Universidade de Brasília - UnB
Faculdade de Direito
Curso de Graduação em Direito

LEI Nº 13.444, DE 11 DE MAIO DE 2017: UMA ANÁLISE À LUZ DOS DIREITOS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

MARIA CRISTINE BRANCO LINDOSO

ANA FRAZÃO

Brasília
Junho, 2017

MARIA CRISTINE BRANCO LINDOSO

LEI Nº 13.444, DE 11 DE MAIO DE 2017: UMA ANÁLISE À LUZ DOS DIREITOS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada à Faculdade de Direito, da Universidade de Brasília – UnB, como requisito parcial à obtenção de diploma no Curso de Graduação em Direito.

Orientadora: Prof.ª Dr.ª Ana Frazão

Brasília

2017

UNIVERSIDADE DE BRASÍLIA
Faculdade de Direito
Curso de Graduação em Direito

Monografia apresentada à Faculdade de Direito, da Universidade de Brasília – UnB, como requisito parcial à obtenção de diploma no Curso de Graduação em Direito.

Lei nº 13.444, de 11 de maio de 2017: Uma análise à luz dos direitos de privacidade e proteção de dados pessoais

Maria Cristine Branco Lindoso

Banca examinadora:

_____
Professora orientadora: Prof.ª Dr.ª Ana Frazão

_____
Professor: Prof. Dr. Alexandre Veronese

_____
Professor: Prof. Me. Thiago Luís Santos Sombra

Brasília, 29 de junho de 2017

AGRADECIMENTOS

Não poderia iniciar qualquer agradecimento sem antes pensar em meu pai, Mauricio, meu grande apoiador, companheiro, inspirador, herói e confidente de todos os momentos da vida. Todos os meus trabalhos são feitos com você em mente.

Agradeço também à minha mãe, Cristine, que é símbolo de luta, carinho e cuidado. Sempre sonhadora, você me ensinou a batalhar incansavelmente para ser quem sou. Sem você não poderia ter chegado até aqui.

Aos meus irmãos, Carol, Luico e Mari, por dividirem comigo todas as angústias e alegrias da graduação. Agradeço especialmente ao Alex, meu irmão e melhor amigo, que é também o verdadeiro motivo do curso na Universidade de Brasília, com suas visitas rotineiras de domingo ao Campus Darcy Ribeiro. Amo vocês!

Agradeço à minha orientadora, Ana, por ter sido tão presente no decorrer de todo o curso, fosse nas aulas ou nos projetos de pesquisa. Obrigada por todos os ensinamentos e pela longa parceria. Que venham muitos trabalhos conjuntos pela frente!

Aos melhores amigos que poderia ter feito ao longo da graduação, Angelo, Amanda, Carlos e Paula. Vocês são responsáveis pela construção da minha maturidade acadêmica, do desenvolvimento desse trabalho e de tantos outros que fizemos juntos. Preciso agradecer as conversas e o companheirismo incansável. Sigamos sempre juntos.

Agradeço à Flávia, irmã de alma que caminha junto comigo por tanto tempo. Você é minha eterna melhor amiga e eu não poderia existir como sou hoje sem você.

Nas pessoas do Mauro, Camila, Lucas e Priscila, agradeço aos companheiros de trabalho, por ensinarem tanto no convívio diário.

Por fim, e não menos importante, agradeço ao Henrique, por ser esse amor com quem posso dividir tantas alegrias e sonhos.

SUMÁRIO

RESUMO

O presente estudo busca analisar a Lei nº 13.444, de 11 de maio de 2017, que institui a Identidade Civil Nacional (ICN), um cadastro único de cidadãos brasileiros, organizado através de um banco de dados a ser administrado pelo Tribunal Superior Eleitoral (TSE). A análise foi feita a partir de uma revisão bibliográfica, entendendo pontos positivos e negativos da Lei, principalmente, à luz das garantias de privacidade e do direito de proteção de dados. Também foram analisadas iniciativas similares nos Estados Unidos e na Índia, a fim de entender se o Brasil está promovendo avanços ou retrocessos na matéria. Espera-se compreender, ao final do trabalho, quais os eventuais problemas existentes em um grande cadastro único sobre os cidadãos, administrado por órgão não especializado do governo.

Palavras-chave: privacidade; proteção de dados; Identidade Civil Nacional (ICN).

ABSTRACT

The present study seeks to analyze the Statute No. 13444, enacted on May 11, 2017. The Statute establishes the National Civil Identity (ICN), a single registry of Brazilian citizens, organized with the use of a database administered by the Superior Electoral Court (TSE). The analysis was based on a bibliographic review, understanding the positive and negative aspects of the Statute, mainly in light of the guarantees of privacy and issues related to data protection rights, also evolving the analysis of similar initiatives in the United States and India. The study seeks to understand what possible problems exist in a large single registry of citizens, administered by non-specialized government organization.

INTRODUÇÃO

A sociedade contemporânea se define, hoje em dia, enquanto sociedade da informação, sendo esse o elemento fundante de toda sua estrutura organizacional (Webster, 2014). Nesse sentido, a informação funciona como mecanismo de comunicação e de acesso ao mundo, pressupondo a existência de uma relação de poder entre quem tem o conteúdo, a informação, e quem a fornece (Castells, 2009).

O comércio, a fiscalização, grande parte do processo comunicativo, dentre vários outros exemplos, ocorrem de forma mais rápida e completa em razão de mecanismos disponíveis na internet, sendo que está em curso um verdadeiro processo revolucionário de migração da realidade para o espaço virtual. O Direito teve dificuldade de acompanhar o rápido desenvolvimento tecnológico, de modo que surgiram diversas discussões sobre as formas de se promoverem garantias individuais aos usuários da rede.

De igual forma, também surgiram debates sobre a dimensão ética dos avanços tecnológicos, uma vez que novos mecanismos de influência são criados diariamente, gerando uma série de vulnerabilidades ao usuário que eram até então inimagináveis, causando violações de direitos que devem ser inadmissíveis na realidade contemporânea.

No contexto, o uso de dados como ferramenta viabilizadora de qualquer atividade da internet assumiu também contornos de instrumento de poder e manipulação das vontades dos usuários, tornando-se uma importante e valiosa mercadoria. Os novos mecanismos de tratamento de dados dos usuários, tornaram-se prática comum enquanto formas de se tentar obter e armazenar uma maior quantidade de conteúdo sobre um indivíduo específico, sempre extraindo a maior quantidade de informações possíveis de um único dado, as vezes sem uma finalidade inicial, mas com a expectativa de que se possa produzir um conteúdo valioso para o futuro.

As razões dessa necessidade de compilar dados são múltiplas e mudam de acordo com os objetivos de cada um dos agentes: podem ser utilizadas para personalizar estratégias de marketing e incentivar o consumo, como também para consolidar informações para a correta instrução de uma política pública de governo, por exemplo. Mesmo com objetivos diversos, os bancos de dados consolidam também os arranjos sociais sobre o acesso à informação enquanto forma de

poder na atual realidade, e representam uma estratégia de controle para qualquer um dos agentes que disponha dessa informação.

Em razão dessa característica, o controle sobre esses bancos de dados prescinde de regulação específica e constantemente atualizada, além de verdadeiras relações de confiança entre os usuários e os agentes detentores da informação. Também são necessárias políticas de transparência sobre o conteúdo armazenado, mecanismos para se facilitar o acesso e o controle, e comprometimento com o respeito à finalidade inicial do fornecimento daquele dado.

No caso do governo, o uso dessas tecnologias de armazenamento de dados implica, ainda, em uma especial atenção aos limites sobre a função fiscalizadora do Estado, notadamente quanto ao necessário respeito aos direitos de privacidade de toda uma nação. A necessidade de aprimorar a eficiência da gestão e do uso de recursos, a disponibilidade e o acesso às políticas públicas e os próprios mecanismos de vigilância, são as principais justificativas utilizadas para a criação desses grandes bancos de dados de domínio estatal, sob os quais, poucas vezes, se tem efetivo controle de conteúdo.

Pouco se discute, contudo, que nem sempre o aprimoramento e a maior eficiência da administração pública podem ser oponíveis a certas garantias constitucionais dos cidadãos, como é o caso da garantia do direito de proteção dos dados pessoais, conformada no atual ordenamento também como um direito de personalidade.

Diante de tais preocupações, surgiram diversas iniciativas legislativas para consolidar formas de atuação na internet, sendo o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014) a mais expressiva delas. Como será detalhado adiante, esse diploma buscou consolidar princípios norteadores do uso da internet no Brasil, deixando de fixar diretrizes regulatórias específicas sobre algumas questões fundamentais para uso da rede no Brasil, como é o caso do armazenamento de dados pessoais.

Em meio a algumas lacunas legislativas, e aliada à ausência de debate público sobre proteção de dados pessoais, surgiram também outras iniciativas controversas, como é o Projeto de Lei Complementar n. 19 de 2017, de autoria do Presidente da República, sancionado como a Lei n. 13.444 em 11 de maio do mesmo ano.

A Lei dispõe sobre a Identidade Civil Nacional (ICN), registro cadastral único dos cidadãos, o qual que busca reunir, organizar e compilar diversos outros dados individuais de registro civil, tais como filiação, cadastro biométrico, gênero, Cadastro de Pessoa Física (CPF), dentre outros, em um único documento. Essas informações serão organizadas através de um banco de dados administrado pelo Tribunal Superior Eleitoral (TSE), e gerido de forma conjunta por um comitê de composição mista de membros dos poderes executivo, legislativo e judiciário, chamado Comitê Gestor da ICN.

Toda a tramitação da iniciativa legislativa foi considerada rápida, sendo que no mesmo ano em que foi enviada ao Senado Federal pelo Presidente da República, foi também sancionada com pouquíssimos vetos e transformada em Lei. No curso desse processo, não foi oportunizada uma consulta pública efetiva sobre eventuais controvérsias da iniciativa, porque sequer se atentou à possibilidade de que um grande cadastro gerido pelo Estado poderia implicar em violações de direitos constitucionalmente assegurados aos cidadãos.

Ocorre que as discussões sobre o armazenamento de informações cadastrais, que podem ser consideradas altamente sensíveis, vem sendo discutida em esfera global, principalmente quando são administradas por um banco de dados do Estado, sob o qual não se poderá exercer muito controle, em princípio. Essas discussões envolvem (i) uso de dados cadastrais como mecanismos de fiscalização excessiva e manipulação de comportamento por parte do governo; (ii) falta de garantias que permitam aos cidadãos qualquer tipo de controle ou acesso das informações armazenadas; (iii) violação de direitos de privacidade, personalidade e proteção de dados em razão do armazenamento desses conteúdos; (iv) excessivo poder de controle sobre o individuo; dentre outros.

Tendo em vista algumas das discussões aventadas acima, e a grande possibilidade de controvérsias da instituição da ICN, o intuito do presente trabalho é analisar os objetivos da Lei 13.444/2017, quais benefícios poderá trazer para a gestão e organização da administração pública, e quais os pontos polêmicos relacionados à proteção da privacidade dos cidadãos. Pretende-se, ao fim, perceber porque a nova Lei precisaria ter sido melhor discutida com diversos grupos da sociedade civil e, principalmente, com especialistas na matéria de proteção de dados pessoais, entendendo também problemas das lacunas importantes que foram deixadas no projeto.

De pronto, é importante ressaltar que alguns conceitos são abordados de forma breve, apenas para corroborar as perspectivas organizadas na discussão central, que corresponde exclusivamente à análise do projeto de Lei. Dessa forma, a partir de uma revisão bibliográfica, não é objetivo deste estudo aprofundar certas discussões que, sem dúvida, são muito mais complexas do que a forma com que foram aqui expostas.

Espera-se que esse estudo consiga perceber que o uso da base cadastral da ICN pressupõe um verdadeiro compromisso de respeito aos princípios e garantias constitucionais na rede, consolidados através do Marco Civil da Internet, além de respeitarem também discussões em nível global sobre o armazenamento e uso de dados cadastrais, enquanto o Brasil não exerce a regulação apropriada e específica sobre o tema.

CAPÍTULO I - PRIVACIDADE E PROTEÇÃO DE DADOS

I.1 - PENSAR A PRIVACIDADE A PARTIR DE WARREN E BRANDEIS

Pensar em privacidade é um diálogo recorrente e atual. Ainda em 1890, Warren e Brandeis[1] foram os primeiros a pensar no direito de ser deixado sozinho como expressão máxima do privado (Warren; Brandeis, 1890). Considerados o marco teórico inicial, ambos os autores inseriram discussões importantes sobre a necessidade de um espaço de privacidade (ou de intimidade, como será melhor discutido adiante), que ainda são relevantes para a organização da sociedade contemporânea do armazenamento de dados e da troca de conteúdo de alta velocidade.

A partir dessa primeira noção do privado como espaço de solidão, profundas discussões sobre o que realmente significa a privacidade criaram corpo e são debatidas até hoje. Alguns acreditam nas percepções envolvendo uma correspondência do privado com a autonomia individual, ou enquanto sendo a capacidade de cada um exercer controle sobre informações disseminadas sobre si[2]. Para outros filósofos, por sua vez, as discussões se aprofundam ora com abordagens reducionistas[3], no sentido de a privacidade ser derivada de outros direitos, ora com abordagens que percebem a privacidade como um valor único em si mesmo[4] (Wong, 2005).

Tais discussões, contudo, não são o objetivo do presente estudo. As diferenças na concepção do privado têm grande relevância para os estudos da doutrina, mas o que se busca nesse momento é perceber que houve uma efetiva transformação da privacidade para o que se chama hoje de direito de proteção de dados.

Hoje, discute-se muito a existência do espaço privado na internet, uma vez que grande parte da vida se organiza em estruturas interligadas pela rede, onde o conteúdo corresponde a um

---

[1] Com o livro "*Right to Privacy*", primeiramente editado em 1890 pela *Harvard Law Review*, os autores inciaram discussões sobre os limites do espaço privado a partir da repercussão de fofocas e do ciclo vicioso que a publicização desse tipo de conteúdo criava. Ambos já mencionavam, à época, o temor relacionado às ameaças ao espaço privado com novas invenções e formas de chamar atenção da população.

[2] Essa é a percepção antropológica do conceito formulada por Alan Westin em "*Privacy and Freedom*", em 1967 (Wong, 2005, p.149).

[3] Judith Jarvis Thomson é uma autora expoente dessa perspectiva com "*Right to privacy*", além de Richard Posner em "*Why Privacy is important*", o qual adota uma perspectiva econômica da privacidade (Wong, 2005, p.149).

[4] O contraponto à é feito por James Rachels em "*Why privacy is important*" e Richard Gavison, em *"Privacy and the limits of the law*" (Wong, 2005, p.149).

dado compartilhado por múltiplos agentes. Tanto a iniciativa privada quanto os agentes governamentais estão transportando grande parte de sua atuação para a esfera digital, não só porque os custos são melhores, como também porque existem estratégias tecnológicas que permitem uma maior otimização dos recursos aplicados. É por esse motivo, também, que a regulação no espaço virtual virou uma necessidade: todas as relações estão se virtualizando, e é necessário promover a garantia de direitos também na internet.

A virtualização das relações corresponde a uma intensa troca de dados, que envolve desde a fiscalização por parte do Estado, a organização de políticas públicas de acesso aos indivíduos e de programas de atuação social direcionadas a um público alvo específico, até a criação de estratégias de *marketing* individual e direcionado, as discussões sobre propriedade intelectual e direitos autorais, dentre vários outros exemplos que utilizam informações individuais para centralizar sua organização.

Em razão da transferência do espaço privado para a *internet,* o que acarretou em um grande desenvolvimento do mercado de dados, pensar a privacidade deixou de se limitar às noções antigas ficar sozinho, ou de não ser vítima de fofocas e boatos, envolvendo, hoje, toda uma percepção de tecnologia da informação como necessária para a organização social contemporânea.

Também cumpre ressalvar que o desenvolvimento tecnológico e a mudança do que se entende por privacidade provocaram verdadeiros questionamentos éticos sobre os diversos comportamentos vida. (Nissenbaum, 2004). Isso porque era comum acreditar que o espaço virtual iria dirimir certos preconceitos existentes na sociedade, como as de gênero e raça, justamente por haver uma convivência comum e não diferenciada para cada um dos usuários.

Foi de grande surpresa quando a internet provou o justo contrário, principalmente em locais virtuais de convivência, como salas de jogos *online*: todos os preconceitos acabam por se reproduzir sob a escusa de serem um comportamento cultural (Nakamura, 2014). Alguns também destacam uma grande frustração o desempenho político e social que a internet deixou de promover, assumindo, por outro lado, um espaço propício aos extremismos e divulgação de conteúdo ofensivo (Schreiber, 2015).

Contudo, deve-se pensar que a tecnologia não pode ser considerada como um problema capaz de mitigar o exercício dos direitos de privacidade na sociedade contemporânea. Ao revés, devem ser feitas escolhas conscientes e seguras sobre as diversas possibilidades de seu exercício (Schertel Mendes, 2014, p. 35). A sociedade como um todo caminha para o que se chama de Sociedade Digital, fruto do desenvolvimento tecnológico. Não se pode, portanto, entender os avanços nessa área como retrocessos aos valores éticos compartilhados amplamente, e nem, especialmente, como fatores prejudiciais ao exercício dos direitos de privacidade em razão de um cyber-espaço de alcance mundial. Devem-se buscar valores comuns, aliados ao conhecimento técnico, para que o Direito consiga resguardar a efetiva tutela da privacidade na internet (Pinheiro, 2016).

Portanto, em razão da convivência social e do aprimoramento tecnológico, a privacidade ganhou novos sentidos em razão, principalmente, da expansão da internet, a qual modificou as concepções do que é o espaço individual, e quais são seus efeitos e limites. Como também será desenvolvido mais à frente, entender a privacidade como direito de proteção de dados faz, hoje, parte da agenda mundial, de modo que o Direito está adaptando seus institutos para acompanhar o desenvolvimento da tecnologia e as mudanças sociais.

I.2 - EVOLUÇÃO DOS DIREITOS DE PRIVACIDADE

Desde Warren e Brandeis (1890), que captaram a essência da privacidade enquanto direito de estar sozinho, diversas foram as concepções encontradas para satisfazerem não só as necessidades de proteção individual, como também os interesses dos vários agentes que buscam conseguir acesso (se possível ilimitado) aos conteúdos. Ambos os autores assumiam uma perspectiva da privacidade enquanto o direito de se estar sozinho, o que não se amolda plenamente à realidade de hoje. O espaço da internet e da troca de informações não permite conceituar o privado como solidão, porque a própria rede prescinde de um espaço de convivência e compartilhamento de conteúdo.

É a partir disso que se percebe que o exercício da privacidade requer um convívio social de um grupo que se comunica, onde é possível a troca de conteúdo entre vários sujeitos. O espaço

privado em si passa, portanto, por uma mudança paradigmática, em decorrência de um fenômeno social que demanda o fortalecimento das estruturas sociais e a troca constante de informações. Isso porque o convívio em meio às frequentes inovações da tecnologia, demandou o compartilhamento de quase todo tipo de conteúdos, não só para garantir a entrada do indivíduo no meio social, como também para permitir seu acesso ao conteúdo difundido na esfera mundial. Por isso, não existe mais a noção de que o privado é sinônimo de secreto, ou de que ter privacidade é o mesmo que um espaço para chamar de seu. Foi preciso "dilatar esse conceito para além de sua dimensão estritamente individualista", nas palavras de Stéfano Rodotá (2008, p. 25).

Constantes são os avanços tecnológicos que promoveram alterações nas diversas concepções do que é o espaço privado, mas sempre se tem em mente a capacidade de inserção ou influência que outros possam vir a ter nesse espaço que se presume intacto. Atualmente, é muito comum encontrar diversas discussões sobre a chamada sociedade da informação, que acabam, inclusive, por colocar a tecnologia como um determinante do futuro da própria realidade democrática. Nessa sociedade da informação, ressalte-se, a tecnologia tem um papel político e social que precisa ser considerado, até para fins de organização das estruturas sociais (Webster, 2014).

Murphy, por sua vez, (1964) fala em privacidade como distância social, enquanto uma esfera de restrição mantida por todos, e que permite a interação entre os vários agentes sociais. Nesse sentido, o autor utiliza a metáfora do véu, uma espécie de distanciamento simbólico entre quem o indivíduo realmente é e a forma como os outros o vem, e que é também a natureza do espaço privado em si, garantindo que as pessoas não saibam tudo umas sobre as outras, não haveria de existir a convivência (Murphy, 1964).

A percepção do autor do véu da distância também encontra dificuldade para garantir direitos em um espaço virtual. Ora, distâncias foram reduzidas ao fluxo de informação compartilhado em segundos entre os diversos agentes, e sequer se pode dizer essa esfera de restrição individual realmente existe na internet. Em certo ponto, contudo, aplicam-se as ideias do autor para se considerar que ainda continua sendo importante que as pessoas não saibam tudo umas sobre as outras.

Hoje, fala-se em uma sociedade que processa a informação a partir da tecnologia e que se organiza a partir de estruturas globais e altamente maleáveis, posto que são facilmente influenciadas e modificadas a partir dos padrões culturais, sociais e econômicos dominantes (Castells, 2009). Toda a estruturação da sociedade se da ao redor de relações de poder e da capacidade de influência e de manipulação que um agente pode exercer sobre o outro. Esse poder vem de uma assimetria de informações que um dos agentes tem em relação ao outro. Na internet, essas informações são dados, e cada vez mais, a tecnologia busca aprimoramentos diferentes para permitir que um dado possa exprimir uma quantidade ainda maior de informações. Ou seja, ainda é importante para que as relações na rede sejam mantidas em níveis mínimos de igualdade que haja um certo distanciamento entre os vários agentes da rede, de forma a evitar disparidades de informação entre os usuários e o detentor do conteúdo.

Westin, em seguida, faz uma abordagem antropológica da organização social ao redor da privacidade, já considerando o aprimoramento das tecnologias de comunicação como determinantes na definição do espaço privado. Surge, para o autor, um temor de que o espaço privado talvez sequer exista, uma vez que a própria estrutura de organização da comunidade se dá em ordens hierárquicas e a partir da informação e da produção de conteúdo (Westin, 1967).

Antes, o homem primitivo conseguia o exercício completo da solidão quando se afastava de outros, mas hoje é incutida a ideia de que nunca se pode estar completamente sozinho, mesmo nessas situações de isolamento profundo. Esse sentimento se deu em razão dos processos de socialização, que ao mesmo tempo que possibilitaram o desenvolvimento, acarretaram também na necessidade de invasão desses espaços altamente privados justamente para fins de proteção do grupo, de reforço das regras construídas coletivamente e do fortalecimento das estruturas hierárquicas estabelecidas (Westin, 1967 pp. 66-69).

A partir desse autor, compreende-se que o conceito de privado para uma sociedade que se organiza em razão de polos de poder e ao redor da informação, é tênue a diferenciação do espaço privado e público. Não se pode mais reclamar solidão para garantir a privacidade, ao mesmo tempo que não existe mais um distanciamento capaz de garantir que a individualidade de cada um será protegida da influência de terceiros.

Tércio Sampaio Ferraz Júnior, ao fim, encontrou uma importante definição da privacidade na resistência individual à violação de terceiros naquilo que pertence única e exclusivamente ao sujeito. Mesmo que a único limite exclusivo do indivíduo seja sua integridade moral, essa é inatingível e inviolável por outros, justamente por implicar na expressão máxima do que é o espaço privado (Ferraz Junior, 1993, p. 440).

Essas são algumas das razões que permitem perceber que privacidade importa em compreender a relação que o desenvolvimento tecnológico causou dentro do corpo social, intensificando a troca de informações, o acesso ao conteúdo. Também se promoveu o desenvolvimento coletivo ao mesmo tempo em que estabeleceram ordens hierárquicas e normativas, aprimorando mais ainda os mecanismos de fiscalização e controle dessas estruturas. Perceber essas mudanças, inclusive, envolve entender que as concepções de privacidade sofreram alterações que agora influem diretamente na vida cotidiana. Em razão do grande domínio tecnológico que os entes fiscalizadores possuem, o simples acesso à informação passou a atuar na realidade (mais ainda) enquanto verdadeiro mecanismo poder, influindo diretamente no processo de controle do indivíduo e em sua capacidade de fazer escolhas. (Doneda, 2006, p. 9).

Como o acesso significa também capacidade de influência de comportamentos, é necessário aprimorar a concepção do que é o espaço privado para além de um espaço apenas de solidão. Enquanto verdadeira forma de constrangimento de terceiros à resistência na violação ao que não lhes diz respeito (Ferraz Júnior, 1993, p. 440), a privacidade será a única forma de permitir a limitação e o abuso das relações hierárquicas estruturadas no poder pelo acesso à informação. Ainda sim, encontra-se a dificuldade de definir com precisão o que é privacidade, uma vez que os contornos e as dimensões do espaço privado e do público são substancialmente mitigados quando se pensa na internet, no compartilhamento de informações, na produção e no armazenamento de dados como forma de existir na rede.

Nesse ponto, a confiança necessária entre o usuário e os diversos agentes detentores da informação ganha grande destaque. Privacidade deixa de implicar na existência de segredos, ou em um espaço de isolamento, e passa a significar uma garantia, pautada na confiança. Os conteúdos produzidos que dizem respeito à individualidade do usuário devem ser armazenados de forma diferenciada, além de não serem compartilhados com finalidade diferente daquela informada inicialmente (Richards; King, 2014). A confiança não irá garantir que a informação

não será do conhecimento de ninguém, mas poderá assegurar que não será divulgada indiscriminadamente

Ter privacidade, portanto, não implica somente ter um espaço individual. Significa também ter segurança e acesso às informações e conteúdos que existem sobre si, e até mesmo compartilha-los, com a garantia de que serão dados preservados de maneira apropriada. É, ainda, um mecanismo de imposição de limites individuais à imposição de comportamentos vindos dos agentes detentores da informação, como forma de controle e limitação do poder.

I. 3 - PRIVACIDADE, INTIMIDADE E VIDA PRIVADA: RELAÇÕES E CONFLITOS

A privacidade, portanto, já foi caracterizada enquanto fundamental para a organização do corpo social que depende da tecnologia e convive, cada vez de forma mais exclusiva, em redes virtuais. As discussões conceituais sobre privacidade fizeram surgir, ainda, diferenciações sobre outros espaços individuais a serem preservados, como é o caso da intimidade e da vida privada. Mesmo antes do desenvolvimento tecnológico e da difusão em massa da internet, a doutrina já permitia diferenciar a privacidade e a intimidade, sempre se atentando ao fato de que o privado existe em razão de um espaço público anterior.

Como visto, ter a informação significa possuir um grande poder em relação a outros, e compreender os limites e o verdadeiro significado da privacidade pode ser um importante mecanismo para se evitarem abusos e manipulações. É por isso que as diferenciações aqui explicitadas podem evitar impropérios quando da discussão da tutela de direitos.

A previsão constitucional é de que a privacidade é tutelada como direito fundamental, sendo determinante para o exercício da personalidade de cada indivíduo. A partir disso, diferenciam-se os atos que se relacionam à vida em comunidade, ou apenas às escolhas íntimas. Em síntese, entende-se a privacidade como gênero, do qual a intimidade e a vida privada são espécies (Maurmo, 2014).

Para Ferraz Júnior, exercitar a solidão ao máximo acarreta uma total ausência de repercussão social dos atos praticados enquanto se está sozinho, e esse seria o entendido por intimidade. Enquanto isso, a vida privada[5] implica na escolha de se reservarem informações e conteúdos sobre si, mas quando do convívio em grupo, de modo que esse ato de escolha, por si só, causa repercussão no espaço coletivo (Ferraz Júnior, 1993, p. 442).

Rui Stoco, por sua vez, considerar que o alcance de cada um dos termos merece uma definição mais precisa por parte da jurisprudência, para que seja efetiva a prestação jurisdicional. Ainda sim, define como intimidade aquele tipo de conteúdo que não se compartilha, "o direito de estar só ou consigo mesmo", e vida privada enquanto o resguardo daquilo que não será violado ou apenas divulgado. (Stoco, 2015).

A partir dessas definições, percebe-se que o "*right to privacy*" abordado por Warren e Brandeis, na verdade, corresponde ao que definimos hoje por intimidade, ao passo que a vida privada corresponde ao conteúdo íntimo, mas que repercute socialmente. A privacidade, por fim, engloba tanto a intimidade, quanto a vida privada, correspondendo a um amplo conceito de direito fundamental que busca preservar as escolhas do indivíduo desde seu espaço mais solitário até o compartilhamento de informações.

É de se destacar que o desenvolvimento tecnológico também acarretou na redução das nuances entre esses diversos conceitos, uma vez que mesmo conteúdos extremamente íntimos, e que não precisam repercutir socialmente, são divulgados – as vezes contra a vontade individual – causando prejuízos e requerendo tutela especial por parte do Direito. Tem-se como exemplo que hoje são os chamados dados sensíveis, melhor analisados à frente, mas que dizem respeito a um conjunto de informações muito íntimas, que apenas dizem respeito ao próprio indivíduo e a mais ninguém, como é o caso da orientação sexual ou das opções religiosas (Solove, 2007, p. 9). Esses são dados com potencial discriminatório, uma vez que produzidos a partir de escolhas íntimas sobre a personalidade do indivíduo, que o definem e caracterizam. Em razão de tais características, são dados que permitem determinar com precisão a quem aquela informação corresponde, e quando divulgados de forma massiva, podem intensificar ainda mais a exposição discriminatória à qual aquele indivíduo está sujeito.

[5] Em seus escritos, o autor utiliza a palavra privacidade, mas com a definição e características do que se entende por vida privada, considerando as definições aqui desenvolvidas.

Portanto, é importante considerar, para fins de estudo e da análise desse projeto, a privacidade como um gênero de direito fundamental que engloba tanto a proteção da vida privada, quanto a proteção da intimidade. De igual maneira, deve-se entender por privado todo aquele conteúdo produzido de forma íntima, que tem possibilidade de repercutir socialmente quando divulgado, tenha ele elevado potencial discriminatório ou não.

I.4 - PROTEÇÃO DE DADOS: O NOVO DIREITO DE PERSONALIDADE

Tendo a privacidade como direito fundamental, percebe-se que esta foi assim consagrada pela Constituição Brasileira em seu art. 5º, X, sendo assegurada sua inviolabilidade e o direito de indenização quando do seu desrespeito. Abordando o exercício à privacidade em meio coletivo, percebe-se que ela assumiu, no âmbito do direito civil, a feição de direito de personalidade: são estes os "direitos atinentes à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade" (Tepedino, 2004, p. 24), caracterizados por serem "intransmissíveis e irrenunciáveis, não podendo seu exercício sofrer limitação voluntária", como bem entende o art. 11 da Constituição Federal de 1988.

Gustavo Tepedino (2004), frente à complexidade da temática em comento, ainda caracteriza os direitos de personalidade em razão de sua generalidade (são concedidos a todos), extrapatrimonialidade (impassíveis de serem avaliados economicamente) e capacidade de se imporem absolutos, oponíveis contra a sociedade. Também é importante mencionar que o Código Civil apresenta uma cláusula geral de tutela referente à proteção da personalidade, e que os direitos de personalidade não figuram em um rol taxativo, mas apenas exemplificativo de tudo aquilo que pode ser tutelado em respeito à dignidade da pessoa humana, mas no âmbito civil de exercício de sua personalidade (Andrade, 2013, p. 86).

Todas essas características são fundamentais para se perceber a privacidade como proteção de dados pessoais, visto que a tecnologia impôs diversos desafios relacionados à forma de se pensar os direitos fundamentais. Como já mencionado, a sociedade atual vive grandes avanços tecnológicos, em um espaço de tempo cada vez menor, mas acaba por oscilar entre os benefícios de tais avanços e a reprodução de padrões culturais ultrapassados (como a

discriminação de gênero e o racismo), ou receio de novas ameaças. Em razão desse padrão complexo de sociedade, estender que o âmbito do direito fundamental de proteção à privacidade corresponde ao direito de proteção de dados também como forma de se resguardar a personalidade, é vital para aumentar a segurança social (Gonçalves; Bertotti; Muniz, 2015).

Assim, um rol taxativo e engessado do entendimento sobre quais são direitos atinentes à personalidade acabaria por provocar a obsolescência desse tipo de proteção no decorrer do convívio social e do avanço da tecnologia. Portanto, a generalidade da cláusula sobre direitos ligados à personalidade permite que o Direito mantenha contato atualizado com o cotidiano, acompanhando o desenvolvimento do que merece uma proteção especial por parte do direito civil. De igual maneira, enquanto direitos oponíveis a todos, os direitos de personalidade são também um elemento importante de limitação de poder dos entes privados e do Estado quando em posse dos dados pessoais, representando uma verdadeira garantia individual.

O direito fundamental à privacidade, garantia constitucional no art. 5º, X, aprofundou-se para assegurar também a proteção da informação disponível na rede, o acesso aos dados armazenados em bancos de dados, e a garantia da inviolabilidade do conteúdo que, mesmo quando compartilhado, deve ser preservado (Doneda, 2011, pp. 94-95). A privacidade passa a ser entendida também como tutela dos dados pessoais compartilhados na internet, ou como compartilhamento de informações em espaço virtual, sendo que o componente digital dos dados pessoais figura como fundamental na vida em sociedade hoje em dia, compondo, portanto, uma parcela importante e significativa da personalidade de cada um (Schertel Mendes, 2014, p. 33).

Nas palavras de Laura Schertel Mendes, portanto:

> "O direito à privacidade transformou-se para fazer emergir a dimensão dos dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados.
> A transformação desse conceito pode ser percebida de forma mais clara a partir da década de 70, com a edição de legislações específicas e de decisões judicias de diversos países, bem como a partir da aprovação de acordos internacionais e transnacionais em diferentes níveis. Todos esses instrumentos compartilham o conceito segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela jurídica." (Schertel Mendes, 2014, p. 29)

É importante destacar, ainda, que o direito de proteção de dados surgiu enquanto o direito de privacidade, mas existe uma diferença importante entre ambos os conceitos. O direito de

privacidade tem natureza negativa, que implica abstenção de condutas de terceiros, para não interferirem no íntimo alheio. Ou seja, terceiros devem se abster de divulgar informações indevidas, violar a intimidade, compartilhar um segredo. Por sua vez, o direito de proteção de dados tem uma natureza não proibitiva, até porque é a partir disso que se entende ser permitido compartilhar e armazenar dados pessoais, como é feito hoje nos grandes bancos de dados (Andrade, 2010).

I.5 - LEGISLAÇÃO E JURISPRUDÊNCIA

Diversas são as iniciativas no Brasil que versam sobre a tutela da privacidade nos mais variados espaços. Notadamente, a Constituição Federal faz a abordagem do tema enquanto direito fundamental assegurado, mas sua regulação depende da edição de leis específicas relacionando as diversas temáticas que podem abordar as questões de privacidade, e até às regulações técnicas, que garantem a efetividade dessa proteção.

A Lei n. 9.472 de 16 de julho de 1997, conhecida como Lei Geral das Telecomunicações, foi uma das primeiras iniciativas legislativas a regular os direitos de privacidade nas telecomunicações. Em seu art. 3º, ficou previsto que o usuário do serviço de telecomunicação tem direito à inviolabilidade de sua comunicação (inciso V) e ao respeito de sua privacidade e de seus dados pessoais (inciso IX)[6]. Após a sua edição, foi criada a Agência Nacional das

[6] A Lei n. 9.472/97 ainda traz, no mesmo artigo 3º, diversos outros direitos garantidos ao usuário dos serviços de telecomunicações, dispostos a seguir:
"O usuário de serviços de telecomunicações tem direito:
I - de acesso aos serviços de telecomunicações, com padrões de qualidade e regularidade adequados à sua natureza, em qualquer ponto do território nacional;
II - à liberdade de escolha de sua prestadora de serviço;
III - de não ser discriminado quanto às condições de acesso e fruição do serviço;
IV - à informação adequada sobre as condições de prestação dos serviços, suas tarifas e preços;
V - à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas;
VI - à não divulgação, caso o requeira, de seu código de acesso;
VII - à não suspensão de serviço prestado em regime público, salvo por débito diretamente decorrente de sua utilização ou por descumprimento de condições contratuais;
VIII - ao prévio conhecimento das condições de suspensão do serviço;
IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;
X - de resposta às suas reclamações pela prestadora do serviço;
XI - de peticionar contra a prestadora do serviço perante o órgão regulador e os organismos de defesa do

Telecomunicações – ANATEL que, enquanto agência reguladora de grande porte, acabou por editar diversas resoluções dispondo sobre o uso de dados, além de formas de se evitar a invasão de privacidade nas telecomunicações[7] (Abreu; Nakagawa; Ruiz, 2016).

Os conhecimentos técnicos da ANATEL, contudo, muitas vezes eram dissociados da vontade política de editar e tramitar leis que buscassem exclusivamente a proteção dos dados pessoais. Pode-se dizer até que a discussão sobre privacidade na internet, mesmo antiga e muito recorrente, passou a ser melhor noticiada pela mídia recentemente a partir da exposição de diversas repercussões negativas do desenvolvimento tecnológico desconectado da regulação, como é o exemplo da divulgação de diversos escândalos de invasão de privacidade por *hackers*, divulgação de conteúdo íntimo (muitas vezes relacionado ao que hoje se chama pornografia de vingança), além de pirataria, violação de direitos autorais, dentre outros.

Em razão dessas divulgações, houve o surgimento de outras vontades políticas para institucionalizar e regular diretrizes sobre o uso da *internet*, o vazamento de dados, fraudes e crimes cibernéticos[8]. Em 2012, por exemplo, foi noticiado um vazamento de fotos íntimas da atriz de televisão Carolina Dieckmann, através da invasão de seu conteúdo pessoal por *hackers*. Foi um crime muito divulgado no noticiário e que conseguiu instigar no legislador o ânimo de editar, no mesmo ano, a da Lei n. 12.737 de 30 de novembro. Esta trata-se de uma iniciativa que buscou tipificar delitos informáticos, como a invasão de computadores pessoais e outros dispositivos, na tentativa de coibir e conseguir enquadrar como ilícito as condutas praticas por *hackers* que disponibilizavam na rede conteúdo de terceiros de forma não autorizada[9].

---

consumidor;
XII - à reparação dos danos causados pela violação de seus direitos."

[7] São exemplos a Resolução n. 426/05 – Regulamento do Serviço Telefônico Fixo Comutado -, a Resolução 477/07 – Regulamento sobre o Serviço Móvel Pessoal, e a Resolução 614/13 – Regulamento do Serviço de Comunicação Multimídia)

[8] Gonçalves, Bertotti e Muniz (2015) destacam o avanço dos crimes cibernéticos e dos problemas de fraude e ataques na rede como decorrentes do aprimoramento constante do sistema de comunicação e troca de conteúdo dentre ausentes. Assim, o próprio desenvolvimento do processo comunicativo, associado ao aumento de lucros em razão da manipulação e do tratamento de dados pessoais, fizeram surgir tais problemas na internet.

[9] A lei dispõe "sobre a tipificação criminal de delitos informáticos e dá outras providências", nos termos de seu artigo 1º, acrescentando ao Código Penal o art. 154-A, prevendo o ilícito de invasão de dispositivo informático alheio, *"conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita*".

O poder legislativo não conseguiu, contudo, acompanhar o ritmo da realidade. Antes da edição de quaisquer leis específicas sobre crimes na internet e invasão de privacidade para divulgação de conteúdo virtual impróprio, diversas demandas similares já haviam alcançado o poder judiciário, muitas delas na tentativa, inclusive, de ensejar a responsabilidade objetiva dos provedores de conteúdo e de internet por permitirem a divulgação desautorizada de conteúdo difamatório. É o caso do Recurso Especial n. 1.193.746/SP, julgado pelo Superior Tribunal de Justiça ainda em 12.04.2010.

Trata-se de um dos primeiros julgados de uma consolidada construção jurisprudencial da Corte no sentido de evitar a censura da informação transmitida ou colocada na rede, mesmo que possa implicar, futuramente, em ofensa aos direitos de outros indivíduos. Isso porque não caberia ao provedor do conteúdo, que muitas vezes atua apenas como plataforma, que apenas disponibiliza a informação, decidir o que tem potencial violador ou não, ou até o mesmo o que está sendo difundido contra a vontade do detentor daquele conteúdo. Confira-se a ementa do mencionado recurso especial, um julgado paradigmático para o assunto, de relatoria da Ministra Nancy Andrighi:

> "DIREITO CIVIL E DO CONSUMIDOR. INTERNET . RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA.
> 1. A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei no 8.078/90.
> 2. O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração" contido no art. 3o, § 2o, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor.
> 3. A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos.
> 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02.
> 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.

> 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo .
> 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet .
> 8. Recurso especial a que se nega provimento."

A Corte entendeu, portanto, que caberia ao provedor realizar a retirada da informação somente quando notificado da violação do direito de personalidade de terceiro, ou do seu potencial violador, sob pena, de ser, então, responsabilizado subjetivamente. É o que se chama de "*notice and takedown*", mecanismo de responsabilidade importado do direito autoral como forma de impor ao provedor uma obrigação de agir: a partir da notificação, o conteúdo deve ser retirado. A crítica feita a essa abordagem é a de que, ao mesmo tempo em que surge uma imunidade para o provedor pela inércia decorrente da própria existência do conteúdo, quem sofreu o dano fica sem efetiva reparação até o momento da notificação, enquanto o conteúdo indevido continua a ser compartilhado (Schreiber, 2015).

O julgado acima transcrito ainda traz outra nuance importante e que também foi consolidada pelo STJ: a existência de relação de consumo na internet. Sob a alegação dos provedores, inexistiria uma relação de hipossuficiência entre usuário e fornecedor de serviço, uma vez que o acesso às redes de conteúdo é gratuito. Contudo, a Corte Superior entendeu que mesmo não havendo cobrança, os provedores conseguem auferir vantagens indiretas, o que deve provocar um entendimento amplo da inteligência do Código de Defesa do Consumidor quanto aos prestadores de serviço. Ainda sim, seria uma relação de consumo excepcionada pela responsabilidade subjetiva, e não objetiva, uma vez que devem ser retiradas, após uma notificação prévia, as opiniões que denigrem a imagem de terceiros. Sobre a defesa do consumidor na internet, também é importante destacar o Decreto Lei n. 7.962, de 15 de março de 2013, que tentou regulamentar alguns aspectos da contratação no comércio virtual, mas deixou de se aprofundar nas discussões sobre retenção e uso de dados pessoais (Abreu; Nakagawa; Ruiz, 2016, p. 15).

Algum tempo depois das primeiras leis regulamentando discussões sobre internet, e das primeiras construções jurisprudências, diversos setores da sociedade civil conseguiram consolidar o fruto de reuniões oriundas ainda de 2007: uma nova iniciativa que buscou reunir os entendimentos da jurisprudência e da doutrina sobre os princípios e orientações de condutas no espaço da internet. Foi quando se editou o chamado Marco Civil da Internet, a Lei n. 12.965, sancionada em 23 de abril de 2014.

Seu art. 1º estabelece "princípios, garantias, direitos e deveres para o uso da internet no Brasil, e determina as diretrizes para a atuação da União, dos estados, do Distrito Federal e dos Municípios em relação à matéria". A partir desse primeiro dispositivo, percebe-se que foi uma organização legislativa pautada em princípios fundamentais para a atuação de diversos agentes, buscando sempre valorizar a privacidade e a liberdade de expressão, além de reconhecer,também, a estrutura da internet como mundial (Madalena, 2016, p. 9).

Dessa vez, observou-se uma elaboração mais sofisticada da lei, que se preocupou em vincular o uso da internet aos valores constitucionais, tais quais a liberdade de expressão (art. 2º, caput), o desenvolvimento da personalidade (inciso II), a pluralidade, a diversidade (inciso III) e a função social da rede (inciso VI). Além de regular propriamente o uso da internet no Brasil, o Marco Civil estabeleceu diretrizes gerais que precisam ser seguidas pelos provedores de rede e pelos usuários, atribuindo deveres quanto ao armazenamento de dados e divulgações de informações, e estabelecendo responsabilidades sobre vazamentos e armazenamento de dados. A atividade fiscalizadora do Estado também foi vinculada ao respeito dos princípios da internet.

Os entendimentos jurisprudenciais, em certa medida, também foram relacionados no Marco Civil, o que mostra ainda mais sua importância. Como no acórdão de relatoria da Ministra Andrighi, mencionado anteriormente, não serão responsabilizados objetivamente, por conteúdo de terceiros, aqueles provedores que disponibilizam ferramentas para divulgação de informações. A ideia se manteve no Marco Civil, reforçando a imunidade dos provedores no mecanismo de "*notice and takedown*" (Shereiber, 2010), com a diferença de que, não basta uma simples notificação requerendo a retirada do conteúdo a fim de que seja imputada a responsabilidade, mas sim uma ordem judicial. É de se ressaltar, contudo, que essa opção legislativa recebeu certas críticas por demandar a intervenção do judiciário para obrigar a retirada do conteúdo. O texto da

lei também isenta da responsabilidade o provedor que demonstrar impossibilidade técnica no cumprimento da decisão, o que acirrou ainda mais a opinião contrária (Teffé, 2015).

O Marco Civil da Internet consolida um processo de colaboração de diversos setores da sociedade civil, mas acabou por não suprir certas lacunas importantes para a regulação dos direitos na internet. Ainda assim, percebe-se que foi uma iniciativa precursora, e que instigou a vontade política sobre o tema, tornando suas discussões mais profundas e persistentes com as diversas iniciativas em trâmite nos órgãos legislativos (Garcia, 2016). Dentre as lacunas relevantes, destaca-se a ausência de normas dispondo especificamente sobre a proteção de dados, a qual ainda pende de regulação (Abreu; Nakagawa; Ruiz, 2016). Exemplo disso é que inexiste, no país, uma autoridade independente, exclusiva, de atuação nacional e de conhecimento técnico que trate exclusivamente sobre a proteção de dados pessoais e seus diversos desdobramentos (Kira; Tambelli, 2016).

Também inexiste um complexo normativo unitário, capaz de consolidar percepções doutrinárias, entendimentos jurisprudenciais, formas de garantir o acesso ao conteúdo e às bases, quais os crimes tipificados, ou até mesmo os princípios direcionados exclusivamente a esse tipo de tutela da privacidade (Doneda, 2011). O Marco Civil da Internet tentou representar esse regulamento, mas sua generalidade, até em razão da necessidade de abranger diversos pontos do direito relacionado à internet, fez com que as matérias de proteção de dados pessoais e privacidade fossem abordadas de forma superficial[10].

Para o presente estudo, essa discussão é importante porque, em meio a lacunas, sobreveio a Lei n. 13.444/2017, a ser analisada no terceiro capítulo, mas que, adiantando, explora justamente a ausência de proposições e diretrizes claras e específicas sobre o armazenamento de dados pessoais em bancos de dados administrados para o governo.

[10] No intuito de suprir tais lacunas, tramita hoje na Câmara dos Deputados o PL 5.2672016, sujeito à apreciação do plenário desde novembro de 2016. Seu principal objetivo é regulamentar o direito à proteção de dados pessoais, deixando claras as prerrogativas em relação ao tema, bem como sanções e conceitos, sempre como forma de garantir o direito fundamental de privacidade (Doneda; Schertel Mendes, 2016).

CAPÍTULO II - USO DE DADOS PESSOAIS NA ATUALIDADE

A privacidade assumiu, ao longo do tempo, a feição de proteção de dados em razão do desenvolvimento tecnológico e das mudanças sociais. Nessas circunstâncias, entender o que são dados, importa em compreender seu escopo de proteção na realidade contemporânea. Proteger a privacidade hoje, pode-se dizer, implica em buscar regulações para a forma e a razão de processamentos de dados além de regular também a obtenção, o armazenamento e o compartilhamento desse tipo de conteúdo (Andrade, 2010).

Ao relacionar privacidade e proteção de dados, por consequência, surgem diversas discussões relevantes, como a necessidade de diferenciação dos conceitos relativos aos vários de tipos de dados. Surgem também discussões sobre o uso de tais dados, seja por entres privados, notadamente na formulação e reorganização das estratégias de consumo, seja pelo próprio governo, na consolidação de novas estratégias de eficiência e estruturação de projetos políticos.

A partir de tais usos, também é importante compreender a dimensão ética envolvendo o tratamento de dados pessoais e o armazenamento desse conteúdo digital, uma vez que as discussões sobre princípios norteadores do uso da internet são globais e envolvem atenção coletiva para preservar o espaço da rede como minimamente seguro, democrático e garantidor de direitos individuais.

Essas serão algumas das discussões abordadas nesse capítulo.

II.1 – CONCEITOS

II.1.1 – DIFERENCIAÇÃO ENTRE DADOS E INFORMAÇÃO

Frequente é a confusão entre os conceitos de dado e informação. A imprecisão das diferenças costuma ser constante no diálogo e em algumas regulações sobre a matéria, sendo que isso pode acabar provocando constrangimentos aos indivíduos que buscam a tutela de seus direitos de privacidade, culminando na mitigação das garantias individuais no espaço da rede.

A distinção entre os dois conceitos se da em razão de um marco temporal de processamento. Ou seja, o dado é uma espécie de conteúdo primitivo, antes de ser efetivamente tratado, compartilhado; enquanto a informação corresponde a um conteúdo que sofreu um processo de interpretação em razão do processo cognitivo de interlocução (Doneda, 2006, p.152).

II.1.2 – CLASSIFICAÇÃO DOS DIVERSOS TIPOS DE DADOS

Existem espécies de dados que têm relação direta com a identidade de um indivíduo determinado ou determinável. Esses são os chamados dados pessoais, que possuem alto valor por representarem um conteúdo que corresponde a alguém, e que por isso pode ser utilizado de forma direcionada àquela pessoa específica.

A definição acima exposta advém da art. 2º[11] da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, 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*". É interessante destacar que se define também quem se considera pessoa singular inidentificável para fim de proteção de dados: "*identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos de sua identidade*"

Nesse sentido, portanto, para percepção correta do que é o dado pessoal, é necessário também levar em consideração o elemento da identidade como sua característica fundamental, mesmo que essa seja passível de ser atribuída de forma indireta em um segundo momento. Entende-se por identidade aquilo que define pessoas e as tornam passíveis de serem reconhecidas, diante de terceiros, por suas atitudes e características. Lessig define como algo além do que a pessoa realmente é, envolvendo também atributos, fatos, comportamentos e padrões, os quais são utilizados como formas de comunicação automática (Lessig, 2006, p. 40).

[11] A diretriz utiliza a palavra "informação", definindo dado pessoal como "*qualquer informação relativa a uma pessa singualar indetificada ou identificável*". Contudo, já foi percebeido nesse estudo que informação e dados são coisas diferrentes, consideradas a partir do momento de processamento de um determinado conteúdo.

No ordenamento brasileiro, também se reconhece a identidade como personalidade, a qual recebe uma tutela especial, justamente por representar característica fundante ao exercício da liberdade de cada um. Como desenvolvido anteriormente, a proteção dos dados pessoais corresponde a um direito de personalidade hoje em dia, uma vez que são dados diretamente relacionados à essência e ao desenvolvimento pessoal do indivíduo.

Tendo e vista a conexão direta que aquele dado faz com uma pessoa, percebe-se que os dados pessoais são uma categoria que merece atenção especial no plano jurídico, devendo representar uma grande preocupação do legislador não só por possuírem alto valor de mercado[12], como também por terem potencial lesivo substancialmente considerável[13].

Ainda sobre os dados pessoais, é importante perceber o que são dados anônimos, classificados a partir da não possibilidade de se identificar a quem aquele conteúdo diz respeito, uma vez que inexistentes os elementos que o associam a uma única identidade (Schertel Mendes, 2014, p. 79).

A partir dos critérios de identificação do dado, inclusive, surgiram relevantes discussões sobre os limites da tutela em relação ao dado anônimo e ao dado não identificável. Muitas vezes, esses dados representam um dado pessoal que foi tratado para não mais corresponder a um indivíduo específico. Isso porque a tecnologia permite, em certa medida, "anonimizar" um dado pessoal para poder compartilhá-lo dentro de padrões de segurança mais flexíveis. Contudo, a mesma tecnologia também permite a reassociação daquele conteúdo ao usuário ao qual diz respeito, podendo causar verdadeiros prejuízos a quem teve seu dado indevidamente compartilhado (Schawartz; Solove, 2011).

Mais simples do que utilizar mecanismos complexos de tratamento de dados para transformar um dado antes anônimo em pessoal, é cruzar as diversas informações de um único

[12] O uso de dados pessoais possui grande valor de troca no mercado de dados em razão da possibilidade de conectar interesses individuais com padrões de consume a partir de estratégias de *marketing* individualizadas. Ou seja, pode-se obter uma informação a partir de um dado pessoal sobre os interesses específicos de uma pessoa, para quem será direcionado exatamente o que deseja comprar, e de uma forma específica. É o que se chama de costomização do consume a partir do processamento de dados pessoais (Schertel Mendes, 2104).

[13] Caso terceiros indesejados tenham acesso aos dados pessoais, será possível identificá-los com precisão, prejudicando a segurança dos usuários. Mais que isso, como será desenvolvido a frente, podem ser processados e armazenados dados pessoais de forma ilimitada, consultados a qualquer momento e para finalidades não conhecidas dos usuários, além de poderem ser combinados para traçar a identidade e perfis específicos, facilitando mecanismos de influência e manipulação das vontades. (Doneda; Schertel Mendes, 2016, p.4).

banco de dados a partir de padrões específicos que também permitem definir a identidade do usuário a quem o conteúdo se refere. (Schawartz; Solove, 2011).

Quanto aos dados anônimos passíveis de serem identificáveis, também existe a preocupação de proteger deduções e inferências relacionadas a eles. Empresas que não têm a tecnologia para relacionar a informação anônima a um indivíduo, podem trabalhar com padrões e estatísticas para se chegar exatamente a quem a informação diz respeito.

Barocas e Nissenbaum citam o exemplo dos registros médicos: enquanto um grupo consegue cruzar os registros anônimos e identificar os usuários, um outro grupo poderá desenvolver padrões que permitem estimar a probabilidade de um certo indivíduo possuir um determinado registro médico anônimo. Essa informação – que apenas corresponde à uma estatística- será compartilhada como verdadeira, podendo causar verdadeiros prejuízos ao usuário, ainda mais se ele não for o real portador, por exemplo, daquele registro médico (Barocas; Nissenbaum, 2014).

Destaca-se, ao fim, que os dados anônimos e não identificáveis têm funções importantes no cotidiano, como a de serem utilizados por pesquisas, ou para a formação e consolidação de políticas públicas de governo, por exemplo. Contudo, e como relacionado acima, seu compartilhamento indevido também pode gerar prejuízos ao indivíduo, sendo necessária atenção jurídica específica a esse tipo de conteúdo.

Enquanto a Diretiva do Parlamento Europeu sobre proteção de dados existe desde 1995, no Brasil a matéria não é regulada de maneira clara e específica. (Doneda; Schertel Mendes, 2016). O próprio Marco Civil da Internet não se prestou a preencher devidamente essa lacuna, dedicando uma seção genérica sobre proteção aos registros, dados pessoais e comunicações privadas. A proteção de dados pessoais foi consagrada no art. 3º como um princípio fundamental para a disciplina do uso da internet no país, além de terem sido especificadas garantias importantes em relação a proteção dos dados pessoais, como a coleta com finalidade justificada e somente através do consentimento (art. 7º, VIII).

Dentro dos dados pessoais, por fim, também existe uma outra classificação que diz respeito a dados ainda mais críticos em termos de eventuais violações de direitos. São os

chamados dados sensíveis, que correspondem ao conteúdo passível de ser utilizado com potencial discriminatório. Nas palavras de Danilo Doneda e Laura Schertel Mendes:

> "A diferenciação da categoria dos dados sensíveis foi consagrada pelo Convênio 108, editado pelo Conselho da Europa em 1981, em seu art. 6º. O convênio previu, em seu dispositivo voltado às "categorias especiais de dados", que os dados pessoais relativos à origem racial, saúde, vida sexual e condenações penais somente poderiam ser objeto de tratamento caso o direito interno previsse as garantias adequadas para o seu processamento"(Doneda; Schertel Mendes, 2016, p. 5).

Orientação sexual, raça, opções políticas e religiosas são alguns dos exemplos de dados sensíveis, e esses exemplos permitem caracterizar o por quê da importância de um efetivo cuidado com o armazenamento e o processamento desses conteúdos: seu uso pode ser utilizado como forma de reproduzir violências sociais ligadas ao preconceito.

Além disso, a internet é um espaço de divulgação de conteúdo de forma muito mais rápida, e que permite o acesso simultâneo de milhares de pessoas e em várias localidades diferentes. Ou seja, conteúdos preconceituosos e discriminatórios ficam disponíveis em questão de segundos para toda a comunidade virtual, em nível até mundial, causando danos que sequer podem ser dimensionados.

II.1.3 – BANCOS DE DADOS E TRATAMENTO DE DADOS PESSOAIS

Todos esses tipos de dados mencionados anteriormente podem ser armazenados em grandes bancos de conteúdo. São os chamados bancos de dados, que correspondem a "um conjunto de informações organizadas segundo uma determinada lógica" (Doneda, 2006, p. 158). Esse tipo de tecnologia existe para sistematizar dados obtidos e armazená-los ao longo prazo, sempre buscando aproveitar aquele tipo de conteúdo ao máximo possível (Doneda, 2011, p. 92).

No Brasil, a proteção ao acesso do conteúdo armazenado em bancos de dados representa inclusive um valor constitucional, tutelado através do *habeas data*: uma ação que garante conhecimento e acesso aos bancos de dados públicos e de entidades governamentais. Pode-se dizer, contudo, que essa tutela não atua em consonância com a efetiva proteção dos direitos de

proteção de dados, uma vez que o texto constitucional fica limitado ao acesso dos dados apenas para eventual retificação de seu conteúdo, quando a informação se mostrar inverídica com a realidade (Mendes; Branco 2014, p. 799-800).

A existência dos bancos de dados facilita a realização de todas as operações que podem ser feitas com aqueles dados, uma vez que o conteúdo se encontra unificado em um único sistema. Dentre as operações possíveis, destaca-se o tratamento dos dados, que corresponde a uma operação (técnica ou não), que permitem refinar o conteúdo a partir de organização, alteração, consulta ou difusão, por exemplo, daquele dado[14]. (Schertel Mendes, 2014, p. 58).

Foi o armazenamento de conteúdos em bancos, aliado, novamente, aos avanços na tecnologia, que permitiram formas de tratamento de dados cada vez mais inovadoras, rápidas e de baixo custo, promovendo uma verdadeira revolução no comércio, na forma de governar e de se relacionar.

II.1.4 – *BIG DATA*

Ao fim, também cabe destacar o conceito de *big data*: um determinado dado com capacidade de processamento de conteúdo muito elevada e superior à existente nos dados usuais. Confira-se:

> "[...]*big data*, um sistema intenso de processamento de informações que trafegam em internet (dados sensíveis, públicos, sigilosos ou de qualquer outra natureza), possibilitado por softwares e equipamentos que trabalham com um volume maciço destes dados e que são utilizados em áreas das mais diversas, algumas das quais sequer claramente definidas, gerando um mundo onde a característica maior é a formação de valor ao dado coletado." (Simão Filho; Schwartz, 2016).

[14] Uma definição completa sobre tratamento de dados pode ser encontrada na Diretiva 95/46/CE do Parlamento Europeu: "Tratamento de dados pessoais (tratamento): qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como o recolhimento, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição."

Definido a partir do conceito dos "3 Vs", o *big data* corresponde a um dado veloz, variado e de grande volume, desenvolvido para ter mais conteúdo, ser processado de uma maneira mais rápida, e em um espaço de armazenamento menor. Suas características sugerem um custo elevado, e, portanto, inacessível. Mas a verdadeira revolução desse tipo dado corresponde ao seu baixo custo, com um valor associado suportável tanto aos interesses públicos quanto aos privados, permitindo sua difusão em larga escala (Dumbill, 2012).

O uso desse tipo de dado trouxe diversas discussões éticas sobre armazenamento e tratamento de dados. Isso porque, antes, o tratamento de dados pessoais era mais moroso ao relacionar os diversos conteúdos armazenados. O *big data*, contudo, trouxe uma inovação em termos de eficiência, mas uma preocupação relacionada à alta capacidade de compilar conteúdo de uma forma barata, facilitando o tratamento de dados pessoais e aumentando a disparidade de poder que existe entre o detentor do dado e o usuário. Essa discussão será detalhada adiante.

II.2 - UTILIZAÇÃO E ARMAZENAMENTO DE DADOS NO COMÉRCIO

A tecnologia que permite a existência de bancos de dados facilitou e revolucionou, de certa forma, as formas de relacionamento entre ausentes. Surgiram novos mecanismos para favorecer a comunicação e o compartilhamento de conteúdo, facilitando o contato, a troca de experiências, e as múltiplas relações que, antes desenvolvidas exclusivamente sob a forma presencial, hoje são cada vez mais presentes na realidade da internet (Gonçalves; Bertotti; Muniz, 2015).

O comércio é um exemplo dessa facilidade: antes, a troca só era feita em espaços físicos específicos, impossibilitando a relação de compra e venda de várias pessoas simultaneamente, ou de lugares distantes. Da mesma forma, existe um custo relacionado à gestão do espaço físico e ao emprego de trabalhadores para viabilizarem as relações. Pela internet, contudo, foi possível aumentar as possibilidades de venda, tornando uma loja acessível as vezes até em escala mundial. Isso, obviamente, veio associado a uma redução de custos, uma vez que não era mais necessário organizar lojas físicas em vários locais, mas tão-somente uma única estrutura de rede capaz de enviar a mercadoria para o local que o consumidor desejasse.

Surge para o comércio na internet uma noção de infinitude, uma vez que um objeto ocupa vários lugares ao mesmo tempo, permitindo a aproximação entre os múltiplos usuários e as várias estruturas que se formam. Ou seja, um produto antes intangível torna-se acessível a várias pessoas de localidades múltiplas, a partir de um espaço compartilhado em que o acesso supera qualquer barreira territorial.

A verdadeira revolução no comércio, contudo, diz respeito ao uso dos dados pessoais produzidos em rede como forma de facilitar ainda mais o acesso às plataformas de venda e de criar estratégias individualizadas de divulgação e *marketing*, cada vez mais direcionadas e imperceptíveis ao consumidor, para que ele sinta que o desejo do consumo não está sendo induzido pelo mercado, mas sim que advém de sua própria vontade. Hoje, essas estratégias envolvem análise de dados para traçar um tipo de padrão de consumo do usuário e direcionar os anúncios, baseando-se nas preferências de cada um. Trata-se de uma estratégia behaviorista, porque cria o marketing individualizado a partir do comportamento do usuário, analisado e moldado com as informações obtidas na coleta de dados (Solove, 2011, p. 1849).

Os dados produzidos e armazenados das mais variadas formas acabaram por aprimorar ainda mais as estratégias de estímulo ao consumo, tornando o desejo de consumir algo incutido no consumidor a partir de uma programação personalizada de acordo com os interesses de cada um, e descoberta através do tratamento de dados pessoais (Madalena, 2016). A capacidade de persuadir o consumidor a adquirir determinado produto é aprimorada pela tecnologia, permitindo que as estratégias de marketing sejam substituídas (ou acrescidas) de mecanismos de manipulação da vontade: há uma falta de obviedade nos anúncios, direcionados exclusivamente para aquele consumidor específico, acarretando uma manipulação do desejo e da vontade de comprar.

Pode-se dizer que houve uma espécie de "dataficação" da vida: os aspectos do cotidiano transformaram-se em dados que são armazenados em bancos por tempo indeterminado, para que empresas possam criar perfis de consumo sobre os usuários e traçar estratégias de como vender cada vez mais (Rhoen, 2015, p. 53). A discriminação, por sua vez, também representa outra preocupação importante: a tecnologia de tratamento de dados permite que as empresas criem rankings de consumo, dando tratamento diferenciado a certos consumidores em razão de suas preferências ou experiências (Lessig, 1999).

Como o *big data* também produz significativa influência na indústria do consumo, é importante preservar o consumidor nos contratos firmados pela internet e até no próprio exercício da escolha. Isso porque o conceito de hipossuficiência do consumidor é levado para outro nível quando se pensa em um tipo de dado que possui um conhecimento prévio sobre o indivíduo a quem se quer vender determinado produto ou serviço. É por isso que as instituições reguladoras têm importante papel na defesa dos interesses do consumidor, como forma de evitar que a tecnologia figure como obstáculo à privacidade (Rhoen, 2015).

É de se destacar, também, que a aplicação do Código de Defesa do Consumidor (CDC) nas relações de consumo da internet representou um significativo reconhecimento da importância de regular esse espaço virtual. Não só através das construções jurisprudenciais evidenciadas anteriormente, como também das iniciativas legislativas que estão sendo discutidas e que foram aprovadas, notadamente o Marco Civil da Internet, observa-se que existe a preocupação de reforçar a proteção ao consumidor em diversos momentos do uso da rede: desde o recebimento da conexão, passando pelo momento da recepção da propaganda personalizada (sendo que essa ainda merece uma especial atenção), até a concretização da compra virtual. Essa preocupação fica evidente no artigo 7º do diploma legal, em que se criam padrões para a manutenção da qualidade contratada da conexão da internet ou do acesso às informações (Madalena, 2016, p.11).

II.3 - GESTÃO E CONTROLE: USO DE DADOS POR PARTE DO GOVERNO

Diversos são os usos do tratamento e armazenamento de dados para o governo. A partir do processamento inteligente, é possível organizar políticas públicas direcionadas para cada comunidade, como às de inclusão de gênero ou raça; fazer monitoramento de áreas de risco, inacessíveis para o sistema policial ou de salvamento; viabilizar a integração de áreas remotas de determinado local a partir da coleta de informações, dentre outros exemplos.

Fato é que vivemos em uma sociedade modernizada em razão da tecnologia, inclusive no que diz respeito à vigilância. O governo, portanto, é um dos grandes interessados nesses desenvolvimentos, porque poderá otimizar recursos para desempenhar suas tarefas de forma mais eficiente e barata. Afinal, para muitos, a tecnologia representa exatamente isso. Frequentemente,

é necessário discutir os limites dessa atuação de fiscalização por parte do Estado, sob risco grave de se impor uma violação aos direitos fundamentais dos usuários de forma despropositada. Novamente, os critérios para imposição de poder do Estado em relação aos indivíduos precisam ser muito bem delimitados, mas nem sempre eles se mostram suficientes.

Daniel Solove (2007) realizou uma pesquisa acerca da opinião dos cidadãos quando da invasão de privacidade sob a escusa da proteção nacional. O contexto base da pesquisa é o da chamada guerra ao terror norte-americana[15], no governo de George W. Bush, citando como exemplo específico a edição secreta de atos de governo que permitiam o acesso às ligações telefônicas dos cidadãos americanos em nome da defesa da segurança nacional. A surpresa da pesquisa foi o uso frequente do que se pode traduzir por "quem não deve, não teme"[16], sugerindo que a vigilância excessiva do governo só seria prejudicial para aqueles e aquelas que efetivamente estivessem cometendo alguma atitude questionável. O que o autor gostaria que a população participante de sua pesquisa tivesse percebido é que a violação da privacidade não prejudica somente quem tem segredos, mas sim a toda a coletividade (Solove, 2007).

Essa questão é interessante e atual, principalmente quando se pensa no recorrente discurso dos entes da administração pública para promoverem políticas de fiscalização como formas de gestão sem a devida atenção aos direitos de privacidade. No caso da guerra ao terror de George W. Bush, por exemplo, o combate ao terrorismo organizado como política de governo era a desculpa para fiscalizar diversos cidadãos de forma despropositada, incorrendo em violações de direitos com proporções até hoje não definidas.

Especificamente quanto aos mecanismos de fiscalização e vigilância, é necessário considerar que o monitoramento de atividades, como feito hoje, já implica em violações à privacidade. Um exemplo é o uso câmeras que conseguem captar imagens e reconhece-las, identificando também padrões de comportamento previamente programados, expondo o cidadão e o que ele estiver fazendo para o Estado. Tais violações, contudo, são permitidas pela legislação em razão da tutela de um bem social maior e comum a todos, qual seja o da segurança coletiva, e somente são toleradas em razão da garantia que o próprio Estado da aos cidadãos de que essas

[15] Utiliza-se a expressão de "guerra ao terror" para nomear o momento vivido nos Estados Unidos da América, pós atentado de 11 de setembro de 2001, em que se perseguiam grupos terroristas possivelmente responsáveis pelo atentado em solo americano.
[16] Tradução livre para "*I've got nothing to hide*".

informações obtidas são sigilosas e não serão divulgadas para terceiros, sendo utilizadas somente em atenção a uma finalidade específica que é a de controle da segurança (Klang, 2005).

Outros exemplos são também excepcionados pela Constituição Federal, a qual permite, em algumas situações, a mitigação da privacidade individual em nome da segurança e da proteção ao bem público maior. Contudo, essas circunstâncias são muito bem definidas, a fim de não criarem relações de abuso do Estado face ao cidadão. Destaca-se a possibilidade de se ter a interceptação telefônica para obter provas sobre possíveis crimes, sendo que essa autorização somente é permitida quando já está em curso uma investigação criminal, e a partir da existência de autorização judicial. (art. 5º, XII da Constituição Federal e Lei n. 9.296, de 24 de julho de 1996).

É nesse sentido que se percebe que a própria atuação do Estado para fiscalizar os indivíduos deve encontrar limites relacionados à própria finalidade da obtenção dos dados e também no interesse público, no interesse da justiça ou no interesse social, situações em que se justifica a relativização de certas garantias em benefício ao bem coletivo (Ferraz Junior, 1993, p. 452). Ainda sim, mesmo com os limites impostos, cabe ressaltar o que Lessig diz sobre a capacidade de controle do individuo por parte do Estado: se existe o conhecimento sobre quem o indivíduo é, onde está e o que está fazendo (e esse conhecimento de fato existe através dos dados), então é possível controlar esse sujeito, regular seu comportamento (Lessig, 2006, p. 38).[17]

Há ainda uma outra dimensão de fiscalização que não por vigilância, mas através do cruzamento e armazenamento de dados cadastrais. Esses são dados utilizados na identificação dos cidadãos a fim de garantir acesso ao mundo jurídico e ao exercício dos direitos fundamentais, além de viabilizarem a relação entre o indivíduo e o Estado. São exemplos de dados cadastrais o Registro Geral (RG) e o Cadastro de Pessoas Físicas (CPF) (Kang; Santos; Doneda, 2016).

A proteção a esses dados envolve a proteção direta do próprio indivíduo, uma vez que são documentos altamente identificadores de cada cidadão, e que, se divulgados indevidamente, acarretam não só a violação aos direitos de privacidade e intimidade, como também um grave risco à segurança individual (Ferraz Junior, 1993. P. 450). Grande parte desses dados cadastrais,

[17] É importante destacar, contudo, que Lessig entende a regulação como fundamental para evitar esse tipo de circunstância que, ao seu ver, não ocorre de forma arquitatada pelo governo, mas sim pelo mau uso da internet e pelo uso de dados pessoais no comércio (Lessig, 2006, p. 38).

até o momento da edição da Lei nº 13.444/2017, que será analisada adiante, encontram-se armazenados em bases de dados dispersas do governo, o que permite criar um certo equilíbrio na relação de poder entre o Estado e cidadão.

Destaca-se a proteção da confiança, necessária para que o cidadão tenha segurança de que seus dados, em posse do governo, serão devidamente preservados. Sabendo do risco que a análise desses dados pode implicar aos usuários, é importante considerar as limitações éticas necessárias para seu uso, como será explicado abaixo.

II.4 - PRINCÍPIOS E LIMITAÇÕES ÉTICAS DO USO DE DADOS PESSOAIS

A coleta de dados pessoais permite uma assimetria relacional entre o usuário e quem realizou a coleta e o armazenamento de seus dados. Essa assimetria que promove organizações hierárquicas de poder e que facilitam mecanismos de instrumentalizar manifestações, manipular vontades e influenciar comportamentos individuais. Vive-se hoje em uma sociedade abastecida de informação e organizada em razão de poder, sendo que muitas vezes se questionam os sentidos dessa relação, as formas de dominação e o que se pode fazer para ter o mínimo controle sobre esse processo. Assim, algumas questões éticas para o compartilhamento de dados devem sempre ser preservadas, sob risco de fortalecerem ainda mais os mecanismos de poder e influência de determinados agentes (como o Estado).

Tais preocupações aumentaram quando se percebeu o rápido crescimento da informação produzida em meio digital, oportunizado pela fácil capacidade de se coletar, transmitir, alocar e manipular dados; pelo baixo custo que as operações de tratamento de dados assumiram em razão do desenvolvimento tecnológico; pela própria natureza da informação digital, que consegue ser processada de forma mais eficiente e eficaz se comparada com a informação difundida em outros meios; e pela própria dinâmica de operação de sistemas de computadores e de rede, que acabam por promover um ciclo vicioso gerando mais dados a partir do processamento de dados anteriores (Klang, 2005, p. 193). Esses também foram os fatores que deram início ao *big data*, um dado com potencial muito mais lesivo do que os demais e que também representa a total ausência de

controle que se tem sobre o desenvolvimento tecnológico que envolve o tratamento de dados pessoais.

Somado ao desenfreado desenvolvimento da tecnologia, que proporcionou a criação diária de novas ferramentas facilitadoras do cotidiano, as diversas discussões sobre privacidade acabaram por intensificar, também, as discussões sobre armazenamento de dados, cruzamento de informações, divulgação e compartilhamento. Quando se pensa na esfera do privado como forma de proporcionar o maior exercício das liberdades, deve-se pensar também que em um espaço que seja capaz de proporcionar diversidade de escolhas, ações, opções políticas, sempre de forma a promover um fomento da diversidade e um sentido de responsabilidade relacionada à proteção da privacidade no meio coletivo (Nissenbaum, 2010). Tornou-se necessário, portanto, destacar aspectos de atuação dos diversos agentes da internet como forma de integrar valores constitucionais também ao espaço virtual.

Um dos primeiros aspectos que se destacam diz respeito à necessária proteção das relações de confiança quando do compartilhamento dos dados individuais. Certos tipos de conteúdos precisam ser compartilhados, seja como forma de acesso a algumas páginas da internet, seja como forma de acesso às garantias individuais perante o Estado, e devem continuar, se assim for necessário, confidenciais. Ou seja, o simples compartilhamento de informações divididas com terceiros ocorreu em razão de uma relação prévia de confiança, impossibilitando a divulgação indiscriminada desse conteúdo (Richards; King, 2014).

O tratamento do *big data* também causou diversos constrangimentos, uma vez que é capaz de criar uma influência programada em diversos comportamentos, desde namorar ou votar, até proporcionar a identificação de terroristas. Isso porque a tecnologia envolvendo esse tipo de dado é muito complexa e envolve uma capacidade de armazenamento significativo, em quantidades muito elevadas, que podem processadas de uma forma muito rápida. Ou seja, a leitura desse tipo de dado consegue extrair muito mais informações utilizáveis, e que conseguem ser manipuladas para influenciar relacionamentos, comportamentos e interações sociais (Richards; King, 2014, p. 405). Seu uso para o governo, por exemplo, representa um conhecimento prévio do Estado sobre comportamentos dos cidadãos, grupos organizados, decisões a serem tomadas, simplesmente através do acesso da informação produzida (Richards; King, 2014, p. 406).

É de se ressaltar ainda que o *big data* envolve um processamento intenso de diversos tipos de dados diferentes, sejam dados sensíveis, anônimos, sigilosos, ou de qualquer espécie. Os equipamentos que analisam esse tipo de conteúdo envolvem softwares complexos, utilizados muitas vezes de forma indefinida, e que acabam favorecendo a vigilância indiscriminada (Simão Filho; Schwartz; 2016, p. 7). Confira-se:

> "O resultado prático se faz no sentido de que, com um *big data* em ação, decompondo sistematicamente os dados estruturados e não estruturados, torna-se possível desenvolver negócios dos mais diversos como demonstrado monetizando o banco de dados, como também operar preditivamente, prevendo comportamentos, identificando padrões e descobrindo o porquê de muitas coisas, além de incentivar o consumo e criar políticas internas empresariais para otimizar resultados e auxiliar na tomada de decisão relacionada, entre outros assuntos, ao enfrentamento de crises econômicas, mercados concorrentes ou geração de nova demanda.
> O sistema *big data* possibilita o cruzamento de dados numa velocidade e precisão espantosa, cujas consequências são inúmeras em seus resultados como, a exemplo, contribuir para localização de hábitos de consumo, conhecimento de grupos de pessoas propensas a sofrer moléstias custosas, detecção de jovens com maior probabilidade de incidir em crimes, verificação de hábitos religiosos e localização de pessoas por geolocalizadores." (Simão Filho; Schwartz; 2016, p. 11).

Portanto, não é mais suficiente armazenar o conteúdo e compartilhá-lo como forma de obter informações sobre os comportamentos de um certo indivíduo com o objetivo, por exemplo, de lhe vender um determinado produto. As formas de tratamento de dados atuam, hoje em dia, traçando perfis detalhados sobre os usuários, para obter o máximo possível de informações sobre aquele indivíduo, atuando, ainda, em um momento anterior: não basta conhecer o indivíduo, mas é preciso também moldá-lo para que ele tenha interesse em agir de determinada forma, comprar aquele produto ou agir em conformidade com um padrão do aceitável.

A coleta sistematizada de dados, agregação de conteúdo, uso do *big data*, por exemplo, acabam levando, portanto, à coerção, para que determinadas condutas sejam impostas na comunidade; à falta de autonomia e à manipulação, uma vez que o tratamento dos dados interfere diretamente na capacidade do indivíduo de pensar sem ser influenciado (Nissenbaum, 2010).

Esses riscos apresentados só podem ser dirimidos com a adoção dos princípios norteadores do uso da internet, a fim de diminuir os riscos de violações decorrentes do uso das novas tecnologias de processamento de conteúdo. Notadamente o respeito à privacidade dos usuários por parte dos agentes, combinado com políticas públicas e regulação forte, são

fundamentais por atuarem como formas de limitação do exercício do poder desenfreado decorrente da posse de dados pessoais. Preservar a finalidade dos dados obtidos, a confidencialidade e o acesso do usuário a que os dados dizem respeito também são formas de garantir que o processamento intenso do conteúdo não seja tão lesivo (Richards; King, 2014, p. 419).

Destaca-se, ainda, que o tratamento de dados pessoais criou uma indústria burocrática e desumanizadora, que analisa comportamentos individuais a partir de padrões matemáticos previstos pela coleta de informações. A adoção de princípios e a consideração das desigualdades relacionais existentes entre os agentes e os usuários da rede são algumas garantias para os usuários de que estes não serão reféns dos padrões pouco rigorosos e não transparentes, tornando a rede um espaço mais humano. O Marco Civil da Internet, como mencionado anteriormente, consolidou muitos desses princípios, e sua importância mais significativa reside em figurar como um diploma que orienta o uso da internet no país em atenção à preservação da personalidade, privacidade, e da garantia de direitos, diversidade e acesso.

Dentre alguns princípios necessários para instruir o uso da internet, destacam-se: (i) garantir que os dados armazenados correspondem ao real (princípio da exatidão); (ii) ter conhecimento sobre a finalidade para a qual esses dados serão utilizados (princípio da finalidade); (iii) ter acesso aos dados armazenados (princípio do livre acesso); (iv) e assegurar que existem precauções tomadas para evitar extravio, modificação ou acesso não autorizado dos dados (princípio da segurança física e lógica) (Doneda, 2011, pp. 100-101).

A transparência e o acesso ao conteúdo armazenado merecem destaque em relação aos demais princípios. Representam verdadeiras garantias fundamentais para o exercício da personalidade, bem como formas de controle do uso dos bancos de dados. Nesse sentido, esses princípios justificam a necessidade de bancos de dados serem de conhecimento público: além de ser uma forma de controle sobre o armazenamento indiscriminado de dados, é também uma forma de assegurar ao usuário conhecimento sobre o conteúdo existente sobre si (Doneda, 2011, p. 100).

Existem ainda razões morais para se pensar a proteção da privacidade, que se justificam por serem motivos ensejadores de discriminações. Considerá-las implica considerar dimensões do

uso da internet que transcendem o simples comportamento individual, uma vez que são características estruturais das formas de organização da rede. Da mesma maneira, são importantes para se pensar em formas de tentar se promover a igualdade, a justiça e a autonomia. A primeira delas é a possibilidade de risco das informações transmitidas, uma vez que a divulgação irrestrita de dados fiscais, de registro, além de senhas e endereços, propiciou o surgimento de diferentes tipos de crimes cibernéticos (Nissenbaum, 2010, p. 78).

A desigualdade de informação também seria uma dessas razões morais. Essa seria uma razão decorrente do não acesso e da transparência de dados, uma vez que os múltiplos usuários e atores da sociedade não tem conhecimento verdadeiro sobre os mecanismos de coleta de dados, o que está sendo coletado e qual a sua forma de uso. Além disso, a coleta seletiva de dados pessoais e seu uso desconhecido acarretam em tratamento diferenciado entre os diversos usuários da rede, o que pode provocar verdadeiras distorções no convívio social, além da reprodução de padrões discriminatórios (Nissenbaum, 2010, p. 79).

A injustiça da informação, por sua vez, corresponde ao compartilhamento de informações de maneira irrestrita, transferindo um conteúdo de uma base de dados com uma finalidade específica e de prévio conhecimento por parte do usuário, para uma outra base de dados que fará uso do conteúdo de forma desconhecida. Por fim, também é importante pensar na autonomia moral do usuário, de forma que as regulações sobre proteção de dados possibilitem ao indivíduo se determinarem em acordo com suas histórias e desejos, fugindo de um padrão único e impositivo (Nissenbaum, 2010, p. 80-81).

Fica claro, portanto, que os princípios funcionam como certas formas de garantir ao usuário que seu conteúdo será armazenado em atenção a padrões pré-determinados, que consideraram a eventual falta de equilíbrio entre o usuário e os agentes que armazenam o conteúdo. Essas garantias fortalecem a proteção dos dados pessoais, criando uma barreira de limitação ainda maior para regulação das relações assimétricas existentes na internet.

CAPÍTULO III - ANÁLISE DA LEI Nº 13.444, DE 11 DE MAIO DE 2017

III.1 - INICIATIVA LEGISLATIVA

Em 07 de março de 2017, o Presidente da República encaminhou ao Senado Federal o Projeto de Lei da Câmara n. 19 de 2017. A proposta encaminhada propunha a criação do Documento de Identificação Civil Nacional (DIN), a ser emitido pela Justiça Eleitoral, ou por delegação do Tribunal Superior Eleitoral, como um documento de fé pública, válido em todo o território nacional. A proposta da DIN buscaria reunir em um único cartão diversos documentos de identificação civil, cujas informações seriam abastecidas por um grande banco de dados a fim de compilar todos os dados cadastrais dos cidadãos brasileiros.

Uma primeira minuta desse Projeto de Lei chegou a ser submetida pelo ex-Ministro da Justiça, José Eduardo Cardozo, à ex-Presidenta da República, especificando os seus objetivos principais. Confira-se:

> "Nesse sentido, pretende-se promover a interoperabilidade entre essas bases de dados, como forma de criar o Registro Civil Nacional - RCN, cujo número, atribuído pela Justiça Eleitoral, permitirá identificar o cidadão com segurança. Vale destacar que não se está pretendendo impor um documento único nem criar um documento novo, pois o documento de RCN poderá futuramente substituir o título de eleitor e conterá diversas informações e números oriundos de outros órgãos do Poder Público, com a finalidade de simplificar, com segurança, a identificação do cidadão."

Contudo, somente no governo do atual presidente Michel Temer é que a proposta foi devidamente encaminhada ao Senado Federal. O tempo de tramitação da proposta é uma das primeiras evidências de que o projeto poderia ter sido melhor discutido com a população, principalmente com setores especializados nas discussões técnicas sobre gestão e uso de banco de dados pessoais. Foi feita uma consulta pública em que se apurou a participação de apenas151 pessoas, sendo 141 favoráveis à criação da DIN e 10 contrárias[18].

[18] Informação disponível em:< https://www25.senado.leg.br/web/atividade/materias/-/materia/128224#tramitacao>. Último acesso em 04.06.2017.

A tramitação na Comissão de Constituição e Justiça (CCJ) do Senado Federal também ocorreu de forma bastante célere. O parecer elaborado pelo relator do projeto na comissão, o Senador Antonio Anastasia, julgou a iniciativa como louvável, "porquanto para contribuir para a eficácia da identificação do cidadão para todos os atos da vida civil"[19]. Consideraram-se preenchidos os requisitos constitucionais, uma vez que a União tem competência privativa para legislar sobre direito civil e registros públicos, não abrangendo qualquer debate profundo sobre proteção da privacidade e proteção de dados. A juridicidade, por fim, também foi ressaltada pelo senador como "irretocável", uma vez que representava um meio apropriado para alcance de seus objetivos, a matéria estaria cercada de inovação e originalidade, dotado de potencial coercitividade, além de ser considerada compatível com os princípios diretores do ordenamento.

Aprovado na Comissão e no Plenário do Senado, o projeto seguiu para a sanção do presidente, o que ocorreu no dia 11 de maio de 2017. Foi quando entrou em vigor a Lei nº 13.444/2017, que instituiu, além do documento único de identificação nacional, o banco de dados da Identificação Civil Nacional (INC), onde todas as informações cadastrais seriam armazenadas. Como dispõe o primeiro artigo da Lei sancionada, a ICN tem "o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados".

O artigo segundo menciona que a ICN utilizará as bases de dados biométricos da Justiça Eleitoral (inciso I), a base de dados do Sistema Nacional de Informações de Registro Civil (inciso II), além de outras informações contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou que tenha sido disponibilizada por outros órgãos (inciso III).

O armazenamento de todo esse conteúdo será feito através de uma base gerida pelo Tribunal Superior Eleitoral, responsável por garantir a atualização dos dados e demais providências necessárias, principalmente para garantir a efetiva correspondência e comunicação das informações entre os diversos sistemas eletrônicos governamentais (art. 2º, parágrafo 1º). O acesso à base de dados, inclusive, é gratuito e limitado apenas quanto às informações eleitorais para os Poderes Executivos, Legislativo, da União, Estados, Distrito Federal e Municípios (art.

[19] Parecer disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=5128368&disposition=inline>. Último acessso em 04.06.2017.

3º). Quanto ao compartilhamento dos dados, a Lei apenas dispõe que é vedada sua comercialização, total ou parcial, sem fixar qualquer sanção em caso de descumprimento (art. 4º, parágrafo 1º).

Fica instituído também o Comitê Gestor da ICN, de composição mista entre membros do Poder Executivo, do TSE, da Câmara e do Senado Federal e do Conselho Nacional de Justiça (CNJ) (art. 5º).

Outro artigo relevante diz respeito à possibilidade do poder público de realizar cruzamento de dados para verificação de benefícios sociais. Confira-se:

> **Art. 11**: O poder público deverá oferecer mecanismos que possibilitem o cruzamento de informações constantes de bases de dados oficiais, a partir do número de inscrição no CPF do solicitante, de modo que a verificação do cumprimento de requisitos de elegibilidade para a concessão e a manutenção de benefícios sociais possa ser feita pelo órgão concedente.

Por fim, fica a critério do Poder Executivo e do TSE editarem atos complementares para regulamentar e executar os objetivos da Lei, nos termos do art. 12.

A seguir, a iniciativa será analisada à luz dos conceitos desenvolvidos até o presente momento, notadamente quanto às possíveis violações aos direitos de privacidade, de proteção de dados e à ética do uso de dados e informações pessoais. Também serão analisadas iniciativas de outros países como forma de reforçar as conclusões aqui apresentadas, tendo em vista a grande problemática que a referida Lei institui.

III.2 - CONSIDERAÇÕES IMPORTANTES SOBRE AS CONTROVÉRSIAS DA LEI

Como visto anteriormente, a sociedade hoje se organiza a partir da tecnologia, modificando suas estruturas constantemente (Castells, 2009), sendo que esse desenvolvimento e o domínio da informação acabam representando também um papel político e social importante (Webster, 2014). O domínio tecnológico possibilita estruturas de poder diferenciadas, a partir do controle da informação de terceiros, ou até mesmo da possibilidade de ter o conhecimento sobre os interesses de cada um.

Além disso, o acesso aos dados viabilizado pelos diversos mecanismos tecnológicos, permite desenvolver estratégias de abordagem do indivíduo considerando seus interesses pessoais e vontades (e as vezes inclusive com o propósito de manipular tais vontades). Foi possível concluir que, a partir desses arranjos existentes em razão da tecnologia, existe um grande processo de controle do individuo que influi diretamente na sua capacidade de fazer escolhas, de se autodeterminar (Doneda, 2006).

Toda essa constelação de relacionamentos e intervenções viáveis existe, principalmente, a partir de grandes bancos de dados, que unificam informações dispersas em um único centro. A seguir, serão detalhadas as principais controvérsias da Lei que institui a ICN, tendo em vista as discussões aventadas nos capítulos anteriores.

III.3 - CARACTERÍSTICAS POSITIVAS DA BASE DE DADOS DA ICN

Os dados cadastrais, como mencionado anteriormente, são importantes por representarem o acesso individual ao mundo jurídico. Alguns desses registros estão dispostos, atualmente, em sistemas de bases não integradas, como é o caso do Registro Geral (RG), o qual é emitido exclusivamente pela Secretaria de Segurança Pública de cada Estado da Federação. A não unificação dessas bases muitas vezes represa um problema, uma vez que viabiliza as possibilidades de fraude. No caso do RG, por exemplo, é possível emitir um documento para uma mesma pessoa em cada um dos 26 estados da federação, uma vez que não há comunicação entre as Secretarias de cada local. (Kang; Santos; Doneda, 2016, p. 43).

Uma primeira característica positiva que se pensa quando da instituição de uma Identificação Civil Nacional (ICN), portanto, é a de dirimir essas possibilidades de fraude em razão de uma base de dados integrada, na qual se estabelece a comunicação de diversos entes da administração e de regiões diferentes. Essa característica é logo associada à possibilidade de se otimizar a disposição de recursos para gerir o armazenamento de informações sobre os cidadãos, tornando a emissão de documentos e o cadastro de cidadãos mais eficiente, sob o ponto de vista da administração pública. Haverá uma disposição unificada de recursos utilizada somente para abastecer e gerir o banco de dados, facilitando o acesso sobre os documentos já existentes para

aquele indivíduo específico. Nesse sentido de pensamento, um único banco de dados representa um certo avanço na identificação dos indivíduos, uma vez que também facilita o acesso ao conteúdo disponível sobre cada um e processos de retificação de dados e informações incorretas.

Em síntese, o modelo de eficiência ideal para o Estado envolve o uso da tecnologia como facilitador da gestão, e isso seria alcançado através de um único banco de dados cadastrais dos cidadãos, já que a centralização das informações representa uma forma rápida e de baixo custo para abastecer o Estado de novos dados, de corrigir aqueles cadastrados indevidamente, evitar fraudes, facilitar a consulta e o compartilhamento, e, por consequência, a capacidade do ente administrador de atuar de forma verdadeiramente eficaz no policiamento e em seus programas de governo (Privacy...,1968-1969[20]).

O banco de dados da ICN também facilitaria o mapeamento de informações para fins de pesquisa por parte do governo. De igual maneira, o fácil acesso aos registros facilita a instituição de políticas públicas específicas e direcionadas a um grupo determinando, o que poderia promover o aprimoramento de um benefício social, por exemplo. Essa possibilidade, inclusive, já encontra previsão na Lei 13.444/2017, sendo que o cruzamento de dados poderá ser utilizado para verificação de requisitos necessários ao acesso dos benefícios sociais.

É de se concluir, portanto, que a organização da ICN tem aspectos importantes a serem considerados.

III.4 – PONTOS CONTROVERSOS DA LEI

III.4.1 - TÉCNICA E GESTÃO DE BANCOS DE DADOS

Primeiramente, pode-se dizer que a participação de especialistas sobre uso e gestão de dados pessoais foi ignorada em vários momentos diferentes da organização da Lei 13.444/2017, o que causou sérios prejuízos ao texto legal em razão da falta de debate e de considerações técnicas importantes que deveriam ter sido abordas.

[20] O artigo "*Privacy and Efficent Goverment: proposalas for a national data center*" foi localizado sem menção de autoria, tendo sido publicado na revista Harvard Law Review, ed. 400, entre os anos de 1968 e 1969.

Enquanto ainda estava em votação no Senado Federal, não foram feitas consultas técnicas sobre a matéria, sendo que uma parcela importante da comunidade, que tem conhecimentos importantes sobre uso e gestão de dados pessoais, teve sua participação excluída na criação da Lei. Percebe-se que existem diversas questões importantes sobre os tipos de dados existentes e as repercussões do armazenamento de cada um desses tipos, as formas de tratamento de conteúdo, a criação e o armazenamento de dados tipo *big data,* dentre outras, que foram completamente desconsideradas nos momentos de trâmite da iniciativa. Apenas foi considerada a competência da União sobre a matéria e a iniciativa "inovadora", como evidenciado pelo parecer do relator da PLC na CCJ, o Senador Antonio Anastasia.

Destaca-se também que um dos principais problemas envolvendo a criação da base de dados da ICN é a atribuição de toda sua gestão ao Tribunal Superior Eleitoral (TSE), órgão não especializado e não exclusivamente destinado à organização, gestão e tratamento de dados pessoais. Será atribuído a um tribunal eleitoral a responsabilidade pela gestão de um dos maiores (se não o maior) banco de dados sobre cidadãos brasileiros do país, em que se consolidarão todas as informações existentes na administração pública. Foi completamente desconsiderada a importância de técnicos em gestão de bases de dados, ou ainda todas as discussões envolvendo a necessidade de se criar uma autoridade técnica e especializada em dados pessoais.[21]

A justificativa da gestão da base de dados da ICN ser do TSE é de que esse órgão já vem coletando cadastro biométrico dos cidadãos para realização de eleições, além de já ter um grande banco de dados uniformizado. Contudo, é de se destacar que a possibilidade de compartilhamento de dados entre os órgãos da administração pública e o armazenamento de outros conteúdos, como a ficha criminal, garantem a esse banco de dados uma especificidade característica que demanda um cuidado muito maior na gestão de dados.

Instituiu-se um Comitê Gestor da base de dados da ICN, responsável por fixar as principais diretrizes de uso e padrões do banco de dados e, novamente, não constam especialistas técnicos sobre uso e gestão de dados em sua composição. A previsão de composição considera apenas representantes do Poder Executivo Federal, do Tribunal Superior Eleitoral, da Câmara dos Deputados, do Senado Federal e do Conselho Nacional de Justiça.

[21] Essa discussão, inclusive, está em trâmite na Câmara dos Deputados com o Projeto de Lei n. 5.267/2016.

Para não se dizer que houve um completo descaso com a técnica, foi prevista a possibilidade de se criarem grupos técnicos, com participação paritária, cuja finalidade seria a de assessorarem o comitê em suas atividades (art.4º, parágrafo 4º). Tais grupos, contudo, não têm qualquer capacidade diretiva, ou qualquer garantia de que as consultas técnicas prestadas serão efetivamente acatadas pelo Comitê.

Obviamente que o processo de gestão de banco de dados envolve questões políticas, relacionadas às intenções de uso desses dados para o governo. Contudo, o uso de dados por parte do governo precisa encontrar limitações claras, como forma de se evitarem abusos por parte do Estado em relação aos seus governados. A própria técnica é uma dessas formas de limitação, mas que foi desconsiderada na Lei: poderiam ter sido adotados critérios mundialmente reconhecidos como importantes no que tange a gestão de dados pessoais, e que atuam como formas de garantia de direitos de privacidade individual e, ao mesmo tempo, de limitação do poder fiscalizador do Estado.

Quanto a esse aspecto, conclui-se, a Lei 13.444/2017 é negligente, posto que desconsiderou a relevância da matéria de proteção de dados pessoais ao não viabilizar a participação de especialistas e ao deixar, a cargo de um tribunal eleitoral não especializado na matéria, a responsabilidade pela gestão do banco de dados.

III.4.2 - FALTA DE DEBATE PÚBLICO SOBRE A INICIATIVA

Também não é possível afirmar que houve um efetivo debate público sobre a criação de uma base de dados como a da ICN. Foi viabilizado um mecanismo de consulta na página do Senado Federal que sequer foi minimamente representativa, uma vez que apenas contou com a participação de 151 pessoas. Nesse mesmo espaço, não era possível expor qualquer manifestação diferente de "sim" ou "não", uma vez que só estavam disponíveis esses dois botões de participação e não havia qualquer campo para considerações mais profundas sobre a matéria.

As discussões sobre a instituição de uma base de dados como a da ICN vão muito além de concordância total ou parcial, envolvendo profundas discussões sobre direitos de privacidade,

personalidade e limitação de poder. Além dos vários critérios técnicos envolvidos, não houve também qualquer divulgação profunda sobre a matéria, quais seriam os benefícios ou prejuízos da instituição de um banco de dados de tamanha magnitude.

Não foram feitas audiências públicas com objetivo de elucidar os objetivos da criação da base de dados da ICN, explicando também quais seriam os critérios de gestão e coleta de dados. O que se tem conhecimento diz respeito apenas à unificação dos diversos registros de identificação civil em um único documento, o Documento de Identificação Civil Nacional (DIN), mas não em relação aos processos que vão culminar nessa unificação.

Tal assertiva pode ser percebida a partir da vinculação de algumas mídias sobre a matéria: jornais relevantes, como o Estadão e a Isto é, vincularam a sanção da Lei como "Temer sanciona documento de identidade único, que deve passar a valer só em 2021"[22]. Ou seja, grande parte da população sequer tem conhecimento da futura existência de um banco de dados cadastrais reunindo tantas informações da população em um mesmo local.

Quanto ao aspecto técnico da criação e da gestão da ICN, portanto, percebe-se que também houve uma falha por parte do Legislativo e do Executivo, uma vez que não possibilitaram debates públicos amplos sobre uma matéria que afeta diretamente a vida de toda a nação, e que nem ao menos se preocuparam em divulgar devidamente todas as razões de criação de uma base de dados da magnitude da ICN.

III.4.3 – SEGURANÇA E ACESSO À BASE DE DADOS DA ICN

Tendo em mente as considerações feitas acima, ainda é de se considerar que o novo diploma legal foi negligente quanto a diversos problemas relacionados à internet: crimes cibernéticos e ataques de hackers, por exemplo, são realidades ante às novas tecnologias de armazenamento de dados.

[22] Artigos disponíveis em: < http://brasil.estadao.com.br/noticias/geral,temer-sanciona-documento-de-identidade-unico-que-deve-passar-a-valer-so-em-2021,70001774487> e http://istoe.com.br/temer-sanciona-documento-de-identidade-unico-que-deve-passar-a-valer-so-em-2021/>. Último acesso em 04.06.2016.

A base de dados da ICN, poderá conter diversas informações consideradas sensíveis, como é o caso dos registros fiscais, sendo que a divulgação desse tipo de conteúdo para entes privados ou terceiros indevidos pode acarretar em diversos problemas para indivíduo, desde, por exemplo, a clonagem de informações bancárias, até quebra e violação do sigilo fiscal. Ou seja, um único banco de dados, com todas as informações do cidadão disponíveis para o governo, administrado e gerido por uma entidade não técnica e não especializada no assunto, se hackeada, poderá implicar o fim da privacidade de toda uma nação.

Quanto aos aspectos de segurança, portanto, é de se notar que a Lei não teceu quaisquer considerações relevantes, uma vez que não fixou previsões concretas sobre mecanismos de proteção da base de dados, investimentos necessários para aprimoramento da tecnologia de segurança, ou sobre formas de organização das informações disponíveis.

Não ficaram expressos quais padrões de segurança poderão ser utilizados para o resguardo do banco de dados. De igual forma, não há qualquer previsão de sanção especial para casos de acesso indevido aos dados da ICN, tendo em vista sua relevância. Tampouco, são atribuídas a entidades especializadas em ataques cibernéticos a segurança da base de dados, ou a criação de padrões rígidos para o acesso.

O artigo 4º do diploma estabelece apenas que "é vedada a comercialização, total ou parcial, da base de dados da ICN". Esse artigo esclarece, em princípio, que entes privados não poderão ter acesso aos dados cadastrados a partir da venda do conteúdo. Contudo, não há clareza sobre a possibilidade de trocas de informações com bancos de dados privados. Cita-se como exemplo o Serasa Experian e o Serviço de Proteção ao Crédito, duas empresas prestadoras de serviços, financiadas por associações comerciais, que organizam dados cadastrais de consumidores. Não se sabe ao certo se essas bases poderão ser abastecidas com dados oriundos da base cadastral da ICN, ou se, de alguma forma, tais empresas poderão ter algum tipo de acesso ao conteúdo.

Ainda sobre esse artigo, é importante destacar que não há qualquer sanção prevista para o caso de comercialização de dados de forma indevida. O projeto de lei original tinha a previsão no parágrafo 1o do art. 4º, estabelecendo pena de detenção de 2 (dois) a 4 (quatro) anos, e multa, no

caso da comercialização das bases de dados da ICN. Contudo, o dispositivo foi vetado pelo Presidente da República:

> **Art. º, §1º - Razões de veto**: A legislação penal vigente já tipifica condutas subsumidas pelo tipo penal que se pretende criar, já estabelecendo as penalidades a serem aplicadas aos agentes públicos, sendo desnecessária a criação autônoma de pena aplicada a essa circunstância específica.

O veto faz menção ao parágrafo 1º do art. 153 do Código Penal Brasileiro, que inclui no tipo penal a divulgação, sem justa causa, de informações contidas nos sistemas de informação ou bancos de dados da Administração Pública. A pena prevista é de detenção de um a seis meses, ou multa, sendo atribuída uma pena mais branda do que a que fora inicialmente planejada para as violações na base de dados da ICN.

A redação da Lei não é clara, portanto, quanto aos padrões de segurança a serem utilizados para proteção da base cadastral da ICN, ou qual será a entidade responsável por fixar tais diretrizes. Também não é claro sobre como será o acesso à base de dados para entidades fora da administração pública será viabilizado de alguma forma.

III.5 - RESPEITO AOS PRINCÍPIOS E ORIENTAÇÕES DE USO DA INTERNET NO BRASIL

De pronto, também é de se ressaltar que o uso e gestão desse banco de dados deverá ser feito em total atenção e respeito aos princípios definidos no Marco Civil da Internet, além de considerar também os princípios gerais mundialmente adotados pela comunidade acadêmica como fundamentais para organização de bancos de dados, uma vez que inexiste no Brasil legislação especial sobre a matéria.

Abaixo, serão feitas algumas considerações sobre eventuais problemas que a concentração de dados na base da ICN pode causar, tendo em vista os pontos aventados acima.

III.5.1 - USO DE DADOS PARA REPRODUÇÃO DE PADRÕES DISCRIMINATÓRIOS

A coleta de dados para a base de dados da ICN será feita a partir do compartilhamento de informações de vários entes da administração pública. Não fica claro pela redação da lei, mas implica-se que as menores autarquias poderão contribuir para o abastecimento de dados a fim de complementar os registros cadastrais dos cidadãos. Assim, dados considerados sensíveis, como ficha criminal e registros fiscais, também vão estar na base de dados.

A Lei não deixa claro também os mecanismos de tratamento desses dados, considerando que podem existir alguns conteúdos ali disponíveis que viabilizem a reprodução de padrões discriminatórios através do tratamento diferenciado a partir de cada tipo de dado.

A grande preocupação envolve, principalmente, o rigor necessário para o tratamento de dados sensíveis, que poderão integrar a base de dados da ICN. Como visto, são dados de potencial uso discriminatório, para os quais devem existir padrões diferenciados de cuidado, tendo em vista seu maior potencial lesivo.

Cita-se como exemplo a possibilidade de se optar pela coleta de certos dados exclusivamente da população carcerária, cruzando essas informações com outras específicas, como gênero, classe social, utilização de algum benefício social e endereço. Tais informações, juntas, permitem traçar perfis digitais de quem são os supostos criminosos, retomando dogmas e estigmas ultrapassado. Perfis semelhantes poderão ser traçados a partir da simples leitura dos dados individuais, relacionando dados sobre orientação sexual, registros médicos e de saúde, gênero, raça, além de outros exemplos, sempre remontando o uso desses dados como possíveis usos discriminatórios (Nissenbaum, 2010).

Um outro exemplo que pode ser evidenciado é o tratamento de dados pessoais com objetivo de aprimorar mecanismos de fiscalização destinado exclusivamente a determinados grupos ou etnias diferentes, como uma forma do governo perseguir determinados padrões específicos em nome da segurança (Privacy..., 1968/1969, p. 411). Ou seja, a reprodução de padrões xenófobos e que estão cada vez mais em alta também podem ser estimuladas pela base de dados da ICN.

Ainda, destaca-se que a concessão de políticas sociais será organizada a partir da verificação dos dados dispostos na base da ICN. Isso também pode representar uma preocupação de que certos benefícios somente serão concedidos a perfis específicos formulados pelos dados coletados, o que poderia prejudicar não só a eficiência de algumas políticas públicas, como também o verdadeiro acesso de grupos marginalizados aos benefícios concedidos pelo Estado.

Essa ressalva precisa ser feita porque, ainda que exista a regulação do Marco Civil da Internet sobre princípios que orientem o seu uso no Brasil, já foi mencionado que alguns aspectos centrais da proteção de dados não foram abordados nesse referido diploma. Assim, a Lei que institui a ICN acaba por não estar inserta em um marco legal preciso sobre armazenamento, gestão e transmissão de dados. Seu uso, portanto, precisa atentar-se não apenas aos princípios consagrados no Marco Civil, dentre os quais se inclui o da diversidade e da pluralidade, mas também em atenção ao que a comunidade mundial considera nas discussões sobre tratamento de dados, principalmente de dados sensíveis, como uma das formas de orientar a gestão da base de dados da ICN de forma segura em relação aos cidadãos.

Deve existir uma pretensão de que a internet seja um espaço de trocas democráticas e de ausência de reprodução de desigualdades ou de discriminações. Essa pretensão não corresponde com a realidade em diversas circunstâncias, como explorado anteriormente, mas deve ser responsabilidade coletiva e do próprio Estado de garantir a existência de regulação capaz de assegurar direitos e mitigar preconceitos. Nesse sentido, os dados coletados a partir da internet, dados pessoais armazenados e o conteúdo disponibilizado para os grandes bancos de dados devem envolver uma espécie de cuidado especial nos diversos processos de tratamento de dados, considerando os princípios de igualdade que devem ser obedecidos.

III.5.2 - VIOLAÇÃO À PRIVACIDADE E AO DIREITO DE PROTEÇÃO DE DADOS

No primeiro capítulo desse estudo, foi possível concluir que as definições de privacidade muito evoluíram ao longo do tempo, e que hoje abrangem, em certo sentido, a proteção de ações e conteúdos que se querem manter em resguardo em relação à terceiros, não envolvendo apenas uma noção egoísta de estar sozinho, mas também uma relação de confiança de que certas informações individuais obtidas permanecerão sigilosas. Nesse sentido, cabem as observações de

Helen Nissenbaum (2010), ao dizer que as diferentes concepções de privacidade perdem importância quando se pensa em quais as hipóteses que violam o exercício do privado, ou quais os mecanismos que serão usados para impedir tais violações, que são as questões que realmente devem ser consideradas para o debate.

Também foi possível concluir que o direito à proteção de dados pessoais é hoje uma das expressões do direito de privacidade, uma vez que os dados que dizem respeito a uma pessoa específica, acabam por integrar sua personalidade, sua capacidade de se apresentar e se definir para o mundo (Schertel Mendes, 2014). Por esse motivo, proteger os dados pessoais é fundamental, uma vez que também envolve, em certa medida, a proteção da própria pessoa.

De natureza não proibitiva, o direito de proteção de dados representa uma forma de resistência às diversas formas de dominação possíveis, viáveis em razão da manipulação de conteúdo pessoal disponibilizado na internet ou armazenado em bancos de dados (Lessig, 1999). Isso porque, como abordado anteriormente, a informação é hoje um importante mecanismo de poder. Ter acesso ao conteúdo implica ter poder em relação a quem aquele conteúdo diz respeito.

A existência do privado, por si, reclama na atualidade conhecimento sobre que tipo de conteúdo está sendo armazenado e sobre qual a real possibilidade de terceiros terem acesso a isso. Os próprios limites da privacidade precisam ser bem definidos, sobre risco grave de não representarem a efetiva garantia de seu exercício (Stoco, 2015). Por esse motivo, é importante considerar todos os desdobramentos da privacidade na realidade contemporânea antes de proporcionar grandes iniciativas legislativas que podem causar tão sérios impactos aos direitos e garantias de toda uma nação

A partir de tais considerações iniciais, percebe-se que a base de dados da ICN confere à administração pública (e a todos os seus órgãos de acesso ilimitado à base) poder praticamente irrestrito sobre cidadãos, uma vez que estarão disponíveis todos os dados cadastrais, além de outros conteúdos que não foram detalhados na Lei, mas que também poderão ser armazenados, como os já mencionados registros criminais, fiscais e de saúde.

Destaca-se que a omissão existente no texto da Lei 13.444/2017 sobre exatamente quais são os dados passíveis de serem armazenados na base de dados da ICN, qual a verdadeira finalidade desse armazenamento e quais serão seus usos específicos, cria dúvidas relevantes

quando se pensa nas garantias individuais de privacidade que estão sendo colocadas em risco. Também não é possível saber ao certo, uma vez que não esclarecido, por quanto tempo os dados serão armazenados, como será a forma de coleta relacionada a cada ente específico da administração, quais as operações de tratamento de dados poderão ser feitas e de que forma, isso sem considerar todos os problemas já elencados em tópicos anteriores.

Já foi mencionado anteriormente que conteúdos de relevante potencial discriminatório não podem ser armazenados sem uma finalidade específica, e sem as garantias de que o seu processamento se dará de forma adequada (Doneda; Schertel Mendes, 2016, p. 5). Ocorre que, em razão das omissões acima relacionadas, dados sensíveis agora poderão ser atrelados a dados cadastrais sem qualquer controle por parte dos cidadãos sobre como as informações sobre si estão sendo utilizadas, ou sobre qual a verdadeira razão de cruzamento de tais dados. Não se pode dizer, sequer, que existe alguma forma de controle desses dados, uma vez que o único instrumento atualmente previsto, o *habeas data*, possui destinação específica relacionada à retificação de informações.

Quanto a esses aspectos, é de se considerar que o Marco Civil da Internet, em seu art. 7º, VIII, deixa expresso que será assegurado ao usuário "informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais". Portanto, caberá ao Comitê Gestor da ICN, futuro responsável por suprir as lacunas deixadas pelo texto legal, a atenção especial aos diversos questionamentos sem respostas, além dos mecanismos facilitadores de acesso que precisarão ser criados para controle do conteúdo disposto na base de dados da ICN.

Veja-se que a inexistência de norma específica sobre proteção de dados importa que a existência da Lei nº 13.444/2017 não será especificamente regulada por qualquer diploma. Não existem prerrogativas expressas sobre direitos de proteção de dados pessoais, sanções específicas em casos de violação, e até mesmo definições uniformes de conceitos importantes, o que acaba privando o cidadão de um aspecto importante da proteção da personalidade na atual realidade (Schertel Mendes; Doneda, 2016).

É de se considerar, ainda, que a capacidade do indivíduo de se relacionar, inclusive com o próprio governo, depende de uma relativa equidade na quantidade de informações disponíveis, sendo que a desproporção do que se deve ser conhecido pode prejudicar os relacionamentos

cotidianos (Privacy..., 1968/1969, p.411). Alguns já consideram que o convívio social é extremamente prejudicado em razão da realidade virtual paralela (Nissenbaum, 2004), e isso de certa forma acaba sendo aprofundado quando se pensa em grandes bancos de dados que promover desproporções unilaterais de conhecimento sobre a vida privada de cada um.

Essa desproporção gera ainda mais ressalvas quando se considera que todos os entes da administração pública poderão fazer consultas indiscriminadas (ao menos até o presente momento) dos conteúdos que antes não tinham acesso, ou que ao menos não eram consolidados em uma única base. Isso acaba por acentuar ainda mais a injustiça da informação (Nissenbaum, 2010, pp. 80-81), uma vez que o cidadão irá fornecer a determinado ente do Estado um conteúdo, o qual, por sua vez, será compartilhado em uma base única e poderá ser utilizado com uma finalidade diferente da inicial, sem prévio conhecimento por parte do indivíduo e também sem seu controle.

Ora, o acesso ao conteúdo das bases de dados da ICN irá conceder ao Estado uma quantidade absurda de informações sobre os cidadãos, permitindo identificar, com precisão, diversas características de cada um dos indivíduos, suas localidades, gostos, preferências e hábitos, entregando ao governo um verdadeiro poder de controle sobre a atividade de cada um, tornando brutalmente desigual a capacidade relacional de um indivíduo com o Estado. Em segundo plano, isso acarreta também o uso de dados para o exercício efetivo desse poder, através de mecanismos de manipulação como forma de induzir o individuo a um comportamento específico.

Pode-se dizer, obviamente, que a administração pública já possui todos os dados que serão compilados na base cadastral da ICN, mas diversos problemas relacionados aos direitos de privacidade existem, justamente, com a criação de um cadastro unificador de tais informações, gerido de forma incerta e, ao que tudo indica, pouco rigorosa (Privacy..., 1968/1969 p. 409). A tecnologia possui diversos mecanismos de tratamento de dados que são aprimorados quando a quantidade de dados é maior, possibilitando-se extrair mais informações desses dados e mais formas de utilizá-los.

Além disso, os próprios dados cadastrais, quando explorados, podem implicar em violação do sigilo assegurado pela Constituição (Ferraz Junior, 1993). Também por tais motivos,

e em atenção ao princípio da finalidade e da transparência, ter controle e acesso aos dados da base de dados da ICN é fundamental.

É de ressaltar, ao fim, que alguns valores da administração pública, como eficiência, não são oponíveis às garantias do cidadão, tal qual a privacidade. Por isso, não há que se sustentar que existe um bem maior a ser protegido, qual seja uma melhor forma de atuação do Estado, quando se colocam em cheque direitos do cidadão que são vitais ao funcionamento da sociedade.

Esse tipo de argumento acaba por promover uma moralização do espaço privado, sugerindo que ele é menos relevante do que questões de segurança. Contudo, o constrangimento individual de que a privacidade é menos importante implica na ausência de garantias coletivas, e que acampam por mitigar também outros valores socialmente compartilhados, sempre para conferir ao Estado um maior poder de controle dos cidadãos (Solove, 2008).

Conclui-se, portanto, que os esforços da administração pública de utilizar os avanços tecnológicos para aprimorar padrões de organização e eficiência precisam estar coordenados com o respeito aos valores compartilhados em termos de privacidade e respeito ao íntimo dos usuários. Investir em tecnologia de segurança de banco de dados, adotar práticas de transparência no uso das informações e priorizar o emprego dos dados para melhor organização de políticas públicas de governo (e não de políticas de fiscalização dos cidadãos) são boas práticas que tentam coordenar a tecnologia dos dados pessoais com a privacidade. (Kraus, 2013).

III.6 - INICIATIVAS SIMILARES EM OUTROS PAÍSES

A criação de bancos de dados compilando informações sobre os cidadãos já foi muito discutida em diversos outros países. Em sua grande maioria, o temor dos cidadãos pela possível (e provável) violação aos seus direitos de privacidade acabou acarretando ao enterro desses projetos.

A primeira iniciativa importante de ser mencionada é o *National Data Center*, de origem norte-americana em meados de 1960, que buscava compilar em um único bando de dados as diversas informações sobre os cidadãos americanos, para uso da administração federal (Doneda,

2011, p. 99). A proposta teve fundamento econômico, de centralizar em uma única base as informações importantes, tornando o acesso para realização de pesquisas mais fácil, e o tratamento de dados da administração mais eficiente (Kraus, 2013).

A iniciativa propunha compilar dados de nascimento, registros cadastrais, militares, da previdência social e até informações de fichas criminais em um banco único, de forma a promover uma certa economia na Administração Pública, que não precisaria de investimento em tecnologia em todas os entes específicos, mas apenas em um grande ente central, responsável pela base de dados. (Schertel Mendes, 2014, p. 39).

Houve grandes discussões sobre a propostas, tendo sido realizadas audiências e consultas públicas sobre sua viabilidade. Contudo, a opinião pública foi feroz no sentido contrário ao da aprovação do *National Data Center*, em razão do temor burocrático da gestão dos dados, da falta de padrões de segurança e dos problemas de privacidade que poderiam ser ocasionados com a existência de tantas informações reunidas em um único espaço (Kraus, 2013).

Dessas discussões, surgiram outras sobre a segurança dos usuários em relação a todos os bancos de dados no geral, o que culminou, em 1974, na edição do *Privacy Act*. As discussões sobre gestão de dados por parte do governo, contudo, continuaram anos adiante, quando se editou, em 1988, uma emenda ao *Act* buscando a não autorização da criação de qualquer banco de dados nacional, mantido por agências federais, capaz de culminar na combinação de informações, resultantes da ligação de dados a indivíduos específicos (Kraus, 2013, p.30).

Mostra-se um certo nível de maturidade nas discussões de privacidade, não só em razão da tradição liberal norte-americana, de temer excessivo poder por parte da administração, e por esse motivo querer limitar seu acesso aos indivíduos, como também em razão do debate público, de pronto oportunizado quando primeiro se pensou na instituição um banco de dados nacional.

Outra iniciativa similar e mais recente ocorreu na Índia, com uma proposta do governo de unificar os residentes com um cadastro único de 12 dígitos que, além de economizar milhões aos cofres públicos, facilitaria a fiscalização, a identificação e até as transferências bancárias, promovendo o suposto acesso de milhões à modernidade. Chamado de Aadhaar, o programa foi aprovado mas acabou tendo pouca adesão da população, de modo que o governo indiano se viu obrigado a forçar o ingresso dos cidadãos, fortalecendo, de forma obrigatória, a base de dados

unificada e gerida pela administração[23]. As discussões locais são similares às que precisam ser feitas sobre a instituição da base de dados da ICN, uma vez que a adesão ao banco de dados ocorreu sem qualquer discussão ou debate.

Essas duas iniciativas, se comparadas com a proposta brasileira, mostram uma tendência dos governos de priorizarem estatísticas de eficiência da administração e mecanismos facilitadores da fiscalização, em detrimento do respeito e da privacidade dos usuários, como se essas fossem questões secundárias na agenda política. Os dois programas, de locais diferentes do globo, mostram que deve existir uma tendência em se discutir regulamentos de proteção de dados pessoais ante o rápido desenvolvimento tecnológico, capaz de permitir e facilitar o armazenamento e o compartilhamento seguro das informações.

Quando se trata de conteúdos geridos pelo governo, essa preocupação fica ainda maior, tendo em vista os receios com os processos burocráticos, a obscuridade da finalidade principal da coleta de dados, as inseguranças sobre o uso das informações ali constantes e as próprias limitações necessárias ao poder fiscalizador do Estado.

No Brasil, todo esse debate parece ter sido obscurecido, em razão da rapidez com que o projeto tramitou nos órgãos legislativos e foi sancionado pelo Presidente da República, talvez até de forma intencional para frear problemáticas sobre privacidade e proteção do conteúdo.

[23] Artigo disponível em: < http://www.economist.com/news/leaders/21720599-bjp-government-should-listen-peoples-qualms-about-snooping-indias-biometric-identity?frsc=dg%7Cd>. Último acesso em 04.06.2017.

CONCLUSÃO

O presente estudo não se esgota nestas páginas. Existem diversas discussões que podem ser aprofundadas para concluir que a existência de um único banco de dados, administrado e gerido de forma não técnica por órgãos do governo, pode implicar em violações de direitos de privacidade e proteção de dados pessoais.

A instituição da base de dados da ICN pode ser capaz de trazer benefícios para a administração, como tornar a fiscalização e a gestão de dados cadastrais mais eficiente e menos sujeita a fraude; facilitar o acesso de pesquisas e sensos; facilitar a retificação de dados cadastrados incorretamente. Contudo, e a partir das discussões desenvolvidas, é possível concluir que a instituição dessa base de dados está eivada de problemas que não foram discutidos sequer pelo próprio governo.

A base de dados será gerida por um órgão não especializado em gestão e armazenamento de conteúdo pessoal, e todas as diretrizes orientadoras do uso desse conteúdo poderão ser fixadas por entidades do governo sem qualquer conhecimento técnico sobre a matéria.

Além disso, o texto da Lei 13.444/2017 não permite concluir quais tipos de dados poderão ser armazenados, com qual finalidade, como será o tratamento de dados pessoais sensíveis, quais os critérios de segurança necessários para a proteção da base de dados, qual o tempo de armazenamento do conteúdo, quais serão as formas de acesso aos dados presentes e como será o controle do compartilhamento das informações, dentre tantas outras questões que sequer foram mencionadas.

Como inexistem leis específicas sobre proteção de dados pessoais, é de se verificar que a Lei 13.444/2017 existe em meio a uma lacuna legislativa, sendo que inexiste qualquer autoridade responsável por proteção de dados pessoais que irá exercer o controle interno da gestão e do uso dessas informações. Não será possível, a partir de uma primeira análise, viabilizar quaisquer prerrogativas dos cidadãos sobre os conteúdos armazenados sobre si.

De igual maneira, existem ainda preocupações importantes sobre o uso de dados como instrumento de exercício do poder do Estado a partir da manipulação de vontades, ou do reforço

de padrões discriminatórios em razão do tratamento e da coleta seletiva de dados pessoais. Essas também foram questões levantas no presente estudo e que não podem ser respondidas a partir de uma análise da Lei sancionada, uma vez que tais questões também não foram aventadas.

É de se notar que a privacidade, atualmente, encontra definição também na proteção de dados pessoais, uma vez que houve uma verdadeira mudança nos processos sociais que acarretaram a transposição da realidade para um espaço virtual. Nesse sentido, é determinante que o Direito se preocupe em estabelecer diretrizes e regulamentos para que a organização, gestão e tratamento desses dados respeito aos princípios de uso da rede consagrados pelo Marco Civil da Internet, e difundidos por toda a comunidade internacional.

Além disso, é necessário também que a gestão da base de dados da ICN seja fiscalizada por órgãos reguladores técnicos, de conhecimentos profundos sobre a matéria, para evitar que as informações ali produzidas e armazenadas sejam utilizadas como forma de propagar preconceitos e discriminações contra os cidadãos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Fábio Siebeneichler. *A tutela dos direitos de personalidade no direito brasileiro em perspectiva atual*. 24 Rev. Derecho Privado 81, 2013.

ABREU, Jaqueline de Souza; NAKAGAWA, Fabiane Midori Sousa; RUIZ, Juliana Pacetta. *Data Protection in Brazil: Draft report/ review of legal background*. Associação InternetLab de Pesquisa em Direito e Tecnologia, 2016. Disponível em: <http:// www.internetlab.org.br> .

CASTELLS, Manuel. *Comunication Power*. Oxford University Press. Inc, Nova Iorque, 2009.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. ed. Renovar, 2006.

_____. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, v. 12, n. 2, p.91-108, jul./dez. 2011.

DONEDA, Danilo; SCHERTEL MENDES, Laura. *Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016*. Revista de Direito Civil Contemporâneo, vol. 9, p.35-48, out-dez 2016.

DUMBILL, Edd. *What Is Big Data?: An Introduction to the Big Data Landscape,* O'Reilly, 2012. Disponível em: <https://www.oreilly.com/ideas/what-is-big-data>.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito, Universidade de São Paulo, São Paulo, v. 88, p. 439-459, jan. 1993. ISSN 2318-8235. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 23 apr. 2017. doi:http://dx.doi.org/10.11606/issn.2318-8235.v88i0p439-459.

GARCIA, REBECA. *Marco Civil da Internet no Brasil: Repercussões e Perspectivas*. Revista dos Tribunais, vol. 964/2016, p. 161-190, fev. 2016.

GONÇALVES, Andrey Felipe Lacerda; BERTOTTI, Monique; MUNIZ, Veyzon Campos. *O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais*.In: *Doutrinas Essenciais de Direito Constitucional*, vol 8, ago de 2015, p. 597-614.

KIRA, Beatriz; TAMBELLI, Clarisse Nassar. *Data Protection in Brazil: Critical Analysis of the Brazilian Legislation*. Associação InternetLab de Pesquisa em Direito e Tecnologia, 2016. Disponível em: <http://www.internetlab.org.br>.

KLANG, Mathias (Org.). *Human Rights in the Digital Age.*The Glass House, Londres, 2005.

KRAUS, Rebecca S. *Statistical Dèjá Vu: The National Data Center Proposal of 1965 and Its Descendantes*. Journal of Privacy and Confidentiality, No. 1, 2013, p. 1-37.

LESSIG, Lawrence. *Code, version 2.0*. Basic Books, 2006.

MAURMO, Júlia Gomes Pereira. *A distinção conceitual entre privacidade, intimidade, vida privada, honra e imagem*. Revista de Direito Privado, vol. 57/2014, p. 33-52, jan-mar. 2014.

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

MURPHY, Robert F. *Social distance and the veil*, In SCHOEMAN, Ferdinand D., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, 1984.

de NARDIS, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.

NAKAMURA, Lisa. *Gender and Race Online*. In: GRAHAN, Mark; DUTTON, Willian H. *Society and the Internet: How Networks of information and Communication are Changing Our Lives*. Oxfor Scolarship Online, 2014.

NISSENBAUM, Helen. *Privacy in context: Technology, Policy and the Integrity of Social Life*. Stanford Law Books, 2010.
NISSENBAUM, Helen. *Etichs*. In NISSENBAUM, Helen, *Information Technology and Etchics*, Berkshire Encyclopedia of Human-Computer Interaction, BerkShire Publishing Group, 2004, p. 235-239.
_____.. *Information Technology and Ethics: Berkshire Encyclopedia of Human-Computer Interaction*. Berkshire Publishing Group, 2004, p. 235-239.
PRIVACY AND EFFICIENT GOVERNMENT: PROPOSALS FOR A NATIONAL DATA CENTER. Harvard Law Review, 4oo, 1968/1969.
RICHARDS, Niel M.; KING, Jonathan H. *Big Data Ethics*. Wake Forest L. Rev. 393, vol. 49 2014, p. 393-432.
SCHERTEL MENDES, Laura. *Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental*. ed. Saraiva, Série IDP, 2014.
SCHREIBER, Anderson. *Marco Civil da Internet: Avanço ou Retrocesso? A responsabilidade Civil por Dano Derivado do Conteúdo Gerado por Terceiro*. In LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira (Org.) *Direito e Internet III. Marco Civil da Internet*. São Paulo, Quartier Latin, 2015.
SCHWARTZ, Paul M.; SOLOVE, Daniel J., *The PII Problem: Privacy and a new personally identifiable information*. N.Y.U L. Rev., 86ªed., 2011.
SOLOVE, Daniel J., "*I've got nothing to hide "and other misunderstandings of privacy*. The George Washington University Law School, Washington DC, 2008, 23 p.
TEPEDINO, Gustavo. *A Tutela da Personalidade no Ordenamento Civil-constitucional Brasileiro*. Temas de Direito Civil, 3ª ed., Renovar, 2004, p. 23-58.
TEFFÉ, Chiara Antonia Spadaccini. *Responsabilidade Civil e Liberdade de Expressão no Marco Civil da Internet: a responsabilidade civil dos provedores por danos decorrentes de conteúdo gerado por terceiros*. Revista de Direito Privado, vol. 63, 2015, p. 59-83, jun-set/2015
WARREN, Samuel D.; Brandeis, Louis D. *The right to privacy*. Harvard Law Review, vol. 4, No. 5, 1890, p. 193-220.
WEBSTER, Frank. *Theories of the information society*. Routledge, Nova Iorque, 4ª ed., 2014.
WESTING, Alan. *The origigins of modern claims to privacy*, In SCHOEMAN, Ferdinand D. *Philosophical Dimensions of Privacy – An Anthology*, Cambridge University Press, New York, 1984.
WONG, Rebecca. *Privacy: Charting its Developments and* Prospects. In: MURRAY, Andrew;