Revista de Direito, Governança e Novas Tecnologias

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 02.12.2017
Aprovado em: 30.12.2017

COMPARTILHAMENTO DE DADOS PESSOAIS E A ADMINISTRAÇÃO PÚBLICA BRASILEIRA

*** José Renato Gaziero Cella[1]**
**** Rafael Copetti[2]**

RESUMO

O artigo analisa a proteção de dados pessoais no Brasil e tem como objetivo demonstrar, por meio do método hipotético-dedutivo, se a garantia individual da privacidade, em especial relativamente aos bancos de dados em poder dos órgãos da administração pública federal brasileira, com as inovações normativas trazidas pelo Decreto Federal nº 8.789, de 29 de junho de 2016, pode ser mitigada em virtude de interesses econômicos dos órgãos públicos e atenuada em nome da agilidade e resultados deco
rrentes do compartilhamento dos dados armazenados, evitando a violação por meio de acordos de cooperação.

Palavras-chave: Proteção de dados pessoais; Tratamento; Decreto Federal; Compartilhamento de dados; Poder Judiciário.

PERSONAL DATA SHARING AND THE BRAZILIAN PUBLIC ADMINISTRATION

ABSTRACT

This article analyzes the personal data protection in Brazil and aims to demonstrate, through the hypothetical-deductive method, if the privacy individual guarantee, specially that ones related with the bank data of the brazilian federal public administration offices, with the normative innovations brought by Federal Decree No. 8,789, dated June 29, 2016, may be mitigated by economic intererests of public bodies and attenueted in the name of the agility and results from data bank sharing, avoiding the violation by cooperation agreements.

Keywords: Personal Data Protection; Treatment; Federal Decree; Data sharing; Judicial Power.

1. INTRODUÇÃO

[1] * Doutor em Filosofia e Teoria do Direito pela Universidade Federal de Santa Catarina - UFSC. Mestre em Direito do Estado pela Universidade Federal do Paraná - UFPR. Professor do Programa de Pós-Graduação *Stricto Sensu* em Direito da Faculdade Meridional - PPGD/IMED, Passo Fundo-RS, Brasil. E-mail: cella@cella.com.br.
[2] ** Mestre em Direito, Democracia e Sustentabilidade da Faculdade Meridional – IMED de Passo Fundo/RS. Especialista em Direito Público pela Faculdade Meridional - IMED/ESMAFE. Servidor Público Federal do Tribunal Regional Eleitoral do Rio Grande do Sul. E-mail: rafaelcopetti@yahoo.com.br.

A proteção de dados pessoais não tem sido motivo de preocupação na elaboração de textos normativos no direito brasileiro. Um exemplo recente é o Decreto Federal nº 8.789/2016, que dispõe sobre o compartilhamento de bases de dados na administração pública federal, editado, em 29 de junho de 2016, pelo Poder Executivo Federal brasileiro. A referida assertiva decorre do fato de que sua justificativa está atrelada exclusivamente a questões de eficiência e simplificação administrativas.

Percebe-se, também, que órgãos da Administração Pública e de outros Poderes, fazem acordos de compartilhamento de informações e dados pessoais sem que exista um regramento claro e um respeito à privacidade. Exemplo típico é o acordo de cooperação firmado entre o Tribunal Superior Eleitoral e o SERASA S/A, no qual dados sensíveis dos eleitores seriam repassados à empresa citada.

Assim, o problema de pesquisa decorre se, diante da ausência de regulação relativamente ao uso e tratamento dos dados, se o texto do Decreto Federal nº 8.789/2016 tem como característica a possibilidade de garantir a não ocorrência de situações de compartilhamento indiscriminado de dados pessoais como a ocorrida no acordo de cooperação técnica firmado entre a Justiça Eleitoral e a empresa de análise de crédito acima identificada.

O artigo, portanto, visa a responder se a garantia individual da privacidade, em especial relativamente aos bancos de dados em poder dos órgãos da administração pública federal brasileira, pode ser mitigada em virtude de interesses econômicos dos órgãos públicos e atenuada em nome da agilidade e resultados decorrentes do compartilhamento dos dados armazenados pelos órgãos citados.

Diante desse problema, visa-se a confirmar a hipótese de que a aplicação dos ditames do Decreto Federal nº 8.789/2016 não garante proteção adequada e se torna temerária na medida em que coloca em risco a garantia individual de proteção da privacidade, pois não assegura a não ocorrência do repasse de dados pessoais em acordos entre órgãos públicos, ratificando o argumento da urgência de uma lei específica de proteção de dados no direito brasileiro.

Com efeito, a tecnocracia, com seus ideais de eficiência, enxerga no compartilhamento de bancos de dados um bem em si mesmo. Diante desse posicionamento reducionista, resulta, aos olhos delirantes dos burocratas, inquestionável a decisão governamental que se enveredou para esse perigoso rumo de intercâmbio de dados pessoais, cuja implementação, sem que se considerem contrapesos e salvaguardas, pode levar a drásticos efeitos colaterais.

2. COMPARTILHAMENTO DE BASES DE DADOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL: O DECRETO FEDERAL Nº 8.789/2016

Com a evolução e aplicação das novas tecnologias nos diversos setores sociais, os indivíduos estão cada vez mais expostos nas suas relações, sejam elas privadas ou públicas. As informações são coletadas de diferentes formas, na navegação ou cadastros em páginas da internet, fornecidas diretamente pelo usuário, em bancos de dados de diversas fontes ou como requisitos para a obtenção de determinado serviço ou documento perante o Poder Público.

Um exemplo típico é o fornecimento de dados biométricos pelos cidadãos que solicitam a emissão do título de eleitor nos Cartórios Eleitorais brasileiros. O indivíduo, além de fornecer informações de caráter pessoal – nome, filiação, data de nascimento, sexo, endereço residencial ou comercial, tempo de vínculo com o município, se possui ou não irmão gêmeo, telefones, escolaridade e profissão – tem sua assinatura coletada digital e fisicamente.

Uma fotografia e as digitais dos dez dedos das mãos são coletadas, muito embora apenas a identificação na urna eletrônica seja realizada por meio dos dedos polegares ou indicadores. Deve-se lembrar que o voto é obrigatório para todas as pessoas maiores de 18 anos e menores de 70 anos, conforme o ordenamento constitucional brasileiro.

Tanto os dados coletados pela Justiça Eleitoral, órgão do Poder Judiciário Federal, quanto os coletados por outros entes da Administração Pública, devem receber proteção jurídica adequada. Não apenas a coleta, mas da mesma forma o armazenamento e o tratamento de dados necessitam de tutela jurídica.

Afinal, trata-se de dados pessoais relativos à personalidade da pessoa, a aspectos da vida privada e que podem comprometer a imagem do indivíduo perante terceiros, sua moral e estrutura psíquica quando indevidamente utilizados ou tornados públicos.

Especial atenção é necessária à possibilidade de compartilhamento desses dados pessoais por órgãos públicos. Diz o *caput* do artigo 1º do Decreto Federal nº 8.789, de 29 de junho de 2016 (disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm), que dispõe sobre o compartilhamento de bases de dados na administração pública federal brasileira:

> Art. 1º Os órgãos e as entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União que forem detentoras ou responsáveis pela gestão de bases de dados oficiais disponibilizarão aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional interessados o acesso aos dados sob a sua gestão, nos termos deste Decreto.

Segundo o governo federal brasileiro[3], a medida seria um importante passo para promover eficácia na gestão de políticas públicas, redução de gastos e conveniência aos cidadãos, com a redução da redundância de informações e do custo operacional para o seu compartilhamento.

Seja como for, os dados que serão compartilhados entre órgãos e entidades federais são, em sua maioria, dados pessoais. Se, de um lado, a iniciativa pretende alcançar eficiência, de outro, parece estar desatenta à proteção devida a essas informações.

O Decreto Federal nº 8.789/2016 facilita o compartilhamento de bancos de dados entre órgãos e entidades da administração pública federal brasileira. A possibilidade desse compartilhamento desses dados não é a novidade, posto que anteriormente ela ocorria por meio de convênios e acordos. O que o decreto faz é dispensar a necessidade desses convênios e, assim, simplificar a transferência de dados, criando uma base única para toda comunicação de dados em nível federal, composto por mais de 20 ministérios, inúmeras secretarias e mais de 150 autarquias, fundações e agências reguladoras.

A motivação do decreto é a de que o compartilhamento serve à "amplificação de oferta de serviços públicos", "formulação e monitoramento de políticas públicas", "fiscalização de benefícios" e "melhoria da fidedignidade de dados" (artigo 2º). Na prática, isso significa explorar as oportunidades do *big data*[4], já que o decreto expressamente incentiva a análise de dados por meio da criação de mecanismos de conferência de dados, "preferencialmente automática", por parte de órgãos competentes pela concessão, pelo pagamento ou pela fiscalização de benefícios (artigo 5º).

No entanto, relativamente à proteção da privacidade a iniciativa é pífia, já que tão somente traz a menção de que devem ser protegidos os dados relativos aos sigilos fiscais e bancários. Sobre o que acontece com o sigilo telefônico – os registros de chamada aos quais a Agência Nacional de Telecomunicações - ANATEL pode ter acesso, por exemplo, não diz nada.

O decreto também não impõe limites expressos à extensão do cruzamento de dados

[3] Cf. http://www.planejamento.gov.br/assuntos/logistica-e-tecnologia-da-informacao/politicas-publicas-serao-monitoradas-com-compartilhamento-de-dados-entre-orgaos-do-governo, acesso em 22 ago. 2017.

[4] Gigantescas massas de dados armazenados em sistemas que agregam inúmeras informações de variadas fontes. Esses gigantes bancos de dados podem ser analisados e estudados de maneiras inovadoras, facilitando a extração de informações e correlações antes indisponíveis ou de difícil acesso.

entre os variados órgãos e entidades do Estado e a classificação das informações que podem ser obtidas.

Quando um indivíduo fornece dados a uma determinada repartição pública ou é pessoalmente associado a informações, ele o faz para um determinado propósito, quase sempre vinculado a área de atuação daquela entidade. Ao quebrar as barreiras entre os diferentes órgãos e entidades do Estado e permitir o compartilhamento, dados podem ganhar novo propósito para além do que foram coletados inicialmente.

É nesse sentido que o acordo de cooperação técnica firmado entre o Tribunal Superior Eleitoral (TSE), órgão do Poder Judiciário, e o SERASA S/A, empresa privada, causam preocupação e estimulam o aprofundamento do estudo do tema.

3. ACORDO DE COOPERAÇÃO TÉCNICA TSE 7/2013

O caso envolvendo o TSE e a empresa SERASA S/A, o qual envolve a temática da privacidade e proteção de dados pessoais no Brasil, gerou repercussão midiática e jurídica. O fato ganhou notoriedade essencialmente pela potencial vulnerabilidade e divulgação de dados pessoais de aproximadamente 142 (cento e quarenta e dois) milhões de eleitores, violando a garantia constitucional da privacidade.

Trata-se do Acordo de Cooperação Técnica TSE nº 7/2013, firmado em 16 de julho de 2013 e publicado no dia 23 do mesmo mês, no qual ao TSE incumbia prestar "informações contendo o nome do eleitor, número e situação da inscrição eleitoral, além de informações sobre eventuais óbitos e validação do nome da mãe e data de nascimento (...)". (TSE, 2013a, grifo nosso).

A entidade poderia, ao receber as informações do órgão eleitoral, nos termos do parágrafo primeiro da clausula 1º (TSE, 2013a), disponibilizá-las a seus clientes quando realizassem consulta ao banco de dados da empresa.

Em contrapartida, o SERASA S/A (SERASA EXPERIAN) iria emitir ao TSE 1.000 (um mil) certificados digitais modelo e-CPF A3, o qual possibilitaria, em essência, que determinados documentos pudessem tramitar e serem validamente assinados digitalmente por integrantes do TSE.

Convém salientar que a instituição SERASA S/A (SERASA EXPERIAN) é uma empresa privada que presta uma série de serviços entre os quais se destaca a análise de

condições econômico-financeiras de determinada pessoa para a concessão de crédito, como empréstimos ou parcelamentos em compras realizadas.

A empresa "dinamiza a expansão dos negócios com segurança e rentabilidade, apontando os melhores caminhos para a tomada de decisão em crédito, marketing e certificação digital a empresas de todos os portes e setores". Aos consumidores, fornece ferramentas que possibilitam a verificação de seus relatórios e scores de crédito e a proteção contra fraudes de identidade. (SERASA, 2015).

Entre os propósitos, refere a empresa, a qual salienta que "é parte do grupo Experian, líder mundial em serviços de informação que fornece dados e ferramentas de análise a clientes ao redor do mundo" (SERASA, 2015), também se encontra a identificação de potenciais consumidores a determinado empreendimento. Neste aspecto, a empresa auxilia "as organizações em suas ações de marketing e vendas, a fim de que possam conhecer e localizar seu público-alvo, utilizar seus canais de comunicação e medir os resultados das suas ações para aprimorá-las continuamente" (SERASA, 2015).

Tendo em vista a repercussão que o fato gerou após a sua publicação, a então Presidente da Corte Eleitoral, Ministra Carmem Lúcia, em 09 de agosto de 2013, avocou os autos para exame e, com base na falta de amparo legal para que o acordo fosse firmado, declarou a nulidade do ato. Destaca-se que este ainda não havia produzido efeito, pois as informações não haviam sido disponibilizadas à empresa privada citada.

O acordo havia sido assinado pelo Diretor-Geral do TSE, após ouvidas as unidades competentes, incluindo a própria Corregedoria Geral Eleitoral, com base no art. 116, inc. XI, do Regulamento Interno da Secretaria do Tribunal Superior Eleitoral, o qual lhe atribuía competência para firmar acordos, convênios ou ajustes.

Não obstante, a presidente do TSE sustentou que o acordo firmado carecia de previsão legal para ser firmado e produzir efeitos. E, nesse sentido, a nulidade poderia ser decretada em virtude da respectiva antijuridicidade, não sendo necessária a análise da conveniência e oportunidade do ato administrativo.

Entre os fundamentos adotados (TSE, 2013b, p. 4-5) foi afirmado, sustendo-se a regra da inacessibilidade da base de dados eleitoral conjugada com o princípio constitucional da privacidade, que o "cadastro eleitoral é patrimônio dos cidadãos brasileiros. Em especial, patrimônio dos eleitores nacionais. E o seu fundamento é a confiança na Justiça Eleitoral e na inexpugnabilidade dos dados a ela confiados".

Como decorrência da decisão foi alterado o texto normativo que permitia ao Diretor-Geral do TSE assinar acordos de cooperação técnica sem que seja por delegação da Presidência do Tribunal. Ainda, foi determinada a formação de um grupo de trabalho para revisão dos acordos de cooperação vigentes e tinham como objeto o cadastro de eleitores ou dados a eles relativos.

Referido episódio é paradigmático para demonstrar não só a relevância das informações constantes nos cadastro eleitoral brasileiro, mas principalmente a existência de um regramento protetivo e claro referente aos dados pessoais.

Um cadastro com quantidade substancial de dados pessoais deve receber proteção legal adequada. Ademais, as responsabilidades por eventual violação devem estar especificadas, notadamente nas situações em que são utilizados ou compartilhados de forma não permitida ou com finalidade diversa ao inicialmente previsto e autorizado pelo cidadão

4. A INSUFICIENTE PROTEÇÃO DE DADOS NO BRASIL

Frente a situações como a descrita o item anterior, possível destacar que o decreto é marcado por uma grande lacuna e não contribui satisfatoriamente para o tema, já que não menciona em nenhum momento o termo "dados pessoais" – optando por falar em "dados cadastrais" e "dados individualizados".

A especificação da finalidade e a limitação do uso são princípios básicos de leis internacionais dessa matéria e também do Projeto de Lei para a Proteção de Dados Pessoais que tramita perante o Congresso Nacional[5]. A noção subjacente é a de que o uso de informações pessoais deve servir à finalidade comunicada na coleta e a outros propósitos compatíveis, nos limites do consentimento do indivíduo.

Com efeito, a finalidade integra os princípios enumerados por Rodotà (2008, p. 60) como norteadores da proteção de dados pessoais, quais sejam:

> *princípio da correção* na coleta de dados e no tratamento das informações;
> *princípio da exatidão* dos dados coletados, acompanhado pela obrigação de sua utilização;
> *princípio da finalidade* da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que especifica na relação entre os dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e a

[5] Projeto de Lei nº 5.276/2016, disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378, acesso em 05.jun.2017.

> utilização dos dados (*princípio da utilização não-abusiva*); na eliminação ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);
> *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> *princípio da segurança* física e lógica da coleta dos dados.

É por isso que um programa de compartilhamento de dados não pode só ser justificado em termos de eficiência de gestão do Estado, como o governo até agora o fez. Ele precisa instituir garantias aos indivíduos afetados, sob pena de já nascer em descompasso com as discussões mais recentes sobre proteção de dados pessoais, que inclusive vê ocorrendo no Congresso Nacional.

Ressalte-se que, independentemente da definição de privacidade que se adote, deve-se ter uma ampliação da tutela da esfera privada dos sujeitos em virtude do tipo e quantidade de informações que são coletas e, como consequência, gerado um dano ao indivíduo.

Para melhor exemplificação, Rodotà (2008, p. 129) traz efeitos do panorama tecnológico essenciais à privacidade, e a define de forma singela como "*o direito de manter o controle sobre as próprias informações"* (RODOTÀ, 2008, p. 92):

> a) impõe como direito fundamental;
> b) especifica-se como direito à autodeterminação informativa e, mais precisamente, como direito a determinar as modalidades de construção da esfera privada na sua totalidade;
> c) apresenta-se, por fim, como precondição da cidadania na era eletrônica e, como tal, não pode ser confiada unicamente à lógica da auto-regulamentação ou das relações contratuais.

A justificativa trazida pelo autor para estipular tais características inerentes à privacidade é a de que "a descrição de um novo panorama tecnológico e as transformações que traz consigo, se apresentam como um caminho que deve ser percorrido para à plena compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação" (RODOTÀ, 2008, p. 127).

Ou seja, "como vivemos em um mundo onde as informações estão divididas com uma pluralidade de sujeitos e a coleta de informações que anteriormente era realizada através de cessões vindas de relações interpessoais e agora ocorre através de transações abstratas, passa-se de um mundo no qual o problema era o controle do fluxo das informações que saiam de dentro da esfera privada em direção ao exterior, para um mundo no qual o problema é o controle

das informações que entram, tal como demonstra a autodeterminação do direito de não saber, pela atribuição dos indivíduos do poder de recusar interferências em sua esfera privada" (RODOTÀ, 2008, p. 128).

Todavia, assumindo os efeitos e seguindo os aspectos da privacidade trazidos por Rodotà, a definição do direito à privacidade compatível com a era moderna-tecnológica se dá como o direito fundamental à autodeterminação e ao controle informativo, decidindo, em sua totalidade, os dados informativos que constroem, adentram e saem da esfera privativa, apresentando-se como precondição da cidadania na era moderna, não sendo restrito à lógica da auto-regulamentação ou das relações contratuais, justificando-se à compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação e de um conjunto de condicionamentos.

Porém, como "vivemos em um mundo no qual aumenta o valor agregado das informações pessoais, onde a referência ao valor da pessoa em si e de sua dignidade passou a ser secundário em relação à transformação da informação em mercadoria" (RODOTÀ, 2008, p. 128), o desafio para aplicação do direito à privacidade é constante.

Informações de todos os tipos são coletadas mediante programas ou objetos de interação social. Seja pelo computador ou pelo *smartphone*, o acesso à uma rede social ou a algum sítio eletrônico da internet, na maioria das vezes se realiza uma pequena coleta de dados por meio de *cookies*[6] de quem o está utilizando ou acessando para com algum objetivo proposto (expressamente) pelos desenvolvedores, e aceito (tácita ou expressamente) pelos usuários.

"O aumento da quantidade de informações pessoais coletadas por instituições públicas e privadas através de aplicativos de *smartphones* ou no acesso em rede, de forma geral, visa sobretudo à dois objetivos: por parte dos poderes púbicos, a aquisição de elementos necessários à gestão de programas de intervenção, e o desenvolvimento de estratégias empresariais privadas; conjuntamente ao controle da conformidade da população à gestão política dominante ou aos comportamentos prevalecentes" (RODOTÀ, 2008, p. 28).

[6] "Um *cookie* é um pequeno texto que os sites podem enviar aos navegadores, anexado a qualquer conexão. Nas visitas posteriores o navegador reenvia os dados para o servidor dono do *cookie*. Um *cookie* é transmitido até que perca a validade, que é definida pelo site. Os sites geralmente usam os *cookies* para distinguir usuários e memorizar preferências." Cf: http://br.mozdev.org/firefox/cookies. Acesso em 28.out. 2016.

Assim, a caracterização da organização social como uma sociedade com bases na acumulação e circulação das informações torna-se clara, trazendo novas situações e tipos de poder. Este, contudo, problemático ao ser legitimado e fundado na informação.

Tais desafios dão-se, "primeiramente, em virtude e a dificuldade de individualizar certos tipos de informações das quais o cidadão estaria disposto a renunciar definitivamente a controlar o seu tratamento e a atividade dos sujeitos que a utilizam, pois publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Em segundo lugar, a nova situação determinada pelo uso de computadores no tratamento das informações pessoais faz-se mais difícil caracterizar o cidadão como simples 'fornecedor de dados', sem que a ele caiba algum poder de tutela e tratamento dessas informações" (RODOTÀ, 2008, p. 36).

"As informações coletadas, além fazer as organizações públicas e privadas capazes de planejar e executar os seus programas, ainda permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes" (RODOTÀ, 2008, p. 37).

Daí a importância da proteção jurídica da privacidade, da vida privada ou da intimidade, cuja definição é trazida por Doneda (2006, p. 101):

> Ao se tratar da privacidade, há de se fazer antes de tudo um esclarecimento inicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representa-la , propriamente ou não, é considerável; além de 'privacidade' propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como 'privatividade' e 'privaticidade', por exemplo. O fato da doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas.

De acordo com Limberger (2007, p. 116), a intimidade como direito fundamental tem sua gênese na "[…] dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional". Para a autora, "[…] As exigências do mundo tecnológico atual fizeram com que o direito tutelasse essa nova face da intimidade. A intimidade deriva da dignidade humana, é um direito fundamental que integra a personalidade. Das relações da informática e a intimidade se desenvolve a autodeterminação informativa. […]" (LIMBERGER, 2007, p. 119).

Para Rodotá (1995, p. 122), a privacidade é "[…] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada […]".

No direito brasileiro, o direito à privacidade pode ser entendido como um direito da personalidade de matiz constitucional, com expressa previsão no artigo 5º, inciso X, da Constituição da República.

Infraconstitucionalmente, a proteção da privacidade se consubstancia na cláusula geral estabelecida no artigo 21 do Código Civil. Ainda, destaca-se que as previsões legislativas específicas para a proteção de dados são escassas. Tem-se, na Lei Federal nº 8.078/1990 - Código de Defesa do Consumidor, a regulamentação dos bancos de dados e cadastros de consumidores em único dispositivo, o artigo 43. Além disso, há a regulamentação do chamado cadastro positivo pela Lei Federal nº 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

No presente estudo, assim se define privacidade:

> [...] um direito fundamental, em sentido amplo, capaz de recepcionar em seu bojo a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet, significa dizer que, na contemporaneidade, o direito de navegar na internet com privacidade, o direito de monitorar quem monitora, o direito de deletar dados pessoais e o direito de proteger a identidade online devem ser tutelados, explícita e expressamente, como um dos pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo. (FORTES, 2015, p. 188).

A proteção dos dados no sistema normativo da União Europeia (UE) é tratada por meio de um sistema de regulamentos e diretivas, na qual é possível encontrar aspectos pioneiros no regramento da matéria. Há registro de legislações, por exemplo, na Alemanha e Suécia desde a década de 1970. Portugal, em 1976, e, posteriormente, Espanha, em 1978, foram os primeiros países a elevar a proteção em nível constitucional, trazendo previsões expressas nas suas respectivas Cartas.

Atualmente, as Diretivas 95/46/CE e 2002/58/CE, e Regulamento 45/2001, trazem diretrizes para os países integrantes da UE. Ganham destaque também os Relatórios e Comunicações de acompanhamento da implantação e eficiência das normativas (FORTES, 2015, p. 132-133).

Cabe mencionar que desde o início de 2012 foi formada a Comissão Europeia para regulamentação sobre a proteção de dados pessoais. Entre os objetivos expostos há referência de que:

> La Comisión europea quiere modernizar la legislación europea de protección de datos para garantizar la intimidad de los consumidores y hacerla compatible con la libre circulación de datos en la UE . [...]
> Las empresas sólo estarán autorizadas a enviar información personal fuera de la UE a países con un nivel similar en sus sistemas de protección de datos. Se trata además de mejorar y simplificar los mecanismos de transferencia internacional de datos. [...]
> El objetivo de la nueva estrategia es consolidar un enfoque común en toda la UE. Las divergencias actuales no permiten determinar con nitidez la legislación aplicable en cada caso. Por eso es necesario armonizar las normas y reforzar el poder de las autoridades de protección de datos con el principio de cooperación y coordinación. (COMISIÓN EUROPEA, 2010).

Referidas premissas servem ao mesmo tempo como alerta à constante mutação e evolução da tecnologia e da forma como os dados podem ser armazenados e manipulados. É importante, ainda, considerar a facilidade do intercâmbio de informações e procurar meios para que essa circulação atenda a requisitos de segurança e preservação da privacidade.

A utilização dos recursos tecnológicos alterou significativamente a circulação, a forma de compartilhamento e o armazenamento de dados. A digitalização de documentos e o arquivamento de informações em bancos de dados digitais é cada vez mais significativo.

Nesse contexto, a proteção de dados pessoais nos sistemas jurídicos em geral necessita de uma análise mais criteriosa, principalmente no sistema jurídico brasileiro, no qual não se tem uma legislação específica acerca da proteção dos dados pessoais.

Ao contrário da legislação encontrada em países da Europa, não há no sistema jurídico brasileiro, por exemplo, uma autoridade responsável e independente, dedicada a preservar o consentimento e o uso de dados pessoais mediante a supervisão do cumprimento das obrigações dos responsáveis pelo tratamento de dados, as quais possuem previsão específica (GALINDO, 2013, p. 136).

De acordo com a normativa europeia, em caso de descumprimento, qualquer cidadão pode reclamar à autoridade de proteção dos dados, a qual estará apta a instaurar procedimento administrativo e aplicar sanções ao responsável. Referida característica, conforme Galindo (2013, p. 137), é relevante, pois:

> ...se completó este cuadro de derechos y obligaciones con la atribución legal a la autoridad de protección de datos de su obligación de velar por el cumplimiento de las

> medidas conducentes a evitar la modificación de los datos personales por la utilización de las técnicas de seguridad de las TIC consideradas más adecuadas en cada momento.

A existência de autoridade responsável pela proteção dos dados, com atribuições claras e voltadas a não transgressão dos dados pessoais, afigura-se, portanto, um relevante mecanismo.

A autodeterminação informativa é um direito que orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico. "Concebido como um direito fundamental (...), o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações" (DONEDA, 2006, p. 196-197).

Em um julgamento (*BverfGE 65,1*) emblemático do Tribunal Constitucional Federal da Alemanha, de 15 de dezembro de 1983, averiguou-se a constitucionalidade da lei que ordenava o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho para fins estatísticos.

Segundo o Tribunal Constitucional Federal da Alemanha, em virtude das condições do moderno processamento de dados, o direito geral da personalidade contido no artigo 2 *I GG*, em conjugação com o artigo 1 *I GG*, passa a abranger a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, que somente podem ser utilizados, em princípio, com sua autorização. Essa norma consubstancia um direito geral à autodeterminação sobre a informação, que somente é restringível se houver a contraposição de um interesse predominante da coletividade (SCHWABE, 2005, p. 233-235).

Na construção dessa norma concreta, o Tribunal Constitucional Federal da Alemanha considerou que o direito ao livre desenvolvimento da personalidade abrange o poder do indivíduo de decidir, por si próprio, quando, quais e em que limites os fatos pessoais serão revelados, poder que, diante da evolução tecnológica atinente ao processamento automático de dados, depende de uma proteção especialmente intensa (SCHWABE, 2005, p. 237).

A faculdade contemporânea e futura de armazenamento ilimitado, transmissão instantânea e consulta irrestrita de dados atentaria contra a autodeterminação individual, uma vez que não mais possibilitaria a determinação, com segurança, de quais informações sobre a sua pessoa são conhecidas, nem por quem são acessadas, inibindo substancialmente a liberdade de planejar ou decidir com autodeterminação (SCHWABE, 2005, p. 237).

Esse direito à autodeterminação informativa, porém, não é absoluto, mas restrito quanto às informações de interesse geral predominante, quer dizer, limitável excepcionalmente

quando imprescindível para a consecução de um interesse público. Tais restrições exigem uma base constitucional que possibilite o conhecimento, pelo cidadão, de forma clara e reconhecível, dos pressupostos e da extensão das limitações, atendendo ao princípio da transparência do Estado de Direito (SCHWABE, 2005, p. 237-239).

O núcleo da autodeterminação informativa, enquanto relacionada ao aspecto básico do direito à intimidade, constitui-se na faculdade que a pessoa detém de escolher sobre a divulgação e a revelação de informações que diretamente a ela se referem.

Para Doneda (2006, p. 201) a terminologia mais adequada é tão somente "proteção de dados pessoais", pois estaria englobada tanto a problemática da privacidade quanto a da informação, que teria como ponto de referência os direitos da personalidade e estaria isenta de uma acepção patrimonialista ou contratual, ao mesmo tempo em que não remonta ao direito à liberdade em uma acepção demasiadamente ampla.

A crítica do jurista citado reside basicamente em três fatores. O primeiro é acerca da correta definição do que seja autodeterminação, pois em determinado sentido poderia dar ao indivíduo a oportunidade de controlar as informações que lhe digam respeito dentro de parâmetros quase ilimitados (DONEDA, 2006, p. 198).

Já para uma segunda leitura, em chave liberal, a autodeterminação concentrar-se-ia no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, afastando a matéria do âmbito dos direitos da personalidade (DONEDA, 2006, p. 198).

Por fim, outro fator seria a possibilidade de se ter a impressão de que as pessoas teriam um direito de propriedade sobre suas informações, o que as transportaria para o campo das situações patrimoniais (DONEDA, 2006, p. 198-199).

Outro aspecto a ser delimitado é a importância da existência de um órgão responsável pela proteção dos dados pessoais. Trata-se de órgão com diversas atribuições sociais, políticas e jurídicas, pois, como se observa em experiências europeias, além de fiscalizar, controlar e aplicar sanções à violação dos dados pessoais, cabe a promoção de ações educativas e de informação tanto para cidadãos quanto para órgãos públicos.

É preciso delimitar as atribuições, estrutura, composição e observar uma autonomia financeira e política a esse órgão. A vinculação a órgãos governamentais e ligados ao Poder Executivo não é desejável. Ainda, a dependência ao Poder Legislativo, Judiciário ou outros da

estrutura jurídico-administrativa (Ministério Público, por exemplo) também podem comprometer a segurança dos dados, notadamente pelo interesse em determinadas demandas.

O novo órgão deve ter autonomia e meios efetivos de executar sanções aos infratores, além de organizar as políticas para a conscientização quanto à utilização e guarda de dados pessoais.

Ademais, sua composição deverá ser híbrida e seus integrantes oriundos de diversos segmentos sociais. Ao mesmo tempo em que é importante que se tenha um órgão com conhecimentos técnicos acerca da criação e manutenção de banco de dados é importante que haja uma interdisciplinaridade em seu Conselho administrativo.

Nesse sentido, referidos integrantes poderão advir de diferentes áreas do conhecimento contribuindo para uma melhor regulamentação da legislação protetiva e adequação à realidade das relações sociais e institucionais.

Ao falar sobre a independência de uma autoridade de proteção de dados, Doneda (2006, p. 393) afirma que referida característica pressupõe a presença de "mecanismos de nomeação de seus membros, geralmente limitando a discricionariedade na sua escolha (através, por exemplo, da exigência de determinada formação ou atuação profissional)", além "da incompatibilidade de sua atuação com outras atividades, atuais ou mesmo pregressas (e também futuras [...]), além da limitação temporal de seu cargo" (DONEDA, 2006, p. 393).

Ainda, a independência pressupõe "a ausência de ingerência governamental sobre seus atos, que se pode obter situando tais órgãos fora de uma posição hierárquica em relação ao governo" (DONEDA, 2006, 393-394).

Além da especificidade referente à matéria e da função de velar pelo fiel cumprimento e respeito à lei, interpretando-a e aplicando-a, o ente independente deve ser dotado de poderes para inspecionar e aplicar sanções. É preciso que os responsáveis pelos arquivos mantenham referido órgão informado acerca das características de seu banco, além de, sendo o caso, quando requisitados, deem acesso aos dados que nele constam.

5. A FRAGILIDADE DA PROTEÇÃO DE DADOS E O DECRETO FEDERAL

O Decreto Federal nº 8.789/2016 tem implicações diretas sobre o tema da proteção dos dados pessoais.

A argumento da eficiência é louvável, todavia é preciso analisar se os direitos fundamentais do cidadão serão preservados e, especialmente para o tema objeto desse artigo, a privacidade.

Os órgãos da administração pública federal do Brasil administram o maior cadastro de cidadãos de toda América Latina, cuja base de dados que poderá ser compartilhada, se não acompanhada de salvaguardas efetivas aos direitos dos indivíduos, é deveras preocupante, de maneira que é preciso que se reflita acerca do controle dos dados relativos à personalidade do indivíduo (sexo, escolaridade, residência, data de nascimento, filiação, entre outros), assim como os biométricos (assinatura digital, foto e impressões digitais dos dedos de ambas as mãos) por órgãos do Estado, especialmente no caso brasileiro que, como referido, não disciplina juridicamente a matéria.

O compartilhamento de informações facilita o acesso a detalhes privados da vida dos cidadãos. Ainda mais na sociedade atual, permeada por dispositivos informáticos que permitem o processamento de milhares de informações a partir de apenas um *click* e possibilita que a informação circule ao redor do mundo com celeridade impressionante.

As tecnologias utilizadas, combinadas com outras informações, como, por exemplo, a utilização de senhas de acesso e dados biométricos, fazem com que se individualize o usuário e seja possível traçar um perfil baseado nas suas atividades diárias e movimentações financeiras.

Trata-se de dados cujo interesse é de grande relevância e possuem imensurável valor, de maneira que a ausência de uma legislação protetiva dos dados pessoais torna ainda mais temerário o seu compartilhamento. É preciso a observância dos princípios protetivos na coleta, tratamento e armazenamento desses dados. Além disso, uma definição clara de responsabilidades e funções, em outras palavras, um sistema de salvaguardas ao direito constitucional da privacidade.

Compartilhar essas informações tem um grande potencial de fragilizar os sistemas de proteção de dados pessoais passíveis de ser implantados, na medida em que uma possível vulneração permitirá o acesso indevido a todos os dados relevantes, inclusive dados sensíveis, do cidadão. Ainda, são disponibilizadas às autoridades estatais informações que não lhes seria legítimo aceder, com a elevação de exercício de controles nem sempre utilizados de forma adequada (CELLA, ARNS DE OLIVEIRA, 2015).

No que tange à imposição de sanções em caso de eventual transgressão aos limites objetivamente definidos na legislação, cabe destacar que não basta apenas a aplicação de sanções pecuniárias e cujo arbitramento fique ao alvitre do julgador.

É preciso que sejam estabelecidos balizas na própria lei de forma proporcional à gravidade da violação à privacidade, de forma que tanto quem irá concretizar a norma ou aquele que a viola tenha possibilidade de saber as consequências dos atos. Do contrário, corre-se o risco de patrimonializar o direito à privacidade, o qual, na realidade, está diretamente relacionado à personalidade do indivíduo.

6. CONCLUSÃO

O tema da privacidade tem relação direta com o nível de desenvolvimento tecnológico da sociedade. Conforme se prolifera o uso das novas tecnologias no meio social, aumenta a necessidade de se pensar as relações de poder, transparência e autonomia individual na sociedade.

O uso de produtos tecnológicos tem crescido significativamente nos últimos anos e tem sido influenciado a rotina das pessoas. Estas passam várias horas em frente à tela do computador, de um *smartphone* ou *tablet*. Utiliza-se as redes sociais e *blogs* para comunicação e divulgação de informações. As informações são buscadas e armazenadas em diversas fontes do ciberespaço ou meio digital.

Na era da informação o tema proteção dos dados pessoais ganha ainda mais relevância, pois a facilidade do acesso a dados e informações e a utilização de recursos e mídias sociais os deixam vulneráveis.

É preciso que os instrumentos normativos estejam em consonância com a aludida mutabilidade social oriunda célere evolução tecnológica. É importante que as normativas acompanhem as novas descobertas científicas, devendo, quando menos, existirem diretrizes transparentes e objetivas que permitam a adaptação legislativa.

O sistema jurídico de proteção dos dados pessoais deve ser constituído de uma estrutura sólida que dê transparência e que estabeleça um sistema de identificação e armazenamento de dados com salvaguardas. É necessária uma definição clara acerca de quem controla, quem fiscaliza, quem é responsável e a forma como os dados podem ser compartilhados.

O Decreto Federal nº 8.789/2016, por exemplo, em nome de economia e simplificação da atividade administrativa, promove a abertura de bases de dados do governo federal brasileiro, suas autarquias e entidades controladas, sem as necessárias salvaguardas referentes à proteção da privacidade e dos dados pessoais.

No presente estudo foi verificado que o sistema jurídico brasileiro não apresenta as salvaguardas necessárias à proteção da privacidade, confirmando-se a hipótese inicial de que de que a aplicação dos ditames do Decreto Federal nº 8.789/2016 não garante proteção adequada e se torna temerária na medida em que coloca em risco a garantia individual de proteção da privacidade, pois não assegura a não ocorrência do repasse de dados pessoais em acordos entre órgãos públicos, ratificando o argumento da urgência de uma lei específica de proteção de dados no direito brasileiro.

O caso envolvendo o TSE e a empresa SERASA S/A é emblemático e serve para acender alerta acerca do uso e tratamento indiscriminado de dados de caráter pessoal. Ainda, observa-se que a ausência regulamentação de regulamentação específica gera insegurança e coloca em risco a privacidade dos cidadãos que fornecem suas informações pessoais, muitos vezes compelidos por motivos diversos, como por exemplo, a obtenção do título de eleitor.

É premente a necessidade de um regramento específico e que delimite as responsabilidades pelo uso irrestrito e desarrazoado por aqueles titulares e responsáveis pelos bancos de dados, sejam eles públicos ou privados.

Não há no Decreto Federal citado salvaguardas hígidas a garantir e evitar que casos semelhantes como o caso envolvendo a Justiça Eleitoral e a grupo privado voltem a se repetir, colocando em risco a proteção do cidadão.

O compartilhamento de dados pessoais pelos órgãos da administração pública federal brasileira, nos moldes do Decreto Federal nº 8.789/2016, compromete o direito à privacidade do cidadão. A norma em referência permite o compartilhamento de dados sensíveis do cidadão ao mesmo tempo em que não existem parâmetros acerca do controle e responsabilidade no tratamento dessas informações.

O uso indiscriminado desses dados, além de vulnerar direito fundamental, facilita o controle e monitoramento dos cidadãos.

Os dados e informações pessoais devem ter um controle mais amplo pelo próprio indivíduo, o qual necessita ter acesso às informações armazenadas nos bancos de dados a seu respeito, podendo exigir a sua retirada ou alteração e atualização. Busca-se, em última análise,

a correção dos dados, conhecimento pelo indivíduo acerca da existência de cadastro e do que consta a seu respeito.

Ademais, a criação de uma autoridade independente pode contribuir, a exemplo do direito europeu, para a efetivação proteção dos dados. Nos moldes apresentados trata-se de ente multidisciplinar, mas ao mesmo tempo especializado no tema, sem subordinação a órgãos estatais e privados.

Outra vantagem de referida autoridade é resolver as demandas ainda no âmbito administrativo, sem necessidade de se recorrer ao Poder Judiciário. Todavia, é preciso que tanto procedimento, funções, sanções e demais atribuições estejam previstas em legislação específica.

Portanto, é imprescindível a instituição de uma legislação protetiva dos dados pessoais no sistema jurídico brasileiro para garantia da privacidade dos cidadãos. É a partir de parâmetros claros, transparentes, e com a especificação de princípios, direitos e deveres acerca do tema que normativas como o Decreto Federal nº 8.789/2016 podem obter êxito sem que se vulnere dados pessoais ou, quando menos, coloque-os em risco em razão de uma proteção deficiente.

7. REFERÊNCIAS

BRASIL, Decreto Federal nº 8.789, de 29 de junho de 2016. **Diário Oficial [da] República Federativa do Brasil**, Presidência da República. Brasília, 30.jun. 2016. Seção1, p. 1.

BRASIL. Mensagem nº 192, de 28 de maio de 2015. **Diário Oficial [da] República Federativa do Brasil**, Presidência da República. Brasília, 29 mai. 2015. Seção1, p. 1.

CELLA, José Renato Gaziero; ARNS DE OLIVEIRA, Marlus H. A unificação do registro de identidade civil e a proteção de dados pessoais no Brasil. In: **III Encontro de Internacionalização do CONPEDI**, 2015, Madrid.

COMISIÓN EUROPEA. **Estrategia de la ue para la protección de datos en internet**. 2010. <http://ec.europa.eu/spain/actualidad-y-prensa/noticias/internet-y-sociedad-de-la-informacion/proteccion-datos-internet-ue_es.htm>. Acesso em: 23 set. 2015.

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

FORTES, Vinícius Borges. **O direito fundamental à privacidade**: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. 2015. 225p. Tese (Doutorado em Direito) - Universidade Estácio de Sá, Rio de Janeiro, 2015.

GALINDO AYUDA, Fernando. Seguridad y sociedad del conocimiento. In: GALINDO, Fernando (ed.). **El derecho de la sociedad en red**. Lefis Series, 14. Zaragoza: Prensas de la Universidad de Zaragoza, 2013. p. 129-154.

LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

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

SCHWABE, Jürgen. **50 anos de jurisprudência do tribunal federal constitucional alemão**. Traduzido por Beatriz Hennig et all. Montevidéu: Fundacion Konrad-Adenauer, 2005.

SERASA. **Serasa Experian**: Quem somos. 2015. Disponível em <http://www.serasaexperian.com.br/quem-somos/>. Acesso em: 22 ago. 2017.

TRIBUNAL SUPERIOR ELEITORAL. **Acordo de Cooperação Técnica TSE nº 07/2013**, de 16 de julho de 2013. 2013a. Disponível em: <http://s.conjur.com.br/dl/acordo-cooperacao-tecnica-72013-tse.pdf>. Acesso em: 14 fev. 2016.

TRIBUNAL SUPERIOR ELEITORAL. **Decisão Procedimento Administrativo n. 29.542/2012-TSE**, de 09 de agosto de 2013. 2013b. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-acordo-cooperacao-serasa>. Acesso em: 14 fev. 2016.