brasileiro se comportará, haja vista que algumas características gerais devem nortear essa definição. A autoridade de controle no regulamento desempenha exatamente o papel da *regulation*, de acordo com o art. 51, tem o objetivo de "defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento"[201], ou seja, tem o objetivo de reforçar as normas de proteção de dados por todos os Estados-Membros da União Europeia e ajudar na interpretação do regulamento.

Um dos atributos da autoridade de controle na União Europeia, e que se tornou padrão internacional[202], é a independência total para promover suas atribuições, não estando condicionadas à influências externas, além de não solicitar nem receber instruções de outrem[203], sendo sujeita apenas a um controle financeiro que não interfere nas suas atividades[204], os preâmbulo 117, 118, 121 e o art. 52, determinam que a autoridade de controle será totalmente independente para a realização de suas funções, sendo apenas subordinadas a procedimento de controle de despesas e à eventuais fiscalizações judiciais, mas que não afetarão sua independência.

A independência da autoridade de controle não é novidade do regulamento. A Diretiva 95/45/EC já compreendia essa forma, a novidade se encontra na amplitude e no maior grau de detalhamento feito pelo regulamento. O órgão terá seus próprios membros que serão selecionados pela própria autoridade ou por organismo independente que deve ser orientado pela autoridade, bem como seus funcionários não poderão exercer nenhum trabalho fora do órgão que não seja compatível com suas atividades e não "estão sujeitos a influencias externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem"[205].

---

[200] Ibid., p. 392-393

[201] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[202] MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014. p. 37

[203] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[204] Ibidem.

[205] UNIÃO EUROPEIA. **Regulamento 2016/679 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

O regulamento já expressa de forma taxativa a necessidade da autoridade de controle ser independente e encontra como respaldo a Carta de Direitos Fundamentais da União Europeia que, de acordo com os estudos de Fortes, confirma a essencialidade da fiscalização ser particularmente autônoma e independente[206]. A independência do órgão se torna importante devido a concepção rígida da estrutura da administração pública direta, uma forte hierarquização que limita atividade que deve ser ágil. Importante preocupação exibida por Doneda, no entanto, é que, devido a total independência do órgão, é possível que haja a admissão de uma legítima tecnocracia. Para que isso não ocorra, o modelo do órgão deve ser o de autoridade de garantia, pois esse tem o papel de "ponderar situações subjetivas garantidas pela Constituição Federal e operar um balanceamento dos direitos em questão sem estarem vinculadas ao interesse público administrativo, no sentido de uma valoração "discricionária". "[207].

No Brasil, as agências reguladoras independentes – qualificadas como autarquias especiais – são as que possuem as características necessárias para fiscalizar e regular as atividades dos agentes de tratamento de forma adequada, seguindo os contornos impostos por lei específica. Para isso, a lei que regulamentará a proteção de dados no Brasil deve respeitar o disposto na Constituição Federal, art. 61, §1º, inc. II, e ter seu projeto formulado por autoridade do Executivo, pois só assim, terá a capacidade de criar cargos, funções ou empregos públicos.

Devido a falta de especificação na lei do Executivo de que o órgão responsável é uma agência reguladora independente, o Legislativo se encontra em situação delicada, pois a alteração do projeto de lei pode incorrer em vício de iniciativa e, por outro lado, a falta de uma especificação dos moldes do órgão regulador pode levar a aprovação da lei sem parte importante para legitimar o órgão de fiscalização.

O capítulo VI do regulamento se debruça na matéria sobre as autoridades de controle, o art. 53 especifica os critérios para a formação do quadro de membro da autoridade e determina que devem ser habilitados, ter experiência e conhecimento técnico necessário,

---

Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[206] FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p. 157

[207] DONEDA, Danilo. **Da Privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 395 - 396

dominando as questões sobre proteção de dados para o exercício de suas funções[208], além de deliberar sobre diversos direitos e deveres da autoridade.

O PL n. 5.276/16 também definiu diversas atribuições ao órgão competente para a fiscalização da proteção de dados, muitos com redação bastante próxima da encontrada no regulamento europeu, como a prerrogativa de informar a população sobre as normas, pois proteção de dados é muito dinâmica, precisando ser atualizada constantemente e a organização deve ter o papel de reduzir essa assimetria entre a informação que o cidadão possui e o domínio das empresas de tratamento de dado sobre o tema.

Algumas questões importantes não foram abordadas. O regulamento 679 determina que qualquer titular pode requerer informações sobre tratamento de dados diretamente da autoridade de controle, além de tornar a autoridade responsável por averiguar todas as reclamações e informar ao titular o andamento de seus pedidos. O PL brasileiro não possibilita o contato do titular com o órgão para informações, assim como não é possível a impetração de reclamações sobre o tratamento dos dados pessoais. No PL brasileiro, o titular apenas poderá fazer reclamações diretamente com as empresas, mais especificamente ao encarregado pelo tratamento de dados pessoais, como dispõe o art. 41, § 2º, e caso não seja atendido, poderá se encaminhar a outras vias para satisfazer seu pedido e apenas provando que já esgotou todos os meios viáveis de reinvindicação, o titular poderá contatar o órgão responsável .

Esse entendimento é plausível ao constatar, como feito pela ABDTIC em comentário pertinente durante o debate público do anteprojeto a quantidade de reclamações acarreta na necessidade de um departamento enorme para registra-las, na União Europeia, de acordo com pesquisa feita pelo "*International Association of Privacy Professionals*", será preciso mais de 28 mil encarregados pelo tratamento de dados para receber todas as reclamações[209], conclui-se que encaminhar todos os tipos de pedidos ao órgão responsável não é viável, devendo servir-se dos outros meios legítimos para a propositura da reclamação.

O regulamento da UE não apenas atribui a autoridade de controle o papel de receber as reclamações, como também investigar e contatar o reclamante em prazo razoável. A investigação da autoridade de controle não se limita às reclamações, também é competente

---

[208] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[209] HEIMES, Rita; PFEIFLE, Sam. **Study: at least 28.000 DPOs needed to meet GDPR requirements**. 2016. Disponível em: <https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/#>. Acesso em: 03 nov. 2017.

para investigar a aplicação do regulamento e conta com a cooperação de outras autoridades públicas. O PL brasileiro, em sua redação, não torna expressa a investigação, mas atribui o dever de zelar pela proteção de dados e realizar auditorias para verificar o cumprimento das normas, não informando se outros órgãos do poder público poderão informar sobre incidentes.

Outra questão divergente é que, apesar de não falar no artigo especifico das atribuições e sim durante o texto da lei, o órgão competente pode exigir das empresas que façam um relatório de impacto, mas no PL não especifica se será dele a responsabilidade de elaborar a avaliação, o regulamento aborda esse tema reafirmando no artigo específico das atribuições o dever de elaborar as avaliações e positiva que também conservará "uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados (...)"[210].

O modelo europeu de proteção de dados delegou à autoridade de controle grande parte da competência legislativa para determinar sobre questões específicas e técnicas, tendo também os poderes de fiscalizar, sancionar e atuar na esfera administrativa, buscando resolver possíveis conflitos entre as partes, e evitando a judicialização das questões[211]. Chamado de modelo-eclético, o regulamento da UE combina normas estatais com soluções tecnológicas e até mesmo com um interessante meio de engajamento ativo[212], ao classificar as empresas por meio de selos que indicam o grau de zelo com os dados de seus usuários.

O PL brasileiro não se preocupa em formas de engajamento das empresas, mas busca estimular que tanto o responsável pelo tratamento como os operadores formulem regras de boa prática, com o intuito de facilitar "o controle dos titulares sobre seus dados pessoais."[213].

Questão interessante é a rigidez que o regulamento trata os casos em que o responsável pelo tratamento encontra a ocorrência de incidente de segurança, ele deverá comunicar à autoridade de controle no prazo de 72 horas, só podendo ultrapassar esse tempo se comprovar que o incidente não acarretará em riscos ao titular. O PL brasileiro não determina um prazo, mas atribuiu ao órgão competente estipular o tempo aceitável, além

---

[210] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[211] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf > . Acesso em: 20 out. 2017

[212] GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf > . Acesso em: 20 out. 2017

[213] BRASIL. **Projeto de Lei n. 5.276,** de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >. Acesso em: 06 de set. 2017.

disso, apenas após a análise do órgão competente e a constatação de que o incidente é grave, ele poderá exigir do responsável pelo tratamento algumas ações, como comunicar o titular, divulgar o fato em meios de comunicação e buscar medidas para mitigar os efeitos.

O regulamento europeu se posiciona de maneira bastante diferente e mais protetiva, além do prazo já estar determinado, pois há a preocupação real que com a falta da segurança dos dados os riscos aos titulares sejam enormes, o responsável pelo tratamento deve informar ao titular o ocorrido assim que constatar a possibilidade de risco, não necessariamente que já ocorreu o dano, pois "a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados"[214].

Além do órgão competente, o PL também traz a figura do Conselho Nacional de proteção de dados e privacidade. A partir da leitura de suas competências, é possível averiguar que terá o papel de dar suporte ao órgão competente por meio de subsídios para a elaboração de normas, sugerindo ações, realizando estudos e debates sobre a proteção de dados e privacidade e, assim como o órgão tem a atribuição de fazer, informar a população sobre o tema.

A União Europeia também possui órgão semelhante, no regulamento, é denominado de Comité – é órgão também independente da UE dotado de personalidade jurídica, e tem atribuições muito próximas das da autoridade de controle, não se restringindo a apenas orientar, mas também podendo "emitir igualmente orientações sobre operações de tratamento de dados que não sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares e indicar quais as medidas adequadas em tais casos para diminuir o risco."[215]

O órgão responsável pela fiscalização exerce um papel de monitorar aqueles que monitoram os titulares dos dados, devendo ser parte central da lei de proteção de dados, pois será ele que fara que as normas apresentadas sejam cumpridas. Dessa forma a regulamentação brasileira sobre o órgão de fiscalização encontrou parte de sua redação no regulamento europeu, mas não se prendeu em questões importantes para a atividade plena do órgão, como o exato tipo de agência para que assim ela tenha a independência necessária para a fiscalização do regulamento. Infelizmente a falta da determinação de que o órgão será uma

[214] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

[215] UNIÃO EUROPEIA. **Regulamento 2016/679 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 20 out. 2017.

agencia reguladora, pode vir a prejudicar o futuro órgão que não poderá exercer todas suas prerrogativas.

Apesar disso outros pontos foram acertados, como não permitir que o órgão receba todas as reclamações dos titulares, tornando a atividade menos sobrecarregada e assim se deter apenas as questões mais gravosas e que não foram resolvidas pelas outras vias e a instituição de um conselho que dê suporte as atividades do órgão de fiscalização.

CONSIDERAÇÕES FINAIS

Não existe mais a possibilidade de um país permanecer inerte às diversas mudanças que os avanços da tecnologia, e principalmente das bases de dados, estão fomentando na sociedade. Essas mudanças atingem diretamente direitos fundamentais de seus cidadãos, e para que isso não ocorra de forma indiscriminada, é preciso que seja discutido a formulação de uma regulamentação clara e eficiente de proteção de dados. O presente trabalho analisou a situação brasileira por meio do Projeto de Lei n. 5.276/2016, utilizando como norma ideal o Regulamento 679/2016 da União Europeia, que, por meio do estudo comparado, procurou responder ao questionamento inicial, qual seja, se a atual redação do PL é suficiente para regular os casos de tratamento de dados no território nacional.

Primeiramente, com o estudo da evolução dos dados pessoais, compreendeu-se que o desenvolvimento do ambiente virtual e as consequências desses avanços estão profundamente interligados com o Direito pois, a garantia de privacidade que antes era limitada aos ambientes físicos teve que ser ampliada para abarcar todos os dados pessoais que são colocados na rede mundial de computadores e que, de acordo com a doutrina, são muitas vezes mais reveladores do que adentrar a casa de um individuo, por exemplo.

Após a breve noção histórica e a constatação das consequências da evolução tecnológica na sociedade, o primeiro capítulo continua apresentando a primeira lei brasileira que legislou especificamente sobre o uso da Internet no Brasil, Lei 12. 965/14 – Marco Civil da Internet – e que, sem dúvida, deu à proteção de dados um grau de relevância muito maior mesmo ainda não se posicionando de forma suficiente, alguns conceitos não foram devidamente abordados, e muitas lacunas deixadas para que uma futura lei específica pudesse regular a proteção de dados pessoais.

A lei específica de proteção de dados pessoais deve trazer conceitos e princípios gerais que serão utilizados para compreender a natureza do objeto que pretende assegurar, além de determinar que autoridade administrativa será a responsável pela fiscalização do cumprimento das normas. Devido a essa urgência para uma regulamentação, alguns projetos de lei foram apresentados, mas o do poder Executivo apresentou o projeto que abordou de forma mais completa e coerente, apresentando conceitos, princípios básicos para o tratamento, obrigações e deveres dos agentes e um órgão responsável pela fiscalização, entre outros pontos importantes para a regulação do tema. A breve análise dos artigos do PL que são relevantes para o presente estudo já pode dar uma base sobre os pontos que poderiam ser melhorados e aqueles que foram plenamente abrangidos pela lei.

Três conceitos foram abordados no segundo capítulo, para que se possa iniciar o estudo da futura lei de dados pessoais entendendo profundamente seu objeto. Começando pela distinção do termo “dados pessoais” se compreende o motivo de serem conceituados de forma ampla, pois os avanços do big data trouxeram a possibilidade de um dado ser combinado de diversas formas e com as mais variadas informações, podendo transformar o que antes não tinha significado em um dado rico de informações. Seguindo a análise dos termos, os dados sensíveis são tipo específico de dados pessoais e devem ser protegidos de forma mais específica por conterem informações tão exclusivas do titular a ponto de o colocar em situação delicada e arriscada quando tratados sem segurança.

Por fim, é possível concluir que a classificação dos dados anônimos deve ficar apenas no âmbito teórico. Atualmente não há mais a possibilidade de afirmar que um dado é anônimo pois, dependendo das demais informações obtidas num dado que antes não se referia a nenhuma pessoa pode se tornar novamente um dado pessoal com um simples cruzamento de informações. Devido a isso se inicia o chamado pseudoanonimização, que é a tentativa de isolar um dado a ponto dele ser, pelo menos naquela situação de tratamento, um dado sem conexão com um indivíduo.

O segundo capítulo também abordou o conceito do consentimento. Por ser questão determinante para o inicio do processamento, é a principal ferramenta de afirmação a autodeterminação informacional e ao mesmo tempo é a forma de abdicar o direito fundamental à privacidade, dessa maneira alguns pré-requisitos são essenciais para que se alcance um consentimento livre de vícios. O Marco Civil já consolidou os princípios para o consentimento e que o PL brasileiro apenas ratificou o requerido.

Ao estudar o consentimento, algumas questões acabam sendo elucidadas, primeiro se afasta a ideia de que o dado pessoa é propriedade do titular, isso porque o individuo não pode ser visto apenas como uma mera fonte de informações, o segundo ponto é a constatação de que o consentimento se assemelha a negócio jurídico e, junto com a necessidade de evitar a “fadiga do consentimento”, deve ser formulado um documento contratual claro e que não seja mais uma barreira para o titular.

O tipo de consentimento também está diretamente ligado ao tipo de responsabilidade civil que o agente de tratamento sofrerá em caso de dano ao titular do dado. A responsabilidade para os casos de dados pessoais deve ter como base a ideia de que a responsabilidade deve ser objetiva por ser esta a forma mais eficaz de resguardar o titular dos dados pessoais em caso de danos, pois este detém menos controle, conhecimento e transparência suficiente para demonstrar que o dano causado foi devido a atividade do agente

de tratamento. Há também a possibilidade da aplicação da teoria do risco, pois, diversas vezes é apresentada na lei a concepção de que a atividade de tratamento é arriscada, inclusive impondo uma avaliação de risco para as empresas. Logicamente, uma atividade de risco deve ter consequências mais severas, inclusive a de ter o ônus de comprovar que suas práticas foram desenvolvidas dentro daquilo que foi pré-determinado.

Após o entendimento desses pontos, é possível esboçar a formulação de como uma lei de dados ideal deveria ser constituída. O último capítulo expõe as uniformidades e as diferenças entre o PL brasileiro e o Regulamento 679 da União Europeia incluindo, além dos pontos explicados nos capítulos anteriores – consentimento e responsabilidade – a análise do órgão fiscalizador da atividade de tratamento de dados, pois será ele o responsável em garantir que o dispositivo seja cumprido.

Durante o estudo comparado, foi possível concluir que o PL brasileiro teve grande inspiração no Regulamento europeu, buscando uma uniformidade com normas internacionais. Apesar de não apresentar uma lei que aborda toda as questões, está apto para assegurar os principais direitos dos cidadãos e, ao mesmo tempo, os interesses tanto do setor privado como do Estado, pois detém as normas básicas para a regulação das atividades de tratamento.

No PL brasileiro, o consentimento para o tratamento foi acatado como um dos principais meios de assentimento ao tratamento. Há no também no PL n. 5.276/2016 a previsão de responsabilização dos agentes – pecando de certa forma ao não inverter o ônus da prova, mas admitindo a responsabilidade solidária e, por fim, apresenta também a necessidade de um órgão fiscalizador e seu caráter de aplicar sanções, além de ter poder de regular sobre o tema de acordo com a permissão da lei.

O Brasil despertou tardiamente para a questão e aprovar rapidamente uma lei de proteção de dados se tornou imprescindível. Apenas a partir de um regramento normativo é possível garantir aos cidadãos segurança sobre seus direitos, o que podem ou não fazer com seus dados, oferecendo segurança jurídica não apenas aos titulares, mas também às empresas que terão um dispositivo que orienta suas atividades.

O estudo sobre proteção de dados pessoais é amplo e deve ser constante, a produção científica sobre o assunto ainda é de maioria internacional o que demonstra que até mesmo as pesquisas nacionais ainda não foram encorajadas a investigar a matéria e suas consequências.

REFERENCIAS BIBLIOGRÁFICAS

ACADEMIA BRASILEIRA DE DIREITO DO ESTADO. **Comentários ao Marco Civil da Internet**. Disponível em: <http://abdet.com.br/site/wp-content/uploads/2015/02/MCI-ABDET..pdf >.

ALVIM, Agostinho. **Da Inexecução das obrigações** 4.ed. Rio de Janeiro: Saraiva, 1972.

ARTIGO19. **Proteção de dados pessoais no Brasil – Análise dos projetos de lei em tramitação no Congresso Nacional**. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>.

AZEVEDO, Ana Cristina Carvalho. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. **Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional**. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >.

BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015.

BRASIL, **Projeto de Lei n. 5.276,** de 26 de outubro de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 >.

BRASIL, Tribunal de Justiça do Estado do Rio Grande do Sul. Ação Coletiva. n. 001/11401789987, Rio Grande do Sul, RS, 28 de agosto de 2015.

BRASIL, Tribunal de Justiça do Estado do Rio Grande do Sul. Processo Civil. Apelação Civil. n. 70063665228, Rio Grande do Sul, RS, 26 de março de 2015.

BRASIL. Câmara dos Deputados. **Marco civil da internet**. 2. ed. Brasília: Edições Câmara , 2015.

BRASIL. **Código Civil. Lei nº. 10.403, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>.

BRASIL. **Constituição, 5 de outubro de 1988**. Constituição da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. Ministério da Fazenda. **1968 A 1981 – Começa a Era da Secretaria da Receita Federal**. Disponível em: <http://idg.receita.fazenda.gov.br/sobre/institucional/memoria/imposto-de-renda/historia/1968-a-1981-comeca-a-era-da-secretaria-da-receita-federal> .

BUCAR, Daniel. **Controle temporal de dados: o direito ao esquecimento**. *Civilistica.com.*, Rio de Janeiro, a. 2, n. 3, p. 01-17, jul.-set./2013. Disponível em:< http://civilistica.com/wp-content/uploads/2015/02/Bucar-civilistica.com-a.2.n.3.2013.pdf >.

CAVALCANTI, Roberto Flávio. **A inconstitucionalidade do artigo 19 do Marco Civil da Internet**. Disponível em: < https://jus.com.br/artigos/30560/a-inconstitucionalidade-do-artigo-19-do-marco-civil-da-internet >.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 3. ed. São Paulo: Malheiros, 2005.

COELHO, Fábio Ulhoa. **Curso de Direito Civil**. Obrigações e Responsabilidade Civil. 5. ed. São Paulo: Saraiva, 2012.

COMISSÃO EUROPEIA. **Reform of EU data protection rules**. Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> .

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS. **Para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal.** Disponível em: < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>.

CUBAS, Marina Gama. **Marco Civil da Internet completa um ano com regulamentação pendente**. Disponível em: < https://www.conjur.com.br/2015-abr-23/marco-civil-internet-faz-aniversario-regulamentacao-pendente > .

DANTAS, San Tiago. **Programa de Direito Civil.** Rio de Janeiro**:** Ed. Rio, 1979.

DE CUPIS, Adriano. **Os direitos da personalidade.** Tradução: Adriano Vera Jardim e Antonio Caciro. Lisboa: Livr. Moraes, 1961.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2013.

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

DONEDA, Danilo. **Um código para a proteção de dados na Itália**. Disponível em: < http://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf >.

ELETRONIC PRIVACY INFORMATION CENTER. **Council of Europe Privacy Covention**. Disponível em: <https://epic.org/privacy/intl/coeconvention/> .

FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016.

FRADA, Manuel A. Carneiro da. **Vinho novo em odres velhos?**. Disponível em: <http://www.oa.pt/upl/%7Bedbdd555-eea1-4f73-bd2d-5808411e4a31%7D.pdf >.

GABEL, Detlev; HICKMAN, Tim. GDPR **Handbook: Unlocking the EU General Data Protection Regulation**. 2016. Disponível em: < https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation >.

GAGLIANO, Pablo Stolze. **Novo curso de direito civil, volume 3: responsabilidade civil** / Pablo Stolze Gagliano, Rodolfo Pamplona Filho. — 10. ed. rev., atual. e ampl. – São Paulo : Saraiva, 2012.

GOMES, Orlando. **Contratos**. 26. ed. Rio de Janeiro: Forense, 2008.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 9 ed. São Paulo: Saraiva, 2014. p. 21.v4.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf > .

HEIMES, Rita; PFEIFLE, Sam. **Study: at least 28.000 DPOs needed to meet GDPR requirements**. 2016. Disponível em: <https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/#>.

HOLVAST, Jean. **History of Privacy**. 2009. Disponível em: < https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf >

IDEC. **À Comissão especial de tratamento e proteção de dados pessoais da Câmara dos Deputados**. Disponível em: <https://www.idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf>.

KEEN, Andrew. **The Internet is not the answer**. Disponível em: <https://books.google.com.br/books?id=D3UkBQAAQBAJ&pg=PT135&dq=future+crystal+man+personal+data&hl=pt-BR&sa=X&ved=0ahUKEwjx9srL08bXAhVDI5AKHdIcCnUQ6AEIJzAA#v=onepage&q=crystal%20man&f=false>.

LIMA, Cíntia Rosa Pereira de Lima. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos**. Disponível em: < http://publicadireito.com.br/artigos/?cod=981322808aba8a03> .

MAYER-SCHÖNBERGER, Victor; CUKIER; Kenneth. **BIG DATA, como extrais volume, variedade e valor**. Tradução: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**, 9. ed. São Paulo: Saraiva, 2014.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. Coelho. **Série Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015.

MENDES, Laura Schertel. **Privacidade, proteção de dados e a defesa do consumidor**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. **Revista de Direito do Consumidor**, São Paulo, ano 22, n. 90, p. 245-260, nov. – dez. 2013.

MONTEIRO, Renato Leite. **A nova regulação de dados pessoais aprovada na União Europeia e sua influência no Brasil**. Disponível em: <http://renatoleitemonteiro.com.br/analises-juridicas/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil/>.

MORAIS, José Luis Bolsan de; NETO, Elias Jacob. **Quem é anônimo no mundo dos metadados? O problema do anteprojeto de lei para a proteção de dados pessoais**. 2015. Disponível em: <http://emporiododireito.com.br/backup/repec-11-quem-e-anonimo-no-

mundo-dos-metadados-o-problema-do-anteprojeto-de-lei-para-protecao-de-dados-pessoais-por-jose-luis-bolzan-de-morais-e-elias-jacob-neto/>.

NAZARENO, Claudio. **Comentários ao PL 5.276/16, que dispõe sobre o tratamento de dados pessoais.** 2016. Disponível em: <http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema11/2016_10154_pl5276-2016-tratamento-de-dados-pessoais_claudio-nazareno > .

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos principais da Lei n. 12. 965, de 2014, o Marco Civil da Internet.: subsídios a comunidade jurídica**. Disponível em: <https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica > .

PENSANDO O DIREITO. **Consulta Pública do Anteprojeto de Lei de Proteção de Dados Pessoais**. Disponível em: < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >.

PENSANDO O DIREITO. **Você sabe o que são dados anônimos?**. Disponível em: < http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/ >

PEREIRA, Caio Mário da Silva. **Instituições do direito civil**. 18º ed. V. III. Rio de Janeiro: Forense, 2014.

PREITE, Francesca *alii*. **The new european regulation on personal data protection: significant aspects for data processing for scientific research purposes**. 2017. Disponível em: <http://ebph.it/article/viewFile/12286/11354>.

RODRIGUEZ, Daniel Piñeiro. **A proteção de dados pessoais sensíveis no contexto do estado democrático de direito**. 2009. Disponível em: <http://www.pucrs.br/edipucrs/IVmostra/IV_MOSTRA_PDF/Direito/72217-DANIEL_PINEIRO_RODRIGUEZ.pdf >

SAENZ, Fabiana Eduardo. **Habeas Data**. Disponível em: < escola.mpu.mp.br/dicionario/tiki-index.php?page=Habeas+data > .

SALDANHA, Jânia Maria Lopes. **Qual direito para os dados pessoais em tempos de Big data?**. Disponível em: < http://justificando.cartacapital.com.br/2015/03/16/qual-direito-para-os-dados-pessoais-em-tempos-de-big-data/ >.

SILVA, Regina Beatriz Tavares da. **Responsabilidade civil: responsabilidade civil na internet e nos demais meios de comunicação**. São Paulo: Saraiva, 2012.

SONG, Yi; DAHLMEIER, Daniel; BRESSAN, Stephane. **Not so unique in the Crowd: a simple and effective algorithm for anonymizing location data**. Disponível em: < http://ceur-ws.org/Vol-1225/pir2014_submission_11.pdf >.

SWEENEY, Latanya. **Simple Demographics Often Identify People Uniquely.** Disponível em: <https://dataprivacylab.org/projects/identifiability/paper1.pdf >.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Parlamento Europeu, Conselho da União Europeia e Comissão Europeia. 2000. Disponível em: < http://www.fd.uc.pt/CI/CEE/pm/Tratados/Nice/Carta%20Direitos%20Fundamentais.pdf >.

UNIÃO EUROPEIA. **Diretiva1995/46CE, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Diário Oficial das Comunidades Europeias*, Bruxelas, 31 jul.2002. Disponível em: <http://eur-http://eur-lex.europa.eu/pt/index.htm>.

VENOSA, Sílvio de Salvo. **Direito civil: Responsabilidade Civil**. 6 ed. São Paulo: Atlas, 2006.