V. 14 N. 2
MAIO-AGO 2018

ISSN 2317-6172

Revista DIREITO GV

FGV DIREITO SP

Recebido: 17.11.2016
Aprovado: 09.03.2018

DOI: http://dx.doi.org/10.1590/2317-6172201821

Os desafios da Administração Pública na disponibilização de dados sensíveis

THE CHALLENGES OF PUBLIC ADMINISTRATION ENABLING ACCESS TO SENSITIVE DATA

Tânia Carolina Nunes Machado Gonçalves[1] *e Marcelo D. Varella*[2]

Resumo

No contexto da Lei de Acesso à Informação – em que a publicidade é a regra e o sigilo a exceção –, do Marco Civil da Internet e de decretos como o que trata da interoperabilidade de bases de dados, um dos desafios da Administração Pública brasileira é lidar com as bases de dados que contêm dados sensíveis. Nesse cenário, o presente artigo buscou analisar o modelo de disponibilização de bases de dados em ambientes denominados seguros. Foram examinados os modelos do Instituto Brasileiro de Geografia e Estatística (IBGE), do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e do Instituto de Pesquisa Econômica Aplicada (Ipea), apontando suas principais semelhanças e diferenças. Verificou-se que as dificuldades perpassam a ausência de legislação específica; bem como a imprecisão e a vagueza de conceitos contidos na legislação, motivos pelos quais se propôs a adoção de uma nova terminologia. Além disso, observou-se que essas instituições apresentam níveis diferenciados de segurança da informação, e o eventual mau uso ou vazamento desses dados pode levar a consequências indesejáveis.

Palavras-chave

Lei de Acesso à Informação; dados pessoais; dados sensíveis; privacidade; bases de dados.

Abstract

In the Brazilian context of the Access to Information Law – where publicity shall rule and secrecy is an exception –, of the Internet Bill of Rights and of the decree that allows sharing databases in the federal public sphere, one of the challenges that the Public Administration is dealing with are databases which contain sensitive data. In this scenario, the present article sought to analyze one of the models of enabling access to sensitive data at the so-called "safe room". The models of the Brazilian Institute of Geography and Statistics (IBGE), of the National Institute for Educational Studies and Research Anísio Teixeira (Inep), and of the Institute for Applied Economic Research (Ipea) were examined, pointing out their main similarities and differences. It has been found that the difficulties start from the absence of specific legislation and the imprecision of several concepts within the legislation, reason why it was proposed the adoption of a new terminology. In addition, it has been observed that these institutions provide different levels of information security and any misuse or leakage of such data can lead to undesirable consequences.

Keywords

Access to Information Law; personal data; sensitive data; privacy; databases.

1 Centro Universitário de Brasília
Brasília – DF – Brasil
https://orcid.org/0000-0003-3795-3596

2 Centro Universitário de Brasília
Brasília – DF – Brasil
https://orcid.org/0000-0001-5538-0838

Introdução

Um dos grandes desafios da Administração Pública na atualidade é tentar atender às regras de transparência e publicidade exigidas pela chamada Lei de Acesso à Informação – LAI (Lei n. 12.527, de 18 de novembro de 2011) e, ao mesmo tempo, respeitar as necessárias restrições quanto à confidencialidade da informação no caso de grandes bases de dados que apresentam informações sensíveis. Os modelos hoje existentes de disponibilização de dados sensíveis adotados por algumas entidades da Administração Pública brasileira parecem ser precários no que tange à segurança da informação e ao elevado risco de divulgação indevida.

O respeito aos dados pessoais tem sido discutido amplamente após a publicação do Marco Civil da Internet e dos decretos de regulamentação, como o Decreto de interoperabilidade de bases de dados. De fato, parte dos atores envolvidos defende a livre circulação de informações entre órgãos públicos ou empresas de um mesmo grupo de prestação de serviços, outros acreditam que as regras de privacidade não se aplicam ao setor público, mesmo no tocante ao fornecimento de informações a atores privados,[1] o que merece ser cotejado com o respeito da individualidade e da privacidade. Com efeito, como afirmam Milagre e Segundo (2015, p. 52), "se a informação não está acessível a todos, esta disparidade gera status e valor àqueles que conseguem acessar e processar tal informação".

1 Sobre o assunto, ver art. 26, parágrafo único do Projeto de Lei n. 5.276/2016, que visa proibir a transferência de bases de dados gerenciadas por órgãos ou entidades da Administração Pública para entidades privadas sem a necessidade de consentimento. Vide, também: a) o item 16 de CNSEG/Feaseg (2015), que sustenta que "essa vedação criará dificuldades para a cooperação entre poder público e privado em diversas áreas, inclusive no combate a atividades criminosas, como no caso do combate à fraude contra o seguro"; b) a p. 19 de Brasscom (2017), que afirma que "ao restringir a transferência de dados (seja total ou parcial) para entidades privadas, a legislação poderá privar o Poder Público de usar tecnologias inovadoras, em sua grande maioria produzidas pelo setor privado. Um bom exemplo são os serviços da *Big Data* via computação em nuvem (*Cloud*), possibilitando ao Poder Público ter acesso a grande poder de processamento e de análise de dados sem, no entanto, ter de investir em infraestrutura física (que envolve altos custos com aquisição e instalação de equipamentos, manutenção, energia elétrica, entre outros). Tal legislação também poderia restringir o acesso do Poder Público a tecnologias de armazenamento de dados e de padrões de segurança criptográficos em nuvem. Ademais, restringir esse tipo de transferência de dados não garante necessariamente que o Poder Público terá as melhores condições de garantia da segurança da informação do que aqueles que são oferecidos hoje por algumas empresas do setor privado. Corre-se o risco de paralisar a execução de serviços importantes, como os sociais, por exemplo, que são prestados pelo Poder Público com o auxílio de entidades privadas"; e c) o comentário de Danilo Doneda na matéria de Cruz e Marchezan (2015, p. 1): "O governo tem algumas prerrogativas e facilidades para obter dados pessoais, você veja que o consentimento para a coleta de dados por parte do governo não é necessário em muitos casos no anteprojeto. E essa é uma regra no governo, os órgãos públicos realizando atividades dentro de suas competências, a princípio, não precisam pedir consentimento. Isso é balanceado com a transparência, você tem que deixar claro o que fazem, como fazem. Transparência seria a compensação pela desnecessidade do consentimento".

Assim, com a entrada em vigor da LAI, em maio de 2012, foi possível positivar a demanda da sociedade por maior transparência, com informações claras, inclusive, de natureza pessoal ou sigilosa, sob a guarda da Administração. De acordo com o Relatório de Pedidos de Acesso à Informação (SISTEMA ELETRÔNICO DO SERVIÇO DE INFORMAÇÃO AO CIDADÃO, 2016), de maio/2012 a setembro/2016, a quantidade de pedidos realizados a todos os órgãos ou entidades da Administração Pública Federal superou a marca de 400 mil.

Entretanto, apesar de o Ministério da Transparência, Fiscalização e Controle (antiga Controladoria-Geral da União – CGU) esclarecer que "não existem informações sistematizadas acerca do número total de pedidos de acesso à informação que dizem respeito a informações pessoais e sigilosas, pois o sistema não coleta esse tipo de dado",[2] a partir do citado Relatório, a quantidade de acessos negados aos cidadãos em razão de tratar-se de: a) "dados pessoais", b) "informação sigilosa de acordo com legislação específica" e/ou c) "informação sigilosa classificada conforme a Lei n. 12.527/2011" corresponde a, aproximadamente, 5,09% dos pedidos respondidos. Se for considerada apenas a quantidade de acessos negados, esses três argumentos representam 56,15% das respostas denegatórias dadas pela Administração, conforme se observa na Tabela 1.

TABELA 1 – **PEDIDOS DE ACESSO À INFORMAÇÃO FEITOS À ADMINISTRAÇÃO PÚBLICA FEDERAL POR MEIO DO E-SIC**

ANO	2012	2013	2014	2015	2016	TOTAL 2012-2016
1. QUANTIDADE DE PEDIDOS REALIZADOS	55.212	86.661	90.167	102.423	84.443	418.906
2. QUANTIDADE DE PEDIDOS RESPONDIDOS	55.162	86.573	89.987	101.940	79.343	413.005
3. QUANTIDADE DE PEDIDOS NEGADOS	4.856	9.618	9.927	7.663	5.385	37.449
3.1. RAZÃO DA NEGATIVA: DADOS PESSOAIS	2.126	3.734	3.182	2.278	1.007	12.327
3.2. RAZÃO DA NEGATIVA: INFORMAÇÃO SIGILOSA DE ACORDO COM LEGISLAÇÃO ESPECÍFICA	627	1.435	1.186	1.128	921	5.297

2 Informação obtida com a antiga Controladoria-Geral da União, a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 00075.000939/2016-76, de 23/08/2016).

3.3. RAZÃO DA NEGATIVA: INFORMAÇÃO SIGILOSA CLASSIFICADA CONFORME A LEI N. 12.527/2011	308	368	1.168	890	669	3.403

Fonte: Elaboração própria, a partir das informações constantes do Relatório de Pedidos de Acesso à Informação e Solicitantes do sítio eletrônico: <http://esic.cgu.gov.br/sistema/Relatorios/Anual/RelatorioAnualPedidos.aspx>.

A problemática enfrentada pela Administração, com demandas dessa natureza, tem início com a falta de definição clara de conceitos diretamente relacionados ao tema. É o caso, por exemplo, da vagueza dos princípios constitucionais de publicidade e privacidade ou de termos técnico-científicos (como "dado" e "informação") utilizados indiscriminadamente. A matéria ainda sofre com a ausência de legislação específica para regulamentá-la, como é o caso dos dados pessoais e sensíveis, tornando o seu entendimento ainda mais dificultoso. A relação entre o Direito e a Tecnologia na proteção dos dados pessoais essenciais para a melhor avaliação de políticas públicas acaba sendo um problema global, enfrentado, com diferentes soluções, por vários países (ROBINSON et al., 2009).

Nesse cenário, é preciso reconhecer a boa iniciativa da Administração Pública ao passar a oferecer esse serviço de disponibilização dos dados sensíveis, mostrando grande avanço quanto à transparência das informações. Os modelos objeto de discussão no presente artigo referem-se a ambientes, denominados seguros,[3] oferecidos por algumas entidades para usuários que necessitam acessar bancos de dados específicos para cruzar informações não disponíveis em microdados públicos.

Em âmbito nacional, no entanto, são poucas as entidades que prestam esse tipo de serviço e com níveis diferenciados de segurança da informação. Nesse artigo, serão apresentados três exemplos e suas principais semelhanças e diferenças. No Instituto Brasileiro de Geografia e Estatística (IBGE), o acesso aos dados restritos é oferecido desde 2003. Já o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e o Instituto de Pesquisa

3 Os ambientes seguros são, inclusive, considerados canais de atendimentos específicos para certas demandas do e-SIC, cujo objeto seja de cunho pessoal ou sigiloso. Nesses casos, as respostas dadas pela Administração integram as estatísticas apresentadas como "acesso concedido" ou "acesso parcialmente concedido", ainda que o cidadão não procure o meio disponível para obter sua resposta, ou seja, não integram as estatísticas da Tabela 1. Exemplos de respostas nesse sentido (podem ser consultadas pelo sistema de busca do e-SIC: <http://www.consultaesic.cgu.gov.br/busca>): Pedidos n. 23480010339201559, n. 03950000471201642, n. 23480017371201565, n. 23480015238201574, n. 23480003441201689, entre outros.

Econômica Aplicada (Ipea) iniciaram essa atividade em 2014. Porém, diferentemente do IBGE, nesses dois casos, os pesquisadores têm acesso à base de dados "crua", ou seja, na íntegra, com todos os dados coletados identificados.

Ao apresentar esses modelos, será possível observar o porquê de ainda existirem divergências acerca do entendimento quanto à legalidade e à segurança na disponibilização desses dados, especialmente nos últimos dois casos. Para isso, esse trabalho foi divido em duas partes: a primeira, que tratará das questões conceituais relacionadas ao tema, e a segunda, que apresenta e diferencia os modelos adotados pelo IBGE, Inep e Ipea a fim de verificar as melhores práticas e as necessidades de aprimoramento em cada um deles, se for o caso. Por fim, diante da complexidade do tema, propõe-se o estudo de outros aspectos no intuito de melhorar os modelos atuais.[4]

1 A problemática na definição dos conceitos sobre dados pessoais

Trata-se de tema novo no Direito, cujos conceitos agora precisam ser mais bem definidos. A interpretação das normas e a definição do seu alcance é um problema da hermenêutica jurídica. Ramo este considerado primordial, tendo em vista que os dispositivos legais muitas vezes trazem enunciados vagos ou dúbios, podendo suscitar diversos problemas na sua aplicação. Como afirma Larenz (1997, p. 439), o motivo de a interpretação de um texto legislativo ser problemática decorre do fato de que a lei se serve da linguagem corrente, com a utilização de "termos mais ou menos flexíveis, cujo significado possível oscila dentro de uma larga faixa e que pode ser diferente segundo as circunstâncias, a relação objetiva e o contexto do discurso, a colocação da frase e a entoação de uma palavra". Nesse caso, segundo o jurista, o intérprete deve conhecer a linguagem da lei e o contexto de regulação da norma que deseja aplicar no fato concreto.

Especificamente no caso da LAI, há que se ressaltar que sua edição representa um avanço na gestão governamental brasileira ao buscar concretizar o ideal democrático do país por meio da garantia do acesso à informação por quaisquer pessoas. O objetivo é chegar a um Estado aberto, no qual haja uma sincronia do conhecimento daquele que detém o poder e daquele que outorga o poder (SILVEIRA, 2012, p. 31). "O acesso à informação coloca o cidadão em pé de igualdade com a administração pública e aí se revela parte da força democratizadora da transparência e da publicidade" (RODRIGUES, 2014, p. 94).

4 A coleta de dados da parte empírica foi feita ao longo do ano de 2016. As informações foram obtidas por meio das normas que disciplinam o serviço em cada um dos três institutos (CDDI IBGE n. 01/2003; Resolução IBGE n. CD-07/2003; Guia do Usuário da Sala de Acesso a Dados Restritos do IBGE, de 27/02/2015; Portaria Inep n. 467/2014, Nota Técnica GT-SAP n. 0001/2016 e Portaria Ipea n. 78/2014; 149/2014). Além disso, também foram analisados outros documentos que tratam do tema e realizadas visitas técnicas e reuniões com representantes dos três institutos.

Mendel (2009, p. 32), por sua vez, ao abordar os princípios que regem a LAI, e fazendo referência ao padrão da Organização para as Nações Unidas (ONU), sustenta que "os órgãos públicos têm a obrigação de revelar informações, e todo cidadão ou cidadã tem o direito correspondente de receber informações, entendendo-se por 'informações' todos os registros mantidos por órgão público, **independentemente de sua forma de armazenamento**" (grifo nosso). Mais ainda,

> para efetivar o direito à informação na prática, não basta simplesmente exigir que os órgãos públicos atendam a pedidos de informação. O acesso efetivo para muitas pessoas depende de que esses órgãos publiquem e divulguem, efetivamente, voluntariamente, de forma pró-ativa, sem necessidade de requisição, categorias-chave de informação, mesmo na ausência de um pedido (MENDEL, 2009, p. 34).

Porém, ao prever a publicidade como regra e o sigilo como exceção, alguns órgãos e entidades da Administração Pública, no afã de se tornarem mais transparentes, cumprirem as novas regras e não sofrerem sanções de órgãos de controles governamentais, passaram a oferecer serviços que podem estar ferindo uma das exceções previstas no texto legal. Em relação a essas exceções, frisa Mendel (2009, p. 36) que:

> a avaliação da legítima abrangência das exceções ao direito de acesso a informação é uma tarefa complicada. Por um lado, um sistema de exceções amplo em demasia pode prejudicar seriamente o direito. Em alguns casos, leis de direito a informação que de outra forma teriam grande efetividade são prejudicadas em grande parte por um regime de exceções excessivamente amplo e aberto. Por outro lado, é obviamente importante que todos os interesses legítimos de sigilo recebam a devida consideração, do contrário os órgãos públicos seriam licitamente obrigados a divulgar informações, mesmo que isso pudesse causar danos desproporcionais.

Assim, como os princípios da publicidade e da transparência compartilham de natureza relativa, ao dispor sobre as informações pessoais, a Lei prescreve que o tratamento dado a elas deve respeitar a intimidade, a vida privada, a honra e a imagem das pessoas, bem como as liberdades e garantias individuais. No entanto, o art. 31, § 1º, inc. II, da LAI, estabelece que: "poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem" (BRASIL, 2011a).

Como pode se observar, nesse caso, a possível dificuldade na interpretação do dispositivo legal diz respeito não apenas à interpretação aberta que pode ser dada aos termos "intimidade, vida privada, honra e imagem", mas ao termo "previsão legal".

1.1 A imprecisão do próprio conceito de lei para restrição de informações sensíveis

Acerca da expressão "previsão legal" contida no art. 31, § 1º, inc. II, da LAI, indaga-se: o termo refere-se à lei em sentido estrito ou a uma norma geral, em sentido amplo, por exemplo, uma portaria baixada por autoridade do Poder Executivo? Essa é a dificuldade inicial encontrada ao analisar a legalidade da prestação do serviço de acesso a informações sensíveis (termo que será discutido a seguir).

O dispositivo da LAI estabelece que informações pessoais só poderão ser acessadas por terceiros: a) mediante expressa autorização da pessoa a que se referir (o que não é cabível para o caso em estudo, uma vez que se refere a bancos de dados com informações de milhares ou milhões de pessoas) ou b) mediante previsão legal.

Lei em sentido amplo seria a norma jurídica escrita que: entrou em vigor por decisão das autoridades estatais competentes; foi estabelecida em conformidade com o procedimento fixado nas normas superiores; objetiva regulamentar direta ou indiretamente a organização da sociedade, apresentando alto grau de generalidade e abstração. Em outras palavras, a proteção de dados pessoais poderia ser realizada por decreto do Poder Executivo. Contudo, por uma interpretação literal da lei de acesso à informação, a Administração Pública apenas poderia restringir o acesso a informações que dispõe por meio de outra lei (DIMOULIS, 2011, p. 168-169).

Contudo, a própria LAI não detalha como ocorrerá o acesso a informações sensíveis. É por uma leitura sistemática da Constituição Federal, que prevê a proteção da intimidade, e da previsão na LAI sobre acesso a dados pessoais que se deduz a possibilidade de competência do Poder Executivo de restringir o acesso a determinadas informações sensíveis.

1.2 Dever de publicidade administrativa *versus* direito à privacidade

Assim como o conceito aberto abordado no item anterior, novamente se observa certa dificuldade na interpretação da LAI: de um lado, o direito constitucional à privacidade, que abrange a intimidade, a vida privada, a honra e a imagem; de outro, o direito fundamental de acesso à informação, pautado pela transparência ativa da Administração Pública, ou seja, a busca pela proatividade na divulgação das informações. Ambos são princípios constitucionais e, como tais, não há hierarquia entre eles. Trata-se de uma antinomia aparente, devendo haver, tão somente na análise do caso concreto, o processo de harmonização e ponderação entre eles.

A jurisprudência sugere a supremacia do interesse público sobre o privado. No entanto,

> é imperioso que o interesse público a sobrepujar o particular, em termos de vida privada, seja indispensável, ou seja, só se justifica o sacrifício, na exata medida da necessidade e **se o interesse superior não puder ser satisfeito por outra forma**, seja ele de natureza pública ou privada (VIEIRA, 2002, p. 28, grifo nosso).

Nesse sentido, pode-se entender que, havendo outros mecanismos para prover o acesso à informação, não haveria que se falar em divulgação das informações pessoais sob o manto do interesse público.

Para tentar entender mais esses conceitos, pode-se tentar traçar um paralelo com o julgamento do Supremo Tribunal Federal quando da análise sobre a divulgação dos salários dos servidores públicos. Na ocasião, o ministro Carlos Ayres Britto em seu voto expressou o seguinte ponto de vista:

> E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua **com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor** (BRASIL, 2011b, p. 1, grifo nosso).

Assim, mesmo sabendo que o conteúdo dos princípios constitucionais está sempre aberto a novas interpretações, inclusive diante das mudanças da própria sociedade, percebe-se que a Suprema Corte já sinalizou que informações como Cadastro de Pessoas Físicas (CPF), registro geral (RG), endereço etc. são informações pessoais que devem ser preservadas em razão do direito à intimidade, à vida privada ou à honra. Nesse sentido, a permissão de acesso ou a divulgação dessas informações, em tese, feriria essa regra.

Frisa-se ainda a parte final do art. 31, § 3º, inc. II, da LAI (BRASIL, 2011a),[5] que veda a identificação da pessoa a que as informações se referirem. Novamente surge um questionamento quanto à interpretação do preceito: o impedimento de visualizar as informações pessoais surge no momento em que é franqueada a consulta ao interessado ou, posteriormente, quando da divulgação dos resultados da pesquisa? Em todo caso, para que a pesquisa seja considerada de interesse público geral, ela deve estar prevista em lei para justificar uma possível quebra de sigilo.

1.3 Dados restritos, sigilosos, protegidos: a ausência de uniformidade e clareza

Além da dificuldade em delimitar exatamente o que está abrangido no direito à privacidade e o que pode ou não ser tornado público, há outra problemática em relação à nomenclatura utilizada no meio administrativo sobre o acesso aos dados. Nos três institutos que serão estudados, a forma de disponibilização dos dados tem características e objetivos semelhantes, porém

5 Art. 31, §3º, inc. II, da Lei n. 12.527 (BRASIL, 2011a): "O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, **sendo vedada a identificação da pessoa a que as informações se referirem**".

a nomenclatura utilizada em cada caso é diferente. Esse fato reflete a falta de harmonia e entendimento acerca de conceitos-chave. As normas que tratam do assunto nessas três entidades apresentam o seguinte:

a) No IBGE (2003): Estabelece os objetivos das salas de acesso a **dados restritos**;

b) No INEP (2014): Institui a norma de acesso às **informações protegidas** do Inep;

c) No IPEA (2014): Institui a sala de pesquisa em **dados sigilosos** no Ipea e os procedimentos necessários para tratamento de informações sigilosas.

Como se pode notar, cada entidade utiliza um nome diferente. Há que se tentar entender, então, o motivo dessas escolhas, o que parte da conceituação de cada um desses termos.

Inicialmente, é necessário ressaltar que a LAI prevê a restrição de acesso a informações governamentais apenas em dois casos excepcionais: ao tratar de informações pessoais ou de informações classificadas por autoridades como sigilosas. Define em seu art. 4º:

> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
> [...]
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável (BRASIL, 2011a).

Assim, apesar de, no caso em análise, não se adentrar nas discussões teóricas no âmbito das Ciências da Informação acerca do conceito de informação,[6] observa-se que, ao se tratar da legística, a falta de uniformidade e de precisão terminológica entre os diferentes instrumentos do ordenamento jurídico podem gerar insegurança, já que permitem interpretações diversas ou dificultam a compreensão do usuário de determinado serviço.

Tal aspecto, como menciona Soares é, em parte, acarretado pela alta densificação normativa no Brasil e pela incorporação de uma "franca atividade de legislação" pela Administração Pública. Segundo a autora,

6 Vide: Capurro e Hjorland (2007); Fonseca (2004); Targino (2000), Semidão (2014), entre outros.

> as contradições, ambiguidades se acentuam deixando o sistema normativo instável e, por consequência, diminuem o nível de segurança jurídica, na medida em que cria incerteza para o emissor/receptor das normas jurídicas quanto ao direito vigente e ao seu teor, em face do esperado diálogo com outras fontes do direito (SOARES, 2007, p. 127).

Assim, nos casos estudados, tendo em vista se tratar do acesso a dados que constam dos diferentes bancos, ao optar pela utilização do termo "dados",[7] o Ipea e o IBGE parecem ter sido mais adequados.

Ainda sob o aspecto terminológico, passa-se, agora, à diferenciação dos termos "restrito", "protegido" e "sigiloso", lembrando que, de acordo com a LAI, as informações pessoais não são públicas. Elas têm seu acesso restrito, independentemente da classificação como sigilosas, por, no máximo, cem anos. Já as informações sigilosas dizem respeito à segurança da sociedade ou do Estado, podendo ser classificadas com grau de reservada, secreta ou ultrassecreta, pelo prazo máximo de 25 anos, renovável uma única vez.

Diante dessa explicação, à primeira vista, no caso do Ipea, que utiliza a expressão "dados sigilosos", esse uso não estaria adequado, pois deixaria de fora as informações pessoais, abrangendo somente aqueles dados que foram classificados pela autoridade competente como sigilosos. Esse raciocínio pode, inclusive, ser levado a cabo quando são diferenciados os termos "informação pessoal", "pública", "restrita" e "sigilosa" constantes da própria Portaria n. 078/2014.

No caso do Inep, a escolha do vocábulo "protegido" parece ter sido feita em razão da própria LAI (art. 6º, inc. III) que estabelece a competência dos órgãos e entidades do poder público em assegurar a **proteção** da informação sigilosa e pessoal, observada a sua eventual restrição de acesso. Nesse sentido, a expressão estaria de acordo com o objetivo da lei. No entanto, a fim de evitar quaisquer dúvidas, seria mais apropriado fazer constar essa definição em seu normativo.

• • •

7 Destaca-se, nesse caso, o comentário de Danilo Doneda (2011, p. 94) acerca da distinção entre dado e informação: "em relação à utilização dos termos 'dado' e 'informação', vale uma especificação. O conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização, Ambos os termos podem ser utilizados para representar um fato, um determinado aspecto de uma realidade. Não obstante, há uma carga semântica específica em cada um desses termos. Assim, o termo dado apresenta conotação um pouco mais primitiva e fragmentada, como se fosse uma informação em estado potencial, antes de ser transmitida; o dado estaria, portanto, associado a uma espécie de 'pré-informação', anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de elaboração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido de ser capaz de, objetivamente, reduzir um estado de incerteza".

Por último, o IBGE optou pelo termo "restrito". Também em alusão à LAI, seria possível inferir que a restrição diz respeito ao prazo determinado na lei para as informações pessoais (máximo de 100 anos) ou ao prazo definido pela autoridade competente para as informações sigilosas. Ocorre que, no caso do IBGE, qualquer informação coletada está sob a proteção da Lei n. 5.534, de 14 de novembro de 1968 (BRASIL, 1968), que garante ao cidadão o direito ao sigilo estatístico, ou seja, toda informação prestada terá caráter sigiloso e será utilizada exclusivamente para fins estatísticos, não havendo prazo estipulado para classificação como tal. Assim, seria mais conveniente inserir a definição do termo "restrito" na norma de serviço que estabeleceu os objetivos da sala, como fez o Ipea, na Portaria n. 78 (art. 4º, inc. VII).

1.4 Proposta de terminologia

Diante da falta de uniformidade e da possibilidade de interpretações diversas nos nomes adotados pelas três instituições, sugere-se a utilização de uma quarta nomenclatura para o serviço ora oferecido: "dados sensíveis". A proposição tem razão diante da sua natureza, que traz consigo uma condição de risco inerente. Usado de modo inadequado ou sem a segurança necessária, pode provocar repercussões indesejáveis, deixando pessoas, empresas ou o próprio governo em situações de vulnerabilidade.

Ainda que não haja no Brasil legislação que trate especificamente dos dados sensíveis, dois projetos de lei procuram regulamentar o tema, um na Câmara, outro no Senado. O Projeto de Lei (PL) n. 5.276/2016 (apensado ao PL n. 4.060/2012), que dispõe sobre tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, pautado pelo princípio da não discriminação tramita na Câmara dos Deputados e o Projeto de Lei n. 330/2013 no Senado Federal.

De acordo com o PL n. 5.276/2016 (BRASIL, 2016b), é considerado dado pessoal aquele: "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa" (Art. 5º, inc. I). E dados sensíveis, os "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos" (Art. 5º, inc. III).

Valoroso destacar que o PL n. 5.276, antes de ser encaminhado ao Congresso Nacional, foi submetido à consulta pública e recebeu cerca de 1,1 mil contribuições.[8] Já o Projeto de Lei do Senado Federal (BRASIL, 2013) define dado pessoal como: "qualquer informação referente a

8 Segundo informações sobre o PL no sítio do Ministério da Justiça, dados sensíveis, pelo potencial discriminatório que apresentam, deveriam ser protegidos de forma mais rígida. Disponível em <http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/dados-pessoais-dados-anonimos-e-dados-sensiveis/>. Acesso em: 1 ago. 2016.

pessoa natural identificável ou identificada" (Art. 3º, inc. I). E dado pessoal sensível: "qualquer dado pessoal que revele a orientação religiosa, política ou sexual, a convicção filosófica, a procedência nacional, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações de saúde, genéticas ou biométricas do titular dos dados" (Art. 3º, inc. II). A literatura também já utiliza essa terminologia há algum tempo e acentua:

> qualquer dado pessoal e não somente o dado sensível é passível de, em determinadas circunstâncias, dar origem à discriminação ou ao controle, diminuindo as liberdades de escolha de uma pessoa. Os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados não sensíveis – tanto é que os dados não sensíveis também merecem proteção, apenas em uma escala inferior. O motivo dos dados sensíveis merecerem uma proteção mais intensa é justamente uma consideração probabilística de que tais dados são mais afeitos a apresentarem problemas mais graves quando de sua má utilização – daí exatamente o fato de denominá-los como "sensíveis" em relação aos demais, enfatizando sua peculiaridade neste sentido (DONEDA, 2010, p. 191).

Melo destaca ainda que:

> dados considerados não-sensíveis, a exemplo de simples dados cadastrais se cruzados com outros de outro sistema, podem detalhar quase todos os passos da vida de uma pessoa. Nesse prisma, pode-se concluir que dados não-sensíveis, se considerados numa determinada circunstância, podem se tornar dados sensíveis (MELO, 2012, p. 88).

Ainda:

> as inúmeras iniciativas de significar dados, por meio de algoritmos e do alto poder de processamento tem impactado em direitos dos titulares dos referidos dados. Dados que jamais poderiam se converter em informação com base em interpretação humana, hoje o são, com apoio da tecnologia (MILAGRE; SEGUNDO, 2015, p. 53).

E é exatamente sob esse enfoque que se propõe a nova nomenclatura. Como se pode notar, ainda há indefinição do próprio conceito de dados sensíveis, o que gera discussão sobre qual informação seria ou não restrita a terceiros. O acesso aos dados pessoais tem crescido para a construção de ferramentas de *big data* que possibilitam identificar com precisão características pessoais para fins comerciais, sociais, médicos, para formulação de políticas públicas, que por definição afetam a vida de todas as pessoas.

O problema se torna complexo porque o serviço oferecido por essas três entidades públicas permite a manipulação e o cruzamento de diferentes bases de dados que abrangem informações

de natureza socioeconômica; sobre a vida escolar dos indivíduos; mercado de trabalho e programas sociais; informações sobre renda; características demográficas; entre outras. E, nesse contexto, até mesmo a análise detalhada e minuciosa dos projetos de pesquisa submetidos à avaliação quanto à possibilidade de acesso aos ambientes denominados seguros, bem como a avaliação posterior dos resultados extraídos podem conter falhas quanto à segurança da informação.

Diante disso, pode-se dizer que dados sensíveis merecem medidas ainda mais robustas de proteção, abrangendo a proteção física dos locais onde são produzidos, armazenados ou tratados os dados; a proteção das pessoas que gerenciam o local ou que vão manusear os dados e a proteção dos sistemas de informação (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2016). E, no caso em apreço, o uso do referido termo parece mais adequado.

2 Três modelos de disponibilização de dados sensíveis pela administração Pública: semelhanças e diferenças

Após apresentar as principais dificuldades conceituais relativas à interpretação da LAI e à nomenclatura utilizada para serviço ofertado, nesse momento, serão brevemente retratados os modelos adotados pelo IBGE, Inep e Ipea.

Como aspectos comuns aos três modelos, tem-se que:

a) o serviço de atendimento ao usuário é feito numa sala denominada segura, com protocolos de acesso e normas de segurança específicos que visam garantir a integridade e a confidencialidade dos dados disponibilizados;

b) a sala é localizada na sede de cada instituição e monitorada em tempo integral;

c) o usuário não pode entrar com qualquer equipamento eletrônico, papel, caneta etc., na sala segura;

d) os computadores são desabilitados para utilização de discos externos, não têm portas USB e nem conexão à internet;

e) o acesso ao banco de dados é apenas de leitura, ou seja, o usuário não consegue efetuar gravações, alterações ou exclusões diretamente na base de dados hospedada no servidor;

f) a assinatura de um termo de aceitação das condições de uso das salas e de um termo de compromisso de uso das informações por meio do qual o usuário se compromete a preservar a confidencialidade das informações é indispensável;

g) o usuário, após a realização da pesquisa, não sai imediatamente com os resultados, devendo estes passar pela avaliação técnica do órgão para verificar se as informações sensíveis estão preservadas e se os cruzamentos não ferem alguma regra de sigilo.

Porém, como se observará adiante, é por meio da análise das diferenças mais relevantes entre esses modelos que será verificado se a Administração Pública está incorrendo em algum problema de ilegalidade ou de falha na guarda e proteção dos dados sensíveis em sua propriedade.

Interessante destacar, também, que os serviços de acesso aos ambientes seguros são utilizados, no caso do IBGE e do Inep, como canais específicos de atendimento ao Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC). Nesses casos, considera-se, para efeito de estatística, que a resposta dada pela Administração atendeu plenamente ou parcialmente o pedido (vide nota de rodapé n. 2).

Além disso, os três institutos ainda utilizam como negativas de pedido de acesso pelo e-SIC as seguintes razões: "dados pessoais", "informação sigilosa de acordo com legislação específica" e "informação sigilosa classificada conforme a Lei n. 12.527/2011", demonstrando que a prestação do serviço de acesso ao ambiente seguro, nesses casos, não é suficiente para atender tais demandas.

TABELA 2 – **PEDIDOS DE ACESSO À INFORMAÇÃO FEITOS AO IBGE, IPEA E INEP POR MEIO DO E-SIC DE MAIO/2012 A SETEMBRO/2016**

ENTIDADE	IBGE	IPEA	INEP	TOTAL 2012-2016
1. QUANTIDADE DE PEDIDOS REALIZADOS	3.672	448	9.497	13.617
2. QUANTIDADE DE PEDIDOS RESPONDIDOS	3.654	447	9.456	13.557
3. QUANTIDADE DE PEDIDOS NEGADOS	104	5	329	438
3.1. RAZÃO DA NEGATIVA: DADOS PESSOAIS	12	0	38	50
3.2. RAZÃO DA NEGATIVA: INFORMAÇÃO SIGILOSA DE ACORDO COM LEGISLAÇÃO ESPECÍFICA	34	0	6	40
3.3. RAZÃO DA NEGATIVA: INFORMAÇÃO SIGILOSA CLASSIFICADA CONFORME A LEI N. 12.527/2011	1	0	32	33

Fonte: Elaboração própria, a partir das informações constantes do Relatório de Pedidos de Acesso à Informação e Solicitantes do sítio eletrônico: <http://esic.cgu.gov.br/sistema/Relatorios/Anual/RelatorioAnualPedidos.aspx>.

2.1 O CASO DO IBGE: MICRODADOS CRIPTOGRAFADOS

A sala de acesso a dados restritos do IBGE, como é chamada, foi inaugurada em 2003 e, desde o início, a entidade já demonstrava preocupação em proteger os dados pessoais e sigilosos por ela coletados, procedendo à criptografia desses dados. Importante destacar que o IBGE cobra pela prestação deste serviço, sendo ele contabilizado pela estimativa de tempo de processamento da máquina (tempo de uso da sala).

Segundo Zacharias, Bianchini e Albieri (2013, p. 2), além da crescente demanda por microdados detalhados,

> o avanço da tecnologia e o aumento da preocupação com questões de privacidade levaram o IBGE, a partir de 2003, a propiciar acesso pelos pesquisadores a arquivos de dados que não são liberados para o público em geral, permitindo análises mais aprofundadas do que aquelas possíveis com dados tabulados ou agregados.

Com maior experiência na prestação desse serviço, o IBGE, ao longo desses 13 anos, vem aprimorando alguns procedimentos. O primeiro deles refere-se aos dados que são fornecidos ao pesquisador. No início, ele tinha acesso a toda base de dados solicitada. Atualmente, deve informar exatamente quais as variáveis desejadas e só terá acesso a elas, pois um servidor do IBGE irá preparar a base para disponibilizá-la na sala segura. Segundo denominação do próprio Instituto, trata-se de "bases de dados não desidentificados (cuja variável de identificação é criptografada)" e as respectivas análises estatísticas serão feitas pelo solicitante *in loco*. Essa conduta demonstra o esforço do Instituto em proteger os dados, restringir o possível mau uso e minimizar os riscos de vazamento.

Outro procedimento a ser destacado refere-se à necessidade de demonstrar o vínculo do pesquisador a uma instituição, ou seja, o seu representante também deverá assinar um Termo de Compromisso, tornando-se solidariamente responsável pelo uso dos dados acessados e posterior divulgação das informações.

O uso de bases de dados externas na sala segura também é franqueado. Porém, o usuário deverá apresentar autorização formal do órgão responsável pela base. O objetivo é garantir que houve consentimento do órgão para utilização daquela base na referida pesquisa.

Outro aspecto distintivo no IBGE é a existência de um Comitê de Avaliação de Acesso a Dados Não Desidentificados (presidido por representante do Comitê de Sigilo da entidade). O Comitê de Avaliação – subsidiado por pareceres das áreas técnicas do Instituto – é responsável

pela avaliação do mérito da pesquisa, observando sua finalidade, objetivo, produto final e questões relacionados ao risco quanto à confidencialidade dos dados.

Além disso, para que a área técnica avalie as informações produzidas, é exigido relatório do usuário, demonstrando todos os passos (procedimentos) realizados na sala segura para consecução do seu trabalho. Esse relatório permitirá a verificação de possíveis impropriedades ou inconsistências.

Esses são os principais aspectos que diferenciam o modelo de disponibilização de dados sensíveis pelo IBGE. Parece um modelo adequado e sem muitas falhas de segurança da informação, tendo em vista o requisito essencial contido na LAI que é a "vedação à identificação da pessoa a que as informações se referirem", além da preparação das bases "reduzidas" pelos próprios servidores.

A existência do Comitê também merece destaque, pois a avaliação quanto aos riscos de segurança e confidencialidade da informação passa a ser de um colegiado e não apenas de um técnico.

2.2 O caso do Inep: bases íntegras e identificadas

A intitulada norma de acesso às informações protegidas do Inep é recente, data de setembro de 2014. Diferentemente do IBGE, o modelo adotado por este Instituto prevê a disponibilização das bases de dados no formato em que se apresentam, sem transformações, ou seja, poderão ser acessadas na sala segura do Inep, informações sigilosas ou pessoais, individualizadas, coletadas pelo Instituto, sem a devida anonimização, conforme dispõe o art. 3º c/c art. 10 da Portaria Inep n. 467/2014.

O critério de vínculo do pesquisador a uma instituição de pesquisa utilizado pelo IBGE também não é exigido. Assim, de acordo com a Portaria, qualquer pessoa física ou jurídica pode solicitar o acesso, bastando apresentar a documentação necessária e assinar os devidos termos de compromisso. Importante lembrar que seu projeto deverá ser avaliado e deferido pela área técnica.

Há omissão da norma quanto à possibilidade de uso de bases de dados externas. Porém, sua utilização tem sido aceita, desde que seja apresentada a devida autorização do órgão produtor. Sob esse aspecto, é importante destacar a necessidade de se ter ainda mais cautela. A depender da pesquisa que será realizada, pode-se ter o cruzamento de dados que tornam a informação bastante sensível, a exemplo do cruzamento das bases sobre educação do Inep com a base da Relação Anual de Informações Sociais (RAIS), do Ministério do Trabalho e Previdência Social; ou a do Cadastro Único para Programas Sociais, do Ministério do Desenvolvimento Social.

Observa-se que, no caso do Inep, como as informações coletadas são disponibilizadas na íntegra a terceiros, ainda que em um ambiente seguro, há certa fragilidade na segurança da informação. Nesse caso, sugere-se a desidentificação dos dados pessoais como providência a ser tomada de forma mais imediata. Ainda que haja a assinatura dos termos de compromisso, o público capaz de acessar os dados sensíveis é amplo, sendo esta uma medida imprescindível.

Ainda, vale ressaltar que, por disponibilizar dados pessoais e sigilosos, o Serviço de Atendimento ao Pesquisador (SAP) também é utilizado como argumento de resposta para pedidos encaminhados ao Serviço de Informação ao Cidadão do Inep. O SIC-Inep[9] informou que, desde setembro de 2014, quando foi publicada a Portaria que instituiu o SAP, 35 pedidos foram respondidos tendo como justificativa a sua existência.

Pelo sistema de buscas de pedidos e respostas do e-SIC (2016) é possível verificar o encaminhamento ao SAP para responder perguntas de cunhos diversos, como "quais universidades possuem o maior número de cotistas (cotas raciais) e quem são esses alunos (dados de contato)"; "lista completa de todos os CPFs que se inscreveram no ENEM desde 2011"; "informações separadas por ano (2011, 2012, 2014, 2015) e por curso, contendo o nome dos professores que a instituição cadastrou, a titulação e o regime de trabalho"; "acesso às máscaras que relacionam os códigos das escolas no INEP com os códigos fictícios utilizados nos microdados do SAEB 2013";[10] entre outras.

Novamente, então, observa-se a necessidade de uma regulamentação mais clara e precisa no que diz respeito a informações pessoais, sigilosas e sensíveis e suas possibilidades e restrições de acesso em âmbito federal para, inclusive, evitar imprecisões na prestação de serviços oferecidos por toda a Administração Pública.

2.3 O caso do Ipea: necessidade de vínculo institucional

A criação da sala de pesquisa em dados sigilosos no Ipea também é recente. Teve início em maio de 2014. Porém, o fundamento para sua concepção foi outro. O Ipea não é produtor de dados, apenas utiliza bases de outros órgãos governamentais para realizar estatísticas e, assim, recomendar a adoção de determinadas políticas públicas.

Nesse contexto, a criação da sala teve por objetivo o uso exclusivo de servidores, bolsistas, consultores e colaboradores, devidamente autorizados, para trabalharem na produção de pesquisas de interesse da Instituição; ou servidores públicos externos que estejam trabalhando na produção de pesquisas de interesse do Estado, também autorizados por autoridade do Ipea. Percebe-se, nesse caso, que o vínculo para utilização da sala é estritamente institucional.

Para acesso aos dados, o Ipea precisa firmar Acordos de Cooperação Técnica ou Convênios. Como explicam Andrade e Nascimento (2015, p. 10-11),

> apesar de se configurar como insumo fundamental à consecução de sua missão institucional, o Ipea não dispõe de instrumento legal que ampare o acesso irrestrito a informações

9 Pedido de informação n. 23480015207201602, realizado por meio do e-SIC.

10 Informações encontradas no sistema de consulta do e-SIC, com os seguintes números de protocolo, respectivamente: 23480013041201681, 23480013438201673, 23480003090201614, 23480017657201541. Disponíveis em: <http://www.consultaesic.cgu.gov.br/busca>. Acesso em: 24 set. 2016.

> individualizadas dos registros administrativos e estatísticos gerados pelos órgãos da própria administração pública federal, mesmo sendo dela integrante. O uso de microdados identificados ainda depende de cuidadosas e muitas vezes recorrentes negociações com cada um dos órgãos responsáveis por produzi-los ou administrá-los. Resultado disto é que com alguns consegue duradouro sucesso, com outros precisa de uma negociação para cada projeto de pesquisa e com a maioria mantém apenas relações pontuais, relacionadas a demandas específicas advindas do órgão parceiro, sendo que com muitos deles o contato nesse sentido é demasiado rarefeito.

Essa dificuldade de articulação entre os órgãos e entidades estatais tem sido alvo de grandes debates, chegando a ser contemplada em anteprojeto de lei orgânica da Administração Pública Federal e Entes de Colaboração. Pires, inclusive, frisou a necessidade de articulação entre eles para planejamento das políticas públicas, por meio de ações de coordenação e de supervisão. Segundo ela,

> a coordenação envolve procedimentos de transversalidade e horizontalidade, que são potencializadas em seus resultados pelo compartilhamento de informações em rede, racionalização no uso de recursos, unificação de procedimentos, permitindo o diálogo das competências em lugar de sobreposição delas e de duplicação de níveis decisórios (PIRES, 2009, p. 189).

Porém, mesmo que se fale em coordenação entre os órgãos e entidades governamentais, em se tratando de dados sensíveis, pessoais e identificados, aspectos relacionados à segurança da informação também devem ser observados. Nesse âmbito, é de se frisar que, assim como no IBGE, os computadores no Ipea são fisicamente isolados de outras redes de computadores e equipamentos externos.

Porém, por ser de uso exclusivo de agentes públicos, eles estão submetidos às regras do serviço público e a cifração (criptografia ou desidentifiação) de dados só precisa ser feita quando tecnicamente viável e não acarretar prejuízo aos procedimentos lícitos de pesquisa. Ademais, a forma de disponibilização depende da negociação feita com os órgãos responsáveis pelas bases. O problema não é que a privacidade inexiste, mas que os mecanismos de controle de dados e de transmissão de dados devem ser repensados a luz dos princípios que regulam a privacidade pessoal (RICHARDS; KING, 2014). Dessa forma, em geral, os dados encontram-se identificados, merecendo ainda mais proteção. Por fim, no caso do Ipea, é preciso destacar que todos os estudos realizados, quando publicados, têm a chancela do Instituto.

É válido realçar, também, que, para os fins a que se destina a sala segura do Ipea, a tendência é que a dificuldade citada por Andrade e Nascimento (2015) nas parcerias com os outros órgãos da Administração Pública seja minimizada. Isso porque em 29 de junho de 2016 foi publicado

o Decreto n. 8.789, que dispõe sobre o compartilhamento de bases de dados na Administração Pública Federal, dispensando a celebração de acordos específicos para o compartilhamento das bases de dados.[11]

Considerações finais

A disponibilização dos dados sensíveis sob a guarda da Administração Pública ainda é uma problemática a ser enfrentada. Apesar de a legislação brasileira e, consequentemente, os órgãos e entidades governamentais caminharem no sentido de uma publicidade ampla, com a implantação de uma política de dados abertos – que tem como um dos maiores desafios a integração das bases –, os problemas relacionados aos dados sensíveis sempre serão atuais.

O problema inicia-se com a própria definição dos conceitos abrangidos pela matéria que ou são demasiadamente abertos ou são impactados por conta de alguma imprecisão legislativa[12] ou sofrem pela ausência de legislação específica. Todas essas questões podem levar tanto as autoridades governamentais quanto a sociedade a interpretações dúbias ou ambíguas, tendo consequências indesejáveis.

No caso específico do acesso a dados disponibilizados pela Administração Pública, observa-se que o serviço é relativamente novo (com exceção do caso do IBGE) e que, apesar de compreensíveis os nomes escolhidos por cada uma das três entidades estudadas, os termos "restrito", "protegido" e "sigiloso" podem gerar interpretações errôneas. Sugere-se, então, a utilização do termo "sensível" por se entender que ele retrata de forma mais fiel os cuidados que se deve ter na disponibilização e uso dos dados, bem como a responsabilização decorrente de eventual má utilização.

Nos três modelos analisados, nota-se, em princípio, diferenciação significante referente ao Ipea. Nesse caso, a entidade não é produtora dos dados. Ela firma acordos com outros órgãos para utilização dos dados identificados. Assim, parece plausível afirmar que o dever da Administração de dar publicidade aos dados sob sua guarda não seria sua responsabilidade, mas dos

• • •

11 Destaque para os seguintes artigos do referido Decreto (BRASIL, 2016a): "art. 6º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou ajustes congêneres para a efetivação do compartilhamento das bases de dados; art. 7º Os órgãos ou as entidades que tiverem acesso a dados e informações compartilhados deverão observar, em relação a esses dados e informações, as normas e os procedimentos específicos que garantam sua segurança, proteção e confidencialidade".

12 Nesse sentido, vale a pena destacar algumas proposições feitas em relatório do governo francês para simplificar as leis e seus entendimentos, produzindo uma lei com qualidade mais alta. Exemplos: incentivar a técnica de microdificação; publicar no jornal oficial, concomitantemente com o texto de uma lei, um documento explicativo; substituir a apresentação cronológica do conjunto de atos administrativos por uma apresentação temática, entre outros (WARSMANN, 2008).

órgãos produtores dos dados. A criação da sala segura no Ipea foi necessária apenas para garantir a segurança destes perante os outros órgãos e, com isso, poder acessá-los para geração e disseminação de conhecimento acerca das políticas públicas do país.

Já o IBGE e o Inep permitem o acesso a dados sensíveis por particulares sem vínculo com a Administração Pública. Nesses casos, o tratamento da segurança da informação deve ser ainda mais forte, devido ao elevado risco de acesso indevido. Percebe-se, no entanto, que o IBGE está num estágio mais avançado que o Inep em termos de segurança da informação, pois este ainda precisa evoluir no sentido de desidentificação dos dados pessoais.

Diante da complexidade do tema, além dos aspectos aqui examinados, também merecem reflexão questões relacionadas: às possíveis falhas no controle da avaliação dos resultados gerados; à avaliação quanto aos mecanismos de controle da divulgação das informações provenientes dos dados acessados e a consequente repercussão de uma análise incorreta e à responsabilização do gestor e do usuário no caso de revelação indevida, por exemplo. Sugere-se, ainda, que seja feito um estudo comparado no intuito de verificar as melhores práticas internacionais e, com isso, buscar o aprimoramento do modelo brasileiro atual.

A disponibilização de "dados sensíveis" pela Administração Pública é um tema que precisa ser construído, tanto por meio legal, como por regulamentações específicas, pois associado às relações de confiança e credibilidade das instituições e ao dever de publicidade governamental. Mais que isso, faz-se indispensável na atualidade a criação de uma política nacional sobre proteção de dados pessoais para evitar a violação aos direitos fundamentais.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. *Programa Nacional de Proteção do Conhecimento Sensível*. 2016. Disponível em: <http://www.abin.gov.br/atuacao/programas/ pnpc/>. Acesso em: 1 ago. 2016.

ANDRADE, Israel de Oliveira; NASCIMENTO, Paulo A. Meyer M. O sigilo em bases de dados sob a tutela da administração pública: o caso Ipea. In: INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Texto para discussão 2100*. Rio de Janeiro: Ipea, 2015.

BRASIL. Decreto n. 8.789, de 29 de junho de 2016. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. *Diário Oficial da União*, Brasília, DF, 30 jun. 2016a - Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm>. Acesso em: 26 jul. 2018.

_____. Lei n. 5.534, de 14 de novembro de 1968. Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências. *Diário Oficial da União*, Brasília, DF, 18 nov. 1968 (retificado em 20 nov. 1968) - Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5534.htm>. Acesso em: 26 jul. 2018.

_____. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União*, Brasília, DF, 18 nov. 2011a - Edição extra. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/ l12527.htm>. Acesso em: 26 jul. 2018.

_____. Projeto de Lei n. 5.276, de 13 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília, 2016b. Disponível em: <https://www.camara.gov.br/ proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 26 jul. 2018.

_____. Projeto de Lei do Senado n. 330, de 2013 - Emenda 31/CCT/CMA – Substitutivo (aprovada SF-CMA, em 10/05/2016). Estabelece princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados pessoais. 2013. Disponível em: <https:// legis.senado.leg.br/sdleg-getter/documento?dm=3928471&disposition=inline# Emenda31>. Acesso em: 26 jul. 2018.

_____. Supremo Tribunal Federal. SS 3902 AgR-segundo, Relator(a): Min. AYRES BRITTO, Tribunal Pleno, julgado em 09/06/2011, DJe-189 DIVULG 30-09-2011 PUBLIC 03-10-2011 EMENT VOL-02599-01 PP-00055 RTJ VOL-00220-01 PP-00149. 2011b. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/visualizarEmenta.asp?s1=000181369&base=baseAcordaos>. Acesso em: 1 ago. 2016.

BRASSCOM. *Contribuições à Comissão Especial:* dados pessoais da Câmara dos Deputados sobre a Lei de Tratamento e Proteção de Dados Pessoais. 2017. Disponível em: <http:// www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/Brasscom.pdf>. Acesso em: 28 dez. 2017.

CAPURRO, Rafael; HJORLAND, Birger. O conceito de informação. *Perspectivas em Ciências da Informação,* Belo Horizonte, v. 12, n. 1, p. 148-207, abr. 2017. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54/47>. Acesso em: 28 dez. 2017.

CNSEG/FENASEG. *Considerações da CNSEG/FENASEG sobre o APL de proteção de dados pessoais.* 2017. Disponível em: <http://pensando.mj.gov.br/dadospessoais/wp-content/ uploads/sites/3/2015/07/85eee8671de5adb2a5ea4a878ad18889.pdf>. Acesso em: 28 dez. 2017.

CRUZ, Francisco Brito; MARCHEZAN, Jonas Coelho. *InternetLab reporta:* consultas públicas n. 05. 2015. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-05/>. Acesso em: 28 dez. 2017.

DIMOULIS, Dimitri. *Manual de introdução ao estudo do Direito.* 4. ed. São Paulo: Revista dos Tribunais, 2011.

DONEDA, Danilo. Privacidade e transparência no acesso à informação pública. In: MEZZAROBA, Orides; GALINDO, Fernando. *Democracia eletrônica*. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p. 179-216.

_____. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico,* Joaçaba, v. 12, n. 02, p. 91-108, 2011. Disponível em: <https://editora.unoesc.edu.br/index.php/espacojuridico/article/viewFile/1315/658>. Acesso em: 28 dez. 2017.

FONSECA, Maria Odila. *Arquivologia e Ciência da Informação:* (RE)definição de marcos interdisciplinares. 2004. 181 f. Tese (Doutorado em Ciência da Informação) - Universidade Federal do Rio de Janeiro/Instituto Brasileiro de Informação em Ciência e Tecnologia, Rio de Janeiro, 2004. Disponível em: <http://ridi.ibict.br/handle/123456789/696>. Acesso em: 28 dez. 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Norma de serviço:* CDDI n. 01, de 10 set. 2003. Disponível em: <ftp://ftp.ibge.gov.br/Censos/Censo_Demografico_2010/metodologia/anexos/anexo_1_ns_cddi_01_2003_dados_restritos.pdf >. Acesso em: 11 de jul. 2016.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. *Portaria Inep n. 467, de 19 set. 2014.* Disponível em: <http://download.inep.gov. br/acesso_a_informacao/documentos/2014/portaria_n_467_19092014_norma_acesso_informacao.pdf >. Acesso em: 11 jul. 2016.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Portaria Ipea n. 078, de 20 mai. 2014.* Disponível em: <http://www.ipea.gov.br/portal/limages/stories/PDFs/140604_ portaria78.pdf>. Acesso em: 11 jul. 2016.

LARENZ, Karl. *Metodologia da ciência do Direito.* Tradução: José Lamego. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 1997.

MELO, Augusto Carlos Cavalcante. A nova interpretação constitucional e o direito fundamental ao sigilo de dados: considerações face o avanço da tecnologia da informação. In: COELHO NETO, Ubirajara. *Temas de Direito Constitucional:* estudos em homenagem ao Prof. Osório de Araújo Ramos Filho. Aracaju: Ubirajara Coelho Neto Editor, 2012. p. 72-96.

MENDEL, Toby. *Liberdade de informação*: um estudo de direito comparado. Brasília: Unesco, 2009.

MILAGRE, José; SEGUNDO, José Eduardo Santarém. A propriedade dos dados e a privacidade na perspectiva da Ciência da Informação. *Encontros Bibli:* revista eletrônica de biblioteconomia e ciência da informação, [s.l.], v. 20, n. 43, p. 47-76, 9 ago. 2015. Universidade Federal de Santa Catarina (UFSC). Disponível em: <https://periodicos.ufsc. br/index.php/eb/article/view/1518-2924.2015v20n43p47>. Acesso em: 28 dez. 2017.

PIRES, Maria Coeli Simões. Esgotamento do modelo de desenvolvimento excludente no Brasil ee ressemantização das atividades de planejamento e articulação governamentais à luz do paradigma democrático. In: MODESTO, Paulo. *Nova organização administrativa brasileira:* estudos sobre a proposta da comissão de especialistas constituída pelo governo federal para reforma da organização administrativa brasileira. Belo Horizonte: Editora Fórum, 2009. p. 171-194.

RICHARDS, Neil M.; KING, Jonathan H. Big Data Ethics. *Wake Forest Law Review*, v. 49, 2014. Disponível em: <https://ssrn.com/abstract=2384174>. Acesso em: 28 dez. 2017.

ROBINSON, David G.; YU, Harlan; ZELLER, William P.; FELTEN, Edward W. Government data and the invisible hand. *Yale Journal of Law and Technology,* v. 160, n. 11, 2009.

RODRIGUES, João Gaspar. Publicidade, transparência e abertura na administração pública. *Revista de Direito Administrativo (RDA)*, Rio de Janeiro, v. 266, p.89-123, mai/ ago 2014.

SEMIDÃO, Rafael Aparecido Moron. *Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação:* contribuições teóricas. 2014. 198 f. Tese (Mestrado) - Curso de Ciência da Informação, Universidade Estadual Paulista, Marília, 2014. Disponível em: <https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciadaInformacao/Dissertacoes/semidao_ram_me_mar.pdf>. Acesso em: 28 dez. 2017.

SILVEIRA, Marco Antônio Karam. Lei de Acesso a Informações Públicas (Lei n. 12.527/ 2011): democracia, república e transparência no Estado constitucional. *Revista Jurídica:* órgão nacional de doutrina, jurisprudência, legislação e crítica judiciária. São Paulo, v. 60, n. 416, p. 29-52, jun. 2012.

SISTEMA ELETRÔNICO DO SERVIÇO DE INFORMAÇÃO AO CIDADÃO. Disponível em: <https://esic.cgu.gov.br/sistema/site/index.html>. Acesso em: 17 set. 2016.

SOARES, Fabiana de Menezes. Legística e desenvolvimento: a qualidade da lei no quadro da otimização de uma melhor legislação. *Revista da Faculdade de Direito da UFMG*, Belo Horizonte, n. 50, p. 124-142, jan./jul. 2007. Disponível em: <https://www.direito. ufmg.br/revista/index.php/revista/article/view/31>. Acesso em: 10 nov. 2017.

TARGINO, Maria das Graças. Comunicação científica: uma revisão de seus elementos básicos. *Informação & Sociedade: Estudos,* João Pessoa, v. 10, n. 2, p. 1-27, 2000. Disponível em: <http://www.ies.ufpb.br/ojs/index.php/ies/article/view/326/248>. Acesso em: 28 dez. 2017.

VIEIRA, Sônia Aguiar do Amaral. *Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos.* São Paulo: Juarez de Oliveira, 2002.

WARSMANN, Jean-luc. Simplifions nos lois pour guérir un mal français*:* rapport au Premier ministre. *Collection des rapports officiels,* p. 81-164, 2008. Disponível em: <http://www. ladocumentationfrancaise.fr/var/storage/rapports-publics/094000276.pdf>. Acesso em: 20 jul. 2018.

ZACHARIAS, Maria Luiza Barcellos; BIANCHINI, Zélia Magalhães; ALBIERI, Sonia. *Aperfeiçoamentos no processo de acesso a microdados restritos no IBGE*. 2013, p. 1-6. Disponível em: <http://artigos.ibge.gov.br/artigos-home/estatistica/8050-aperfeicoamentos-no-processo-de-acesso-a-microdados-restritos-no-ibge.html>. Acesso em: 16 mai. 2016.

Tânia Carolina Nunes Machado Gonçalves

Especialista em Gestão em Controladoria Governamental. Mestranda em Direito e Políticas Públicas do Centro Universitário de Brasília (UniCeub).

taniacarol@gmail.com

Marcelo D. Varella

Doutor e Livre Docente em Direito. Professor do curso de Mestrado e Doutorado do Centro Universitário de Brasília (UniCeub). Pesquisador do CNPq.

marcelodvarella@gmail.com