TÂNIA CAROLINA NUNES MACHADO GONÇALVES

GESTÃO DE DADOS PESSOAIS E SENSÍVEIS PELA ADMINISTRAÇÃO PÚBLICA FEDERAL: DESAFIOS, MODELOS E PRINCIPAIS IMPACTOS COM A NOVA LEI

Biblioteca de Referência em Políticas Públicas

UniCEUB
Centro Universitário de Brasília

Gonçalves, Tânia Carolina Nunes Machado.

Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei / Tânia Carolina Nunes Machado Gonçalves; Orientador Prof. Dr. Marcelo Dias Varella. – Brasília, 2019.

147 p.

ISBN: 978-85-7267-010-4

Dissertação (Mestrado em Direito) – Centro Universitário de Brasília (UniCEUB), 2019.

1.Proteção de Dados Pessoais e Sensíveis. 2. Políticas Públicas. 3. Direitos da Personalidade. 4. Compartilhamento de Dados.

I. Varella, Marcelo Dias, orient. II. Título.

Lista de abreviaturas e siglas

Ajuferjes	Associação dos Juízes Federais do Rio de Janeiro e Espírito Santo
Anatel	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
APD	Autoridade de Proteção de Dados
APF	Administração Pública Federal
API	Application Programming Interface
APL	Anteprojeto de lei
CCS	Cadastro de Clientes do Sistema Financeiro Nacional
CDC	Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990)
CEF	Caixa Econômica Federal
CF88	Constituição da República Federativa do Brasil de 1988
CGU	Ministério da Transparência e Controladoria-Geral da União
CJF	Conselho da Justiça Federal
CNH	Carteira Nacional de Habilitação
CNJ	Conselho Nacional de Justiça
CNMP	Conselho Nacional do Ministério Público
CNPD	Comissão Nacional de Proteção de Dados
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CRMI	Comissão Mista de Reavaliação de Informações
CSJT	Conselho Superior da Justiça do Trabalho
Dataprev	Empresa de Tecnologia e Informações da Previdência
Denatran	Departamento Nacional de Trânsito
DU-E	Declaração Única de Exportação
e-Ping	Padrões de Interoperabilidade de Governo Eletrônico
e-SIC	Sistema Eletrônico do Serviço de Informação ao Cidadão
e-Social	Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas
FGTS	Fundo de Garantia do Tempo de Serviço
GovData	Plataforma de Análise de Dados do Governo Federal
IBGE	Instituto Brasileiro de Geografia e Estatística
IDH	Índice de Desenvolvimento Humano
Inep	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
INSS	Instituto Nacional do Seguro Social
Ipea	Instituto de Pesquisa Econômica Aplicada

IRPF	Imposto de Renda da Pessoa Física
LabContas	Laboratório de Informações e Controle do Tribunal de Contas da União
LAI	Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011)
LCP	Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011)
LGPD	Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)
MCI	Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014)
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MDIC	Ministério da Indústria, Comércio Exterior e Serviços
MDS	Ministério do Desenvolvimento Social
MEC	Ministério da Educação
MESP	Ministério Extraordinário da Segurança Pública
MF	Ministério da Fazenda
MJ	Ministério da Justiça
MP	Medida Provisória
MPDFT	Ministério Público do Distrito Federal e Territórios
MPDG	Ministério do Planejamento, Desenvolvimento e Gestão
MPF	Ministério Público Federal
MT	Ministério do Trabalho
NF-e	Nota Fiscal eletrônica
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico
ONU	Organização para as Nações Unidas
PaaS	Plataforma como Serviço
PDA	Política de Dados Abertos
PDL	Projeto de Decreto Legislativo
PGFN	Procuradoria-Geral da Fazenda Nacional
PGR	Procuradoria-Geral da República
PL	Projeto de Lei
PLS	Projeto de Lei do Senado
RAIS	Relação Anual de Informações Sociais
Renach	Registro Nacional de Carteiras de Habilitação
Renavam	Registro Nacional de Veículos Automotores
RG	Registro Geral (Carteira de Identidade)
RGPD	Regulamento Geral de Proteção de Dados nº 679/2016 da União Europeia
SAP	Serviço de Atendimento ao Pesquisador do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

Sedap	Serviço de Acesso a Dados Protegidos Estudos e Pesquisas Educacionais Anísio Teixeira
Serpro	Serviço Federal de Processamento de Dados
Setic	Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão
Siafi	Sistema Integrado de Administração Financeira do Governo Federal
Sinpa	Sistema Nacional de Passaportes
Sisp	Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal
SLTI	Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão
SNE	Sistema de Notificação Eletrônica
SNI	Sistema Nacional de Informações
SPC	Serviço de Proteção ao Crédito
Sped	Sistema Público de Escrituração Digital
SRF	Secretaria da Receita Federal do Ministério da Fazenda
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SUS	Sistema Único de Saúde
TCMS	Termo de Compromisso de Manutenção de Sigilo
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TRF	Tribunal Regional Federal
TSE	Tribunal Superior Eleitoral
UE	União Europeia

Lista de figuras

Figura 1 – Práticas de segurança da informação na Administração Pública Federal..... 90
Figura 2 – A regulamentação de proteção de dados pessoais e sensíveis no mundo..... 94

Lista de quadros

Quadro 1 - Planos de análise para formulação da política pública de proteção a dados pessoais (primeiro ciclo: normatização do tema) 26
Quadro 2 – Pedidos de acesso à informação feitos à Administração Pública Federal por meio do e-SIC (maio/2012 a julho/2018) 46
Quadro 3 – Pedidos de acesso à informação feitos ao IBGE, ao Ipea e ao Inep por meio do e-SIC (maio/2012 a julho/2018) 51
Quadro 4 – Soluções utilizadas pelo IBGE, Inep e Ipea para disponibilizar dados pessoais e sensíveis para fins de pesquisa 59
Quadro 5 – Atendimento às especificações e-Ping 64
Quadro 6 - Estudo InternetLab: Permissões solicitadas por aplicativos do governo federal 75

Sumário

INTRODUÇÃO 10

1 OS DESAFIOS DECORRENTES DA DICOTOMIA: "MELHORIA DE POLÍTICAS PÚBLICAS" X "PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS" 20

1.1 A recente visibilidade da temática da proteção de dados pessoais e sensíveis e a sua inserção como política pública 21

1.2 As normas abertas, o princípio da publicidade e as consequentes dificuldades em administrar os dados pessoais e sensíveis 29

1.3 A utilização de novas tecnologias nos serviços públicos e as vulnerabilidades delas resultantes 34

1.4 A interdisciplinaridade como possível entrave aos operadores jurídicos e aos gestores públicos 39

2 OS PRINCIPAIS MODELOS DE GESTÃO DE DADOS PESSOAIS E SENSÍVEIS UTILIZADOS PELA ADMINISTRAÇÃO PÚBLICA E SUAS PRINCIPAIS COMPLEXIDADES 42

2.1 A requisição e a disponibilização de dados pessoais e sensíveis via Sistema Eletrônico do Serviço de Informação ao Cidadão 44

2.2 O acesso aos dados pessoais e sensíveis por meio de ambientes denominados seguros para fins específicos de pesquisa 49

2.2.1 IBGE: microdados criptografados 51

2.2.2 Inep: bases íntegras e identificadas 53

2.2.3 Ipea: vínculo institucional 57

2.3 O modelo de compartilhamento de dados, as janelas únicas e os seus aspectos controvertidos 60

2.3.1 E-Ping: iniciativa que resultou em baixa adesão 62

2.3.2 Modelo single window: padronização de informações, documentos e redução das redundâncias para o cidadão 65

2.3.3 Data Lake: um único repositório capaz de possibilitar a análise de dados 71

2.3.4 Aplicativos governamentais: a coleta e o uso excessivo de dados 73

2.4 Os impactos decorrentes da opção por centralizar ou descentralizar a gestão de dados pela Administração Pública 78

2.4.1 A possível comercialização indevida de dados pelo Serpro 78

2.4.2 O argumento de sigilo e confidencialidade como óbice para responder quaisquer solicitações de informação 85

2.4.3 As barreiras na gestão de dados públicos: baixo índice de planejamento, ausência de política de segurança da informação e deficiências no quadro técnico 87

3 A PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS COMO DIREITO DA PERSONALIDADE E OS IMPACTOS NAS POLÍTICAS PÚBLICAS DIANTE DAS NOVAS DISPOSIÇÕES LEGAIS 93

3.1 A evolução normativa e a construção do entendimento da proteção de dados pessoais como direito da personalidade 95

3.2 A adoção do modelo europeu como parâmetro para a legislação brasileira e suas principais divergências 99

3.3 O respeito à finalidade e à transparência para suprir a necessidade do consentimento no setor público 111

3.4 A imperatividade da independência funcional da autoridade nacional de proteção de dados 115

3.5 A utilização dos dados pessoais e sensíveis para fins penais, de controle e de fiscalização 118

3.6 A responsabilização com a eventual divulgação indevida e as dificuldades inerentes ao arbitramento do valor do dano 127

CONCLUSÃO 132

Introdução

Recentemente inserida na agenda pública, a proteção de dados pessoais e sensíveis pelo setor público merece ser discutida em profundidade e com grande responsabilidade já que associada ao elevado grau de ingerência que o Poder Público pode ter na vida dos cidadãos. Por um lado, o tratamento de dados está associado à melhoria da eficiência e da eficácia na Administração Pública. De outro, pode afrontar o direito à privacidade e à intimidade dos indivíduos, além de gerar políticas discriminatórias.

De fato, na atualidade, muito se discute sobre o direito à privacidade e sobre a proteção de dados pessoais e sensíveis. Tal preocupação não é fruto de devaneios ou de preocupações desarrazoadas. Ao contrário, advém dos inúmeros casos relatados pela mídia ou de informações acerca de ações movidas na Justiça buscando a reparação de danos causados em razão do mau uso ou uso indevido desses dados.

Entretanto, observa-se que a maioria das discussões volta-se exclusivamente ao âmbito privado, mais ainda às relações consumeristas. Os debates giram em torno, especialmente, do uso dos dados em redes sociais, da necessidade de preenchimento de cadastro para relações de compra e venda, da comercialização dos dados por provedores de acesso à internet, sítios eletrônicos e aplicativos, da utilização não-autorizada de imagens, entre outros.

Essa polêmica tem sido acentuada diante da presente realidade em que são enormes as quantidades de dados e informações acumulados pelos setores público e privado. Porém, no caso do setor público, apesar de os debates acerca do uso dos dados já existirem há algumas décadas em outros países[1], no caso brasileiro, especialmente, só

[1] A proteção legal à privacidade, de fato, já é citada desde 1890 quando da publicação do artigo: "O direito à privacidade", que fala sobre o direito de ser deixado sozinho, no original: "*right to be left alone*", visando à proteção contra intromissões não desejadas na vida do indivíduo que poderiam afetar seu próprio senso sobre "independência, individualidade, dignidade e honra" (WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 28 jul. 2018). Porém, foi nas décadas de 60/70, especialmente nos Estados Unidos, que se demonstrou maior preocupação da população com a intervenção estatal injustificada na esfera privada. Naquele país, os debates culminaram na edição do Privacy Act, em 1974, que continha princípios fundamentais para a segurança da vida privada a serem observados pelo Governo norte-americano. "*O contexto histórico da Lei é importante para a compreensão de seus propósitos corretivos: em 1974, o Congresso preocupou-se em restringir a vigilância e a investigação ilegal de indivíduos por agências federais que haviam sido expostas durante o escândalo de Watergate; também se preocupou com possíveis abusos apresentados pelo crescente uso de computadores do governo para armazenar e recuperar dados pessoais por meio de um identificador universal, como o número do seguro social de um indivíduo*", (JUSTICE INFORMATION SHARING. **Privacy Act of 1974.** Disponível em: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>. Acesso em: 28 jul. 2018.). Na Europa, apesar da existência de diversas leis federais editadas na década de 70 (ex: na Alemanha, Suécia, Dinamarca, França, entre outros), foi com a Diretiva 95/46/CE, aprovada em 1995 e com *vacatio legis*

têm ganhado força recentemente. Com o caso Snowden[2], notícias acerca da venda de dados por empresas ligadas ao Governo, utilização de dados por candidatos com vistas a ganhar vantagens em eleições, como o que ocorreu nos Estados Unidos[3], para citar apenas esses exemplos, fazem com que os diferentes países não possam mais olvidar a nova conjuntura.

Assim, numa relação fragilizada entre cidadão e Governo, onde a parte mais forte é o Governo, válida e premente é a discussão sobre o uso que tem sido conferido aos dados dos indivíduos e os rumos que devem ser concedidos a eles. Notadamente no caso da formulação e da execução de políticas públicas, a dicotomia "melhoria das políticas públicas" x "privacidade dos indivíduos" fica visível e, por esse motivo, merece atenção especial. Tal cenário necessariamente abrange a discussão acerca do modelo de regulamentação da proteção de dados pessoais e sensíveis adotados nos países.

A compreensão acerca da escolha de determinada abordagem legal em detrimento de outras torna clara, também, a forma de atuação dos grupos de pressão e a relação de forças entre eles. Num processo dinâmico, a elaboração das normas jurídicas envolve conflitos e alianças entre os diferentes atores. E, ainda que o resultado final não seja consensual, decorre dessas relações que moldam, direcionam e determinam as futuras políticas públicas.

No Brasil, até a primeira metade de 2018, existiam normas esparsas que tratavam de forma superficial ou de aspectos específicos do tema. Por exemplo, o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), a Lei de Acesso à Informação – LAI (Lei nº 12.527, de 18 de novembro de 2011), o Marco Civil da Internet – MCI (Lei

---

de três anos, que se tentou harmonizar a circulação de dados nos países-membros. O modelo se tornou exemplo mundial, tendo por objetivo assegurar a proteção das liberdades e dos direitos fundamentais das pessoas, nomeadamente quanto à vida privada, no que diz respeito ao tratamento de dados pessoais, não havendo tratamento diferenciado para os setores público e privado. (PARLAMENTO EUROPEU, **Diretiva 95/46/CE**. Disponível em: <http://www.wipo.int/wipolex/en/text.jsp?file_id=313012>. Acesso em: 28 jul. 2018).

[2] Edward Snowden foi um agente da CIA (Agência Central de Inteligência) e da NSA (Agência Nacional de Segurança), dos Estados Unidos, acusado de espionagem por vazar informaçoes sigilosas de segurança nacional do país. Ele revelou a existência de programas de vigilância norte-americanos utilizados para espionar, além dos próprios cidadãos, cidadãos estrangeiros, a partir do cruzamento de dados coletados por empresas como Google, Apple e Facebook, por exemplo. Houve a revelação, inclusive, de que dados e informações da então presidente da República brasileira, Dilma Rousseff, entre outros ocupantes de cargos políticos do alto escalão ao redor do mundo, estavam sendo monitorados, coletados e tratados pela Agência.

[3] Em março de 2018 foi revelado que a empresa de consultoria Cambridge Analytica, contratada para auxiliar a campanha das eleições de 2016 de Donald Trump, nos Estados Unidos, teve acesso indevido a dados de mais de 80 milhões de cidadãos norte-americanos a partir de um vazamento de dados de usuários do Facebook. Estes foram utilizados para influenciar as eleições presidenciais de Trump, havendo acusação de manipulação da opinião pública, por meio da sua utilização em campanhas de marketing direcionado, já que o perfil de cada um daqueles indivíduos era conhecido.

nº 12.965, de 23 de abril de 2014) e a Política de Dados Abertos – PDA (Decreto nº 8.777, de 11 de maio de 2016). Porém, a falta de harmonização e a ausência de normas para tratar de certos temas resultavam em múltiplos problemas no cotidiano da Administração Pública.

Não havia discordância, entretanto, acerca da necessidade de uma regulamentação específica acerca da proteção de dados pessoais e sensíveis. O que ocorria era a discussão sobre como harmonizar os diferentes interesses envolvidos. No caso do setor público, uma regulamentação muito restritiva poderia engessar a inovação, o desenvolvimento e a melhoria de políticas públicas. Por outro lado, uma legislação muito aberta e principiológica poderia ser inefetiva do ponto de vista prático, deixando indefeso o particular que sentir sua privacidade e intimidade ameaçadas, tornando inócua uma fiscalização mais pontual e especializada e mantendo a necessidade de judicializar a maioria das controvérsias.

Assim, após muitas discussões, em 14 de agosto de 2018, foi sancionada, com vetos[4], a Lei nº 13.709, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). Ela entrará em vigor apenas em 2020 (após 24 meses de sua publicação oficial[5]). O momento atual, então, é de preparação para os novos ditames legais.

Especificamente no âmbito governamental, a realidade apresenta-se desafiadora. É preciso aprimorar novas práticas e implementar políticas capazes de explorar todo potencial dos novos recursos tecnológicos. É preciso superar estigmas, como os relatados por Catherine Bracy, consultora de tecnologia da equipe de campanha de Barack Obama: "cidadãos usando ferramentas do século 21 para falar, Governo usando ferramentas do séc. 20 para ouvir e processos do séc. 19 para responder"[6]. Ou ainda o que menciona o historiador Harari: "enquanto a desajeitada burocracia governamental fica matutando a respeito de uma regulação cibernética, a internet se metamorfoseou dez vezes. A tartaruga governamental não é capaz de se emparelhar com a lebre tecnológica. Ela é soterrada pelos dados"[7]. Diante desse panorama, apesar de ser possível nominar experiências exitosas em termos de utilização desses recursos no governo, parece que não tem sido possível utilizá-los de forma proeminente.

Assim, uma das questões primordiais da atualidade no que diz respeito à atuação do Poder Público refere-se à sua capacidade e velocidade de atualização e adaptação para

---

[4] A discussão sobre os vetos e sobre alguns pontos específicos da nova lei será abordada no Capítulo 3.

[5] A *vacatio legis* inicial estipulado pela Lei no 13.709/2018 era de 18 meses. Porém, a Medida Provisória nº 868, de 27 de dezembro de 2018 alterou esse período para 24 meses.

[6] HUBLI, K. Scott. **The Legislative Openness Movement.** Disponível em: <https://www.ndi.org/sites/default/files/TheLegislativeOpennessMovement-030917-final.pdf>. Acesso em: 10 jan. 2018.

[7] HARARI, Yuval Noah. **Homo Deus: Uma breve história do amanhã**. São Paulo: Companhia das Letras, 2016, p. 327.

aproveitar os recursos disponíveis (diga-se aqui, o potencial dos dados por ele coletados, tratados e armazenados) com vistas a aprimorar a execução das políticas públicas. Com a melhoria na qualidade da prestação dos serviços, seria possível, inclusive, recuperar a imagem desgastada do Estado em razão da "desconfiança nas instituições políticas que administram a sociedade" e da "degradação das condições materiais de vida e crise de legitimidade dos governantes encarregados de conduzir os assuntos públicos"[8]. Para isso, seria necessário, também, estimular a participação dos cidadãos no planejamento das ações destinadas a solucionar problemas específicos, encorajando o exercício da cidadania, aprimorando o regime democrático consagrado pela Constituição Federal brasileira de 1988 (CF88) e, por fim, concretizando os direitos humanos[9].

Por outro lado, não se pode esquecer a necessidade de garantir a segurança e a proteção dos dados pessoais e sensíveis dos indivíduos. Qualquer mau uso, uso indiscriminado ou mesmo a sua divulgação indevida pode acarretar graves prejuízos políticos, ações de danos morais, além, é claro, da perda, já mencionada, da confiança e da credibilidade no governo. Ressaltam-se, também, os problemas relacionados à dignidade humana no caso do indivíduo que teve seus dados tornados públicos indevidamente.

Diante desse quadro, manter as regras de transparência e publicidade impostas atualmente pela legislação, da qual se destaca a LAI[10], e, ao mesmo tempo, respeitar as necessárias restrições quanto à confidencialidade da informação no caso de grandes bases que apresentam dados pessoais e/ou sensíveis é difícil. Por outro lado, a preparação da Administração Pública para lidar com os novos conceitos, terminologias e regras disciplinadas pela LGPD são essenciais.

Nesse momento, importante se faz apresentar os conceitos de dados pessoais e sensíveis apresentados pela LGPD:

---

[8] CASTELLS, Manuel. **Redes de indignação e esperança**: Movimentos sociais na era da internet. Rio de Janeiro: Jorge Zahar Editor Ltda., 2013, p. 127.

[9] É importante destacar, desde já, a observação feita por Tepedino acerca do que são os direitos humanos e os direitos da personalidade: "Daí considerar-se que os direitos humanos são, em princípio, os mesmos da personalidade, mas deve-se entender que quando se fala dos direitos humanos, referimo-nos aos direitos essenciais do indivíduo em relação ao direito público, quando desejamos protegê-los contra as arbitrariedades do Estado. Quando examinamos os direitos da personalidade, sem dúvida nos encontramos diante dos mesmos direitos, porém sob o ângulo do direito privado" (TEPEDINO, Gustavo. **Temas de direito civil.** Renovar: Rio de Janeiro, 2004, p. 33). Nesse sentido, no presente trabalho, será utilizado o termo direitos humanos quando se abordar a proteção de dados pessoais num âmbito mais global, ou seja, como uma política pública e, especialmente no capítulo 3.

[10] Art. 3º. Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção; (…) IV - fomento ao desenvolvimento da cultura de transparência na administração pública.

> Art. 5º Para os fins desta Lei, considera-se:
> I – dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Nota-se que dados sensíveis são aqueles que apresentam alto potencial discriminatório, devendo ser objeto de proteção mais elevada. Entretanto, é possível observar também que, apesar de extremamente positiva a iniciativa de inserir a definição desse tipo particular de dado pessoal na Lei[11], não houve, nesse caso, preocupação com o que dizem especialistas em cruzamento e/ou tratamento de dados sobre os diferentes níveis de agregação existentes.

Como explica Melo, "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"[12]. Alguns relatos demonstram esse tipo de situação:

> Pictures of individuals provide information about their ethnic origin and profiling people based on the kinds of films and entertainment they like (Netflix, on-demand TV, etc.) provides clues to their political opinions and/or their religious beliefs, just as tracking supermarket shopping habits can also provide information about customers' current and future health status, or their religious practices.
>
> Deloitte accordingly explains that it is possible, using a supermarket shopping database, to determine a person's current and future health status with a degree of accuracy comparable to that of a medical examination. These "consumer profiles" are apparently sufficient to detect individuals' propensity to develop diseases such as diabetes, women's cancers, smoking-related cancers, cardiovascular disease, depression, etc. Whereas traditionally, people wishing to take out insurance have had to declare only pre-existing conditions, diseases and disabilities of which they are aware, the fact that

[11] Na legislação brasileira vigente, o conceito de "informações sensíveis" ocorria apenas na Lei nº 12.414/2011, conhecida como "Lei do Cadastro Positivo" e era destinada unicamente a regular as relações que diziam respeito à concessão de crédito.

[12] 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, p.88.

> insurers might in future be able to detect diseases and propensities for diseases in their customers, without the latter even knowing about their condition, would create an information asymmetry highly detrimental to the insured persons[13].

Igualmente, no âmbito das discussões sobre os dados sensíveis, há que se considerar a finalidade para a qual foram coletados. Em princípio, como exceção à regra da publicidade máxima, esses dados não deveriam ser utilizados nem tornados públicos para quaisquer outros fins[14]. Isso porque o motivo de eles "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"[15].

Ainda sobre esse ponto, é essencial discutir o verdadeiro alcance e efetividade da lei quando se refere ao Poder Público. Apesar de ter destinado o Capítulo IV (arts. 23 a 30) especialmente para regular o tratamento de dados pessoais pelo setor, ele foi sempre alvo de debates, inclusive tendo sido cogitada sua retirada. Aliado a isso, outros dispositivos foram inseridos no texto normativo, com notáveis exceções ao setor público de forma a facilitar o tratamento e o compartilhamento de dados pessoais e sensíveis pelos órgãos e entidades da APF.

Tal privilégio pode ser observado na inteligência do inc. III do art. 7º c/c a al. "b" do inc. II do art. 11 (que trata dos dados sensíveis), que dispensam o consentimento do titular e permitem o tratamento de dados pessoais pela Administração Pública para executar políticas públicas quando estas estiverem previstas em leis e regulamentos ou quando respaldadas em contratos, convênios ou instrumentos congêneres. Percebe-se, assim, uma grande amplitude de situações que poderão ser abarcadas pelo referido dispositivo.

Releva-se, por outro lado, que o legislador buscou atenuar ou compensar tais exceções quando inseriu, no § 2º do art. 11 c/c art. 23 da LGDP, a obrigação de os órgãos e entidades darem ampla publicidade à dispensa de consentimento. Compeliu-os, também, a informar em veículos de fácil acesso as hipóteses em que realizam o

---

13 ROUVROY, Antoinette. "**Of Data and Men**": Fundamental Rights and Freedoms in a World of Big Data. Bepress. 2016. Disponível em: < https://works.bepress.com/antoinette_rouvroy/64/>. Acesso em: 05 set. 2018.

14 DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p.91-108, jul/dez2012. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658>. Acesso em: 30 mai. 2018.

15 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.

tratamento de dados pessoais, sua previsão legal, finalidade, procedimentos e práticas utilizadas para executar tais atividades.

Não se trata, portanto, de uma autorização para o setor público compartilhar de forma geral e indiscriminada os dados sensíveis. Porém, não se pode deixar de olvidar que o controle acerca da publicidade conferida aos atos da APF, bem como a forma de sua disponibilização, até mesmo nos seus sítios institucionais, não costumam ser tão claros, transparentes e efetivos.

Assim, ainda visando assegurar aos titulares a devida proteção de seus dados (corroborando com o modelo adotado por 90% dos países que atualmente possuem regulação específica de proteção de dados), a criação de uma autoridade nacional de proteção de dados é defendida por várias entidades, dentre as quais a Procuradoria-Geral da República[16]. Tal dispositivo, entretanto, foi, inicialmente, vetado na nova lei alegando-se vício de iniciativa, por se tratar de prerrogativa do Executivo.

Em 27 de dezembro de 2018, porém, um dos últimos atos do ex-presidente da República foi a edição da Medida Provisória (MP) nº 869[17]. Além de promover alterações na LGPD, a MP criou a Autoridade Nacional de Proteção de Dados (ANPD), com vigência a partir de 28 de dezembro de 2018.

Percebe-se, assim, que o tema goza de grande atualidade, perpassando diversos aspectos da gestão pública. Entre eles, os riscos de segurança na disponibilização dos dados; a avaliação dos mecanismos de controle de divulgação das informações provenientes dos dados acessados; a responsabilização da Administração, do gestor ou do usuário no caso de eventual vazamento de informações ou de revelação indevida (as chamadas *data breaches* ou violação de dados*)*; além de questões específicas relacionadas à Tecnologia da Informação e à disponibilidade de recursos humanos especializados.

Nota-se que a disponibilização de dados pela Administração ainda é um tema que carece de estudos e melhorias pois associado às relações de confiança e credibilidade

---

16 PRESCOTT, Roberta. PGR defende criação de uma autoridade nacional de proteção de dados. **Associação Brasileira de Internet**, 24 ago. 2016. Disponível em: <http://www.abranet.org.br/Noticias/PGR-defende-criacao-de-uma-autoridade-nacional-de-protecao-de-dados-1179.html#.WCnjudIrKM9>. Acesso em: 30 mai. 2018.

17 No dia anterior, em 26 de dezembro de 2018, também foi publicado o Decreto nº 9.637, instituindo a Política Nacional de Segurança da Informação (PNSI), dispondo sobre a governança da informação e sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Esse Decreto revogou os de nºs 3.505/2000 e 8.135/2013 que tratavam do tema e tem fundamental importância, pois, além de estabelecer diversas competências aos órgãos e entidades da APF relacionadas ao tema, define como instrumento da PNSI, a Estratégia Nacional de Segurança da Informação que conterá ações estratégicas e os objetivos relacionados à segurança e defesas cibernéticas, à segurança das infraestruturas críticas e da informação sigilosa, bem como à proteção contra vazamento de dados, devendo ser elaborada com ampla participação da sociedade e órgãos e entidades da APF (art. 6º e art. 15, Decreto nº 9.637/2018).

das instituições públicas e ao dever de publicidade governamental. Ademais, dispõe de grande complexidade em sua regulamentação. Assim, surgiu o seguinte problema: no cenário atual, a tutela aos direitos pessoais e sensíveis pela Administração Pública é realizada de modo satisfatório?

Com o objetivo de responder esse questionamento, foi necessário analisar e compreender os modelos atuais de gestão, tratamento e disponibilização de dados pessoais e sensíveis, a fim de verificar se atendem aos princípios da publicidade e da transparência, sem violar o princípio da privacidade. Com isso, a seguinte hipótese veio à tona: a tutela aos direitos pessoais no Brasil, quando se trata das bases de dados geridas pelo governo, é deficiente.

Isso porque, além de, numa análise preliminar, ter sido possível observar que a ausência e a morosidade na edição de uma legislação específica impactaram severamente as políticas públicas, notou-se que a terminologia até então utilizada ainda é vaga, imprecisa e pode gerar interpretações errôneas por parte da Administração Pública. Além disso, o modelo de gestão de dados é diferente entre os órgãos, que possuem graus diferentes de segurança da informação, podendo, inclusive, incorrer em ilegalidades. Não há clareza sobre as sanções decorrentes do mau uso desses dados e a possibilidade de interoperabilidade ou compartilhamento de bases[18] é dificultada em razão dos limites impostos, atualmente, pela Lei de Acesso à Informação, por exemplo.

A falta de uma normatização clara e concreta sobre os direitos pessoais e sensíveis gera insegurança jurídica, pois afeta diretamente a esfera privada dos indivíduos já que associada a conceitos como autodeterminação informativa e livre consentimento. No caso do setor público, esses conceitos merecem ainda mais atenção, pois precisam ser analisados quanto à sua efetividade e ao impacto que podem causar no caso de políticas públicas.

Assim, no contexto atual, em que mundialmente é discutida a temática da proteção de dados[19] – e notadamente no caso brasileiro, em que, após amplo debate, a nova lei foi promulgada -, avaliar os modelos atuais de disponibilização de dados (os quais abrangem dados pessoais e/ou sensíveis) da Administração Pública é tarefa complexa, porém indispensável para a busca do aprimoramento da condução das políticas públicas de dados, já que adaptações e aprimoramentos se farão necessários.

---

[18] Importante destacar que, neste estudo, não estão sendo considerados o compartilhamento e a transferência de dados de forma transnacional, mas, tão somente, entre os órgãos da Administração Pública.

[19] Vale frisar que o debate também foi impulsionado pela entrada em vigor, em 25 de maio de 2018, das novas regras de proteção de dados da União Europeia, trazidas pelo Regulamento Geral sobre a Proteção de Dados (em inglês, GDPR – *General Data Protection Regulation*), conferindo aos cidadãos maior controle sobre os seus dados e exigindo condutas mais rígidas e transparentes das empresas e governo.

Para tentar contribuir com as discussões e visando ao aperfeiçoamento das políticas públicas do Estado, algumas atividades foram essenciais. Entre elas, o levantamento e o exame de vasta bibliografia especializada e da legislação pertinente ao tema, inclusive normas infralegais referentes aos órgãos e entidades analisados. Além destas, foi de suma relevância a análise dos PLs que tramitavam nas Casas Legislativas, bem como o acompanhamento dos debates realizados nas respectivas audiências públicas, pois elas acabavam por refletir os principais pontos de divergência e as diferentes argumentações sobre cada aspecto das propostas.

Ainda, com o intuito de verificar o funcionamento da gestão de algumas bases de dados no setor público, optou-se por delimitar a quantidade de Ministérios para estudo, a partir da relevância de suas bases. Foram escolhidos: os Ministérios do Desenvolvimento Social (MDS), da Educação (MEC), da Fazenda (MF), da Justiça (MJ) e Extraordinário da Segurança Pública (MESP), do Trabalho (MT) [20]. Para garantir o efetivo posicionamento dos órgãos, foram realizados diversos pedidos de acesso à informação por meio do Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC)[21].

Além dos pedidos, foram feitas entrevistas e enviados questionários via e-SIC para o Ministério do Planejamento, Desenvolvimento e Gestão (MPDG)[22], responsável pela coordenação das ações que dizem respeito ao compartilhamento, integração ou tratamento de dados em diferentes órgãos e entidades da Administração Pública Federal (APF), bem como entrevistas com representantes do Tribunal de Contas da União (TCU), órgão responsável pelo controle externo da APF.

Não fez parte do escopo da pesquisa observar se as bases de dados estão ou podem ser disponibilizadas em formato aberto, se poderiam ser cruzadas com outras bases visando à melhoria de políticas públicas e se seus campos são uniformizados, mas tão somente analisar como se dá o fluxo de dados no interior dos órgãos responsáveis e

[20] A Medida Provisória nº 870, de 1º de janeiro de 2019, com o novo mandato presidencial no Brasil, estabeleceu nova estrutura organizacional para os órgãos da Presidência da República e para os Ministérios. Com isso, o MDS passou a integrar a estrutura do Ministério da Cidadania. Os Ministérios da Fazenda e do Trabalho, por sua vez, integraram a estrutura do Ministério da Economia. Já o Ministério da Justiça e Segurança Pública (MJSP) sofreu duas transformações durante o período da pesquisa (2016-2019). Com a Medida Provisória nº 821, de 27 de fevereiro de 2018, foi criado o Ministério Extraordinário da Segurança Pública e, assim, o MJSP voltou a se chamar Ministério da Justiça. Em 2019, a MP nº 870 fundiu, novamente, as duas estruturas, retomando a nomenclatura Ministério da Justiça e Segurança Pública. No presente trabalho, adotar-se-á a nomenclatura utilizada à época das respectivas entrevistas / coleta de dados.

[21] BRASIL. Ministério da Transparência e Controladoria-Geral da União. **E-SIC:** sistema eletrônico do Serviço de Informação ao Cidadão. Disponível em: <https://esic.cgu.gov.br/sistema/site/index.aspx>. Acesso em: 09 ago. 2018.

[22] Na nova organização da Administração Pública Federal estabelecida pela MP nº 870/2019, o MPDG foi integrado à estrutura do Ministério da Economia.

entre estes e os demais. Para isso, buscou-se verificar quais são as principais dificuldades de gestão, se em razão de ordem técnica, financeira, legal ou de pessoal.

Diante desse quadro, também foi indispensável tratar de relevantes questões referentes ao Serviço Federal de Processamento de Dados (Serpro) e à Empresa de Tecnologia e Informações da Previdência (Dataprev), empresas públicas que desenvolvem sistemas para o setor público, bem como hospedam e processam algumas das bases de dados mais relevantes da Administração Pública Federal.

O presente trabalho também discute os benefícios, os problemas e os desafios relativos aos diferentes modelos de disponibilização de dados para fins de pesquisa ofertados por três entidades: Instituto Brasileiro de Geografia e Estatística (IBGE), Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e Instituto de Pesquisa Econômica Aplicada (Ipea). Trata-se de ambientes denominados seguros, criados com o objetivo de cruzar informações não disponíveis em microdados públicos.

Por fim, apresenta os principais aspectos que poderão impactar o fluxo de dados na Administração Pública devido às novas regras a serem obedecidas a partir de 2020. Ao discorrer sobre a opção brasileira pela adoção de um modelo de proteção de dados pessoais e sensíveis como o europeu, abrangidos pelos direitos da personalidade, serão discutidos conceitos como consentimento, finalidade e transparência, além dos riscos e da responsabilização diante de uma divulgação indevida.

1 Os desafios decorrentes da dicotomia: "melhoria de políticas públicas" x "proteção de dados pessoais e sensíveis"

A oposição entre as possibilidades de aperfeiçoamento das políticas públicas e a necessidade de cautela com o uso dos dados pessoais e sensíveis tem sido uma constante no dia-a-dia da Administração Pública. Diante de uma ampla gama de recursos tecnológicos, a APF tem de se modelar, adaptar, ajustar, criar e inovar. Por um lado, muitos são os desafios. Por outro, as possibilidades advindas com essas novas tecnologias são imensas.

A sociedade do conhecimento, como é chamada na atualidade, é marcada pelo avanço tecnológico, pelo *boom* de informações e maior facilidade em seu acesso, pela suavização das fronteiras no mundo globalizado e, ainda, pela enorme quantidade de dados e informações acumulados pelos setores públicos e privados. Nessa abundância de dados, se eles forem coletados, armazenados, tratados e geridos de forma apropriada, podem ser transformados em inteligência, tornando-se importantes ferramentas para a formulação e implementação de políticas públicas.

Com a evolução da internet, as pessoas podem interagir de diversas formas e com as finalidades mais variadas possíveis. Num país com cerca de 209 milhões de habitantes[23] e grandes desigualdades sociais - ocupando, atualmente, a 79ª posição de 188 nações no ranking do Índice de Desenvolvimento Humano (IDH)[24] -, observa-se o aumento contínuo do número de domicílios com acesso à internet. Em 2015, aproximadamente 58% dos domicílios brasileiros tinham acesso à internet, dentre os quais 99,6% possuíam conexão em banda larga[25].

Nessa era da Big Data, questões como compartilhamento, integração e tratamento de dados pela Administração Pública, desenvolvimento de softwares e aplicativos visando

[23] BRASIL. Instituto Brasileiro de Geografia e Estatística. **Projeção da população do Brasil e das Unidades da Federação.** Disponível em: <http://www.ibge.gov.br/apps/populacao/projecao/>. Acesso em: 20 jun. 2018.

[24] UNITED NATIONS DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 2016.** Washington, Dc, USA: Communications Development Incorporated, 2016. Disponível em: <http://www.br.undp.org/content/dam/brazil/docs/RelatoriosDesenvolvimento/undp-br-2016-human-development-report-2017.pdf>. Acesso em: 21 ago. 2017.

[25] BRASIL. Instituto Brasileiro de Geografia e Estatística. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal: 2015.** Rio de Janeiro: IBGE, 2016. p. 49 Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/livros/liv99054.pdf>. Acesso em: 21 ago. 2017. (OBS: trata-se do suplemento da Pesquisa Nacional por Amostra de Domicílios - PNAD 2015).

ampliar a participação popular e o processo democrático, por meio, por exemplo, do *crowdsourcing*[26], vêm à tona. Mas, junto a elas, também aparecem questionamentos acerca da forma como estão sendo utilizados os dados coletados pelo Poder Público e da segurança a eles conferidos.

Esses problemas decorrem de uma variedade de questões. Entre elas, o reconhecimento muito recente da necessidade de se ter uma política pública de proteção de dados pessoais no país; a ausência, até meados de 2018, de um marco legal sobre o tema; a terminologia aberta das normas; a necessidade de atendimento aos princípios da publicidade e a dificuldade de se entender conhecimentos técnicos de várias áreas, como da Tecnologia da Informação e da Comunicação.

1.1 A recente visibilidade da temática da proteção de dados pessoais e sensíveis e a sua inserção como política pública

As atividades de formular e executar políticas públicas são complexas. Envolvem diversos fatores, dentre os quais a conjuntura política e as influências internas ou externas ao Poder Público. Nesse contexto, o Direito tem o papel essencial de conformar os diferentes interesses por meio de institutos normativos.

Segundo Bucci, é necessário compreender as políticas públicas como categoria jurídica para buscar formas de concretização dos direitos humanos e, em particular, dos direitos sociais. A construção de leis, especialmente aquelas advindas de proposições do Poder Executivo, tende, em última instância, à realização de uma política pública, definida como "*um programa ou quadro de ação governamental, porque consiste num conjunto de medidas articuladas (coordenadas), cujo escopo é dar impulso, isto é, movimentar a máquina do governo, no sentido de realizar algum objetivo de ordem pública ou, na ótica dos juristas, concretizar um direito*"[27]. No caso em apreço, o direito do indivíduo de ter seus dados protegidos.

---

[26] O termo foi cunhado em 2006 pelo jornalista e editor da revista Wired, Jeff Howe, no artigo **The Rise of Crowdsourcing** (HOWE, Jeff. **The Rise of Crowdsourcing.** Disponível em: <https://www.wired.com/2006/06/crowds/>. Acesso em: 23 ago. 2017.). O fenômeno diz respeito à coleta de informações a respeito de determinado tema, utilizando a inteligência e o conhecimento coletivos e voluntários por meio da internet, para criar conteúdo e soluções. Busca incrementar o nível democrático na gestão e formulação de políticas públicas de temas relevantes e de interesse do cidadão, tornando-a não apenas representativa ou colaborativa, mas participativa. Exemplos recentes são as discussões dos projetos de lei do marco civil da internet (que veio a se tornar a Lei nº 12.965/2014) e do projeto de lei nº 5.276/2016 que trata da proteção de dados pessoais.

[27] BUCCI, Maria Paula Dallari. **O conceito de política pública em direito**. In Políticas Públicas: Reflexões sobre o Conceito Jurídico (Maria Paula Dallari Bucci, org.) São Paulo: Saraiva, 2006, p.14.

Coutinho[28], por sua vez, aponta quatro papeis a serem desempenhados pelo Direito nas políticas públicas: o Direito como objetivo, o Direito como arranjo institucional, o Direito como caixa de ferramentas e o Direito como vocalizador de demandas. No caso da política de proteção de dados pessoais e sensíveis, observa-se a conformação de todos esses papeis.

Dois deles podem ser claramente constatados na recente percepção da necessidade de se regular o uso e a proteção de dados pessoais e sensíveis no país. Como arranjo institucional, são vistas as discussões sobre quem deve centralizar as possíveis novas atribuições de fiscalização e controle sobre o uso dos dados pela Administração Pública[29]. Como vocalizador de demandas, observa-se o atendimento a critérios de participação popular, como a discussão aberta e a possibilidade de colaboração pelo público e por todos interessados na implementação da lei. Sob esse aspecto, frisa-se, ainda, que foi a partir das demandas apresentadas pela sociedade que essa temática ganhou visibilidade e o Poder Público passou a ser pressionado a pautá-la ou optou por inseri-la em sua agenda institucional.

Interessante, então, verificar se a proteção de dados pessoais e sensíveis, de fato, se tornou uma política pública e em que estágio do denominado "ciclo de políticas públicas" se encontra. De modo geral, esse ciclo abrange sete etapas interdependentes[30]: 1) identificação do problema, 2) formação da agenda, 3) formulação de alternativas, 4) tomada de decisão, 5) implementação, 6) avaliação e 7) extinção.

Segundo Secchi, "apesar de sua utilidade heurística, o ciclo de políticas públicas raramente reflete a real dinâmica ou vida de uma política pública. As fases geralmente se apresentam misturadas, as sequências se alternam"[31]. Porém, a classificação é útil no sentido de contribuir com a organização de ideias, de simplificar problemas complexos e de auxiliar políticos, administradores e pesquisadores a criarem um referencial comparativo para casos heterogêneos.

Sob essa perspectiva, pode-se dizer que a política de proteção de dados encontra-se na quinta etapa do ciclo de políticas públicas, qual seja, sua implementação. A primeira, **identificação do problema**, já foi realizada. Como afirma Secchi, o problema foi percebido. A situação pública da atualidade tornou-se insatisfatória, pois passou

---

[28] COUTINHO, Diogo R. **O direito nas políticas públicas.** Disponível em: < http://www.fd.unb.br/images/Pos-Graduacao/Processo_Seletivo/Processo_Seletivo_2016/Prova_de_Conteudo/14_05_12_15O_direito_nas_politicas_publicas_FINAL.pdf>. Acesso em: 10 jun. 2018.

[29] Cf. item 3.4.

[30] SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012, p. 33.

[31] Ibidem, p. 34.

a afetar a percepção de muitos atores relevantes[32]. O problema identificado foi: a sociedade brasileira carecia de legislação específica para proteção dos dados pessoais e, em especial, dos dados sensíveis.

Apesar de existirem dispositivos exclusivos para proteção da privacidade e dos dados ao longo da Carta Magna e algumas normas esparsas na legislação infraconstitucional (como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet, entre outros), no Brasil, inexistia lei específica que tratasse do tema.

No país, já na década de 90, o Poder Judiciário se mostrava preocupado quanto à "coleta geral e indiscriminada dos dados pessoais"[33] do cidadão. Quando da análise dos serviços de bancos de dados de proteção ao crédito (SPC), previsto no art. 43 do CDC, o ministro Ruy Rosado destacou:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita a sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular, para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica (STJ, REsp. 22.337-8-RS, relator Min. Ruy Rosado de Aguiar, DJU 20.04.1995).

A análise feita no voto desse REsp (que, na verdade, discutia o tempo prescricional para ações de cobrança dos débitos no SPC e, consequentemente, o tempo de manutenção dos registros nos bancos de dados), é de grande importância, pois, pela primeira vez, foi feita a associação do direito à privacidade e à proteção de dados pessoais aos riscos advindos da prática do tratamento de dados e à vulnerabilidade

---

[32] SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012, p. 35.

[33] BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de protecão ao crédito.** São Paulo: Revista dos Tribunais: 2003, p. 99.

dos cidadãos. O ministro "inova na jurisprudência brasileira ao chamar a atenção para os riscos advindos da atividade de processamento de dados, tanto pelo setor público quanto pelo setor privado"[34].

Porém, o assunto só começou, de fato, e ganhar repercussões consideráveis pelo Poder Público[35] em 2010. Especialmente sob a gestão do MJ, em parceria com o Observatório Brasileiro de Políticas Digitais do Comitê Gestor da Internet no Brasil, foi proposto debate com a sociedade sobre o anteprojeto de lei de dados pessoais que seria encaminhado ao Poder Legislativo em 2011. O texto, porém, só foi enviado à Câmara dos Deputados em maio de 2016, após passar por nova consulta pública, em 2015. Isso porque, como já apontado, verifica-se que, na maior parte das vezes, é necessária a eclosão de um problema público para inseri-lo na agenda governamental.

E assim o foi. O esquecimento do tema foi cessado com os vários escândalos de vazamento de dados que emergiram no período, como o do caso Edward Snowden. Foi em 2015 que vieram à tona as repercussões sobre a utilização de dados pessoais e sensíveis, inclusive, da ex-presidente Dilma Rousseff, de ministros, diplomatas e assessores brasileiros (uma lista de nomes classificada como ultrassecreta) pelo serviço de espionagem dos Estados Unidos[36].

O tema avançou. E foi a partir desse momento que, podemos dizer, passou-se à **formação da agenda**. "Se um problema é identificado por algum ator político, e esse ator tem interesse na resolução de tal problema, este poderá então lutar para que tal problema entre na lista de prioridades de atuação. Essa lista de prioridades é conhecida como agenda"[37].

Assim, com o tema da proteção de dados incluído na pauta do dia não apenas do Poder Executivo, mas de todo Poder Público, o enfrentamento da questão tomou força e percebeu-se que a melhor alternativa seria, de fato, a sua regulamentação por meio da criação de um marco legal.

---

34 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental.** São Paulio. Saraiva, 2014, p. 99-100.

35 Em 1980, a deputada Cristina Tavares (PMDB/PE) apresentou o Projeto de Lei n. 2.796, que buscava assegurar aos cidadãos acesso às informações sobre sua pessoa constantes de bancos de dados e dava outras providências, e dispunha sobre "tratamentos automatizados de informações nominativas operadas por conta do Estado, de estabelecimento público ou de entidade de direito privado", mas que não dão conta da dinâmica atual da sociedade e, por esse motivo, não está sendo considerado na presente análise (Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=206829&st=> Acesso em: 09 ago. 2018) .

36 EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. **G1**: online. Disponível em: <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. 04/07/2015. Acesso em: 05 nov. 2018.

37 SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012, p. 36.

Para que isso acontecesse - nesta terceira etapa do ciclo de políticas públicas, a **formulação de alternativas** -, o Poder Executivo, por meio do MJ, elaborou um anteprojeto de lei para tratar da proteção de dados pessoais, o que veio a se tornar o PL nº 5.276/2016. As Casas Legislativas, por sua vez, voltaram sua atenção aos seus respectivos projetos de lei que dispunham sobre o tema (PL nº 4.060/2012 e PLS nº 330/2013) e, apesar das diferenças, percebeu-se que, naquele momento, havia um consenso em todo o Poder Público acerca da necessidade da regulação do tema.

Atingiu-se, então, a etapa da **tomada de decisão**, "o momento em que os interesses dos atores são equacionados e as intenções (objetivos e métodos) de enfrentamento de um problema público são explicitadas"[38]. Nesse estágio, o MJ optou por realizar consultas públicas[39], em meio digital[40], para discutir o anteprojeto de lei (APL) e depois encaminhá-lo ao Congresso Nacional. Câmara e Senado, por sua vez, realizaram mais de dez dias de audiências públicas com participação dos diferentes atores da sociedade civil, do governo e do setor privado para debater o tema.

Ao pensar sobre a etapa de tomada de decisão devida ao Poder Público, e em termos do modelo teórico desenvolvido por Jobert e Muller, as políticas públicas operam por meio de modelos de referência que asseguram a continuidade de sua ação. Esses modelos têm uma tripla dimensão: cognitiva, normativa e instrumental[41].

Assim, para o primeiro[42] ciclo de formulação da política pública de proteção de dados pessoais, qual seja, a normatização do tema, as seguintes dimensões da política pública foram consideradas:

---

38 SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012, p. 40.

39 BRASIL. Ministério da Justiça. **Pensando o Direito:** Proteção de Dados Pessoais. Disponível em: <http://pensando.mj.gov.br/dadospessoais/> . Acesso em: 09 ago. 2018.

40 A prática de *crowdsourcing*, como a que foi utilizada, ainda que timidamente, tem sido difundida no setor público. (cf. N.R. 26)

41 Segundo Solanas, as três dimensões são as seguintes: "1. Cognitiva: el código debe proporcionar elementos de interpretaciones de las fuerzas que determinan la evolución probable del sector y la sociedad; 2. Normativa: el código define los valores a través del cual habrá que asegurar el respeto en esta evolución; 3. Instrumental: el código define también un conjunto de principios de acción que quieren orientar la acción pública (en función de su saber y valores)". SOLANAS, Facundo. **La ley de educacion superior en Argentina: un analisis en terminos de referenciales de la accion publica.** Disponível em: <http://publicaciones.anuies.mx/pdfs/revista/Revista149_S4A2ES.pdf>. Acesso em: 25 ago. 2017.

42 Para fins deste estudo, denomina-se primeiro ciclo a fase até a normatização do tema. Como é sabido, as políticas públicas são dinâmicas e interdependentes. Assim, no caso em apreço, trata-se de uma política pública cujo plano de normatização foi recém-aprovado; ainda restando a elaboração de normas complementares editadas, por exemplo, pela Autoridade Nacional de Proteção de Dados (art. 41, § 3º).

Quadro 1 - Planos de análise para formulação da política pública de proteção a dados pessoais (primeiro ciclo: normatização do tema)

Dimensão cognitiva	Proteção à dignidade humana e aos direitos fundamentais da pessoa humana, em particular a liberdade, a igualdade e a privacidade
Dimensão normativa	Constituição Federal de 1988, trata do tema nos seguintes dispositivos: art. 1º, inc IV; art. 5º, inc. IX e XXXII; art. 170 e art. 220. **Até 2018 apenas existiam normas esparsas e setoriais. Tratavam indiretamente do tema:** Lei nº 8.078/1990, Código de Defesa do Consumidor Lei nº 12.414/2011, Lei do Cadastro Positivo Lei nº 12.527/2011, Lei de Acesso à Informação Lei nº 12.965/2014, Marco Civil da Internet Lei nº 13.444/2017, Identificação Civil Nacional (ICN) Lei nº 13.460/2017, Participação, proteção e defesa dos direitos do usuário dos serviços públicos Lei Complementar nº 105/2001, Sigilo das operações de instituições financeiras Decreto nº 3.505/2000, Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (revogado pelo Decreto no 9.637/2018) Decreto nº 7.724/2012, Regulamenta a Lei de acesso à informação Decreto nº 7.845/2012, Procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo Decreto nº 8.135/2013, Comunicações de dados da administração pública federal direta, autárquica, fundacional (revogado pelo Decreto no 9.637/2018) Decreto nº 8.270/2014, Sistema Nacional de Informações de Registro Civil (Sirc) Decreto nº 8.373/2014, Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (e-social) Decreto nº 8.638/2016, Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional Decreto nº 8.764/2016, Sistema Nacional de Gestão de Informações Territoriais Decreto nº 8.777/2016, Política de Dados Abertos do Poder Executivo Federal Decreto nº 8.789/2016, Compartilhamento de bases de dados na Administração Pública Federal Decreto nº 8.936/2016, Plataforma de Cidadania Digital e oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional Decreto nº 9.094/2017, Simplificação do atendimento prestado aos usuários dos serviços públicos Além de diversas Portarias de órgãos e entidades vinculadas da Administração Pública Federal que tratam de suas competências específicas
Dimensão instrumental	Democracia participativa: consultas e audiências públicas com os diversos setores da sociedade civil organizada, empresarial e poder público; redação e proposição do projeto de lei; encaminhamento e acompanhamento da tramitação pelo Legislativo.

Esse contexto reforçava a necessidade de um marco legal, único e uniforme, para a proteção de dados pessoais e sensíveis. Então, em 2018, o tema tomou ainda maior relevância por se tratar de ano eleitoral no Brasil e terem sido divulgadas informações acerca da utilização de dados de usuários do Facebook obtidos de forma não consentida

pela Cambridge Analytica para direcionamento na campanha eleitoral de Donald Trump, nos Estados Unidos, por exemplo.

A pressão aumentou após a entrada em vigor das novas regras estabelecidas pelo Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, em maio de 2018. Isso porque, por não possuir os requisitos que exigem o consentimento dos usuários, a celebração de contratos e cláusulas-padrão e normas corporativas vinculantes ou acordos e tratados bilaterais, o Brasil não era reconhecido pela União Europeia (UE) como um Estado com o qual poderiam ocorrer transferências internacionais de dados[43].

O RGPD, em termos de transferência internacional de dados pessoais, pode ser considerado uma lei com eficácia e aplicação extraterritorial, ou seja, se aplica a empresas localizadas em qualquer um dos países da UE e, também, àquelas que prestam serviços a pessoas neles localizadas.

De acordo com o regulamento, três são as formas para haver a referida transferência. Em primeiro lugar, existe a possibilidade de autorização ("decisão de adequação") pela Comissão Europeia, caso os países avaliados se adaptem aos parâmetros da nova lei (Capítulo V, arts. 44 a 50 da RGPD) e assegurem um nível adequado (e equiparável) de segurança e proteção dos dados[44]. Nesses casos, a avaliação é feita periodicamente e não há necessidade de autorização específica para a transferência.

Em segundo lugar, para haver o fluxo de dados para países os quais ainda não tenham sido reconhecidos, são necessárias regras vinculativas que estabeleçam garantias de adequação (*binding corporate rules*). Entre elas, podem ser exigidas: assinatura de contrato aprovado pela autoridade de proteção de dados, adoção de códigos de conduta, procedimentos de certificação, ou disposições, nos contratos administrativos, que contemplem os direitos dos titulares dos dados nos acordos administrativos entre as autoridades ou organismos públicos.

Por último, a transferência só poderá ocorrer em situações muito específicas e para uma quantidade limitada de dados. Por exemplo, caso haja o consentimento do titular, razões de interesse público, proteção de interesses vitais do titular ou interesse legítimo quando da avaliação do caso concreto. Em todas essas circunstâncias, o

---

[43] SOMBRA, Thiago Luís. GDPR e proteção de dados pessoais: uma agenda também brasileira. **JOTA**, Brasília, 25 mai. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/gdpr-agenda-brasileira-25052018>. Acesso em 15 jun. 2018.

[44] COMISSÃO EUROPEIA. Adequacy of the protection of personal data in non-EU countries. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. Acesso em 28 nov. 2018.

descumprimento das regras poderá ensejar advertências, multas ou, até mesmo, suspensão do tratamento de dados por prazo a ser estabelecido.

Nesse panorama, o Brasil se viu pressionado a fazer parte de um novo modelo de Direito que passa a cuidar não apenas de suas normas internas positivadas, mas segue tendências e movimentos universais que impactam diretamente o Direito interno. E, diante desse quadro, novas audiências públicas foram realizadas, dessa vez pelo Poder Legislativo, reforçando ainda mais a ideia de que "normas jurídicas podem levar políticas públicas a serem mais democráticas uma vez que, por meio de regras procedimentais que disciplinem consultas e audiências públicas e a publicidade dos atos administrativos, as obriguem a estar abertas aos *inputs* de uma pluralidade de atores"[45], ou seja, transformando a democracia não apenas em representativa ou colaborativa, mas em participativa[46].

Assim, como já apontado, a LGPD foi aprovada em agosto de 2018, dando início à fase de **implementação** das novas regras impostas pela lei. Após o período de vacância, que visa à preparação e ao planejamento das políticas de proteção de dados, de estratégias, programas e ações pelos órgãos públicos e empresas privadas, é na etapa de implementação que, segundo Secchi, poderão ser produzidos os resultados concretos. As falhas na implementação, a despeito dos mais bem-intencionados planejamentos, também podem ser vistas nessa fase:

---

[45] COUTINHO, Diogo R. **O direito nas políticas públicas.** Disponível em: < http://www.fd.unb.br/images/Pos-Graduacao/Processo_Seletivo/Processo_Seletivo_2016/Prova_de_Conteudo/14_05_12_15O_direito_nas_politicas_publicas_FINAL.pdf>. Acesso em: 10 jun. 2017.

[46] Destaca-se que não foi objeto deste estudo analisar as relações políticas e de poder nesses mecanismos que visam aumentar a participação popular durante a implementação de uma lei, por exemplo. Mas vale ressaltar a importância de estudos no sentido de averiguar se o Direito é apenas mais um veículo consagrador do "estado da relação de forças entre os grupos" ou se, de fato, atua como vocalizador de demandas, inclusive das partes menos favorecidas ou subrepresentadas, como as minorias. Como ressalta, por exemplo, o sociólogo Bourdieu: "o direito limita-se a consagrar simbolicamente, por um registro que eterniza e universaliza, o estado da relação de forças entre os grupos e as classes que produz e garante praticamente o funcionamento de tais mecanismos". (BOURDIEU, Pierre. **A produção da crença**: contribuição para uma economia dos bens simbólicos.São Paulo: Zouk, 2a Ed., 2004, p. 199) Questões relacionadas à assimetria da informação, à capacidade discursiva e ao poder de argumentação são alguns dos aspectos a serem considerados, especialmente quando os mecanismos utilizados são virtuais. Sob esse aspecto, destaca-se, também, pesquisa realizada em 2015 sobre o processo de participação popular no canal e-Democracia, da Câmara dos Deputados, para discussão do então projeto de lei que tratava do Marco Civil da Internet (tema que recebeu o maior número de contribuições em relação aos demais temas já disponibilizados no canal). De acordo com pesquisa realizada, "o perfil dos usuários está muito aquém de representar os vários grupos políticos e estratos sociais existentes no Brasil, especialmente entre os usuários de iniciativas de participação política digital criadas e coordenadas por órgãos governamentais" (FREITAS, Christiana Soares de. Mecanismos de dominação simbólica nas redes de participação política digital. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso (orgs.). **Democracia Digital**, **Comunicação Política e Redes:** Teoria e Prática. Rio de Janeiro: Folio Digital: Letra e Imagem, 2016. p. 110-135. Disponível em: <http://livro.democraciadigital.org.br/files/2017/05/Democracia-Digital.pdf>, p. 114. Acesso em: 25 ago. 2017.

> São muitos os exemplos brasileiros de "leis que não pegam", "programas que não vingam" ou projetos de solução a problemas públicos que acabam sendo totalmente desvirtuados no momento da implementação. A importância de estudar a fase de implementação está na possibilidade de visualizar, por meio de instrumentos analíticos mais estruturados, os obstáculos e as falhas que costumam acometer essa fase do processo nas diversas áreas de política pública (saúde, educação, habitação, saneamento, políticas de gestão etc.). Mais do que isso, estudar a fase de implementação também significa visualizar erros anteriores à tomada de decisão, a fim de detectar problemas mal formulados, objetivos mal traçados, otimismos exagerados[47].

Essa fase será sucedida, por fim, pela **avaliação** e, se for o caso, sua **extinção**.

1.2 As normas abertas, o princípio da publicidade e as consequentes dificuldades em administrar os dados pessoais e sensíveis

A realidade das questões relacionadas à proteção de dados pessoais e sensíveis pela Administração Pública têm relação direta com a interpretação das normas. O motivo de a interpretação de um texto legislativo ser problemática decorre do fato de a lei se servir 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"[48].

Ao falar em legística[49], 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 é, em parte, acarretado pela alta densificação normativa no Brasil e pela incorporação de uma "franca atividade de legislação" [50] pela Administração Pública:

---

47 SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012, p. 44/45.

48 LARENZ, Karl. **Metodologia da ciência do Direito.** Tradução: José Lamego. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 1997, p. 439.

49 Atualmente, a produção das normas em âmbito federal deve seguir a metodologia estabelecida no Decreto nº 9.191, de 1º de novembro de 2017.

50 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, p.127.

> 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[51].

Assim, mesmo tentando produzir normas com qualidade, várias dificuldades continuam decorrendo da linguagem utilizada, ainda mais quando se trata de um cenário em que o ordenamento jurídico brasileiro é vasto, com muitas normas esparsas e específicas de acordo com as diferentes áreas temáticas[52].

O problema também ganha peso no chamado movimento "neoconstitucionalista", por meio do qual são valorizados os princípios jurídicos na aplicação do Direito, reconhecendo-se sua força normativa. Com conceitos demasiadamente abertos, como publicidade, intimidade e comunicações de dados[53], a Carta Magna e demais normativos infraconstitucionais de caráter principiológico podem levar gestores e administradores públicos a interpretações errôneas ou dúbias; gerar interpretações diferentes quanto à extensão e ao alcance das normas; bem como acabar aumentando a judicialização de questões cotidianas da Administração.

As diretrizes de governança atuais -, de um governo aberto, democrático e transparente - também podem ser dificultosas. No caso da disponibilização de dados, a transparência e o grau de publicidade estão relacionados ao nível de agregação e à verificação da sensibilidade de determinadas informações no caso concreto. Esse fato também tem relação com o orçamento disponibilizado para a área de Tecnologia da Informação e Comunicação (TIC) quanto às questões de segurança da informação, aquisição de softwares para criptografia e anonimização, estruturação dos bancos de dados, equipe própria destinada a realizar essas ações, entre outros. Assim,

---

51 Ibidem, p. 127.

52 Sublinha-se, nesse momento, que a norma atual que trata da legística propugna a reunião das leis federais com matérias conexas ou afins em codificações e consolidações em um único diploma legal, "com a revogação formal das leis incorporadas à consolidação e sem modificação do alcance nem interrupção da força normativa dos dispositivos consolidados" (art. 45, caput e p. ún., do Decreto nº 9.191/2017), o que seria de grande valia no que tange às diversas normas que tratam da proteção de dados.

53 Da Constituição Federal:
Art 5º, inc. X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.
Art. 5º, inc. XII: é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.
Art. 37: A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência.

> o governo transparente não é tão simples como parece à primeira vista. A possibilidade de reorganizar os dados por meio de processos novos e melhores, abrindo repositórios de dados governamentais para os cidadãos, de forma acessível, organizada e neutra, sem afetar a privacidade de informações ou exposição de dados sensíveis que podem prejudicar a função do Estado torna-se uma tarefa titânica.[54]

Importante destacar, também, que, no caso dos direitos à privacidade e à publicidade, alguns defendem ser "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"[55]. Nesse sentido, pode-se entender que, havendo outros mecanismos para prover o acesso à informação ou o tratamento de dados, não haveria que se falar em divulgação das informações pessoais sob o manto do interesse público.

Observa-se, por outro lado, que dados indiscutivelmente pessoais, como nome e remuneração dos servidores públicos, tiveram sua publicação autorizada em sítios institucionais, tendo sido priorizado o acesso à informação em detrimento à privacidade[56]. Foi o caso do entendimento do STF no tema de Repercussão Geral nº 483: "É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias". Destaca-se trecho do voto do ministro Carlos Ayres Britto na ocasião:

> 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**

---

[54] SANDOVAL-ALMAZÁN, Rodrigo. Open government and transparency: building a conceptual framework. **Convergencia Revista de Ciencias Sociales,** México, v. 68, p.1-24, mai/ago. 2015. Disponível em: < http://convergencia.uaemex.mx/article/viewFile/3660/2613>. Acesso em: 12 nov. 2016.

[55] VIEIRA, Sônia Aguiar do Amaral. **Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos.** São Paulo: Editora Juarez de Oliveira, 2002, p. 28.

[56] Importante lembrar, nesse momento, que o próprio conceito de privacidade ganha contornos diferentes a depender da situação e do contexto em que está inserido. Danilo Doneda, por exemplo, destaca diferenças nas concepções de privacidade adotadas pela common law e pela *civil law.* Apesar de observar que há uma tendência em se uniformizar a noção de privacidade, buscando ao menos um conteúdo mínimo, afirma que "privacidade é um termo que se presta a uma certa manipulação pelo próprio ordenamento – pois não raro ela é utilizada para suprir necessidades estruturais dele próprio, assumindo determinado sentido em função de determinadas características de um ordenamento e dificultando ainda mais a sua redução a um sentido comum". Por outro lado, em sua visão, essa indefinição não é um defeito ou obstáculo, mas uma característica intrínseca da matéria (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 64/66.)

> **a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor**. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. (ARE 652777/SP, 2015, p.9, grifo nosso)

Desse trecho, existe apenas uma sinalização da Suprema Corte de que as informações como CPF, RG, endereço, etc., são dados pessoais que devem ser preservados 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. O nome do indivíduo, por outro lado, mesmo que junto ao órgão em que trabalha (seu domicílio profissional) e à sua remuneração, não seria considerado sensível, pois, nesse caso, entendeu-se a transparência e a publicidade como preponderantes.

O tema voltou ao Supremo, em 2018, com o pedido da Associação dos Juízes Federais do Rio de Janeiro e Espírito Santo (Ajuferjes), por meio da Ação Ordinária nº 2.367, para desobrigar o Tribunal Regional Federal da 2ª Região de observar a Resolução nº 215/2015 do Conselho Nacional de Justiça que determina a divulgação da remuneração e proventos dos membros, servidores e colaboradores do Poder Judiciário. Segundo o pedido, além de extrapolar o poder regulamentar, a divulgação dos nomes e salários desses indivíduos violaria sua privacidade e intimidade, bem como afrontaria o princípio da proporcionalidade.

O ministro Luís Roberto Barroso, no entanto, rejeitou o agravo interposto contra a decisão do então ministro relator Joaquim Barbosa. Ratificando os entendimentos anteriores, Barroso afirmou que o tema já havia sido objeto do tema 483 da Repercussão Geral e o entendimento fixado é no sentido de que é legítima a publicação dos nomes, vencimentos e locais de lotação dos agentes remunerados pelo Poder Público.

> Ementa: DIREITO CONSTITUCIONAL. RESOLUÇÕES N.ºs 151/2012 e 215/2015, DO CONSELHO NACIONAL DE JUSTIÇA. DIVULGAÇÃO DE REMUNERAÇÃO. 1. **Não há violação à intimidade ou à vida privada na divulgação nominal e pormenorizada da remuneração de magistrados, pois os dados são de interesse público e a transparência se impõe.** Precedentes. 2. A jurisprudência do STF entende prevalecer, no caso, o **princípio da publicidade administrativa**, que concretiza a República como forma de governo. 3. Pedido julgado improcedente. (…) 14. No mérito, destaco que a jurisprudência desta Corte firmou-se no sentido de que, sendo o agente remunerado pelo Poder Público, seus vencimentos, acompanhados de nome e de lotação, representam **informação de caráter estatal**, decorrente da natureza pública do cargo: (…) 15. Portanto, não havendo violação à intimidade e à vida privada, não

> existe conflito de normas, nem desrespeito ao princípio da legalidade. (…)18. Não há dúvidas de que o entendimento reiterado do STF se aplica aos magistrados federais, seja porque são agentes públicos, seja porque as informações são de interesse coletivo e geral, o que atrai a aplicação da regra do art. 5º, XXXIII, da CF, sem que a eles se aplique a exceção prevista na parte final do mesmo dispositivo ("todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado"). 19. Os atos do Conselho Nacional de Justiça não apenas densificam a interpretação constitucional conferida pelo Supremo Tribunal Federal, como promovem a transparência. Como venho afirmando nesta Corte, **a transparência se impõe porque decorre (i) do princípio democrático (CF/1988, art. 1º, caput), (ii) do sistema representativo (CF/1988, art. 1º, parágrafo único), (iii) do regime republicano (CF/1988, art. 1º,caput), e (iv) do princípio da publicidade (CF/1988, art 37, caput).** Ao especificar o conteúdo desses princípios no exercício de suas competências constitucionais, **o ato do CNJ não exorbita do poder regulamentar, mas antes confere efetividade ao disposto na Constituição Federal**. 20. Por todo o exposto, julgo improcedente o pedido formulado na inicial, e prejudicado o agravo interno interposto, declarando legítima a determinação do Conselho Nacional de Justiça de que devem ser publicados nos sítios eletrônicos do Poder Judiciário a remuneração e proventos percebidos por todos os membros e servidores ativos, inativos, pensionistas e colaboradores do órgão, incluindo-se as indenizações e outros valores pagos a qualquer título, bem como os descontos legais, **com identificação individualizada e nominal do beneficiário e da unidade na qual efetivamente presta serviços, com detalhamento individual de cada uma das verbas pagas** sob as rubricas 'Remuneração Paradigma', 'Vantagens Pessoais', 'Indenizações', 'Vantagens Eventuais' e 'Gratificações', conforme quadro descrito no anexo da Resolução CNJ n.º 215/2015. 21. Sem custas. Fixo os honorários em R$ 5.000,00 (cinco mil reais), na forma do art. 85, §8º, do CPC. Publique-se. Intimem-se. Brasília, 23 de agosto de 2018. Ministro Luís Roberto Barroso Relator (AO 2367, Relator(a): Min. ROBERTO BARROSO, julgado em 13/03/2017, publicado em PROCESSO ELETRÔNICO DJe-176 DIVULG 27/08/2018 PUBLIC 28/08/2018, grifo nosso)

Interessante realçar que, para Barroso, no caso em apreço, como inexiste violação à intimidade e à vida privada, não há, também, que se falar em conflito de normas. A União, em sede de contestação também afirmou que a pretensão da Associação "acaba, em verdade, por impedir a concretização de importante política pública de sede constitucional, que objetiva dar efetiva publicidade aos gastos públicos do Poder Judiciário".

A transparência ativa almejada pela Lei de Acesso à Informação e promovida pelos dispositivos da Resolução do CNJ, pode-se dizer, seria fruto do caráter estatal dessas informações, de interesse coletivo e geral, decorrentes da natureza pública dos cargos ocupados. E, da mesma forma que o entendimento foi fixado para a APF, também é válido para os agentes públicos do Poder Judiciário.

Apesar de a Associação ter solicitado que a divulgação dos salários fosse feita apenas com a matrícula do servidor, sem a revelação do nome e local de sua atuação, "evitando-se, assim, a desnecessária personificação e individualização de dados que integram a intimidade de cada pessoa", Barroso entendeu que o princípio da publicidade administrativa e a transparência se impunham. Nessa perspectiva, também, a ressalva constante do art. 5º, inc. XXXIII, da CF88, que prevê a possibilidade de sigilo quando imprescindível à segurança da sociedade e do Estado, foi afastada.

Para o ministro, os atos do CNJ, além de densificarem a interpretação constitucional conferida pelo STF em decisões anteriores, encorajam a publicidade e a transparência, dando efetividade e concretude aos princípios da CF88.

Nesse contexto, apesar de ser possível observar a dificuldade e as diferenças de entendimento diante da linguagem aberta das normas, essa flexibilidade também se faz real diante da necessidade de elas serem elaboradas com fins prospectivos, diferentemente das regras que, normalmente, são criadas a partir de um fato pretérito. Ocorre que, também em decorrência disso, várias situações, como a apresentada, deverão continuar sendo decididas casuísticamente, já que atualmente a LAI apenas define informação pessoal como aquela relacionada à pessoa natural identificada ou identificável (art. 4º, inc. IV), e a LGPD, quando entrar em vigor, confere diversas exceções ao Poder Público, sendo difícil, por exemplo, definir o conteúdo de informações sensíveis já que estas dependem de seu contexto e da interrelação com outras variáveis.

1.3 A utilização de novas tecnologias nos serviços públicos e as vulnerabilidades delas resultantes

O aumento vertiginoso das novas tecnologias e da coleta, armazenamento, processamento e utilização de dados na internet, no Brasil e no mundo, impacta as relações comerciais, econômicas e de confiança entre o Estado e a sociedade; entre a sociedade e as entidades privadas; entre as entidades privadas e o Estado; e entre os órgãos do próprio Estado. Vazamento de dados pessoais, comercialização, cruzamento

de dados com objetivos preditivos ou de perfilagem comportamental direcionando as políticas ou opiniões públicas são algumas das vulnerabilidades resultantes desse processo.

Sem a pretensão de profetizar, o historiador Harari, baseado em experiências e fatos já ocorridos no mundo, lança questionamentos importantes relacionados à ética no uso da tecnologia e, especialmente, dos dados pessoais e sensíveis – frequentemente considerados o novo petróleo da internet e a nova moeda do mundo digital[57] - para a humanidade. Segundo ele, a tecnologia do século XXI é capaz de capacitar os algoritmos externos a serem "*hackers da humanidade*". Tais algoritmos seriam mais especialistas no conhecimento de um indivíduo do que ele próprio, transferindo a crença no individualismo para os algoritmos em rede.

As pessoas, com isso, passariam a ter suas vidas constantemente monitoradas e guiadas por uma rede de algoritmos eletrônicos criados para, em tese, proporcionar uma experiência ou qualidade de vida melhor[58]. "Para que isso se concretize, não há necessidade de um algoritmo externo que me conheça perfeitamente e que nunca cometa nenhum erro; basta que esse algoritmo me conheça melhor do que eu me conheço e que cometa menos erros do que eu. Então fará sentido confiar a eles cada vez mais decisões e escolhas na vida".[59]

Ao falar sobre a corrente filosófica denominada dataísmo, que utiliza basicamente a ciência da computação e a biologia, e necessita do compartilhamento e conexão das experiências, o autor novamente traz reflexões importantes:

> o dataísmo inverte a pirâmide tradicional do aprendizado. Até então, os dados eram considerados apenas o primeiro passo na longa cadeia de atividade intelectual. Supunha-se que os humanos refinassem dados em informação, informação em conhecimento e conhecimento em sabedoria. Os dataístas, contudo, acreditam que os humanos não são mais capazes de lidar com os enormes fluxos de dados, ou seja, não conseguem mais refiná-los para obter informação, muito menos para obter conhecimento ou sabedoria. O trabalho de processamento de dados deveria, portanto, ser confiado a algoritmos

---

[57] KUNEVA, Meglena. European Consumer Commissioner, '**Keynote Speech**: Roundtable on Online Data Collection, Targeting and Profiling' (Brussels, 2009) <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> Acesso em 25 mai. 2018.

[58] Destaca-se aqui, também, a visão de Rouvroy, ao falar sobre a evolução, em tempo real, das redes de dados para elaborar perfis, padrões, etc., que acaba gerando uma crise de representação ou, até mesmo, uma crise da capacidade crítica dos indivíduos. (ROUVROY, Antoinette; STIEGLER, Bernard. **Le régime de vérité numérique:** De la gouvernementalité algorithmique à un nouvel État de droit. Socio, 4, 2015, p. 113-140. Disponível em: <http://journals.openedition.org/socio/1251>. Acesso em: 05 set. 2018.

[59] HARARI, Yuval Noah. **Homo Deus: Uma breve história do amanhã**. São Paulo: Companhia das Letras, 2016, p. 288.

> eletrônicos, cuja capacidade excede muito a do cérebro humano. Na prática, os dataístas são céticos no que diz respeito ao conhecimento e à sabedoria humanos e preferem depositar sua confiança em megadados e em algoritmos computacionais[60].

O autor aborda, em outras palavras, a questão dos cruzamentos de dados com objetivos de perfilagem comportamental dos indivíduos (*profiling*) na era da Big Data. Esta, é reconhecida, essencialmente, pela existência de três elementos (os chamados 3Vs): volume, velocidade e variedade.

Em termos de volume, são considerados tanto os dados estruturados quanto não-estruturados, gerando uma extensa quantidade. Quanto à velocidade, considera-se a agilidade de processamento possibilitada pelas novas técnicas e tecnologias. Por último, a variedade refere-se às inúmeras fontes de dados disponíveis, seja em termos de formato, de mídias, etc. Juntos, esses três elementos "permitem a utilização de sistemas automatizados para buscar correlações entre dados distintos a fim de estabelecer sistemas preditivos"[61].

Há autores que falam, ainda, no 4º e no 5º "Vs", que seriam a veracidade e o valor dos dados. A veracidade diz respeito à qualidade e à confiabilidade dos dados. E o valor significa que a imensa gama de dados só faz sentido se for capaz de agregar algum tipo de valor aos gestores e às organizações. Percebe-se, assim, que, na Big Data, a diferença não é o volume acumulado de dados e informações, mas o processamento, a análise e o uso que se pode fazer a partir deles para a tomada de decisão.

Essa problemática já se tornou realidade no mundo contemporâneo e a sua utilização pelo Governo suscita ainda mais receio por parte de algumas pessoas, já que associada à vigilância em massa e ao controle do cidadão[62]. Hoje, o Poder Público é considerado o maior detentor de dados e informações dos cidadãos. São dados provenientes de controles de acesso aos órgãos e departamentos públicos, câmeras em rodovias e vias

---

60 Ibid, p. 322.

61 OLIVEIRA, Carlos Eduardo Goettenauer de. **Credit scoring e big data no regime jurídico brasileiro**. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gama Prata de. (Coord.) Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240.

62 Exemplos de questionamentos suscitados pelo diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-RIO), Carlos Affonso Souza: "Há desafios muito relevantes a serem trabalhados em relação à legislação de privacidade de dados, principalmente quando o próprio poder público não parece dar muita atenção à questão. Temos o CPF na nota. Qual o interesse do Estado em saber o que e quando você compra? O que ele faz com os dados coletados a partir disso? O mesmo acontece com as informações fornecidas para utilização do bilhete único de transporte ou o WiFi público - exemplifica". (ver: Brasil é o país mais vunerável a vazamento de informações, diz pesquisador. **AGÊNCIA O GLOBO**. Disponível em: <http://revistapegn.globo.com/Tecnologia/noticia/2017/09/brasil-e-o-pais-mais-vulneravel-vazamento-de-informacoes-diz-pesquisador.html . Acesso em: 10 jan. 2018.)

de circulação, uso da biometria e de reconhecimento facial para identificação, bases de dados cadastrais como a do Sistema Único de Saúde (SUS), dos Censos Demográficos e Educacionais, de Programas de Assistência Social, como Bolsa Família, entre outros.

Assim, além da falta de confiança nas instituições públicas – que, segundo o estudo global Edelman Trust Barometer 2018[63] é de 82% no caso brasileiro, ou seja, apenas 18% das pessoas acreditam no Governo no país -, as pessoas temem que seus dados parem nas mãos de terceiros não autorizados e sejam utilizados para fins não legítimos. Isso pode ocorrer, por exemplo, em razão de falhas na segurança das redes e sistemas dos órgãos e entidades do Poder Público[64]. São os casos, por exemplo, de hackeamentos, vazamentos ou comercialização de dados pessoais, os quais podem degradar a imagem e reputação de determinado indivíduo, provocando danos irreparáveis, atentando contra a dignidade humana.

Há de se mencionar, igualmente, a possibilidade de haver a chamada "discriminação estatística" na elaboração de ações afirmativas pelo Governo. Com isso, alguns grupos receberiam tratamentos diferenciados em razão de determinados atributos, podendo gerar riscos de discriminação e estigmatização unicamente em razão de um resultado probabilístico. "O principal problema da discriminação estatística é a atribuição de uma suposta característica do grupo ao indivíduo, sem levar em conta as suas características e condições individuais."[65].

E mais: "é problemático, contudo, acreditar que os resultados desse processamento de dados sejam "verdades matemáticas" – embora sejam derivados do uso da matemática. Os algoritmos de computador não são neutros – possuem erros, vieses e interesses políticos e econômicos –, de modo que o conhecimento derivado desses mecanismos deve ser sempre questionado". Isso porque podem possuir "consequências nefastas para os direitos humanos", de forma que "os juristas e os responsáveis pela elaboração

---

63 EDELMAN. **2018 Edelman Trust Barometer: Global Report**. Disponível em: <https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf>. Acesso em 07 ago. 2018, p. 41.

64 Atualmente, surgiram notícias de que informações pessoais de servidores públicos (contracheques, CPF e comprovantes de residência, por exemplo) eram acessadas por terceiros para fraudar empréstimos de até R$500 mil. Para isso, utilizavam dados do Sistema de Gestão de Pessoas (Sigepe), administrado pelo atual Ministério da Economia (antigo MPDG). A investigação está em curso pela Polícia Civil do Distrito Federal. (MARQUES, Marília. Grupo fraudava empréstimos de até R$ 500 mil com dados de servidores federais no DF; três foram presos. G1, Brasília, 09 jan. 2019. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2019/01/09/grupo-fraudava-emprestimos-de-ate-r-500-mil-com-dados-de-servidores-federais-no-df-tres-foram-presos.ghtml> . Acesso em 25 fev. 2019.)

65 MENDES, Laura Schertell. **A Tutela da Privacidade do Consumidor na Internet:** Uma Análise à Luz do Marco Civil da Internet e do Código de Defesa do Consumidor. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coordenadores). Direito & Internet III – Tomo I: Marco Civil da Internet (Lei 12.965/2014). São Paulo: Quartier Latin do Brasil, 2015, p. 36.

de políticas precisam compreender essas ferramentas pelo que elas realmente são: simulações"[66].

Na era digital, as possibilidades e potenciais de utilização do Big Data pelo setor público carregam, também, outras questões éticas que devem ser observadas. Nesse caso, a privacidade *versus* o interesse público. Em termos de privacidade, a edição do Decreto nº 8.789/16, que dispõe sobre o compartilhamento de bases de dados entre órgãos e entidades federais, dispensando a necessidade de assinatura de convênios ou acordos de cooperação, gerou algumas polêmicas. Ao mesmo tempo em que facilita a exploração das oportunidades do Big Data, segundo alguns, o normativo não impõe limites expressos à extensão do cruzamento de dados.

> O que acontece se informações pessoais que podem prejudicar ou causar discriminação (como de saúde ou previdência social) acabarem em bases de dados consultáveis por entes privados (como seguradoras)? Lembrando do polêmico caso em que o Tribunal Superior Eleitoral (TSE) permitiu que o Serasa tivesse acesso a sua base de dados[67], não dá para dizer que essa seja uma hipótese absurda. Se ela tivesse sido turbinada com outras informações, as consequências seriam ainda mais graves. O que dizer, também, de órgãos de investigação (como a Polícia Federal) criando perfis de "potenciais criminosos"[68] a partir do cruzamento de dados sobre a saúde do indivíduo fornecidos pelo Ministério das Saúde, dados sobre escolaridade pelo Ministério da Educação e dados socioeconômicos pelos Ministérios das Cidades e do Desenvolvimento Social, por exemplo? Considerando o policiamento preditivo à base de big data que começa a ser implementado ao redor do mundo, não se pode descartar o seu uso aqui. A Polícia Federal já tem histórico de cruzar dados para otimizar o controle das alfândegas[69].

---

66 DE MENEZES NETO, Elias Jacob; DE MORAIS, Jose Luis Bolzan. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. Novos Estudos Jurídicos, [S.I], v. 23, n.3, p. 1129-1154, dez. 2018. ISSN 2175-0491. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/13769>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.14210/nej.v23n3.p1129-1154. p. 1141; 1146.

67 TSE firma acordo para repassar dados de eleitores à Serasa. *G1,* Brasília, 07 ago. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/08/tse-firma-acordo-para-repassar-dados-de-eleitores-serasa.html>. Acesso em: 20 jul. 2018. OBS: Devido à grande repercussão, o acordo foi suspenso em menos de um mês.

68 A Lei nº 12.654, de 28 de maio de 2012, por exemplo, prevê a coleta de dados de perfil genético como forma de identificação criminal de condenados por crimes violentos ou hediondos a serem armazenados em banco sigiloso gerenciado por unidade oficial de perícia criminal. [OBS: "Possui repercussão geral a controvérsia relativa ao exame da constitucionalidade, à luz de direitos da personalidade e do princípio da não autoincriminação, do art. 9-A da Lei de Execução Penal (Lei nº 7.210/1984), introduzido pela Lei nº 12.654/2012, que prevê a identificação e o armazenamento de perfis genéticos de condenados por crimes violentos ou por crimes hediondos". RE 973.837 RG/MG, rel. min. Gilmar Mendes].

69 ABREU, Jacqueline de Souza. **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016>. Acesso em: 10 jan. 2018.

Além desses questionamentos, seria possível citar inúmeros outros casos de uso indevido de banco de dados públicos por seus agentes, mas que não chegam a reverberar tanto quanto os citados[70]. Como afirma Doneda, "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". Mais que isso, segundo ele, "os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados não sensíveis"[71], ou seja, eles também merecem proteção, só que num nível inferior.

Observa-se, assim, que as indagações suscitadas são pertinentes e devem ser levadas em consideração no momento da formulação de políticas públicas. Não se trata, entretanto, de restringir o fluxo de informações. É preciso, na verdade, que a regulamentação seja clara e explícita quanto à garantia do uso ético dos dados, informações e ferramentas tecnológicas, de forma a não gerar disfuncionalidades. E mais: de forma a garantir o regime democrático, a cidadania e a proteção dos direitos humanos, é essencial que os cidadãos conheçam o propósito, o uso e a destinação dos dados fornecidos ao governo para poder debater e participar das decisões quanto à sua melhor utilização, e, finalmente, proteger-se contra eventuais abusos.

Para isso, é preciso dar concretude aos princípios constitucionais abertos e analisar mecanismos de proteção mais efetivos, como o consentimento informado - inclusive considerados por alguns como utópicos -, o princípio da finalidade e a vasta gama de exceções previstas para o setor público, o que será mais especificamente discutido no Capítulo 3.

1.4 A interdisciplinaridade como possível entrave aos operadores jurídicos e aos gestores públicos

Além da vagueza conceitual das normas, deixando um amplo leque de interpretação para os administradores públicos, bem como aos operadores do Direito (como explicado nos itens anteriores), a interpretação das normas e a definição do seu alcance, no

[70] Ver exemplos de artigos e notícias que tratam do tema e foram veiculados em diferentes meios de comunicação: https://www.conjur.com.br/2012-nov-07/policial-civil-condenado-uso-indevido-sistema-dados; https://canalcienciascriminais.com.br/poder-publico-tecnologia-e-crimes/; http://g1.globo.com/jornal-nacional/noticia/2017/08/dados-sigilosos-sao-vendidos-para-bancos-financeiras-e-ate-advogados.html

[71] 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, p. 191.

caso da proteção de dados, também perpassa a necessidade do domínio ou, ao menos o aprendizado, de outras áreas do conhecimento, como a Ciência da Informação e, especialmente, a Tecnologia da Informação e da Comunicação (TIC).

Há, nessa realidade, um conflito entre as características do Direito e da elaboração normativa e as características da tecnologia. Como se sabe, o Direito é considerado, por excelência, moroso e conservador; suas normas jurídicas passam por ritos solenes e evoluem lenta e gradualmente, de modo que, em geral, não conseguem acompanhar as mudanças e a evolução da sociedade, inclusive, em razão dos intensos e vertiginosos avanços tecnológicos e dos movimentos de globalização.

A linguagem e a complexidade técnicas próprias da tecnologia, com algoritmos e códigos que só os programadores são capazes de decifrar[72], envolvem questões de segurança da informação em nível transnacional e inovações que os operadores jurídicos não conseguem acompanhar ou entender. Seus mecanismos de processamento, como nas tecnologias utilizadas para o *e-commerce*, gestão de patentes e direitos autorais na internet, serviços de *streaming*, além das chamadas tecnologias disruptivas (ex: Internet das Coisas, *blockchain*, *cloud computing*, realidade aumentada, impressão 3D, inteligência artificial, drones, etc.), são exemplos dessas dificuldades.

Assim, a regulação da tecnologia acaba sendo demasiadamente complexa, pois é necessário conseguir decodificar esse linguajar próprio para o Direito e para os gestores públicos, de forma a conseguir alcançar a interlocução entre essas duas áreas. No caso das discussões acerca da proteção de dados pessoais e sensíveis, termos como anonimização, criptografia, cifração, engenharia reversa, nível de agregação, modelos estatísticos, classificação dos dados, avaliação de *inputs* e *outputs* são utilizados cotidianamente.

Alerta importante faz Faria ao tratar da tendência do Direito de alargamento e desformalização nos tradicionais procedimentos de elaboração legislativa, especialmente em relação a questões de caráter mais técnico e interdisciplinar (como é o caso da temática "proteção aos dados pessoais"). De acordo com o autor, isso se dá em razão da complexidade e dos riscos inerentes às matérias em discussão, o que leva, cada vez mais, os poderes Executivo e Legislativo a procurarem:

> dividir ou partilhar essa responsabilidade, por meio de

[72] Ver o caso do whatsapp (ADPF 403/SE, de 03/05/2016), em que uma das principais discussões no Judiciário dizia respeito à possiblidade técnica ou não de interceptação e quebra do sigilo de conversas realizadas por meio do aplicativo diante de requisições judiciais (argumento: utilização da criptografia ponta a ponta – *end to end* - utilizado na troca das mensagens).

> sistemas de consultas públicas, painéis de discussão, entendimento com setores sociais interessados, colaboração com comunidades profissionais estruturadas, assessoria de centros de pesquisa, diálogo com instituições universitárias de elite e pedidos de relatórios técnicos e pareceres a cientistas, peritos e especialistas das mais diferentes áreas do conhecimento – enfim, o que os analistas de viés funcionalista chamam de 'comunidades epistêmicas[73].

Porém, como todo modelo tem aspectos positivos e negativos, realça que, apesar de possibilitar um regime mais democrático devido à inserção e à participação da comunidade e dos especialistas da respectiva área do conhecimento nas tomadas de decisão, pode, também, encerrar:

> o risco de sua "captura" pelos setores sociais, econômicos e políticos interessados, que tendem a dispor de amplo controle da produção e circulação das informações específicas às suas respectivas áreas e campos de atuação, podendo assim resultar no retorno a velhas práticas decisórias de natureza corporativista ou, então, numa autoprodução do direito em circuito fechado e imune a controles externos[74].

Conclui-se, assim, que o tema é complexo e exige dos operadores do Direito uma formação além de meramente normativa. Para esse desafio específico, diante dos problemas da sociedade da informação, contemporânea, há a necessidade de uma reformulação radical da forma como as instituições jurídicas e judiciais do Estado-nação estão estruturados de forma a poder oferecer oportunas "respostas nacionais para questões de alcance global e conseguir neutralizar e/ou enfrentar esses problemas com um mínimo de efetividade"[75].

---

73 FARIA, José Eduardo. **Sociologia Jurídica:** direito e conjuntura. 2 ed. São Paulo: Saraiva, 2010, p. 65/66.

74 Ibidem, p. 67.

75 FARIA, José Eduardo. op. cit., p. 27.

2 Os principais modelos de gestão de dados pessoais e sensíveis utilizados pela administração pública e suas principais complexidades

O Poder Público, e em especial o Poder Executivo, tem papel central na definição dos programas que serão implementados para garantir o exercício pleno da cidadania[76], sem qualquer tipo de discriminação, buscando a concretização dos direitos fundamentais e promovendo ações com a maior eficácia e efetividade possíveis. Os desafios para dar concretude aos ideais democráticos e, por consequência, à cidadania e à proteção dos direitos humanos, entretanto, são grandes e dependem do modelo a ser adotado para a gestão de dados.

Nesse contexto, a administração pública gerencial, em oposição ao caráter auto-referido do modelo burocrático, passou a utilizar os preceitos do modelo *citizens center design* (serviços centrados no cidadão[77]), que significa pensar os processos pela visão do cidadão, preocupando-se com a qualidade e a excelência na prestação dos serviços públicos, permanecendo aberta à participação do cidadão, orientada para ele e permitindo o controle social da gestão. Como afirma Bresser Pereira, "o cidadão-cliente é um cidadão-cidadão, um cidadão pleno, que é o objeto dos serviços públicos e também seu sujeito, na medida em que se torna partícipe na formação das políticas públicas e na avaliação dos resultados"[78].

A abordagem voltada para o cidadão iniciou-se nos anos 80 em países da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) e se estendeu aos

[76] Relevante destacar as divergências em relação ao conceito de cidadania e, consequentemente, de cidadão apontadas pelo jurista Dalmo de Abreu Dallari já em 1984, ou seja, momentos antes do início do processo de democratização no país. Com grande acuidade, ele preferia utilizar o termo pessoa humana a cidadão, já que "este é criação da vontade do Estado e pode ser facilmente reduzido em sua medida e sua importância", se utilizado numa concepção mais restritiva (ver: DALLARI, Dalmo de Abreu. **Ser cidadão**. Revista Lua Nova, São Paulo, vol.1, n.2, p.61-64, jul/set 1984.). Assim, não se adentrará, no presente trabalho, nas discussões acerca desse conceito, optando apenas por ater-se ao seu sentido mais amplo, sendo cidadão o sujeito detentor de direitos e deveres civis, políticos e sociais, expressando a igualdade dos indíviduos perante a lei e pertencendo a uma sociedade democrática e organizada, que é, na essência, o foco do modelo dos serviços centrados no cidadão.

[77] Sobre o assunto, ver histórico da Administração Pública voltada para o cidadão e o seu desenvolvimento conceitual em: COUTINHO, Marcelo James Vasconcelos. Administração pública voltada para o cidadão: quadro teórico-conceitual. **Revista do Serviço Público,** Brasília, Ano 51, n. 3, p.40-73, jul/set 2000. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/331/337>. Acesso em: 10 jan. 2018.

[78] BRESSER PEREIRA, Luiz Carlos. (1998), **Reforma do Estado para a Cidadania**: A Reforma Gerencial Brasileira na Perspectiva Internacional. Brasília: ENAP; São Paulo: Editora 34, p. 118.

Estados Unidos e ao Brasil na década seguinte. Ela teve início, em grande medida, em função da crise do atendimento aos cidadãos pelo setor público e passou a buscar o prevalecimento do diálogo, da transparência e do engajamento.

A mudança na forma de pensar a Administração Pública foi beneficiada pelo avanço nas TICs. Com a modernização, diversas iniciativas têm sido buscadas a fim de aprimorar os serviços públicos e dar concretude aos direitos humanos, entre elas a simplificação do atendimento ao público, a possibilidade de participação de elaboração de projetos de leis ou de programas de governo por meio de redes sociais, o compartilhamento de dados entre os órgãos da Administração para planejamento e execução de políticas públicas, a promoção dos dados abertos para facilitar o acesso, a transparência e o controle pelos cidadãos, entre outros. Todas elas, de alguma maneira, perpassam a gestão de dados.

Para viabilizar tais ações, algumas normas, como o decreto que trata da interoperabilidade de bases de dados, são editadas. Porém, elas costumam gerar amplos debates. 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[79].

---

[79] Sobre o assunto, ver a) o item 16 de CNSeg/ FENASEG (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.), 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 pg. 19 de BRASSCOM (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.), afirmando 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 citada (CRUZ, Francisco Brito; MARCHEZAN, Jonas Coelho. **InternetLab Reporta** – Consultas Públicas nº 05. InternetLab, 2015. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-05/>. Acesso em: 28 dez. 2017.): "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

Assim, mesmo diante da vastidão de recursos tecnológicos, não são muitos os casos elencados de utilização desse potencial pelo Poder Público. Há que se questionar, então, qual é o motivo disso acontecer: limitações técnicas, de pessoal, financeiras, legais? Receio das reações da sociedade, que tem medo de uma possível supervigilância ou que o governo trace perfis comportamentais para controle e punição?

Ademais, não se pode perder de vista as questões éticas que permeiam a utilização dessas novas tecnologias, como discutido no capítulo anterior. Publicidade, privacidade, segurança, consentimento, sigilo, igualdade, liberdade de expressão são termos que sempre deverão pautar as discussões e ações do Governo.

Por fim, é preciso mencionar que, caso seja observado algum descumprimento dos valores constitucionais pelo Poder Executivo, o papel do Judiciário não pode ser olvidado para fazer valer o mais "onivalente repositório de valores jurídico-democráticos"[80] e concretizar os Direitos Humanos: núcleo dos Direitos Fundamentais, centro da Democracia.

Assim, serão apresentados, de forma breve, os principais mecanismos de funcionamento da circulação de dados dentro do Governo Federal e as formas de fornecimento desses dados aos cidadãos. Para isso, a base da análise será a legislação vigente e os modelos de compartilhamento de dados existentes frente às dificuldades já mencionadas em relação ao possível uso discriminatório ou eventual falta de segurança quanto ao uso e à proteção dos dados.

2.1 A requisição e a disponibilização de dados pessoais e sensíveis via Sistema Eletrônico do Serviço de Informação ao Cidadão

Não há como negar que a LAI 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[81]. "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"[82].

desnecessidade do consentimento".

80 BRITTO, Carlos Ayres. **O humanismo como categoria constitucional**. Belo Horizonte: Fórum, 2012, p. 87.

81 SILVEIRA, Marco Antônio Karam. **Lei de Acesso a Informações Públicas (Lei nº 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, p. 31.

82 RODRIGUES, João Gaspar. **Publicidade, transparência e abertura na administração pública**. RDA: Revis-

Mendel, 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**"[83] (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[84].

Fato é que, no Brasil, antes da LAI, era difícil ao cidadão obter informações, inclusive pessoais[85], em órgãos públicos. Por esse motivo, para atender aos seus dispositivos, foi criado o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC), que consiste num sistema que permite que qualquer pessoa, física ou jurídica, encaminhe pedidos de acesso à informação para qualquer órgão, suas entidades vinculadas e empresas estatais da Administração Pública Federal[86], conhecendo as regras, trâmites e prazos que devem ser seguidos por ambas as partes.

O Ministério da Transparência e Controladoria-Geral da União (CGU)[87] é o órgão responsável por monitorar o cumprimento da Lei. Aos pedidos de acesso negados existe a possibilidade de recorrer em quatro instâncias: 1ª. À autoridade superior àquela que proferiu a decisão; 2ª. À autoridade máxima do órgão; 3ª. À Controladoria-Geral da União; 4ª. À Comissão Mista de Reavaliação de Informações (CMRI). Esta, é um órgão colegiado composto por nove órgãos (art. 46, Decreto no 7.724/2012), cujas atribuições também dizem respeito ao tratamento e à classificação de informações sigilosas.

---

ta de Direito Administrativo, Rio de Janeiro, v. 266, p.89-123, mai/ago 2014, p. 94.

83 MENDEL, Toby. **Liberdade de informação:** um estudo de direito comparado. Brasília: Unesco, 2009, p. 32.

84 Ibidem, p. 32.

85 Note-se a existência do instituto do Habeas Data, instituído pela Lei n. 9.507, de 12 de novembro de 1997, para obtenção de informações de interesse próprio em órgãos públicos. Ressalta-se, porém, que a ação somente poderá ser impetrada com a prévia negativa da autoridade administrativa.

86 Importante destacar que esse serviço, em nível estadual e municipal, deve possuir regulamentação própria, obedecidas as normas gerais estabelecidas na LAI (art. 45, Lei nº 12.527/2011)

87 Com a nova estrutura organizacional trazida pela Medida Provisória nº 870, de 1º de janeiro de 2019, o Ministério da Transparência e Controladoria-Geral da União foi transformado em Controladoria-Geral da União.

Nesse sentido, a entrada em vigor da LAI, em maio de 2012, permitiu positivar a demanda da sociedade por mais 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[88], de maio/2012 (período inicial disponível para realização da consulta e geração do Relatório) a julho/2018, a quantidade de pedidos realizados a todos os órgãos ou entidades da APF se aproxima dos 650 mil.

Entretanto, apesar de a 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",[89] 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 nº 12.527/2011" corresponde a, aproximadamente, 4,61% dos pedidos respondidos. Se for considerada apenas a quantidade de acessos negados, esses três argumentos representam 54,28% das respostas denegatórias dadas pela Administração, conforme se observa na Quadro 2.

Quadro 2 – Pedidos de acesso à informação feitos à Administração Pública Federal por meio do e-SIC (maio/2012 a julho/2018)

ANO	2012	2013	2014	2015	2016	2017	2018	TOTAL maio/2012-julho/2018
1. Quantidade de pedidos realizados	55.212	86.661	90.167	102.423	111.669	121.536	79.007	**646.675**
2. Quantidade de pedidos respondidos	55.162	86.573	89.987	101.940	111.631	121.324	72.825	**639.442**
3. Quantidade de pedidos negados	4.856	9.618	9.927	7.663	8.111	8.552	5.559	**54.286**
3.1. Razão da negativa: Dados pessoais	2.126	3.734	3.182	2.278	1.543	2.435	1.562	**16.860**
3.2. Razão da negativa: Informação sigilosa de acordo com legislação específica	627	1.435	1.186	1.128	1.236	1.678	838	**8.128**

[88] BRASIL. Ministério da Transparência e Controladoria-Geral da União. **E-SIC:** Relatório de pedidos de acesso à informação e solicitantes. Disponível em: <https://esic.cgu.gov.br/sistema/Relatorios/Anual/RelatorioAnualPedidos.aspx>. Acesso em: 09 ago. 2018.

[89] 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).

ANO	2012	2013	2014	2015	2016	2017	2018	TOTAL maio/2012-julho/2018
3.3. Razão da negativa: Informação sigilosa classificada conforme a Lei nº 12.527/2011	308	368	1.168	890	819	519	409	4.481

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>.

Observa-se, assim, que as demandas por informações pessoais e/ou sensíveis ainda sofre com a negativa da Administração. Acentua-se aqui as conclusões mencionadas por Kodama, quando do estudo sobre a proteção da honra em relação à divulgação de dados pessoais pelo governo por meio da LAI.

No trabalho, apresentado antes da edição da LGPD, demonstra-se que o desenvolvimento do sistema e-SIC durante a *vacatio legis* da LAI foi exíguo para a construção do sistema, exigindo que a motivação "dados pessoais" se referisse tanto à negativa total quanto parcial do pedido de informação com base no art. 31 da LAI, sendo esta uma "definição imprecisa"[90].

Além disso, a falta de um marco legal de proteção de dados pessoais e as lacunas deixadas pela LAI na definição de conceitos como "dados sensíveis" acabaram levando a soluções "bastante improvisadas"[91], exigindo, por exemplo, que a CGU construísse suas decisões com base em normas esparsas na tentativa de salvaguardar o direito à honra e à privacidade dos indivíduos e evitar a revelação de juízos de valores negativos dos titulares dos dados.

Nesses casos, apesar do cuidado desse órgão em não disseminar os nomes dos recorrentes, procedendo ao seu tarjamento, essa prática não foi seguida pelas decisões da CMRI quando da divulgação de suas decisões, expondo, de toda forma, o nome dos recorrentes. Espera-se que, com a LGPD, dificuldades interpretativas como essas sejam mitigadas, possibilitando soluções mais claras, concretas e garantindo maior segurança jurídica a partir da sua entrada em vigor.

Ainda, em relação à negativa de acesso à informação em razão de classificação conforme a LAI, vale destacar a polêmica criada com a edição do Decreto nº 9.690, de

[90] KODAMA, Roberto. **Tratamento dos dados pessoais no acesso a informações públicas: a honra relegada na sociedade da informação.** 2018. 224 f. Dissertação (Mestrado) - Curso de Direito, Uniceub, Brasília, 2018. p. 138.

[91] Ibidem, p. 140.

23 de janeiro de 2019, pelo governo recém-empossado. A nova regra alterou o decreto que regulamenta a LAI, ampliando o rol de autoridades que poderiam impor sigilo a dados e informações governamentais, nas classificações ultrassecreta e secreta.

Com o Decreto, as autoridades elencadas no art. 30 da LAI (presidente, vice-presidente, ministros de Estado e autoridades com as mesmas prerrogativas, comandantes das Forças Armadas e chefes de missões diplomáticas do Brasil) poderiam delegar competência para imposição da classificação ultrassecreta aos dados e documentos (por até 25 anos) a ocupantes de cargos em comissão do grupo de Direção e Assessoramento Superior - DAS de nível 101.6 ou superior, ou de hierarquia equivalente, e para os dirigentes máximos de autarquias, fundações, empresas públicas e sociedades de economia mista. "Estendia-se essa prerrogativa para quase 2 mil servidores, incluindo não concursados"[92].

Para classificação no grau secreto (por até 15 anos), o rol foi ampliado às mesmas autoridades anteriores, bem como aos ocupantes de cargos em comissão do Grupo DAS de nível 101.5 ou superior, ou de hierarquia equivalente.

Frisa-se que esses cargos podem ser ocupados por servidores públicos ou de livre nomeação e exoneração, o que poderia vir a facilitar uma possível retomada da cultura de sigilo. Diante disso, a medida adotada pelo governo foi considerada um retrocesso pelos defensores da ampla publicidade e transparência da APF[93]. O Congresso Nacional, por sua vez, chegou a apresentar o Projeto de Decreto Legislativo (PDL) nº 3/2019, que tinha por objetivo vedar a delegação de competência criada no decreto presidencial.

Consequentemente, diante das várias críticas – e apesar da justificativa do governo de se tratar da necessidade de um "balanceamento" entre a segurança e a transparência, além de diminuir a burocracia para acesso a documentos[94] -, a presidência voltou atrás e revogou esta parte do Decreto, repristinando a redação anterior (Decreto nº 9.716, de 26 de fevereiro de 2019). Com isso, o PDL também foi arquivado.

---

92 BRESCIANINI, Carlos Penna. **Com revogação de decreto, senadores arquivam projeto sobre sigilo de informações**. Senadonotícias, 27 fev. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/02/27/com-revogacao-de-decreto-senadores-arquivam-o-texto-que-anularia-mudanca-na-lei-de-acesso-a-informacao>. Acesso em 05 mar. 2019.

93 HESSEL, Rosana. **Governo altera Lei de Acesso à Informação e aumenta sigilo em dados.** Correio Braziliense, 24 jan. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/politica/2019/01/24/interna_politica,732627/governo-altera-lei-de-acesso-a-informacao-e-aumenta-sigilo-em-dados.shtml. Acesso em 25 fev. 2019.

94 URIBE, Gustavo. **Para Mourão, mudança de regra sobre sigilo de dados não afeta transparência.** Folha de S. Paulo, 24 jan. 2019. Disponível em: https://www1.folha.uol.com.br/poder/2019/01/para-mourao-mudanca-de-regra-sobre-sigilo-de-dados-nao-afeta-transparencia.shtml. Acesso em 25 fev. 2019.

2.2 O acesso aos dados pessoais e sensíveis por meio de ambientes denominados seguros para fins específicos de pesquisa

No contexto de disponibilização de dados e tendo a publicidade como regra e o sigilo como exceção, existe ainda outro meio de fornecimento de dados pessoais e sensíveis efetuado pela Administração Pública, dessa vez, para terceiros interessados. Trata-se da disponibilização de bancos de dados para fins de pesquisa.

Nesse caso, o propósito de publicidade, no dia a dia da Administração se torna ainda mais desafiador, pois associado, entre outros fatores, à preparação e integração das bases (com variáveis-chave comuns ou passíveis de cruzamento), à classificação dos dados segundo seu nível de agregação, à dificuldade de controle de avaliação de *outputs* das pesquisas de tal forma que não possa haver chance de revelações de informações pessoais ou sensíveis por posteriores cruzamentos, à tecnologia e segurança da informação, além da necessidade de planejamento, priorização do serviço e capacitação das equipes gestoras e das complexidades de interpretação da legislação decorrentes dos problemas conceituais já mencionados.

Apesar das dificuldades, algumas entidades da Administração têm buscado impulsionar a realização de pesquisas utilizando os dados por elas coletados, também por pesquisadores externos, com o objetivo de proporcionar maior transparência nos termos da Lei de Acesso à Informação e, consequentemente, visando à melhoria das políticas públicas.

Uma das formas vislumbradas pelas entidades para esse trabalho foi a disponibilização dos dados, ainda que pessoais ou sensíveis, em ambientes denominados seguros. Em âmbito nacional, esse tipo de serviço tem sido prestado por poucas entidades e com níveis diferenciados de segurança da informação. Destaca-se tal iniciativa no Instituto Brasileiro de Geografia e Estatística (IBGE), no Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) e no Instituto de Pesquisa Econômica Aplicada (Ipea) e trata-se do acesso a bancos de dados específicos para cruzar informações não disponíveis em microdados públicos[95].

[95] A coleta de dados da parte empírica foi feita ao longo do ano de 2016, tendo sido atualizada a parte do Inep em 2018, devido à mudança das regras de acesso ao ambiente seguro. 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 02/09/2015; Portaria Inep n. 467/2014 e 465/2017, 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.

Os maiores desafios na gestão desses serviços ocorrem pois eles permitem 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.

Como aspectos comuns aos modelos adotados nos três órgãos, 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.

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 e-SIC, ou seja, eles são caminhos indicados para o requisitante da informação. Nesses casos, considera-se, para efeito de estatística, que a resposta dada pela Administração atendeu plenamente ou parcialmente o pedido.

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 nº 12.527/2011", demonstrando que a prestação do serviço de acesso ao ambiente seguro, nesses casos, não é suficiente para atender tais demandas.

Quadro 3 – Pedidos de acesso à informação feitos ao IBGE, ao Ipea e ao Inep por meio do e-SIC (maio/2012 a julho/2018)

Entidade	IBGE	Ipea	Inep	Total maio/2012-julho/2018
1. Quantidade de pedidos realizados	5.803	605	13.554	19.962
2. Quantidade de pedidos respondidos	5.777	602	13.535	19.914
3. Quantidade de pedidos negados	167	7	749	923
3.1. Razão da negativa: Dados pessoais	18	0	43	61
3.2. Razão da negativa: Informação sigilosa de acordo com legislação específica	69	0	36	105
3.3. Razão da negativa: Informação sigilosa classificada conforme a Lei nº 12.527/2011	2	0	57	59

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>.

Em relação às diferenças percebidas nos serviços oferecidos, observa-se que, no IBGE[96], cujo serviço existe desde 2003, os dados são criptografados. Já no Ipea e no início da prestação do serviço no Inep[97] (ambos iniciaram essa atividade em 2014), os pesquisadores tinham acesso à base de dados "crua", ou seja, na íntegra, com todos os dados coletados identificados. As demais diferenças serão descritas nos itens a seguir.

2.2.1 IBGE: microdados criptografados

A sala de acesso a dados restritos do IBGE, desde 2003, quando foi inaugurada já demonstrava preocupação em proteger os dados pessoais e sigilosos coletados pela

[96] Vale ressaltar que a Lei nº 5.534, de 14 de novembro de 1968, garante que toda informação fornecida ao IBGE terá fins exclusivamente estatísticos e que o cidadão tem garantido o seu sigilo em decorrência disso. ("art. 1º, p.ún. As informações prestadas terão caráter sigiloso, serão usadas exclusivamente para fins estatísticos, e não poderão ser objeto de certidão, nem, em hipótese alguma, servirão de prova em processo administrativo, fiscal ou judicial, excetuado apenas, no que resultar de infração a dispositivos desta lei.")

[97] O Inep, por sua vez, não tem lei específica para respaldar o sigilo estatístico, como o IBGE. Destaca-se que o art. 62 da Lei nº 13.709/2018, inseriu a possibilidade de edição de regulamento específico para tratar do tema: "Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004. Porém, esse artigo foi revogado pela Medida Provisória nº 869/2018."

entidade, procedendo à sua criptografia. O serviço é cobrado, sendo contabilizado pela estimativa de tempo de processamento da máquina (tempo de uso da sala).

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[98].

Com maior experiência na prestação desse serviço, o IBGE, com o passar dos 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 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.

---

[98] 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.

Além disso, para que a área técnica avalie as informações produzidas, é exigido relatório do usuário, demonstrando todos os passos (procedimentos) realizados 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" (art. 31, § 3º, inc. II), 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.

2.2.2 Inep: bases íntegras e identificadas

O Serviço de Atendimento ao Pesquisador (SAP) teve seu início em setembro de 2014, com a Portaria Inep nº 467. Diferentemente do IBGE, o modelo outrora adotado previa a disponibilização das bases de dados no formato em que se apresentavam, sem transformações, ou seja, podiam ser acessadas, para fins institucionais e científicos, informações sigilosas ou pessoais, individualizadas, coletadas pelo Instituto, sem a devida anonimização.

Após discussões internas sobre segurança e proteção dos dados pessoais e sensíveis, em maio de 2017, o nome do serviço foi alterado para Serviço de Acesso a Dados Protegidos (Sedap), por meio da Portaria nº 465. Com isso, novos critérios foram estabelecidos e aprimorados.

Quando do SAP, o critério de vínculo do pesquisador a uma instituição de pesquisa utilizado pelo IBGE não era exigido. Assim, qualquer pessoa física ou jurídica poderia solicitar o acesso, bastando apresentar a documentação necessária e assinar os devidos termos de compromisso, tendo seu projeto avaliado, deferido ou não, pela área técnica. Com a nova Portaria, passou-se a exigir "documento emitido pela instituição de vínculo do pesquisador titular, atestando ciência quanto ao acesso a dados protegidos"[99].

Na norma do SAP também havia omissão quanto à possibilidade de uso de bases de dados externas. Porém, sua utilização era aceita. Com o Sedap, esse quesito foi

[99] BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Texeira. **Serviço de Acesso a Dados Protegidos - Sedap:** Solicitação de acesso. Disponível em: <http://portal.inep.gov.br/dados/sedap/solicitacao-de-acesso>. Acesso em: 01 ago. 2018.

aprimorado. Agora, é obrigatória a autorização de uso e certificação de conteúdo das bases externas, emitida pela instituição produtora dos dados. Além disso, o Inep pode indeferir seu uso caso vislumbre riscos relacionados à exposição indevida de dados pessoais ou quebra de sigilo. Esse aspecto é de grande relevância tendo em vista que, a depender da pesquisa 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; ou a do Cadastro Único para Programas Sociais, do Ministério do Desenvolvimento Social.

Observa-se que, no caso do SAP/Inep, como as informações coletadas eram disponibilizadas na íntegra a terceiros, ainda que em um ambiente seguro, havia certa fragilidade na segurança da informação. Nesse caso, como providência tomada, a nova Portaria do Sedap incluiu o seguinte dispositivo:

> as bases de dados a serem disponibilizadas pelo SEDAP serão aquelas produzidas pelas áreas técnicas do INEP e disponibilizadas pela DTDIE na Sala de Acesso a Dados Protegidos (SADAP) **a partir de tratamento para proteção de informações pessoais** nos termos da Lei nº 12.527 e conforme a finalidade e destinação aprovada por esse serviço (art. 5º , Portaria nº 465/2017, grifo nosso).

Com isso, apesar da análise dos novos pedidos submetidos, o acesso às bases de dados ficou temporariamente suspenso por ausência do mascaramento dos dados pessoais e/ou sensíveis. Acresceu-se a isso, a previsão de publicação de um Guia do Usuário para o Sedap, "estabelecendo procedimentos, requisitos, documentos, prazos e orientações necessárias para a produção de dados gerados a partir de informações pessoais coletadas no âmbito do INEP" (art. 4º, Portaria 465/2017).

Em 28 de janeiro de 2019, a Portaria Inep nº 52 revogou a de nº 465/2017 e passou a disciplinar o acesso às bases de dados protegidos no âmbito do Instituto. A partir dela, e com o mascaramento concluído de algumas bases (Censo Escolar, Censo da Educação Superior, Enem e Prova Brasil), o serviço foi retomado.

O Guia[100], por sua vez, também foi publicado e atualizado com as novas regras de utilização do Sedap. Diferentemente do procedimento anterior, a partir da nova norma, as atividades de triagem, análise e acompanhamento do processo de solicitação

[100] BRASIL. Ministério da Educação, Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Serviço de Acesso a Dados Protegidos (Sedap):** Guia do Usuário - versão 1.0. Brasília: Inep, 2019. Disponível em: <http://inep.gov.br/documents/186968/0/Guia+do+usu%C3%A1rio+-+Servi%C3%A7o+de+Acesso+a+-Dados+Protegidos+%28Sedap%29/bc9e1642-e937-430a-b5b4-b360bfa6f176?version=1.2>. Acesso em 02 mar. 2019.

de acesso a dados protegidos, bem como a autorização de acesso e avaliação da extração dos resultados concentra-se em um técnico responsável do Sedap, e não mais passa pelas diferentes áreas técnicas do órgão (art. 3º, inc. IX, da Portaria nº 52/2019). Entretanto, pode o técnico requisitar parecer técnico à Diretoria produtora dos dados solicitados pelo pesquisador para execução de suas atividades.

Em relação aos servidores ou às pessoas físicas que tenham acordos com o Inep para pesquisas institucionais, para a realização da pesquisa, é necessária autorização do Diretor da unidade responsável pela base. Além disso, a pesquisa não precisará ser feita na sala segura (Sadap), mas nas próprias estações de trabalho dos servidores, dentro do Inep (art. 7º, inc. I, II e §§ 1º e 3º, Portaria nº 52/2019).

Por fim, vale ressaltar que, por disponibilizar dados pessoais e sigilosos, o SAP/Sedap, inicialmente, também era utilizado como argumento de resposta para pedidos encaminhados ao Serviço de Informação ao Cidadão do Inep. O SIC-Inep[101] informou que, de setembro de 2014, quando foi publicada a Portaria que instituiu o SAP, a maio de 2016, 35 pedidos foram respondidos tendo como justificativa a sua existência.

Pelo sistema de buscas de pedidos e respostas do e-SIC é possível, inclusive, verificar o encaminhamento de perguntas de cunhos diversos para o SAP/Sedap, 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"; "alunos matriculados no ensino médio e superior em Joinville SC, separados por escola e curso", "relação dos professores de língua portuguesa efetivos do município", "combinar (por docente e escola) o banco de Docentes da Prova Brasil de 2015 com o banco de Docentes do Censo Escolar 2015", "liberação de acesso ao espelho das 53 redações nota mil do ENEM 2017", "situação do aluno da escola do ano de 2017 do censo escolar de todas as turmas, com nome do aluno, código do aluno e situação"[102], entre outros.

Nota-se que, apesar de o Sedap continuar sendo utilizado como solução para os pedidos recebidos via e-SIC, houve mudanças nos encaminhamentos dados pelo

[101] Pedido de informação n. 23480015207201602, realizado por meio do e-SIC.

[102] Informações encontradas no sistema de consulta do e-SIC, com os seguintes números de protocolo, respectivamente: 23480013041201681, 23480013438201673, 23480003090201614, 23480017657201541, 23480003950201873, 23480019553201732, 23480003904201874, 3480014446201807. Disponíveis em: <http://www.consultaesic.cgu.gov.br/busca>. Acesso em: 06 ago. 2018.

Instituto (especialmente após a publicação da Portaria nº 52/2019). Com a nova norma, não mais se indica o Sedap para acesso aos dados pessoais identificados, mas para realização dos cruzamentos das bases mascaradas. Por exemplo: para o pedido "Gostaria do percentual de alunos que adentraram ao ensino superior recém saídos do ensino médio, por ano, nos anos 2010 a 2018", trecho da resposta foi:

> O "cruzamento" entre as bases da Educação Básica e da Educação Superior, a fim de saber o contingente de alunos que concluíram o ensino médio e adentraram no ensino superior só é possível por meio dos CPFs (Cadastro de Pessoa Física). Por ser um dado pessoal e com acesso restrito, seu acesso deve ser feito por meio do Serviço de Acesso a Dados Protegidos do INEP (Sedap). Por meio dele, pesquisadores podem acessar, para fins institucionais e científicos, às bases de dados protegidos do Instituto. Cumpre destacar ainda que, O SAP (criado pela Portaria Inep nº 467, de 19 de setembro de 2014) evoluiu para o Sedap, garantindo assim a continuidade de desenvolvimento de pesquisas de interesse público e a manutenção do sigilo e identidade de indivíduos e instituições. O Sedap foi instituído pela Portaria nº 465, de 31 de maio de 2017, em cumprimento à Lei nº 12.527, de 18 de novembro de 2011, à Lei nº 9.448, de 14 de março de 1997 e ao Decreto nº 8.789, de 29 de junho de 2016. O Sedap, por meio da Norma de Acesso às Informações protegidas do Inep deve permitir acesso controlado e restrito a bases de dados protegidos, por meio de um conjunto de protocolos e ferramentas que garantam processos seguros de utilização que preservem a integridade e a proteção de acesso a tais informações. Sendo, portanto, um ambiente seguro na sede do Inep em Brasília, onde os pesquisadores e sociedade em geral podem ter acesso às bases de dados restritas relacionadas aos Censos e Avaliações produzidas pela autarquia, exclusivamente para fins de pesquisa e de estudo. Esse ambiente garante, além de segurança, transparência ao processo de consulta. Por questões de segurança da informação e proteção da informação pessoal, O acesso do pesquisador ao ambiente seguro requer algumas formalidades processuais, não sendo permitido ao pesquisador entrar ou sair do ambiente seguro com materiais impressos ou de informática não autorizados. (…) Mais informações podem ser obtidas no seguinte link: http://portal.inep.gov.br/web/guest/dados/sedap[103].

Observa-se, assim, que as discussões acerca da proteção de dados pessoais e sensíveis no Instituto têm surtido efeito e as ações visando protegê-los vêm sendo, gradativamente, aprimoradas. Apesar de, até o momento, não ter sido possível alcançar o objetivo inicial da criação do serviço, possibilitando aos pesquisadores o acesso a todas as bases

[103] Informação encontrada no sistema de consulta do e-SIC, com o seguinte número de protocolo: 23480022880201852. Disponível em: <http://www.consultaesic.cgu.gov.br/busca>. Acesso em: 23 fev. 2019.

de dados geradas pelo Inep, com a devida proteção aos dados pessoais e sensíveis e buscando o atendimento ao preceito de publicidade máxima, nesse caso, a possível ilegalidade gerada ao franquear o acesso do pesquisador a bases não desidentificadas parece ter sido sanada.

2.2.3 Ipea: 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 sua criação 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:

> 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 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[104].

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[105]. Por esse motivo, a promoção

[104] 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, p. 10-11.

[105] BRASIL. Anteprojeto de Lei Orgânica da Administração Pública Federal e Entes de Colaboração. 2009. Disponível em: <http://www.direitodoestado.com.br/leiorganica/anteprojeto.pdf> . Acesso em 30 jul. 2018.

de ações de coordenação e de supervisão para planejamento das políticas públicas também é incentivada:

> 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[106].

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 de equipamentos externos.

Porém, por ser de uso exclusivo de agentes públicos, eles estão submetidos às regras do serviço público e a cifração (criptografia ou desidentificação) 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 inexistia, mas que os mecanismos de controle de dados e de transmissão de dados devem ser repensados à luz dos princípios que regulam a privacidade pessoal[107]. 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 encontrada[108] para firmar parcerias com os outros órgãos da Administração Pública seja minimizada. Isso porque em 29 de junho de 2016 foi publicado o Decreto nº 8.789, que dispõe sobre o compartilhamento de bases de dados na Administração Pública Federal, dispensando a celebração de acordos

---

106 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.

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

108 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.

específicos para o compartilhamento das bases de dados.[109]

Quadro 4 – Soluções utilizadas pelo IBGE, Inep e Ipea para disponibilizar dados pessoais e sensíveis para fins de pesquisa

Requisitos / Soluções Adotadas	IBGE	Inep	Ipea
Existem protocolos de acesso e normas de segurança específicos	SIM	SIM	SIM
A sala é monitorada em tempo integral	SIM	SIM	SIM
Equipamentos eletrônicos ou outros tipos de materiais (caneta, papel, etc.) são proibidos	SIM	SIM	SIM
Computadores não têm conexão à internet e são desabilitados para uso de drives externos	SIM	SIM	SIM
Usuários só têm acesso ao banco de dados no modo leitura	SIM	SIM	SIM
É exigida assinatura de termo de condições do uso da sala e termo de compromisso de manutenção de sigilo	SIM	SIM	SIM
Os resultados da pesquisa passam por avaliação técnica do órgão antes de serem entregues ao pesquisador	SIM	SIM	SIM
O serviço é indicado nas demandas via e-SIC como canal específico para atendimento dos pedidos de acesso a dados pessoais e sensíveis	SIM	SIM	NÃO
Há necessidade de comprovação de vínculo à instituição de pesquisa ou órgão público	SIM	SIM*	SIM**
Cobra-se pelo uso do serviço	SIM	NÃO	NÃO
É permitido o uso de bases de dados externas (com autorização do órgão responsável)	SIM	SIM*	NÃO
Há acesso a dados identificados	NÃO	NÃO*	SIM
Existe um Comitê para avaliação dos projetos e dos resultados da pesquisa	SIM	NÃO	NÃO
O pesquisador deve apresentar relatório de pesquisa	SIM	SIM*	NÃO

* Esses parâmetros mudaram em 2017, com a Portaria nº 465/Inep. Antes dessa data, o acesso a bases de dados externas era possível sem autorização do órgão responsável e não havia necessidade de comprovar vínculo a alguma instituição de pesquisa. Em relação ao acesso a dados pessoais identificados, em razão de sua proibição pela Portaria nº 465/2017, o serviço ficou suspenso por um período para mascaramento. Posteriormente, com a Portaria nº 52/2019, o serviço foi retomado com a disponibilização de apenas algumas bases de dados já mascaradas.

** No Ipea, as pesquisas são de interesse institucional, sendo necessário firmar Acordos de Cooperação Técnica ou Convênios com as organizações interessadas. Não basta, portanto, apenas a comprovação de vínculo à uma instituição de pesquisa.

Fonte: Elaboração própria.

[109] Destaque para os seguintes artigos do referido Decreto (BRASIL, 2016): "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".

2.3 O modelo de compartilhamento de dados, as janelas únicas e os seus aspectos controvertidos

Um dos aspectos mais relevantes sobre o respeito aos dados pessoais tem sido a discussão gerada em torno, por exemplo, do decreto que trata da interoperabilidade de bases de dados (Decreto nº 8.789/16). "O Decreto é um marco no relacionamento entre os órgãos da APF, que tendem a atuar de forma fragmentada, com estruturas isoladas cujas responsabilidades são específicas e restritas. Sob a ótica do cidadão, contudo, a administração pública é vista como uma unidade. Para melhor servir o cidadão, é necessário superar a cultura de isolamento e investir na soma de capacidades."[110]

Com efeito, "se a informação não está acessível a todos, esta disparidade gera *status* e valor àqueles que conseguem acessar e processar tal informação"[111]. Por outro lado, uma informação coletada ou exigida pela Administração Pública para promoção de ações que visam melhorar o acesso à cidadania não pode ser utilizada de forma discriminatória contra o cidadão.

Sob esse aspecto, a interoperabilidade está relacionada à qualidade dos dados e refere-se à capacidade de um sistema computacional trabalhar com outros a partir de padrões ou processos comuns[112]. Trata-se de uma atividade crítica quando se busca melhorar a colaboração e o compartilhamento de informações entre as instituições governamentais, tanto para alcançar o almejado governo eletrônico[113] quanto para garantir a segurança nacional, além de estar relacionada aos processos de mineração de dados[114].

---

110 VARELLA, Marcelo D.; OLIVEIRA, Clarice G.; MOESCH, Frederico. **Salto digital nas políticas públicas**: oportunidades e desafios. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, p. 560-583, 2017. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4808/0>. Acesso em:15 mar. 2019. DOI: http://dx.doi.org/10.5102/rbpp.v7i3.4808, p. 566.

111 MILAGRE, José; SEGUNDO, José Eduardo Santarém. **A propriedade dos dados e a privacidade na perspectiva da Ciência da Informação.** Encontros Bibli: revista elerôtnica 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.

112 SEIFERT, Jeffrey W. **Data mining and homeland security: an overview.** 2008. Prepared for Members and Comittes of Congress - Congressional Research Service. Disponível em: <https://fas.org/sgp/crs/homesec/RL31798.pdf>. Acesso em: 13 nov. 2016.

113 "O conceito de Governo Eletrônico surge a partir de aspectos oriundos da evolução da TIC, especialmente a Internet, constituindo novas formas de relacionamento da Administração Pública com a sociedade e vice-versa, evidenciando a prestação de serviços sem a necessidade da presença física." (BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Governo Eletrônico.** Disponível em: <https://www.governodigital.gov.br/EGD/historico-1/historico>. Acesso em 01 out. 2018.)

114 Mineração de dados (*data mining*) é "definida em termos de esforços para descoberta de padrões em bases de dados. A partir dos padrões descobertos, têm-se condições de gerar conhecimento útil para um processo de tomada de decisão. Trata-se, portanto, da aplicação de técnicas, implementadas por meio de algoritmos com-

Baird[115] classifica cinco facetas do processo de interoperabilidade: a) técnica; b) organizacional; c) jurídica ou de políticas públicas; d) semântica e; e) de efeitos decorrentes de forças políticas, econômicas, culturais ou sociais. No presente estudo, pretende-se enfatizar as problemáticas relacionadas à interoperabilidade organizacional e à jurídica ou de políticas públicas que, segundo ele, a depender da forma como são definidas, podem operar como barreira - intencional ou não -, catalisador ou facilitador das interações intergovernamentais.

Ainda, de acordo com o autor, a depender do contexto e da evolução tecnológica, quando se trata de compartilhar dados pessoais ou sensíveis, pode ser necessário que os governos alterem com mais frequência leis e regulamentos a fim de atender às exigências de privacidade ou divulgação impostas. Isso pode vir a se tornar uma dificuldade em termos de planejamento, desenvolvimento e manutenção de determinada política e, principalmente, da eficiência[116].

Entende-se por eficiência, nesse trabalho, a boa utilização dos recursos escassos disponíveis a fim de garantir os melhores resultados possíveis, em termos de quantidade, qualidade e tempestividade, com o menor custo. Di Pietro apresenta dois aspectos do princípio da eficiência:

> Pode ser considerado em relação ao **modo de atuação do agente público**, do qual se espera o melhor desempenho possível de suas atribuições, para lograr os melhores resultados; e em relação ao **modo de organizar, estruturar, disciplinar a Administração Pública**, também com o mesmo objetivo de alcançar os melhores resultados na prestação do serviço público.[117] (grifo nosso)

Assim, tendo em vista o interesse público como finalidade última das ações e programas das políticas públicas, "poder-se-ia enunciar o conteúdo jurídico do

putacionais, capazes de receber, como entrada, um conjunto de fatos ocorridos no mundo real e devolver, como saída, um padrão de comportamento, o qual pode ser expresso, por exemplo, como uma regra de associação, uma função de mapeamento ou a modelagem de um perfil". (SILVA, Leandro Augusto da; PERES, Sarajane Marques; BOSCARIOLI, Clodis. **Introdução à mineração de dados:** com aplicações em R. Rio de Janeiro: Elsevier, 2016, p.)

115 BAIRD, Stacy A., **Government Role and the Interoperability Ecosystem** (Summer 2009). Journal of Law and Policy for the Information Society, Vol. 5, No. 2, p. 219, Summer 2009. Available at SSRN: <https://ssrn.com/abstract=1482752> . Acesso em: 13 nov. 2016.

116 O princípio da eficiência passou a figurar no texto constitucional por intermédio da Emenda nº 19/1998, a partir do movimento da Reforma da Gestão Pública (iniciado em 1995). A Reforma buscava implantar o modelo gerencial, por meio da descentralização e da delegação de poderes, e foi encabeçada por Bresser Pereira, tendo como marco a publicação do Plano Diretor da Reforma do Aparelho do Estado (PDRAE/1995). Consta, também, expressamente do art. 2º da Lei nº 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

117 DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** 27. ed. São Paulo: Atlas, 2014, p. 84.

princípio da eficiência nos seguintes termos: a Administração Pública deve atender o cidadão na exata medida da necessidade deste com agilidade, mediante adequada organização interna e ótimo aproveitamento dos recursos disponíveis."[118].

Antes, porém, de analisar alguns dos modelos de uso, tratamento e compartilhamento dos dados atualmente utilizados pela APF, é importante destacar uma das ações adotadas pelo Governo Federal visando ao governo eletrônico e a interoperabilidade entre os órgãos. Trata-se dos Padrões de Interoperabilidade de Governo Eletrônico (e-Ping).

2.3.1 E-Ping: iniciativa que resultou em baixa adesão

O documento de referência do e-Ping define a interoperabilidade como "uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente"[119].

Associado às medidas que tiveram início nos anos 2000 visando à implementação do Governo Eletrônico no país, em 2004, foi publicada a primeira versão do documento que tratava do e-Ping. Em 11 de agosto de 2009, foi publicado o Decreto nº 6.932, conhecido como Decreto Cidadão, revogado pelo Decreto nº 9.094, de 17 de julho de 2017, que visa simplificar ainda mais a prestação dos serviços públicos, diminuindo, por exemplo, o número de exigências de documentos aos cidadãos. O estabelecimento de padrões para interoperabilidade (que abrangem três dimensões: organizacional, semântica e técnica) facilitará ainda mais o compartilhamento de dados.

Atualmente na versão 2018, a arquitetura e-Ping define um conjunto de especificações técnicas para regulamentar a utilização das TICs nos serviços do governo eletrônico federal quanto a: a) interconexão, b) segurança, c) meios de acesso, d) organização e intercâmbio de informações, e) áreas de integração para governo eletrônico.

De acordo com a Portaria SLTI/MP nº 92, de 24 de dezembro de 2014, a adoção dos padrões e políticas estipulados no e-Ping visa à racionalização de investimentos em TICs, bem como está diretamente relacionado à qualidade e integridade das soluções e informações. Seu uso é obrigatório para os órgãos do Poder Executivo para todos os novos sistemas de informação que vierem a ser desenvolvidos ou implantados no

---

[118] COSTODIO FILHO, Ubirajara. **A Emenda Constitucional 19/98 e o Princípio da Eficiência na Administração Pública**. In : Cadernos de Direito Constitucional e Ciência Política, São Paulo : Revista dos Tribunais, n. 27, p. 210-217, abr./jul. 1999, p. 214.

[119] BRASIL. **Padrões de Interoperabilidade de Governo Eletrônico – e-PING** (versão 2018). Disponível em: <http://eping.governoeletronico.gov.br/> . Acesso em 10 ago. 2018.

governo; para sistemas legados que envolvam serviços de governo eletrônico; e para a aquisição ou atualização de equipamentos de TIC.

As especificações técnicas contidas no documento são classificadas em quatro níveis, de acordo com o grau de aderência às políticas gerais de arquitetura: a) Adotado (já homologado); b) Recomendado (atende aos padrões, mas não foi homologado); c) Em transição (não atende a um ou mais requisitos, com tendência à desativação); d) Em estudo (em avaliação e poderá ser adotado após processo de avaliação ser concluído).

Porém, sua implementação é uma tarefa difícil, entre outros fatores, porque abrange uma quantidade imensa de órgãos e entidades administrativas com seus sistemas, ferramentas e modelos tecnológicos próprios de gerenciamento de dados; depende da priorização por parte de cada um deles (já que cada órgão é autônomo e tem interesses e necessidades diversos); além do custo e das restrições orçamentárias para adaptação dos sistemas já existentes.

Porém, o fato de essas especificações não serem utilizadas podem fazer surgir problemas de duplicidade ou redundância nas bases, por exemplo. De acordo com levantamento do TCU[120], até 2016, apenas 6% dos serviços governamentais via internet disponíveis ao cidadão haviam implementado as diretrizes e especificações e-Ping para intercâmbio de dados, informações e processos governamentais; 41% haviam adotado parcialmente; e 13% haviam apenas iniciado seu plano de adoção. Os demais resultados se dividem em "não se aplica" e "não adota essa prática", com 15% e 25%, respectivamente.

Ainda, como ferramenta de apoio ao e-Ping, está prevista a disponibilização de um Catálogo de Interoperabilidade, que objetiva reunir o catálogo de serviços interoperáveis, o catálogo de bases oficiais e o catálogo padrão de dados.

> O Catálogo de Serviços Interoperáveis tem por objetivo tornar públicas as interfaces (pontos de integração) de sistemas que apoiem a oferta de serviços de Governo Eletrônico.
>
> O Catálogo de Bases Oficiais tem por objetivo tornar públicos os serviços interoperáveis que atendem ao Decreto Cidadão na parte dos dados comprobatórios de pessoa física.
>
> O Catálogo de Padrão de Dados tem por objetivo estabelecer padrões de tipos e itens de dados que se aplicam às interfaces dos sistemas que fazem parte do setor público.[121]

---

120 BRASIL. Tribunal de Contas da União. **Levantamento de Governança de TI.** Brasília: TCU, 2016. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15E39AE45015E58A53AB44700/>. Acesso em: 30 nov. 2018.

121 BRASIL. Portal do SISP. **Catálogo de Interoperabilidade.** Disponível em: <http://www.sisp.gov.br/faq_in-

Esse documento seria de grande valia para a compreensão das bases de dados e sistemas existentes na Administração Pública e para posterior utilização das informações nas políticas públicas. No entanto, o documento ainda não está disponível. Segundo consta da página do Catálogo (http://catalogo.governoeletronico.gov.br/), ele "*está sendo alterado para atender ao Decreto 8789/2016". Por favor, aguarde pela nova versão ou entre em contato*". Assim, em contato com o MPDG[122], foi explicado que não existe previsão para sua publicação, "*pois depende da disponibilidade de cada órgão em preencher o novo catálogo e ainda estamos em negociação com os órgãos".*

Acrescente-se que, na consulta realizada, foi disponibilizado um endereço do catálogo antigo (2011) com as respectivas documentações. Mas, ao acessar o link fornecido[123], é possível notar que se trata de vários documentos dispersos, disponibilizados numa página não-oficial do Governo (está armazenada no GitHub, plataforma de hospedagem de código aberto e gratuito, para construção colaborativa de documentos), sem estar consolidado, tampouco estruturado de forma simples e de fácil compreensão pelo cidadão, nos termos da LAI.

Por fim, corroborando os dados apresentados no Relatório do TCU quanto ao padrão e-Ping, nos cinco Ministérios consultados via e-SIC, tem-se que apenas um (SRF/MF) afirmou atender aos padrões especificados pelo e-Ping; MEC e MJ afirmaram estar em fase de estudos para adequação. MT e MDS apenas informaram que não atendem aos padrões estabelecidos (ver Quadro 4).

Quadro 5 – Atendimento às especificações e-Ping

Atende aos padrões e-Ping	Ministério da Educação	Ministério da Fazenda (Secretaria da Receita Federal)	Ministerio da Justiça e Ministério Extraordinário da Segurança Pública	Ministério do Trabalho	Ministério do
SIM					
NÃO					

Fonte: elaboração própria[124].

Sabe-se que a mera adoção dos padrões e-Ping não é suficiente para que ocorra a interoperabilidade, pois há outras condições como requisitos de segurança, custo e

teroperabilidade/one-faq?faq_id=13997087>. Acesso em 10 ago. 2018.

122 Informação obtida com o Ministério do Planejamento, Desenvolvimento e Gestão, a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 03950003576201734, de 22/11/2017).

123 Link encaminhado pelo MPDG por meio da consulta e-SIC n. 03950003576201734, de 22/11/2017: https://github.com/govbr/catalogo-govbr/blob/e1201312eae676034d8c6e574a71d5466eef774a/docs/index.Md>

124 Informações obtidas com os respectivos Ministérios, a partir de consultas realizadas pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (respectivamente, Pedidos n. 23480027095201713, 16853008268201745, 08850005196201786, 46800002074201712, 71200000732201748, de 22/11/2017).

atendimento à legislação, por exemplo. Por outro lado, apesar de obrigatória, faltam mecanismos de *enforcement* para concretização dessas ações. Em relação à construção do Catálogo, entende-se, também, que, se realmente fosse efetivada, seria uma ação que teria impacto bastante benéfico no que tange à interoperabilidade.

2.3.2 Modelo single window: padronização de informações, documentos e redução das redundâncias para o cidadão

Exemplos da boa utilização da tecnologia em prol da melhoria da qualidade dos serviços públicos e, consequentemente, da vida dos cidadãos e dos seus direitos fundamentais, são os avanços em termos dos sistemas de gestão dos diversos cadastros correspondentes aos documentos e números de identificação do cidadão.

Pode-se citar nesse caso o projeto " e-Social"[125] (Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas), que cruzou bases de dados de cinco órgãos e entidades do governo federal, fazendo diversos batimentos em cadastros oficiais, a fim de padronizar e simplificar o envio de informações ao governo federal, bem como diminuir a redundância das informações prestadas.

Os sistemas do e-Social são divididos em dois: a) e-Social doméstico (pessoas físicas quando na condição de empregadores); b) e-Social para empresas. De acordo com o Ministério do Trabalho[126], o e-Social, apesar de não ser possível precisar, deve eliminar cerca de 99% das redundâncias nas informações prestadas por pessoas jurídicas, uma vez que não serão mais pedidas informações em duplicidade. Todo trabalho de preparação e integração das bases, bem como o desenvolvimento do sistema foi feito pelo Serpro e, segundo informações da Receita Federal, todos sistemas acessados pelo e-Social atendem à arquitetura e-Ping.

Releva-se, entretanto, que o trabalho foi árduo. Segundo Varella, Oliveira e Moesch, foram gastos quase dois anos para sanear as inconsistências nas bases de dados que seriam integradas. "Os detentores das bases, Caixa, Fazenda e Previdência Social, em uma constante disputa por espaço, recursos e micropoder, não cediam os dados necessários, ou, quando o cediam, não destinavam os recursos necessários para o saneamento entre as bases"[127].

---

[125] BRASIL. **Conheça o eSocial.** Disponível em: <http://portal.esocial.gov.br/institucional/conheca-o>. Acesso em: 10 jan. 2018.

[126] Informações obtidas com o Ministério do Trabalho , a partir de recurso apresentado à consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 468000002073201778, de 22/11/2017).

[127] VARELLA, Marcelo D.; OLIVEIRA, Clarice G.; MOESCH, Frederico. **Salto digital nas políticas públicas**: oportunidades e desafios. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, p. 560-583, 2017. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4808/0>. Acesso em:15

Outra iniciativa, a do Porto sem Papel[128], integra bases de dados de seis órgãos diferentes da Administração Pública a fim de alimentar um sistema de informação único. Esses dois casos são chamados de modelos de atendimento *single-window* (ou janela única ou modelo de gestão de atendimento integrado), na categoria *seamless service.* O objetivo é tornar:

> os serviços públicos menos complicados e embaralhados em uma rede complexa de interseções burocráticas. Esses centros de atendimento visam oferecer serviços em área específica ou para um grupo específico de cidadãos, independente das jurisdições e níveis de governo. Geralmente nesse modelo, os serviços são oferecidos cruzando fronteiras departamentais dentro de um mesmo governo, e até mesmo fronteiras governamentais que dividem união, estados e município.[129].

O acesso dos cidadãos aos serviços públicos em postos de atendimento como o "Na Hora", no governo do Distrito Federal (em outras unidades da federação, possuem outros nomes, como TudoFácil no Rio Grande do Sul e PoupaTempo no Rio de Janeiro) também é um caso de sucesso. Trata-se de representações de diversos órgãos públicos federais e distritais em um único local, de forma articulada (possível devido ao uso da tecnologia), com a finalidade de facilitar o acesso do cidadão aos serviços públicos, também adotando o modelo de atendimento *single-window*, mas na categoria *one-stop shopping*.

Nesta esteira, ao avaliar o uso de tecnologias digitais como parte da estratégia de modernização governamental, o TCU percebeu que diversas ações podem ser tomadas a fim de melhorar a eficiência na prestação de serviços. Várias delas, inclusive, estão relacionadas à gestão de dados, como pode se observar das recomendações apresentadas pelo ministro Benjamin Zymler, no Acórdão TCU nº 1.496/2017. No referido documento, é recomendado à Casa Civil da Presidência da República a adoção de medidas para "atribuir competências de Governança de Dados a uma instância

---

mar. 2019. DOI: http://dx.doi.org/10.5102/rbpp.v7i3.4808, p. 575.

128 "O Porto sem Papel é um sistema de informação que tem como objetivo principal reunir em um único meio de gestão as informações e a documentação necessárias para agilizar a análise e a liberação das mercadorias no âmbito dos portos brasileiros (…) O responsável pela embarcação, o armador ou a agência de navegação disponibiliza as informações obrigatórias e necessárias para a entrada ou liberação das mercadorias em uma única base de dados." (BRASIL. Ministério dos Transportes, Portos e Aviação Civil. **Porto sem Papel.** Disponível em: <http://www.portosdobrasil.gov.br/assuntos-1/inteligencia-logistica/porto-sem-papel-psp>. Acesso em: 10 jan. 2018.)

129 COUTINHO, Marcelo James Vasconcelos. Administração pública voltada para o cidadão: quadro teórico-conceitual. **Revista do Serviço Público,** Brasília, Ano 51, n. 3, p.40-73, jul/set 2000. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/331/337>. Acesso em: 10 jan. 2018.

administrativa que seja capaz de: arbitrar as questões relativas ao compartilhamento de informações, no que diz respeito à normatização, coordenação de iniciativas e resolução de conflitos acerca das informações de posse da Administração Pública Federal".

Também, recomenda ao MPDG que, para atender ao princípio da eficiência, apresente plano de ação que contenha: a) "mecanismos de mediação para os conflitos de entendimento sobre compartilhamento e confidencialidade de informações"[130], b) "um modelo de custeio para os serviços de integração de dados, incluindo demandantes, gestores, custodiantes e empresas públicas prestadoras de serviços de TI, de forma a obter um custo final vantajoso para administração pública" e c) "estratégias para minimizar redundâncias e ineficiências na atuação das empresas estatais de tecnologia, em especial Serpro e Dataprev, de modo a otimizar o provimento de aplicações e serviços de TI, bem como maximizar o apoio dessas empresas à integração de dados e sistemas da administração pública"

Esses trechos do Relatório do Acórdão indicam que ainda existe uma "área cinzenta" no que tange à gestão e ao entendimento sobre o compartilhamento e demais usos conferidos aos dados pessoais e sensíveis pela APF. Percebe-se, por sua leitura, o quanto a Administração Pública ainda tem de melhorar para garantir a eficiência, eficácia e efetividade administrativas em termos de gestão de dados. Outro trecho do relatório que deu ensejo ao Acórdão citado também merece destaque:

> **Os órgãos e entidades da APF não compartilham os dados de que dispõem em suas bases de forma a obter as informações necessárias de que o cidadão precisa para o exercício de seus direitos ou o cumprimento de seus deveres.**
>
> Ao contrário, a APF ainda possui a prática de transferir para a sociedade a tarefa de buscar informações que precisam ser obtidas em diversos órgãos da administração, a exemplo de certidões, fazendo com que a sociedade atue na função de **despachante administrativo**, substituindo o Estado.
>
> No entanto, ainda que o Decreto Cidadão date de 2009,

[130] Pode-se citar, nesse momento, as divergências acerca da interpretação do art. 9º do Decreto nº 8.789/2016 ocorridas entre a Polícia Rodoviária Federal (PRF) e Departamento Nacional de Trânsito (Denatran) no que tange à responsabilidade do custeio ao acesso de cinco bases de dados do Denatran, utilizadas pela PRF, para prestação de serviços essenciais à segurança pública e viária de sua competência, e armazenadas pelo Serpro. Assim dispõe o referido artigo: "o órgão ou a entidade interessado deverá arcar com os custos envolvidos, quando houver, no acesso ou na extração de informações da base de dados, exceto quando estabelecido de forma diversa entre os órgãos envolvidos". À época, o Denatran notificou a Polícia de que suspenderia o seu acesso caso esta não passasse a custeá-lo. Por falta de consenso, o caso foi objeto de discussão na Câmara de Conciliação e Arbitragem da Administração Federal, órgão da Advocacia-Geral da União e, posteriormente, no Ministério Público Federal. Este instaurou inquérito civil, gerando a Recomendação nº 27/2018 – MPF/PRDF/1OFCID encaminhada à Presidência da República para que fossem adotadas as medidas necessárias para o acesso contínuo e permanente da PRF às bases de dados do Denatran. (Recomendação do MPF/DF visa assegurar acesso da Polícia Rodoviária Federal a sistemas do Denatran**. Assessoria de Comunicação da Procuradoria da República no Distrito Federal.** Disponível em: <http://apps.mpf.mp.br/aptusmpf/index2#/detalhe/41000000000085255421?modulo=0&sistema=portal>. Acesso em: 04 mar. 2019).

> atualmente a sociedade continua a ser obrigada a apresentar informações que já são custodiadas pela Administração Pública ao buscar um serviço público. Isto é observado na existência de diversos casos de serviços públicos que solicitam informações que já estão sob custódia da administração pública, a exemplo do programa de Financiamento Estudantil (Fies) , quando um candidato, para comprovar a sua renda e ter direito ao financiamento, necessita deslocar-se até uma agência do INSS para solicitar uma declaração, que poderia ser obtida eletronicamente pelo Fundo Nacional de Desenvolvimento da Educação (FNDE), na qualidade de agente operador do programa (peça 52, p.6).
>
> **Esta situação demonstra que as diretrizes determinadas pelo Decreto Cidadão e pelo Marco Civil da Internet ainda não são uma realidade por completo, em função da falta de integração e compartilhamento de informações entre os órgãos e entidades governamentais**, conforme já observado nos parágrafos 82 a 83. (trecho do relatório de Auditoria referente ao Acórdão TCU nº 1496/2017- Plenário. Relator: Benjamin Zymler – grifo nosso)

Das evidências apresentadas pela auditoria, depreende-se, também, a preocupação com a privacidade dos cidadãos e a dificuldade de se colocar em prática iniciativas como as apresentadas. Isso ocorre em função, especialmente, de três aspectos: a) custo de integração para o demandante; b) remuneração e ônus decorrentes dos serviços para o gestor da informação e; c) confidencialidade dos dados (falta de consenso no entendimento jurídico).

Em relação ao primeiro item, tem-se a dificuldade quanto à integração eletrônica entre os diferentes órgãos, advinda do modelo de custeamento atual, que requer vultosos investimentos em tecnologia caso o serviço deixe de ser presencial. Apesar disso, pensando no longo prazo:

> Os efeitos da falta de integração entre os órgãos e entidades da APF e a consequente transferência para a sociedade da tarefa de buscar informações podem ser estimados. Em entrevista com a Seges/MPDG, os gestores apresentaram estudos (peça 116) em que, considerando apenas os exemplos de marcação de consulta em hospitais e de matrícula em escolas públicas, o impacto para a sociedade pode chegar a R$ 486.000.000,00 por ano pelas horas de trabalho desperdiçadas pelos cidadãos em filas de atendimento. Da mesma forma, os estudos apontaram uma potencial redução no custo operacional para o Estado em R$ 562.000.000,00 por ano caso o atendimento fosse realizado de forma eletrônica.

Acerca do segundo aspecto, o custo de integração pode "afetar também a instituição gestora que detém a informação, uma vez que existem custos de criação e manutenção de serviços de compartilhamento de informações que não são sempre, nem totalmente, suportados pelo demandante, acarretando um ônus para o gestor dono da informação, ao qual ele não deu causa".

Por último, em relação à confidencialidade dos dados, o relatório do TCU destaca que:

> Em entrevistas com os gestores da Dataprev e do MPDG, em comum encontrou-se o relato de que **divergências no entendimento jurídico sobre a possibilidade de compartilhar dados é um entrave à integração de informações.**
>
> A solicitação de informações para um órgão gestor passa pela análise jurídica da possibilidade de permitir o acesso a dados restritos custodiados pelo órgão. Contudo, as regras que definem as situações em que isto pode ser feito não são claras. Um estudo do MPDG indicou **normas com expressões vagas e discricionariedade ao órgão concedente** (peça 77, 2-3). Por seu turno, a Dataprev citou a **ausência de um marco regulatório objetivo para a definição das regras de sigilo das informações** como uma das pendências para a evolução dos modelos de serviços eletrônicos (peça 78, p. 4, item 7) .
>
> (…) a necessidade de pareceres jurídicos sobre as solicitações que envolvam dados que não estão no rol exemplificativo continuará sendo demandada, mesmo que o decreto [8.789/16] tenha eliminado a necessidade de celebração de acordos ou outros instrumentos congêneres. No caso da divergência de entendimento entre órgãos, **não há uma instância que possa servir de mediadora ou de arbitragem para resolver os conflitos**[131].

Ao contrário dos pontos apresentados, do relatório também podem ser apreendidos aspectos positivos, como as tratativas que estão em curso entre Poder Executivo e Tribunal Superior Eleitoral para viabilizar o consumo da base de dados biométrica para utilização nos serviços públicos digitais[132].

---

[131] Destaca-se, nesse caso, a possibilidade de atuação da Câmara de Conciliação e Arbitragem da Administração Federal, vinculada à Advocacia-Geral da União, criada em 2007, cujas competências estão definidas no Decreto nº 7.392, de 13 de dezembro de 2010, e alterações posteriores. Segundo o art. 18 da norma, À Câmara, compete: III – dirimir, por meio de conciliação, as controvérsias entre órgãos e entidades da Administração Pública Federal, bem como entre esses e a Adminstração Pública dos Estados, do Distrito Federal, e dos Municípios.

[132] Esse assunto voltou à tona no início de 2019, sob a atual Presidência. O Governo Federal criou um grupo de trabalho para analisar a viabilidade de criar um documento único em base digital, a partir da base de dados biométrica da Justiça Eleitoral. (COSTA, Gilberto. Governo pretende unificar documentos em base digital. **Agência Brasil**, Brasília, 14 jan. 2019. Disponível em: < http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/governo-pretende-unificar-documentos-em-base-digital>. Acesso em: 25 fev. 2019.)

No entanto, o que se nota é que a prática de integração e compartilhamento, como os modelos de janela única apresentados, envolvem muito mais do que a mera existência de normativos que almejam essas melhorias. Elas envolvem questões econômico-financeiras, de articulação política e priorização, bem como de consenso em relação a um modelo de custeio vantajoso capaz de incentivar tanto os órgãos gestores quanto os demandantes a compartilharem seus dados e informações em prol do interesse e da melhoria dos serviços públicos.

Da análise desses aspectos e das recomendações do TCU, enfim, também não se pode deixar de apontar o alerta feito por Bolzan de Morais no que tange à eficiência administrativa. Segundo o autor, na perspectiva de que o Estado vem se tornando "uma imensa empresa de serviços", pautado no "poder numérico" de indicadores e "valores agregados" de determinada política pública,

> pode-se dizer que o modelo neoliber(al)ista substitui traiçoeiramente os princípios da ação estatal, por outros critérios como a eficiência, as vantagens comparativas ou a segurança, estabelecendo uma competição entre o direito e a eficiência. E, esta, baseada em um conhecimento técnico aletéico, estabelece o princípio do interesse ou da utilidade como o princípio normativo supremo, como o único "natural", o único possível, o único evidente. Ele se impõe às sociedades e aos homens e deve se tornar o guia da reforma geral das instituições[133].

Com essa compressão, o autor evidencia o perigo de o Estado (Liberal) de Direito, que passa a calcular suas possibilidades em termos de custo-benefício, não mais se submeter aos conteúdos do *Rule of Law*, que, em última instância, garante a Democracia e o respeito aos direitos humanos. Para ele, a nova conjuntura trazida pela revolução da internet - com a transterritorialidade e a linguagem algorítmica-funcional -, é uma forma de maximização do neoliberalismo, o que torna indispensável pensar a maneira como o Estado pode regular essa nova realidade em termos de eficácia e não apenas de eficiência.

Sob esse ponto de vista, e em comparação aos modelos de *single window* e ao de *data lake* (comentado no próximo tópico), que invariavelmente necessitam do compartilhamento de dados pessoais e sensíveis, não é demais postular cautela em relação à proteção dos dados pessoais e sensíveis, diretamente atrelada à dignidade da pessoa humana.

---

[133] BOLZAN DE MORAIS, Jose Luis. **O Estado de Direito "confrontado" pela Revolução da Internet!** Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, RS, v. 13, n. 3, p. 876-903, dez. 2018. ISSN 1981-3694. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/33021>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.5902/1981369433021, p. 890.

2.3.3 Data Lake: um único repositório capaz de possibilitar a análise de dados

Outro exemplo de uso da tecnologia visando ao aprimoramento da formulação e execução de políticas públicas é a Plataforma de Análise de Dados do Governo Federal (GovData)[134], lançada em maio de 2017, em decorrência do já mencionado Decreto nº 8.789/2016, que dispõe sobre o compartilhamento de bases de dados na Administração Pública Federal.

A ideia é ter, no contexto da Big Data e Analytics, um imenso repositório de dados (um "*lago de dados")*[135] da Administração Pública Federal, único e centralizado, capaz de viabilizar diversas análises e estatísticas com fins de melhorias das políticas públicas, por meio da simplificação para acesso, compartilhamento e avaliação dos dados. A lógica, nesse caso, é que as políticas públicas devem focar na finalidade e não no órgão que coletou os dados. O objetivo é conferir mais eficiência às ações do governo, melhorar a gestão e identificar fraudes, alcançando maiores ganhos fiscais.

Os dados são armazenados na forma bruta, estruturados (geralmente, em linhas e colunas, encontrados em banco de dados relacionais) ou não-estruturados (não organizados em tabelas, como vídeos e imagens), para que possam ser utilizados quando necessário e por quem se interessar. No caso da GovData, a plataforma terá uma estrutura compartilhada entre o Serpro e a Dataprev.

Importante destacar que a Plataforma será para acesso exclusivo de órgãos da Administração direta, autárquica e fundacional do Poder Executivo Federal (integrantes do SISP – Sistema de Administração dos Recursos de Tecnologia da Informação, atualmente composto por 225 órgãos). As bases de dados disponíveis foram escolhidas pelo Ministério do Planejamento segundo o que seus gestores classificaram como de maior interesse do Governo Federal.

Assim, oferecerá, mediante contratação de uma Plataforma como Serviço (PaaS), com pacotes mensais de usuários (por tecnologia), fontes e quantidades de dados, as vinte bases de dados mais acessadas do governo. Entre elas, o Cadastro de Pessoas Físicas (CPF), o Sistema Integrado de Administração Financeira do Governo Federal (Siafi) e o Registro de Veículos Automotores (Renavam). Isso possibilitará aos

---

[134] BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **GovData**: Perguntas Frequentes. Disponível em: <http://govdata.gov.br/>. Acesso em 01 ago. 2018.

[135] O conceito de *Data Lake* se diferencia do *Data Warehouse*, pois, diferentemente do primeiro em que os dados se apresentam no estado bruto; neste, os dados já estão limpos, organizados e estruturados, o que, por vezes, impossibilita atender novas demandas e cruzar conteúdos que não foram anteriormente planejados. Ressalta-se, também, que existem críticas ao modelo de *data lake* para que ele não vire um amontoado de dados sem relevância, devendo, cada um de seus dados, ser bem gerido e identificado.

órgãos autorizados o cruzamento de informações por meio da utilização de diversas ferramentas para mineração de dados e análises estatísticas, por exemplo.

Até dezembro/2017, nenhum órgão ainda havia contratado a GovData[136]. Porém, alguns já haviam feito a chamada "degustação" (ex: Instituto Federal do Rio Grande do Norte, Agência Espacial Brasileira, Ministério do Trabalho e Ministério das Cidades) e outros estavam em estado de "degustação" (ex: Ministério da Indústria, Comércio Exterior e Serviços, Ministério da Ciência, Tecnologia, Inovação e Comunicações, Instituto de Pesquisa Econômica Aplicada, Controladoria-Geral da União, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, entre outros).

Em entrevista ao representante da Setic/MPDG, Roberto Lyra, em janeiro/2018, foi informado que, na verdade, há interesse de vários órgãos, mas a contratação ainda não havia sido feita em razão de a minuta de contrato ser muito complexa e ainda estar sob análise da Procuradoria Jurídica do órgão, pois é muito complexo (ex: o custo não é fixo, variando em função do volume de dados, quais softwares e quantas licenças para cada um; a discussão do nível de serviço).

Trata-se de exemplo típico da utilização do ambiente de Big Data pelo Poder Público e que, por esse motivo, muitas vezes é alvo de críticas e exige cuidados específicos para não atentar, por exemplo, contra o direito à privacidade e preservar os dados pessoais e sensíveis.

Por exemplo, no sítio do Ministério do Planejamento a explicação sobre como será garantida a segurança dos dados pessoais apresenta-se extremamente genérica:

> **8) Como será realizada a segurança dos dados pessoais?**
> As informações e dados serão disponibilizadas para órgãos do governo federal que já tem acesso, porém de uma forma muito mais eficiente com o uso da GovData. O governo federal tem aprimorado os seus controles e normativos de segurança da informação, a exemplo do Decreto nº 8.789, que trata especificamente das regras e procedimentos para a garantia da segurança quando se trabalha com o compartilhamento de dados entre os órgãos da Administração Pública Federal[137].

Em relação à proteção dos dados pessoais e sensíveis, com informação mais precisa, o representante da SETIC/MPDG explica: a GovData, na verdade, não possui a base

[136] Informação obtida com o Ministério do Planejamento, Desenvolvimento e Gestão, a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 03950003575201790, de 22/11/2017).

[137] BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **GovData**: Perguntas Frequentes. Disponível em: <http://www.planejamento.gov.br/govdata-privado/perguntas-frequentes>. Acesso em 01 ago. 2018.

integral de todas as vinte bases disponibilizadas, mas extratos delas, que podem ou não conter a identificação de pessoas. Segundo ele, no entanto, nem todos os órgãos têm acesso irrestrito a todo o Lago de Dados. Além dos níveis de acesso de acordo com a permissão concedida para cada órgão, é feita, também, uma verificação quanto ao pedido.

Lyra dá o seguinte exemplo: o Ministério da Agricultura contrata a utilização da Plataforma GovData e solicita autorização para a base do Renavam (Registro Nacional de Veículos Automotores) e do Renach (Registro Nacional de Carteiras de Habilitação). Nesse caso, antes de acessar a base, é investigado se ele já possui autorização para tanto. Se sim, o acesso será concedido. Se não, ele continuará sem acesso até que haja a devida análise e seja autorizado pelo órgão responsável.

Nessa situação, é importante refletir sobre a possibilidade ou não de utilização de decreto para regulamentar o compartilhamento de dados pessoais e sensíveis entre os diferentes órgãos e entidades da Administração Pública. O Decreto nº 8.789/2016, que trata do assunto, por exemplo, fundamenta-se unicamente no art. 84, inc. VI, al. "a", da CF88, que atribui ao presidente da República a competência para dispor, mediante decreto, sobre "organização e funcionamento da administração federal, quando não implicar aumento de despesa nem criação ou extinção de órgãos públicos".

Ocorre que, além de o mencionado decreto ter sido editado sem a existência da norma geral de proteção de dados pessoais, a Constituição resguarda os direitos à intimidade, à vida privada, à honra e à imagem das pessoas (art. 5º, inc. X, CF88). Outrossim, apesar de o Marco Civil da Internet apresentar como diretriz a promoção da interoperabilidade tecnológica dos serviços de governo eletrônico de forma a permitir o intercâmbio de informações e a celeridade de procedimentos pelo Poder Público (art. 24, inc. III), ele obriga o respeito aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (art. 11), o que abrange as discussões acerca da anonimização ou encriptação dos dados.

2.3.4 Aplicativos governamentais: a coleta e o uso excessivo de dados

Atualmente, o uso de aplicativos faz parte da rotina das pessoas. E o governo, na tentativa de se equiparar ao setor privado, também tem buscado desenvolver aplicativos para facilitar a vida dos cidadãos.

Porém, desde já se encontram alguns problemas em termos de privacidade no uso dos dados sob a guarda e gestão da Administração. Além do acesso a dados contidos nos

aparelhos móveis, aplicativos podem "descobrir" padrões de uso, registrar mensagens de reclamação, denúncia ou solicitações dos usuários para composição de um registro histórico ou elaboração de um futuro perfil do usuário, o que tem natureza pessoal e pode se tornar sensível.

Segundo estudo da InternetLab, em análise de 13 (treze) softwares da administração nacional ou regional, foram encontradas "*flagrantes violações da privacidade dos cidadãos, principalmente no que toca a coleta de informações sem autorização e sem necessidade, uma vez que tais dados não são essenciais para a utilização dos aplicativos*"[138]. De acordo com o estudo, na esfera federal, foram analisados os aplicativos do Bolsa Família, Caixa Econômica Federal, Anatel Consumidor, FGTS, Meu INSS, SNE (Sistema de Notificação Eletrônica, do Denatran), Meu Imposto de Renda e CNH Digital.

O estudo mostrou que informações como localização aproximada ou precisa dos usuários; permissão para conhecer todas as contas cadastradas pelo usuário no dispositivo (redes sociais, serviços online, etc.) e permissão de acesso à câmera ou ao sensor biométrico são coletadas sem necessidade. Observa-se que no caso de permissão à câmera ou sensor biométrico, as soluções utilizadas pelos aplicativos da Caixa e do INSS, segundo o estudo, "são efetivamente utilizadas pelos apps para leitura de documentos e validação, entretanto, para os especialistas, representam risco de segurança, pois permitem, também, a coleta de informações sensíveis"[139].

O estudo empregou o aplicativo Lumen Privacy Monitor, desenvolvido pela Universidade de Berkeley, para realizar o levantamento das permissões utilizadas em aplicativos. De acordo com o Lumen, são classificadas como de alto risco permissões como acesso à câmera, à geolocalização às contas cadastradas, além das permissões de leitura e registro da memória externa e de realização de chamadas.

---

138 DEMARTINI. Felipe. **Apps do governo estão invadido privacidade dos usuários, diz estudo.** Canatech, 28 mai. 2018. Disponível em: <https://canaltech.com.br/seguranca/apps-do-governo-estao-invadindo-privacidade-dos-usuarios-diz-estudo-114680/>. Acesso em: 03ago. 2018.

139 Ibidem, *s/ pag*.

Quadro 6 - Estudo InternetLab: Permissões solicitadas por aplicativos do governo federal

PERMISSÕES	FGTS	CAIXA	BOLSA FAMÍLIA	MEU INSS	CNH DIGITAL	ANATEL	SNE DENATRAN	MEU IR
Acessar a localização aproximada	■		■	■		■		
Acessar a localização precisa	■	■	■	■		■	■	
Acessar as contas	■		■			■		■
Ler memória externa	■	■	■	■		■	■	■
Escreve em memória externa	■	■	■	■		■	■	■
Ler estado do telefone	■	■	■			■		■
Realizar ligações								
Acessar a câmera		■	■					
Acessar a internet	■	■	■	■	■	■	■	■
Acessar o estado da rede	■	■	■		■	■	■	■
Acessar o estado do wi-fi	■	■	■			■		
Receber informações do boot do aparelho							■	
Requisitar instalação de pacotes			■					
Vibrar		■				■		■
Manter o aparelho ativo	■				■	■	■	■
Usar hardware de impressão digital		■	■					
Acessar a lanterna			■					
Acessar as tarefas						■		
Criar janelas		■						
OBS: Preenchimento significa que o app possui permissão de acesso.								

Fonte: InternetLab (Disponível em:<http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo;>. Acesso em 03 ago. 2018.)

Esses usos vão de encontro às atuais discussões acerca da privacidade, da finalidade e do mínimo necessário para coleta e tratamento e, também ao Marco Civil da Internet (sem mencionar a nova LGDP que também deve aumentar essas preocupações) que prevê:

> art. 7º - VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas

> contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei.

Acrescenta-se o fato de que nenhum dos aplicativos analisados solicitou o consentimento expresso e específico para acessar os dados pessoais dos usuários. Em alguns deles, a autorização é genérica e ocorre no momento da instalação. Em outros três (SNE, IRPF e INSS), apesar de específico, o consentimento só era solicitado no caso do uso dos dados de geolocalização, sendo que no SNE, a solicitação da permissão explica para que será usado.

Outra crítica que se faz à utilização dos aplicativos é o modelo "tudo ou nada", como num contrato de adesão, em que a autonomia do consumidor ou cliente é mitigada, ou mesmo extinta, já que não pode negociar o conteúdo das cláusulas[140]. Fala-se, inclusive, que o consentimento, nesses casos não seria mais do que uma ficção. Nesses termos, estaríamos diante de um "mito do consentimento" em que a pessoa, caso não concorde, simplesmente ficará sem o serviço[141].

Por exemplo, no caso do aplicativo do Denatran, em que o cidadão consegue desconto de até 40% (quarenta por cento) para pagar as multas de trânsito (e que não apresenta uma Política de Privacidade). Apesar do benefício, há que se questionar sobre a coleta e utilização dos dados para - o que poderia ser considerado – fins comerciais, ou seja, como moeda de troca. Além disso, ressalta-se a necessidade de obediência ao princípio da legalidade, com fins ao atendimento do interesse público. Seria possível indagar, ainda, se o usuário teria outra alternativa para garantir o desconto (por boleto, por exemplo).

Diante dessa observação, seria possível traçar paralelo com a recente decisão do Superior Tribunal de Justiça (STJ), em que analisava contrato de adesão para fornecimento de cartão de crédito no qual constava cláusula autorizando o compartilhamento de dados dos consumidores entre entidades financeiras.

A decisão, considerando a referida cláusula ilegal e abusiva, trouxe alguns elementos importantes e que poderiam ser aplicados também no caso ora apresentado dos aplicativos: a) necessidade de transparência e confiança nos contratos de adesão; b)

---

[140] OLIVEIRA, Carlos Eduardo Goettenauer de. *Credit scoring* e *big data* no regime jurídico brasileiro. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gama Prata de. (Coord.) **Tecnologia jurídica e direito digital:** I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240.

[141] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 372-375.

necessidade de ofertar a opção para negar o compartilhamento de dados, c) necessidade do consentimento real e espontâneo do consumidor, d) necessidade de vinculação entre os dados coletados e o serviço prestado, ou seja, o dado não pode servir como objeto de negociação para a oferta do serviço. Como se pode observar:

> RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. (…) 3. **É abusiva e ilegal cláusula** prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, **sem que seja dada opção de discordar daquele compartilhamento**. 4. **A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança**. 5. A impossibilidade de contratação do serviço de cartão de crédito, **sem a opção de negar** o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, **a imprescindibilidade da autorização real e espontânea quanto à exposição**. 7. **Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado**, qual seja obtenção de crédito por meio de cartão. 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44). (…) (RESP 1.348.532-SP, RELATOR(A): MIN. LUIS FELIPE SALOMÃO, , DJE-2331 DIVULG 29-11-2017 PUBLIC 30-11-2017)

Por fim, medida básica em termos de proteção à privacidade, diz respeito à disponibilização da Política de Privacidade. Nesse caso, segundo o estudo[142], no caso

[142] ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloísa. **ESPECIAL: Por que se preocupar com o que o Estado faz com nossos dados pessoais.** InternetLab, 21 mai. 2018. Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo//>. Acesso em: 3 ago. 2018.

dos aplicativos federais, apenas o da Caixa, o do Bolsa Família, o do FGTS e o Meu INSS apresentavam ao usuário sua Política de Privacidade. No Meu IRPF, o link fornecido apenas redirecionava o usuário para o site da Receita Federal. E os aplicativos do Denatran, Anatel Consumidor e CNH Digital simplesmente não possuíam uma Política de Privacidade explicitada.

Nesse contexto e tendo em vista a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, será necessário que o Governo tenha de se adaptar às novas regras, investindo em mais transparência quanto à Política de Privacidade e ao uso e tratamento dos dados coletados pelos aplicativos.

2.4 Os impactos decorrentes da opção por centralizar ou descentralizar a gestão de dados pela Administração Pública

A gestão de dados pelos órgãos da Administração Pública não tem se dado de forma uniforme. Percebe-se que alguns optam por utilizar sua própria infraestrutura para hospedagem, desenvolvimento e tratamento dos dados. Outros, firmam contratos, em geral, utilizando a modalidade de dispensa de licitação, com o Serviço Federal de Processamento de Dados (Serpro) ou com a Empresa de Tecnologia e Informações da Previdência (Dataprev), ambas as empresas públicas vinculadas ao Ministério da Fazenda. Nos dois casos, observam-se problemas relacionados à terceirização da equipe de TI e à infraestrutura existente, como quantidade de pessoal, orçamento destinado ao setor e priorização das ações a serem desenvolvidas.

2.4.1 A possível comercialização indevida de dados pelo Serpro

Com objetivo de saber como funcionava o controle dos dados pelo Serpro, em 08 de abril de 2018, foi feito questionamento à empresa, via e-SIC, solicitando os nomes das bases de dados por ele hospedadas, armazenadas, mantidas, gerenciadas ou tratadas referentes aos Ministérios em análise nessa dissertação. Além disso, indagou-se se essas bases possuíam dicionário de dados[143] e se alguma delas era disponibilizada a outros órgãos da Administração Pública Federal ou a terceiros. O objetivo era conhecer o

[143] Dicionário de dados "consiste numa lista organizada de todos os elementos de dados que são pertinentes para o sistema. Sem o dicionário de dados o modelo não pode ser considerado completo, pois este descreve entradas, saídas, composição de depósitos de dados e alguns cálculos intermédios. O DD consiste num ponto de referência de todos os elementos envolvidos na medida em que permite associar um significado a cada termo utilizado. (…)permite inventariar e descrever os seguintes itens: depósitos de dados, fluxos de dados, dados elementares que constituem fluxos e depósitos de dados". **Dicionário de dados.** Disponível em*: https://moodle.unesp.br/ava/pluginfile.php/24935/mod_resource/content/2/4-DicionarioDados.pdf* Acesso em 03 ago. 2018.)

quanto as bases são estruturadas e se suas informações poderiam, posteriormente, ser facilmente utilizadas para o compartilhamento ou para conferir mais transparência, já que o dicionário permite ao usuário conhecer de forma mais precisa os relacionamentos e usos dos dados.

Em resposta, a empresa informou que "por regras contratuais o Serpro mantém sigilo das informações produzidas pelos contratos"[144], sendo necessário requisitar essas informações diretamente aos órgãos federais ou gestores dos serviços/contratos.

Ao interpor recurso em primeira instância, o Serpro novamente indeferiu o pedido alegando tratar-se de inovação recursal, já que foram solicitados os dispositivos dos contratos que determinam o referido sigilo. O argumento do recurso foi que, na primeira resposta apresentada pelo Serpro, não estavam sendo solicitadas informações **produzidas** a partir dos contratos, mas apenas os nomes das bases de dados e a existência ou não de permissão de acesso a elas por terceiros.

Ao recorrer novamente, em 30 de maio de 2018, o Serpro informou que as hipóteses de sigilo previstas nos contratos estão embasadas em seu Estatuto Social[145]. Assim: não se justificava "o esforço do levantamento solicitado, para fornecimento do(s) trecho(s) do(s) contrato(s) que dispõe(m) sobre o sigilo que deve ser resguardado por este órgão, uma vez que este é um preceito inerente à condição do Serpro de prestador de serviços"[146].

Nessa mesma data, o Ministério Público do Distrito Federal (MPDFT) encaminhou ao Ministério Público Federal (MPF)[147] informações colhidas durante investigação[148]

---

144 Informação obtida com o Serviço Federal de Processamento de Dados (Serpro), a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 99928000208201871, de 18/04/2018).

145 Art. 3º O Serpro tem por objeto social desenvolver, prover, integrar, comercializar e licenciar soluções em tecnologia da informação, prestar assessoramento, consultoria e assistência técnica no campo de sua especialidade, **bem como executar serviços de tratamento de dados e informações, inclusive mediante a disponibilização de acesso a estes e a terceiros, desde que assim autorizado pelo proprietário**
Parágrafo único. Os serviços prestados pelo Serpro envolvem matérias afetas a imperativos de segurança nacional, essenciais à manutenção da soberania estatal, em especial no tocante à garantia da inviolabilidade dos dados da administração pública federal direta e indireta, bem como aquelas relacionadas a relevante interesse coletivo, orientadas ao desenvolvimento e ao emprego de tecnologia brasileira para produção e oferta de produtos e serviços de maneira economicamente justificada. (Estatuto Social do Serpro)

146 Informação obtida com o Serviço Federal de Processamento de Dados (Serpro), a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 99928000208201871, de 18/04/2018).

147 MARQUES, Marília. MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro. **G1**, Brasília, 01 jun. 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml>. Acesso em: 15 jun. 2018.

148 Ofício n. 20/2018 – CPDP/MPDFT, de 30 de maio de 2018, que encaminha ao MPF documentos relativos à prática da chamada extração de CPFs e de CNPJs realizada pelo Serpro. Disponível em: http://www.

que apontava suposto esquema de venda[149] de dados pessoais dos brasileiros e proposta de serviço de extração de bases de dados do Cadastro de Pessoas Físicas (CPF) e do Cadastro Nacional de Pessoas Jurídicas (CNPJ) pela empresa.

O MPDFT alega que há um esquema comandado pelo Serpro de venda de dados pessoais e sensíveis, inclusive, para a própria Administração Pública, cujo valor ultrapassa R$ 270 mil (Contrato nº 027/2013, com o Conselho da Justiça Federal). A investigação teve início quando o site Consulta Pública passou a disponibilizar - de forma muito atualizada e estruturada - dados (como nome, data de nascimento, CPF, endereço, nome da mãe, entre outros) da população brasileira. De acordo com o MPDFT, esse foi um indicativo de que sua origem era a própria Administração.

Em apresentação à Comissão de Transparência, Governança, Fiscalização e Controle e Defesa do Consumidor, no Senado Federal, o promotor de Justiça e coordenador da Comissão de Proteção de Dados Pessoais do MPDFT, Frederico Meiberg Ceroy, apresentou cópia do Ofício COJUR/DP – 014971/2018, de 16 de maio de 2018, em que o Serpro responde à consulta formulada sobre diversos serviços prestados pela empresa da seguinte forma:

> A lei de criação do SERPRO, Lei n. 5.615, impõe o dever legal de sigilo nos termos do seu artigo 8º. Por essa razão e, de acordo com as cláusulas contratuais que regem a relação SERPRO/SFRB, ao informar os dados solicitados esta empresa estaria descumprindo o Termo de Confidencialidade e Sigilo constante do contrato assinado entre as partes. Diante disso, sugere-se que a requisição seja encaminhada para: Secretaria da Receita Federal do Brasil[150].

Percebe-se, assim, que a previsão de sigilo vem sendo utilizada pelo Serpro como embasamento para diversas consultas, seja por meio da requisição de informações via e-SIC, seja, inclusive, para fins de investigação, como solicitado pelo MPDFT.

---

mpdft.mp.br/portal/pdf/noticias/maio_2018/Of%C3%ADcio_MPF_SERPRO_Lock.pdf. Acesso em 28 nov. 2018.

149 Algumas pessoas chegam a dizer que o foco atual na proteção de dados e na privacidade vai ser superado, sendo o próximo grande tema a discussão sobre a venda e a propriedade de dados (o que abrange a discussão sobre a disponibilidade ou não de dados pessoais em se tratando de direitos da personalidade. (Ver, por exemplo: MAWAD, Marie; FOUQUET Helene; GRANT, Nico; LI, Dandan. Venda de dados pessoais é o próximo passo da revolução de big data. **Bloomberg**, 08 jun. 2018.Disponível em: <https://www.bloomberg.com.br/blog/venda-de-dados-pessoais-e-proximo-passo-da-revolucao-de-big-data/>. Acesso em: 15 jun. 2018.)

150 CEROY, Frederico Meinberg. **Audiência Pública Interativa:** A oferta de serviços de extração de base de dados de CPF e de CNPJ pelo Serviço Federal de Processamento de Dados (Serpro) para órgãos da Administração Pública, mediante remuneração. 13 jun. 2018. 30 slides. Diponível em: <https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=13787> Acesso em: 03 ago. 2018.

Ceroy também questionou o serviço de API (Application Programming Interface)[151] oferecido pelo Serpro a todo mercado: uma "solução que integra, de forma simples, o seu negócio a dados atualizados do Governo, permitindo o acesso a informações oficiais com rapidez, segurança e confiabilidade" e cujo slogan é: "Você sabia que é possível acessar dados oficiais do Governo em tempo real para reduzir fraudes e alavancar seu negócio?".

Na página da Biblioteca de API's do Serpro constam as seguintes possibilidades: consulta CPF e consulta CNPJ (diretamente das bases da Receita Federal); consulta NF-e (diretamente do SPED - Sistema Público de Escrituração Contábil), Integra Siafi (diretamente do Sistema Integrado de Administração Financeira - Siafi), consulta Dívida Ativa da União (diretamente das bases da Procuradoria Geral da Fazenda Nacional) e Consulta DU-E (Declaração Única de Exportação, diretamente das bases da Receita Federal e do MDIC).

O pagamento para acesso ao serviço é mensal. Atualmente, para as API's de CPF, CNPJ, NF-e, Dívida Ativa, é necessário desembolsar R$ 662,40/mês para até 999 consultas, mais quantia adicional por consulta no caso de excedentes. Para acesso à base do Siafi, o preço é de R$ 264,56/mês para até 399 consultas e da DU-E R$2.520/mês para até 999 consultas. Os contratos podem ser feitos online, com acesso imediato. O MPDFT vem indagando sobre quesitos como: a) quem autorizou? b) desde quando? c) quais obrigações são impostas às pessoas jurídicas ou pessoas naturais que obtêm esses dados por meio da API?

Segundo o Serpro, a empresa apenas disponibiliza o meio de acesso ao dado após autorização do órgão gestor da informação definindo quais dados podem ser disponibilizados, em qual meio, para qual ente e com que finalidade. Além disso, deve haver a celebração de convênios ou contratos. Só a partir dessa autorização que os dados são disponibilizados em um ambiente seguro, monitorado, auditado e com acesso controlado[152].

Assim, em nota, o Serpro divulgou que a "empresa repudia veemente a distorção que vem sendo feita a respeito de sua atuação na prestação de serviços ao governo e à sociedade" e afirmou que a empresa nunca teve contato ou repassou conteúdo ao site "Consulta Pública. Segundo Nota divulgada à imprensa, o Serpro afirma que:

---

151 BRASIL. Serviço Federal de Processamento de Dados. **API Serpro.** Disponível em: https://servicos.serpro.gov.br/api-serpro/. Acesso em: 03 ago. 2018.

152 SANTOS, Maria da Glória Guimarães dos. **Audiência Pública Interativa:** A oferta de serviços de extração de base de dados de CPF e de CNPJ pelo Serviço Federal de Processamento de Dados (Serpro) para órgãos da Administração Pública, mediante remuneração. 13 jun. 2018. 30 slides. Diponível em: https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=13787> Acesso em: 03 ago. 2018.

> b) O que é chamado "venda de informações", na verdade, é um procedimento legal e legítimo amparado por lei de disponibilização, previamente autorizada, de dados e informações já públicos, pertencentes aos órgãos e entidades da Administração, procedimento que, em nenhuma medida, atenta contra o sigilo de dados do cidadão (…)
>
> f) A empresa não fornece ou comercializa dados pessoais do cidadão brasileiro com exposição de sua privacidade;
>
> g) As informações, às quais os contratantes têm acesso, são informações cadastrais dos bancos de dados da administração pública, no limite do que permite a Lei e o princípio do sigilo das informações.[153]

Logo após a veiculação de notícias acerca da referida investigação, em 05 de junho de 2018, a Câmara dos Deputados apresentou Projeto de Decreto Legislativo para sustar a Portaria nº 457, de 8 de dezembro de 2016, do Ministério da Fazenda, que "dispõe sobre a disponibilização de acesso, para terceiros, pelo Serviço Federal de Processamento de Dados, a dados e informações que hospeda, **para fins de complementação de políticas públicas**" (grifo nosso).

Já em seus artigos iniciais, assinalava a Portaria que, para que essa disponibilização ocorra, devem ser atendidas algumas condições. Em primeiro lugar, deve haver a anuência do órgão ou entidade, atestando a inexistência de risco institucional ou que afronte ao sigilo do titular do dado. Além disso, o acesso aos dados e informações só poderá ser franqueado a órgãos e entidades que tenham autorização legal para isso, ou ao próprio titular ou à sua ordem (sendo necessária, nesse caso, a identificação inequívoca do destinatário autorizado pelo titular). Por último, a disponibilização de dados agregados deve garantir a não-identificação do titular.

O art. 3º da Portaria, por sua vez, estabelece que "**o Serpro será remunerado diretamente pelos terceiros**, usuários da solução de disponibilização de dados e/ou informações, de modo a ressarcir os valores necessários à sustentabilidade dos sistemas informatizados envolvidos".

Por outro lado, assim como nos questionamentos acerca da legalidade do Decreto de compartilhamento relatados anteriormente, na justificação da proposta de sustação do ato também são suscitados problemas de competência e legalidade.

Inicialmente, o documento relata causar estranheza o fato de o Serpro rechaçar as acusações citando uma Portaria de 2016 como embasamento legal para a prática,

---

153 BRASIL. Serviço de Processamento de Dados. **Nota à imprensa:** Serpro assegura compromisso com o sigilo de dados dos cidadãos brasileiros. Disponível em: <http://serpro.gov.br/menu/imprensa/notas-a-imprensa-1/nota-oficial-01-06-2018> Acesso em 03 ago. 2018.

quando, a investigação do MPDFT aponta a existência de contratos que demonstram que essa prática já vinha sendo exercida anteriormente, como no caso do contrato de 2012 firmado com o Conselho Nacional de Justiça e o de 2013 firmado com o Conselho da Justiça Federal.

Ressalta, ainda, que a norma não atendeu ao princípio da legalidade. A Portaria só apresentou como fundamento a competência do ministro de Estado, prevista no art. 87, p. ún., inc. I, da CF88, para exercer a orientação, coordenação e supervisão dos órgãos e entidades da administração federal na área de sua competência. Assim, não restou demonstrada a autorização legal prévia para que a Administração pudesse autorizar a conduta de disponibilizar dados pessoais a terceiros.

Relevante destacar, também, que a Portaria apresenta disposição que exorbita o poder regulamentar do Ministério da Fazenda. O ato infralegal, ainda que exija a anuência dos demais órgãos ou entidades da APF para a disponibilização de dados a terceiros, dispõe sobre quaisquer bases de dados hospedadas no Serpro (e não somente as do Ministério da Fazenda), extrapolando sua área de competência.

> Analisando detidamente esse ato infralegal, verifica-se claramente que **a norma não possui nenhum amparo legal**. Sequer menciona a lei que embasaria uma medida tão grave e inconstitucional, aplicando referência tão somente à competência constitucional atribuída ao Ministro de Estado da Fazenda de editar normas no âmbito daquela Pasta.
>
> É, por assim dizer, um ato administrativo que busca legitimar, fragilmente, uma conduta absolutamente **desamparada de base jurídica prevista em lei**.
>
> E somente a lei poderia dispor nesse sentido.
>
> Está claro, portanto, que o Ministro da Fazenda agiu em desconformidade com suas atribuições legais e editou **norma que extrapola o poder regulamentar** que este Congresso, através da lei, lhe autorizou fazer: a Lei nº 13.502, de 1º de novembro de 2017.
>
> **Produção de efeito a organização básica dos órgãos da Presidência da República e dos Ministérios, em momento algum autoriza a comercialização, cessão ou compartilhamento de dados pessoais de cidadãos brasileiros a qualquer entidade pública ou privada**[154] (grifo nosso).

[154] BRASIL, Projeto de Decreto Legislativo de Sustação de Atos Normativos do Poder Executivo n. 960/2018. Susta a Portaria nº 457, de 08 de dezembro de 2016, do Ministério da Fazenda, que dispõe sobre a disponibilização de acesso, para terceiros, pelo Serviço Federal de Processamento de Dados, a dados e informações que hospeda, para fins de complementação de políticas públicas. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2177641>. Acesso em: 26 jul. 2018.

Outra denúncia surgiu em agosto de 2018. Reportagens[155] sobre a venda e o uso indevido de dados pelo Serpro foram veiculadas. Com isso, o MPDFT abriu novo inquérito civil público para investigar se três empresas (CredDefense, Certibio e Acesso Digital) comercializam o acesso, para bancos e lojas, de dados biométricos dos brasileiros com o intuito de realizar o reconhecimento facial[156]. O objetivo seria, entre outros, a checagem de identidade de clientes para evitar possíveis fraudes ideológicas.

Segundo o Parquet, a face humana mapeada tecnologicamente é considerada um dado biométrico e, portanto, sensível. Nesse sentido, a Constituição Federal resguarda a inviolabilidade da intimidade, da vida privada, da honra e das imagens das pessoas (art. 5º, inc. X) e o Marco Civil da Internet assegura que os dados pessoais não sejam fornecidos a terceiros, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, inc. VII).

Ocorre que, no caso em apuração, o banco de dados utilizados pela Certibio, com imagens de mais de 70 milhões de brasileiros, conteria informações armazenadas pelo Serpro, a partir das fotos de carteiras de motoristas do Departamento Nacional de Trânsito (Denatran). Essa informação, inclusive, consta de maneira implícita no site da empresa: "O Certibio FaceCheck usa o número do CPF como referência e compara a foto da pessoa, tirada ao vivo, com a foto existente no cadastro de motoristas habilitados, retornando um percentual de similaridade que indica se o CPF informado pertence mesmo ao indivíduo consultado"[157].

Além disso, mais duas preocupações são apresentadas pelo MP: a falta de eficiência da tecnologia atualmente disponível para reconhecimento facial[158] quando se trata dos indivíduos de pele negra e a ausência de critérios transparentes sobre o funcionamento dos algoritmos utilizados pelas empresas. Esses aspectos podem ensejar novas formas

---

155 GOMES, Helton Simões. Bancos e lojas pagam até R$ 4,70 por acesso a dados do seu rosto. **UOL**, 06 ago. 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/08/06/bancos-e-lojas-pagam-ate-r-47-para-acessar-dado-do-rosto-de-brasileiros.htm>. Acesso em: 20 set.. 2018.

156 A técnica de reconhecimento facial já vinha sendo usada também em nível estadual, por exemplo, pela concessionária de metrô de São Paulo, a empresa ViaQuatro. Nesse caso, a Justiça do Estado (processo n. 1090663-42.2018.8.26.0100) proferiu decisão liminar determinando o desligamento dos equipamentos, uma vez que não está clara a exata finalidade da captação das imagens e como esses dados serão tratados. (ver: Justiça de SP proíbe uso de câmeras de reconhecimento facial em painel do Metrô. **G1:** online. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2018/09/14/justica-de-sp-proibe-uso-de-cameras-de-reconhecimento-facial-em-painel-do-metro-de-sp.ghtml>. 14/09/2018. Acesso em 16 out. 2018.)

157 Biometria de face com validação de identidade em 70 milhões de registros. **Certibio.** Disponível em: <https://www.certibio.com.br/noticia-na-integra?id=7>. Acesso em 28 nov. 2018.

158 Não será objeto de análise no presente estudo, mas é de grande valia destacar o primeiro episodio ocorrido no Brasil, em 05 de março de 2019, de prisão após reconhecimento facial por meio de câmeras, durante o carnaval em Salvador, Bahia. (Governo do Estado da Bahia. Secretaria da Segurança Pública. Reconhecimento Facial impede entrada de homicida em circuito. **SSP/BA.** Disponível em: <http://www.ssp.ba.gov.br/2019/03/5310/Reconhecimento-facial-impede-entrada-de-homicida-em-circuito-.html>. Acesso em 06 mar. 2019.)

de discriminação em diversas áreas como "recrutamento de candidatos para vagas de emprego; acesso aos cargos públicos; ingresso em instituições de ensino; filiação a entidades; participação em organizações religiosas, concessão ou negativa de crédito etc." [159].

Por enquanto, as investigações relatadas ainda não ensejaram ações judiciais, nem foram, de fato, comprovadas. As empresas divulgaram notas negando as acusações. A Certibio afirmou que usa apenas a API Datavalid do Serpro para validação dos dados. O Serpro, por sua vez, afirmou que não realiza o repasse de dados, mas oferece serviço que calcula um "percentual de similaridade" com o dado encaminhado pela empresa que contratou o serviço de checagem[160].

Ocorre que há indícios significativos de tais práticas pela Administração Pública, os quais são dignos de investigação e, se for o caso, de responsabilização. Especificamente no segundo caso mencionado, pode-se dizer que a situação é ainda mais alarmante. Diferentemente do primeiro em que haveria a comercialização de dados entre órgãos e entidades da própria APF, no último, o acesso a dados pessoais e sensíveis estaria sendo liberado, sem fundamento legal, a empresas privadas, as quais não visam diretamente à melhoria ou complementação de serviços públicos, mas à obtenção de vantagens competitivas no mercado.

2.4.2 O argumento de sigilo e confidencialidade como óbice para responder quaisquer solicitações de informação

Em relação à Dataprev, os mesmos questionamentos feitos pelo e-SIC ao Serpro foram dirigidos à empresa. Esta, inicialmente informou que "diante das cláusulas de propriedade intelectual e de confidencialidade constantes nos contratos firmados com seus clientes, a Dataprev não está autorizada a disponibilizar as informações solicitadas"[161]. Porém, ao contrário do Serpro, desde logo encaminhou os trechos dos contratos que dispunham sobre o sigilo.

As cláusulas dos contratos que regem as relações jurídicas com os quatro diferentes ministérios e tratam da confidencialidade assim dispunham:

---

159 Portaria nº. 10 /2018, de 15/08/2018, Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e dos Territórios. Disponível em: <http://www.mpdft.mp.br/portal/pdf/noticias/agosto_2018/ICP_Reconhecimento_Facial_Certibio_e_Outras.pdf>. Acesso em 12 out. 2018.

160 Valente, Jonas. MPDFT investiga empresas que vendem serviço de reconhecimento facial. **Agência Brasil.** Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-08/mpdft-investiga-empresas-que-vendem-servico-de-reconhecimento-facial>. Acesso em 28 nov. 2018.

161 Informação obtida com a Empresa de Tecnologia e Informações da Previdência (Dataprev), a partir de consulta realizada pelo Sistema Eletrônico do Serviço de Informação ao Cidadão (Pedido n. 99920004372018460, de 18/04/2018).

a) **Contrato com o MTE:** Cláusula Décima Sétima – Confidencialidade: "*A CONTRATADA compromete-se a manter em caráter confidencial todas as informações, a que tiver acesso ou que lhe seja dado acesso, relativas: a) à política de segurança adotada pelo MTb e configurações de hardware e software decorrentes; b) a processo de instalação, configuração e customização de produtos, ferramentas e equipamentos e atendimento aos itens de segurança adotados pelo MTb; c) a quaisquer dados que venha a ter conhecimento em decorrência da execução dos serviços objeto do presente Contrato".* (Além disso, o contrato também prevê a assinatura de Termo de Compromisso com declaração de manutenção de sigilo e respeito às normas de segurança assinado pelo representante legal do fornecedor e de Termo de ciência da declaração de manutenção de sigilo e das normas de segurança assinado por todos os empregados da contratada envolvidos na contratação).

b) **Contrato com o Ministério do MPDG**: Cláusula Sexta – Da propriedade intelectual: "A propriedade intelectual dos sistemas incluídos no escopo deste Contrato será da Contratante, incluindo a propriedade sobre os dados, código-fonte, documentação de projeto e de usuário, observado o definido na IN 02 da SLTI/MP, de 30/04/2008, e no art. 4 da Lei nº 9.609/98 e as seguintes: (…) c) *a CONTRATADA deve se abster de divulgar ou repassar quaisquer dados e informações, salvo se expressamente autorizado pelas unidades da CONTRATANTE"*

c) **Contrato com o MDS:** "*10.1.11. Zelar e responder pela privacidade e sigilo das informações constantes na base de dados do CadÚnico e tomar medidas para assegurar que as informações de propriedade do CONTRATANTE não sejam divulgadas ou distribuídas pelos empregados ou agentes sob sua responsabilidade. 10.1.12. Não disponibilizar qualquer informação de propriedade do CONTRATANTE por qualquer meio a qualquer terceiro e para qualquer finalidade, sem sua anuência expressa".*

d) **Contrato com o MF:** Cláusula Décima Terceira – Da propriedade intelectual: *"Os dados, informações e sistemas do objeto do Projeto Básico são de propriedade do Ministério da Previdência Social e não podem ser utilizados pela prestadora sem autorização expressa do Gestor do Contrato".*

Pela redação apresentada, entende-se que o sigilo e a confidencialidade dos dados e informações relativas aos contratos dizem respeito àqueles constantes das próprias bases por elas hospedadas ou às ações decorrentes da execução dos contratos. No entanto, parece que as empresas contratadas tendem a se resguardar negando qualquer informação solicitada, até mesmo aquelas que, sendo de caráter estatal, deveriam ser tornadas públicas sem mesmo a necessidade de requisição, em obediência ao princípio da publicidade e visando dar mais concretude à prática da transparência ativa.

O pedido formulado via e-SIC se enquadra nessa situação. Nele, assim como para o Serpro, foi solicitado apenas o nome de cada uma das bases de dados hospedadas, gerenciadas ou tratadas pela Dataprev; indagado se essas bases possuíam dicionário de dados e se elas eram disponibilizadas a terceiros. Entende-se que nenhum desses questionamentos está amparado por restrições de acesso em razão de sigilo negocial, cláusulas de confidencialidade ou de propriedade intelectual, já que não dispõem sobre dados pessoais ou sensíveis.

Ao contrário, pela LAI, "é dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas **ou custodiadas**. (art. 8º, grifo nosso). Conclui-se, assim, que as respostas apresentadas tendem, na verdade, a reforçar a tradicional história brasileira de cultura do sigilo, "tão do agrado da minoria dominante brasileira, sempre receosa do exame livre e crítico de sua conduta pública, muitas vezes tão nociva aos interesses nacionais"[162].

2.4.3 As barreiras na gestão de dados públicos: baixo índice de planejamento, ausência de política de segurança da informação e deficiências no quadro técnico

Além dos casos apresentados, diversas são as notícias de vazamentos de dados pessoais[163]; de comercialização[164] de bancos de dados que deveriam estar exclusivamente sob a gestão de órgãos públicos para terceiros, possibilitando realizar a perfilagem dos

---

[162] RODRIGUES, José Honório. **A pesquisa histórica no Brasil.** 3. ed. São Paulo: Nacional, 1978. p. 133. Disponível em: <http://www.brasiliana.com.br/obras/a-pesquisa-historica-no-brasil/pagina/133/texto>. Acesso em: 16 out. 2018.

[163] Ver exemplos em: Fenafar. **Vazamento de dados do E-Saúde expõe informações de milhões de brasileiros.** Disponível em: < http://www.fenafar.org.br/2016-01-26-09-32-20/saude/1992-vazamento-de-dados-do-e-saude-expoe-informacoes-de-milhoes-de-brasileiros>; Agência Brasil. **AGU pede investigação sobre vazamento de dados da Petrobras.** Disponível em: <http://agenciabrasil.ebc.com.br/politica/noticia/2014-04/agu-pede-investigacao-sobre-vazamento-de-dados-da-petrobras>; MEC. **Ministro adia exame e Polícia Federal vai apurar o vazamento** <http://portal.mec.gov.br/index.php?option=com_content&view=article&id=14403:ministro-adia-exame-e-policia-federal-vai-apurar-o-vazamento&catid=201>.; Gazeta do Povo. **Financeiras acessam dados sigilosos de aposentados para empurrar empréstimos** <http://www.gazetadopovo.com.br/blogs/lucio-vaz/2017/06/12/financeiras-acessam-dados-sigilosos-de-aposentados-para-empurrar-emprestimos/>; Saúde no Ar. **Dados pessoais de usuários do Cartão do SUS vazam na internet.** <http://www.portalsaudenoar.com.br/dados-pessoais-de-usuarios-do-cartao-do-sus-vazam-na-internet/>; Diário de Pernambuco. **Vazamento no INSS: seus dados pessoais podem estar em mãos erradas.**<http://blogs.diariodepernambuco.com.br/espacodaprevidencia/vazamento-no-inss-seus-dados-pessoais-podem-estar-em-maos-erradas/> (Acessos em: 18 fev. 2018).

[164] Ver exemplos em: G1. **Dados sigilosos são vendidos para bancos, financeiras e até advogados** <http://g1.globo.com/jornal-nacional/noticia/2017/08/dados-sigilosos-sao-vendidos-para-bancos-financeiras-e-ate-advogados.html>; IstoÉ.PF deflagra operação que apura comercialização de dados internos da Receita. <https://istoe.com.br/pf-deflagra-operacao-que-apura-comercializacao-de-dados-internos-da-receita/>. (Acessos em: 18 fev. 2018).

indivíduos para variados fins; de pagamentos indevidos[165] de benefícios sociais em razão das dificuldades nos cruzamentos de dados entre os diferentes sistemas e órgãos ou entidades da Administração Pública; de crimes cibernéticos[166]; entre outros[167].

Diante dessas ocorrências, as pessoas temem que seus dados parem nas mãos de terceiros não autorizados e sejam utilizados para fins não legítimos em razão de, por exemplo, falhas na segurança das redes e dos sistemas dos órgãos e entidades do Poder Público. Tudo isso demonstra os problemas ou desafios na gestão dos dados, como a falta de planos e planejamento de TI, ausência de políticas de segurança da informação, entre outros.

Nessa direção, acórdãos do Tribunal de Contas da União (TCU) também apontam a necessidade de melhorias na política de segurança da informação dos órgãos e a correção de vulnerabilidades nos sistemas, como no caso do sistema do CadÚnico, onde foram identificadas evidências tais como:

> Procedimentos não padronizados relativos à segurança; Deficiência nos controles internos; Dificuldade de responsabilização; Possibilidade de inclusão de famílias e/ou alteração de dados de forma indevida; Risco de acessos não autorizados e vazamento de dados e informações; Comprometimento do processo de disseminação da cultura de segurança da informação para os usuários do CadÚnico, Siiso e Sibec.
>
> (trecho do Acórdão TCU nº 906/2009 - Plenário. Relator: Augusto Nardes)

O Tribunal recomenda ainda atenção aos princípios da eficiência e da economicidade e realização de estudo técnico de avaliação qualitativa e quantitativa do quadro de TI

---

165 Ver exemplos em: O Globo. **Governo suspende R$ 9,3 bi em benefícios indevidos** < https://oglobo.globo.com/economia/governo-suspende-93-bi-em-beneficios-indevidos-21505260>; Estadão. **CGU acha R$ 1,3 bi em 'pagamentos indevidos' no Bolsa Família** <http://politica.estadao.com.br/blogs/fausto-macedo/cgu-acha-r-13-bi-em-pagamentos-indevidos-no-bolsa-familia/>; Fenacon. **Ministério do Trabalho aperta cerco contra fraudes em benefícios sociais** http://fenacon.org.br/noticias/ministerio-do-trabalho-aperta-cerco-contra-fraudes-em-beneficios-sociais-1430/?utm_source=akna&utm_medium=email&utm_campaign=Press+Clipping+Fenacon+-+24+de+janeiro+de+2017. (Acessos em: 18 fev. 2018).

166 Ver exemplos em: PSafeBlog. **Sistema vulnerável do governo brasileiro permite invasão de hackers**.<http://www.psafe.com/blog/hackers-phishing-invadir-sistema-governo-brasileiro/>; G1. **Veja lista de sites do governo afetados por onda de ataques virtuais.** <http://g1.globo.com/tecnologia/noticia/2011/06/veja-lista-de-sites-do-governo-afetados-por-onda-de-ataques-virtuais.html>; **TechTudo. Brasil é o país com mais ataques hacker a sites do governo, diz pesquisa.** <http://www.techtudo.com.br/noticias/noticia/2014/11/brasil-e-o-pais-com-mais-ataques-hacker-sites-do-governo-diz-pesquisa.html>. (Acessos em: 18 fev. 2018).

167 Ver exemplos em: G1. **TSE firma acordo para repassar dados de eleitores à Serasa** <http://g1.globo.com/politica/noticia/2013/08/tse-firma-acordo-para-repassar-dados-de-eleitores-serasa.html>; Portal da Câmara. **Comissão especial debate comercialização de dados pessoais nesta tarde** <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/526953-COMISSAO-ESPECIAL-DEBATE-COMERCIALIZACAO-DE-DADOS-PESSOAIS-NESTA-TARDE.html>. (Acessos em: 18 fev. 2018).

para futuros pleitos de recomposição e concursos. Em relação ao perfil de governança e gestão na área de TI da APF, o TCU realiza levantamento a cada dois anos, baseado em questionários, com informações declaratórias.

Assim, no Relatório Sistêmico de Fiscalização de TI de 2014, foram avaliadas 355 organizações, dentre as quais, 214 integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), do Poder Executivo Federal. Resultados significantes podem ser extraídos em relação à eficiência na gestão de TI pela Administração Pública, o que abrange a gestão de dados:

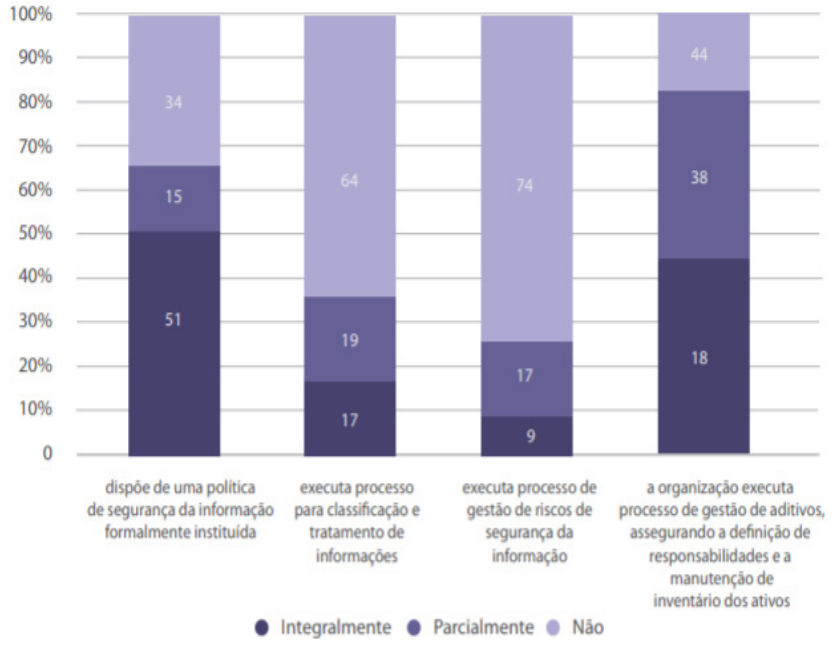
> Acerca dos documentos de planejamento mais relevantes, ainda surpreende que 16% das organizações não possuam processo de planejamento institucional. Já **em relação ao planejamento de TI, 25% não adotam processo de planejamento de TI (PPTI)**, embora 67% disponham de um plano vigente. Em outros termos, as ausências mencionadas significam que **há risco elevado de que os projetos e atividades executados pela área de TI não estejam correlacionados com as prioridades da instituição**, ou pior, de que essas prioridades não estejam suficientemente claras aos envolvidos.
>
> Sobre o atendimento das áreas de TI, nota-se que ainda há muito por fazer no chamado processo de informatização do setor público. **Apenas 42% das organizações suportam os principais processos de negócio por meio de sistemas informatizados.**
>
> Já em relação aos usuários, **em 57% das organizações não há qualquer catálogo com os sistemas disponíveis**, o que pode limitar a atuação dos servidores e empregados públicos[168]. (grifo nosso)

Novamente, dados alarmantes referem-se ao quesito segurança da informação, considerada pelo TCU como "uma das áreas com adoção mais baixa de boas práticas". De acordo com o Relatório, 34% das instituições não possuíam uma política de segurança da informação, com definições de responsabilidades e eventuais sanções. Apenas 17% classificavam suas informações, expondo a instituição a risco de divulgar ou expor documentos indevidamente, já que, de acordo com a Lei de Acesso à Informação, a publicidade é a regra; o sigilo, a exceção. E, em relação a gestão de riscos, apenas 9% possuíam processos de gestão nessa área (ver Figura 1).

---

[168] BRASIL. Tribunal de Contas da União. **Relatório sistêmico de fiscalização de tecnologia da informação.** Brasília: TCU, 2015. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/sumario-relatorio-sistemico-de-fiscalizacao-de-tecnologia-da-informacao-fiscti.htm>. Acesso em: 10 ago. 2018.

Figura 1 – Práticas de segurança da informação na Administração Pública Federal



Fonte: Tribunal de Contas da União. **Relatório sistêmico de fiscalização de tecnologia da informação.** Brasília: TCU, 2015, p. 39.

Ainda sobre o fator segurança da informação, cabe destacar importante distinção feita por Bambauer[169]. Para ele, a segurança dos dados (ou da informação) está diretamente associada às soluções tecnológicas necessárias para a implementação das escolhas e decisões normativas sobre os critérios de privacidade da informação definidos pelas instituições. Em contrapartida, os critérios de privacidade seriam apenas uma espécie de quadro normativo sobre quem pode legitimamente acessar ou alterar determinadas informações.

Assim, muitas vezes as Cortes Jurídicas e demais operadores do Direito tendem a confundir privacidade e segurança, quando na verdade, essas duas questões deveriam ser objeto de análises e decisões distintas, apesar de complementares. O autor explica que as discussões sobre segurança dos dados são, em geral, técnicas, o que pode gerar uma assimetria de informações. Além disso, as decisões sobre a arquitetura da segurança envolvem escolhas (de acordo com os critérios estabelecidos pela privacidade) que estão sempre associadas a custos. Nesse sentido, são as opções feitas entre as diferentes arquiteturas de segurança[170] que tornam os regimes mais ou menos sustentáveis. Por consequência, as falhas de segurança devem ser apenadas mais prontamente e com mais intensidade que os problemas de privacidade.

---

169 BAMBAUER, Derek E. **Privacy Versus Security**. The Journal of Criminal Law & Criminology, v. 103, n. 3, 2013, p. 667/684.

170 Sob esse aspecto, destacam-se as denominadas *Privacy Enhancing Technologies – PET* (ou tecnologias de

Nesse quesito, é importante, também, destacar a posição do especialista Paul Ohm. Para ele, não se trata apenas da arquitetura de segurança. Com a descoberta, pelos cientistas de dados, de que a anonimização é uma solução tecnológica extremamente falha, os problemas de privacidade se ampliaram. O "robusto pressuposto de anonimização" ("robust anonymization assumption"), que justificava indevidamente o armazenamento perpétuo e o compartilhamento indiscriminado de dados, não serve mais para garantir a privacidade[171]. Não importa o quanto o administrador de dados faça para anonimizar os dados, alguém que tenha informações externas corretas poderá, a partir da utilidade residual de dados, revelar outras informações, ou seja, a anonimização perfeita é impossível[172].

Hoje, é possível reidentificar ou desanonimizar dados com bastante facilidade. Assim, caso se queira proteger a privacidade, será necessário, invariavelmente, reduzir o fluxo de informação na sociedade, mesmo que valores como inovação, liberdade de expressão e segurança estejam em jogo[173]. Trata-se de uma relação direta entre utilidade e privacidade. Apesar de reconhecer que técnicas como agregação, controles de acesso e auditorias reduzem o risco de reidentificação, o autor ressalta que elas não coincidem com as promessas de privacidade. Além disso, são mais lentas, complexas e caras do que a simples anonimização[174].

Além da segurança da informação, outra característica de notório conhecimento em relação ao princípio da eficiência é que ele está diretamente associado à capacidade e qualidade técnica e especializada das equipes de TI. O aumento vertiginoso de dados e informações a serem trabalhados necessitam de métodos eficientes para sua interpretação e resposta adequada. Saber coletar, armazenar e analisar dados para gerar valor e melhorar políticas públicas, com celeridade e transparência, obedecendo aos parâmetros legais, requer profissionais com alta qualificação.

Sob esse aspecto, pela primeira vez, também em 2014, o TCU realizou levantamento para traçar o perfil de pessoal de TI na Administração Pública Federal. A despeito da criação de carreira específica para a área, qual seja a de Analista de Tecnologia da Informação (ATI), em 2009, segundo o relatório, em relação ao Poder Executivo, de

---

aprimoramento da privacidade, em tradução livre), como as soluções para garantir o anonimato ou o segredo das comunicações, a encriptação, a certificação eletrônica, entre outras.

171 OHM, Paul. **Broken Promises of Privacy**: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: <https://ssrn.com/abstract=1450006>. Acesso em: 14 mar 2019. P. 1706.

172 Ibid, p. 1742.

173 Idem, p. 1706.

174 OHM, Paul. Op. cit. p. 1751.

um total de 1,15 milhão de servidores efetivos, apenas 53,6 mil são das áreas de TI (4,7%), sendo 60,6% (32.529) do quadro efetivo. Esse valor representa 2,8% do total de efetivos.

Além da deficiência no quantitativo de pessoal, o relatório indicou que a baixa remuneração, comparada a de outros cargos da Administração Pública, é uma das principais causas da rotatividade de pessoal nessa área. No entanto, "as principais ações adotadas são voltadas para o incentivo à qualificação, demonstrando falta de sintonia entre o problema existente e a solução apresentada."[175] Isto posto, destaca-se fragmento do voto condutor do seguinte acórdão:

> 5. Como resultado do levantamento, constatou-se que a estrutura de recursos humanos de TI da APF, de forma geral, apresenta problemas, notadamente quanto à falta de cargos e carreiras específicas; à carência de pessoal especializado para gestão de TI; à ocupação de cargos de gestão por pessoas estranhas ao quadro, como requisitados, temporários e até mesmo terceirizados; à ausência de planejamento para preenchimento contínuo de vagas de TI; à dificuldade de retenção de pessoal especializado; à política de qualificação executada sem o devido planejamento e, em alguns casos, à atuação tímida dos OGSs [órgãos governantes superiores] na identificação e solução dos problemas. (Acórdão 1.200/2014 – TCU – Plenário)

Como se pôde observar, a Administração Pública sofre diversas limitações de ordem técnica e operacional; limitações de pessoal; além de limitações legais (para não adentrar no mérito das limitações orçamentária-financeiras) na realização de políticas públicas eficientes, capazes de utilizar todos os recursos atualmente disponíveis no setor privado.

Apesar das melhorias e de iniciativas exitosas, na área de governança de TI que utilizam ferramentas de TI modernas e atualizadas, como computação em nuvem e mineração de dados, o setor público ainda tem muito o que melhorar. Porém, frisa-se, diante de tantos recursos tecnológicos disponíveis na atualidade, esses limitadores não devem constituir empecilho para o planejamento e a execução de políticas públicas mais eficientes que visam sanar os diversos problemas da sociedade.

---

[175] BRASIL. Tribunal de Contas da União. **Relatório sistêmico de fiscalização de tecnologia da informação.** Brasília: TCU, 2015. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/sumario-relatorio-sistemico-de-fiscalizacao-de-tecnologia-da-informacao-fiscti.htm>. Acesso em: 10 ago. 2018.

3 A proteção de dados pessoais e sensíveis como direito da personalidade e os impactos nas políticas públicas diante das novas disposições legais

O desafio regulatório na era digital e na sociedade do conhecimento perpassa diversas questões éticas e impactantes para as políticas públicas. Por um lado, deve ser capaz de encorajar a implantação de mecanismos de proteção dos dados pessoais e sensíveis como direitos da personalidade e de ser aplicada para gerações futuras. De outro, deve buscar garantir o desenvolvimento da economia e das políticas públicas, de tal forma que não seja muito restritiva e engesse as possibilidades de inovação dentro do Poder Público ou demasiadamente genérica e principiológica de modo que seja inócua e continue demandando a judicialização das diversas questões.

Vale dizer, ainda, que, apesar da existência da LAI e de outras normas terem grande importância para estabelecer "contornos mínimos" para a proteção de dados pessoais sob o domínio e guarda de órgãos públicos (art. 31, da LAI), um marco normativo para proteção de dados, como o recentemente sancionado, era indispensável.

Como afirma Doneda[176], o mais usual na maioria dos países é a existência de normas com regras específicas sobre transparência e, paralelamente, uma norma geral sobre a proteção de dados pessoais. No caso brasileiro, esse processo ocorreu de maneira diferente: a LAI foi promulgada sem a coexistência de uma norma de caráter geral, provocando desequilíbrio "ante a carência de regras específicas e dinâmicas capazes de fornecerem soluções para questões que envolvam transparência e privacidade"[177].

> Eu acredito que este era um passo indispensável ante a marcante ausência de uma legislação sobre proteção de dados e que a implementação da LAI neste particular teve como consequência um notável aumento da consciência a respeito da necessidade de proteção de informação pessoal com regras mais claras e específicas, seja para a proteção do cidadão, seja para a maior harmonização e clareza quanto às práticas de transparência que envolvam informações pessoais[178].

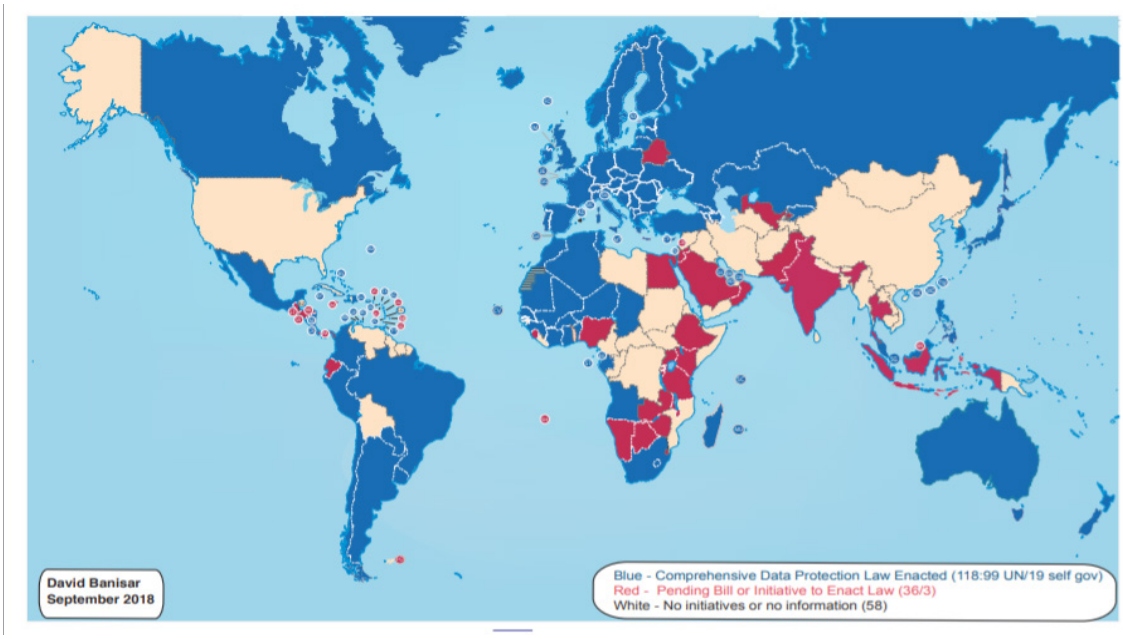
[176] DONEDA, Danilo. **Proteção de Dados Pessoais e LAI.** [13 jun. 2017] Brasília, CGU. Entrevista concedida ao site Governo Aberto – CGU. Disponível em: <http://www.governoaberto.cgu.gov.br/noticias/2017/protecao-de-dados-pessoais-e-lai.> . Acesso em: 05 ago. 2018.

[177] Ibidem, s/pag.

[178] Idem, s/pag.

Agora, com a aprovação da Lei Geral de Proteção de Dados Pessoais, o Brasil se insere no rol dos mais de cem países no mundo que já possuem regulamentação sobre o tema. Conforme explica o autor da ilustração (Figura 2), as leis nesses países disciplinam as informações pessoais em meio eletrônico e físico e a todas (ou quase todas) temáticas. Em quase todos os países, as leis se aplicam, indiscriminadamente, a órgãos privados e estatais. Atualizado em setembro de 2018, é possível observar no mapa a inserção do Brasil, Bahrein e São Cristóvão e Névis como países que adotaram leis ainda naquele ano.

Figura 2 – A regulamentação de proteção de dados pessoais e sensíveis no mundo



Fonte: Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (27 set. 2018). Disponível em SSRN: https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416. Acesso em: 10 nov. 2018.

(Legenda: Em azul, países que possuem lei de proteção de dados vigente. Em vermelho, países que possuem projetos de lei de proteção de dados em andamento; Em branco, países que não possuem iniciativas para edição de lei de proteção de dados ou essa informação é desconhecida.

A nova lei brasileira considerou a proteção de dados como um dos paradigmas da dignidade humana, nos moldes do Regulamento Geral de Proteção de Dados da União Europeia (RGPD). Neles, considera-se os direitos da personalidade como projeção da dignidade humana e a proteção de dados como espécie daquele. Assim, elementos como consentimento informado e legítimo interesse, além do princípio da finalidade, por exemplo, são parâmetros utilizados para preservar a autonomia da vontade e o controle, pelos cidadãos, do uso dos dados e informações a seu respeito, como será visto adiante.

3.1 A evolução normativa e a construção do entendimento da proteção de dados pessoais como direito da personalidade

Os modelos de proteção de dados se dividem basicamente em dois: os mais restritivos e os mais ampliativos, de acordo com o grau de preocupação que determinado país – e sua população - tem em relação ao uso que é feito com os seus dados pessoais e sensíveis. Mais uma vez vem à tona a dicotomia privacidade *versus* publicidade e transparência que, no caso brasileiro, já pode ser observada na Carta Magna, em seu art. 5º, que trata dos Direitos e Garantias Fundamentais e dispõe:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.
>
> LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem.

Além desses dispositivos, por vezes, outras garantias e princípios constitucionais, como as liberdades de expressão (art. 5º, inc. IX e art. 220) e de informação (art. 5º, inc. XIV, XXXIII e XXXIV e art. 220) e a inviolabilidade do sigilo de dados (art. 5º, inc. XII), por exemplo, também são colidentes com a privacidade. No caso específico da Administração Pública, a Constituição destaca, no art. 37, a publicidade como um dos preceitos a serem obedecidos, tornando ainda mais evidente essa problemática no cotidiano do serviço público.

Por fim, como garantia para "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público", bem como para retificação de tais dados, a Lei Maior consagrou o *habeas data* (art. 5º, LXXII, CF88).

Contudo, destaca-se que, no Brasil, esse remédio surgiu no contexto da redemocratização brasileira, mas tem demonstrado "reduzida importância prática"[179] em razão, por exemplo, da superação da situação política anterior, em que se observava o uso do sigilo como forma de cometimento de violências e arbitrariedades pelas autoridades políticas (especialmente pelo então Sistema Nacional de Informações – SNI, órgão existente de 1964 a 1990 com objetivo de coordenar as atividades de informações e contrainformações do Estado).

[179] DALLARI, Dalmo de Abreu. **O habeas data no sistema jurídico brasileiro.** Revista Da Faculdade De Direito, Universidade De São Paulo, *97*, 239-253. Disponível em: <https://doi.org/10.11606/issn.2318-8235.v97i0p239-253>. Acesso em: 25 set. 2018.

Além disso, há críticas ao *habeas data* no Brasil pelo fato de: a) seu objeto também poder ser arguido por meio de Mandado de Segurança; b) constar exceção para o fornecimento dos dados quando eles forem de "uso privativo do órgão ou entidade produtora ou depositária das informações" (art. 1º, p. ún)[180]; c) os tribunais rejeitarem liminarmente os pedidos impetrados por terceiros por entenderem que se trata de direito personalíssimo[181]. Diante desses motivos, é nítida a percepção de que houve um esvaziamento do conteúdo desse instituto. E, com isso, ele não conseguiu, de fato, atingir a proteção de dados pessoais.

Em relação a leis infraconstitucionais, o Código Civil[182] também faz menção aos direitos da personalidade em seu capítulo II, sendo que, especificamente nos artigos 20 e 21, remete à inviolabilidade da vida privada da pessoa natural e às restrições de divulgação quando são atingidas a honra, a boa fama ou a respeitabilidade de um indivíduo. O Código de Defesa do Consumidor, por sua vez, menciona especificamente o acesso e retificação de informações constantes dos bancos de dados e cadastros de consumidores.

Anos mais tarde, a LAI trouxe uma mudança de paradigma, apresentando diferenças substanciais quanto à classificação do que seria informação pública, sigilosa e restrita e evidenciou a diretriz da publicidade como regra e do sigilo como exceção. Além disso, trouxe um "micro-estatuto" de proteção de dados pessoais em seu art. 31, reforçando que: "o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" [183].

Ainda conforme a LAI, as informações pessoais devem ter seu acesso restrito a agentes públicos legalmente autorizados e à pessoa a quem elas se referirem. Ademais, salvo as exceções previstas no § 3º do referido dispositivo[184], a divulgação ou o acesso

---

180 BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, DF. Disponível em: <http://www.planalto.gov.br/CCivil_03/LEIS/L9507.htm>. Acesso em: 20 set. 2018.

181 DALLARI, Dalmo de Abreu. **O habeas data no sistema jurídico brasileiro.** Revista Da Faculdade De Direito, Universidade De São Paulo, *97*, 239-253. Disponível em: <https://doi.org/10.11606/issn.2318-8235.v97i0p239-253>. Acesso em: 25 set. 2018., p. 246.

182 Há críticas, no entanto, sobre o tratamento "excessivamente rígido e puramente estrutural" conferido aos direitos da personalidade pelo Código Civil, tornando de difícil aplicação as soluções previstas para os problemas da atualidade. Para o assunto, ver: SCHREIBER, Anderson. **Direitos da Personalidade.** Rio de Janeiro: Atlas, 2011. p. 1-30.

183 DONEDA, Danilo. **Proteção de Dados Pessoais e LAI.** [13 jun. 2017] Brasília, CGU. Entrevista concedida ao site Governo Aberto – CGU. Disponível em: <http://www.governoaberto.cgu.gov.br/noticias/2017/protecao-de-dados-pessoais-e-lai.> . Acesso em: 05 ago. 2018.

184 As disposições a seguir dispensam a necessidade do consentimento expresso do titular dos dados: "I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única

por terceiros de tais informações só poderão ocorrer caso estejam previstos em lei ou tenha havido consentimento expresso do titular dos dados.

Com o uso cada vez mais facilitado da rede mundial de computadores, num país progressivamente digital, o Marco Civil da Internet[185] (e o Decreto nº 8.771/2016 que o regulamentou) foi mais uma norma que tentou regular a oposição liberdade de expressão e privacidade. Visando garantir a privacidade dos indivíduos, dispôs sobre o Princípio da Retenção Mínima de Informações para a coleta, armazenamento e tratamento dos dados, tendo como barreira a finalidade para a qual os dados foram coletados. Não tratou, todavia, dos dados sensíveis ou anônimos e nem da proteção de dados fora do âmbito da internet (como informações sobre cartões de crédito, planos de saúde, entre outros).

Observa-se, assim, que até aquele momento, apesar de diversos indicativos, não havia uniformidade na compreensão acerca de como deveria se dar a proteção de dados pessoais no Brasil e, por vezes, os diferentes setores, seja privado, seja público, ou até mesmo os próprios indivíduos, não sabiam como se portar ou reconhecer quais eram seus direitos e deveres, para poder exercê-los ou reivindicá-los.

Apesar da grande quantidade de dispositivos e normas que tratavam do tema, não havia no país uma lei geral capaz de disciplinar e orientar os diversos casos que se apresentavam, ocasionando mais abusos por parte das empresas ou até mesmo do Estado na utilização dos dados dos cidadãos.

A discussão não era nova, mas os avanços tecnológicos, aliados às notícias de mau uso, uso indevido, comercialização ou mesmo vazamentos de dados pessoais e sensíveis, impulsionavam cada vez mais as discussões sobre o assunto, já que poderiam gerar graves prejuízos políticos, no caso do setor público, além de ações de danos morais, perda de confiança e de credibilidade em relação, também, às instituições privadas.

Nesse contexto, ainda que não abertamente, o debate da proteção de dados pessoais e sensíveis sempre foi permeado pela "necessidade de fixar o sentido e o alcance da ideia de dignidade humana em termos práticos", bem como seu conteúdo mínimo, que inclui três elementos: o valor intrínseco de cada ser humano, a autonomia individual

---

e exclusivamente para o tratamento médico; II - 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; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante".

185 BRASIL. Lei nº Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 set. 2018.

e o valor comunitário[186], tomando sempre a pessoa como um fim (sujeito de direitos) e não como meio (reduzindo-a à condição de objeto)[187].

A partir dessa definição, seria possível passar para o nível seguinte, tentando-se estabelecer o conteúdo do direito à privacidade e o seu âmbito de proteção jurídica. Só então seria possível definir se a proteção de dados pessoais e sensíveis integraria o direito à privacidade, que é espécie dos direitos da personalidade e que, por sua vez, são abrangidos pela dignidade humana.

Para Barroso, a dignidade humana é um valor fundamental e princípio constitucional que funciona como "fundamento jurídico-normativo dos direitos fundamentais" e que, na maioria dos casos, deve ter precedência sobre os demais, devendo ser limitada apenas em face de restrições legítimas decorrentes de valores sociais ou de interesses estatais, ou seja, comunitários. Sabe-se que o uso indiscriminado do conceito de dignidade humana e, consequentemente, dos direitos da personalidade pode acarretar a sua banalização. Ao mesmo tempo, seu conteúdo não é rígido e "deve ser apreendido por cada sociedade em cada momento histórico, a partir de seu próprio substrato cultural"[188].

Paralelamente, o direito à privacidade está relacionado ao senso de individualidade e à necessidade de autonomia do indivíduo, ou seja, ao desejo de evitar ser manipulado ou dominado por outros. Segundo Bessa, é um conceito vago, ambíguo e controvertido. "Na verdade, a necessidade humana de não compartilhar com outros - ou de restringir a pessoas mais próximas - alguns fatos, desejos e informações pessoais é tão patente que o senso comum considera a privacidade, ao contrário do que defendem os estudiosos, um valor em si mesmo"[189].

Assim, na atualidade, frente às novas tecnologias, o uso descomedido e a exposição desregrada dos dados e informações pessoais por empresas e governo acabou se tornando motivo suficiente para buscar a proteção dos dados pessoais e sensíveis dos indivíduos, inclusive, tornando-a uma política pública merecedora de destaque na agenda do dia. Conforme Doneda, a proteção da privacidade, nesse contexto, não se restringiria mais à garantia de "isolamento e segredo", mas fora expandida para uma perspectiva de controle da circulação e do uso que outras pessoas fazem acerca das informações pessoais do titular[190].

---

186 BARROSO, Luis Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 9-87.

187 SCHREIBER, Anderson. **Direitos da Personalidade**. Rio de Janeiro: Atlas, 2011. p. 7.

188 Ibidem, p. 8.

189 BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de protecão ao crédito**. São Paulo: Revista dos Tribunais: 2003, p. 88.

190 DONEDA, Danilo Cesar. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Disponivel em http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm#_

E esse acabou sendo, também, o entendimento brasileiro para legislar acerca da matéria, buscando conferir maior controle pelo próprio individuo sobre a circulação de dados e informações que lhe dizem respeito. Ao longo dos anos, por meio da construção normativa, doutrinária e jurisprudencial, os debates foram se moldando. E o Brasil acabou optando por seguir o padrão europeu, que entende a proteção de dados como um direito da personalidade, atrelado ao princípio da dignidade da pessoa humana, fundamento do Estado Democrático de Direito da República Federativa do Brasil (art. 1º, inc. III, da CF88). Resultou, assim, na edição da Lei nº 13.709, de 14 de agosto de 2018.

3.2 A adoção do modelo europeu como parâmetro para a legislação brasileira e suas principais divergências

Seguindo os moldes de classificação das gerações ou dimensões dos Direitos Humanos, Doneda, ao tratar da proteção de dados pessoais e sensíveis, fala, também, em "gerações de leis"[191]. Segundo ele, o contexto da doutrina da privacidade teve início com o individualismo exacerbado, no contexto do direito a ser deixado só, de Warren e Brandeis. Essa característica, ainda que mantida, evoluiu para uma nova noção de privacidade que tinha a própria sociedade democrática como requisito para outras liberdades fundamentais, superando, também, uma característica estritamente patrimonialista e elitista para ter uma abrangência maior.

Porém, a sociedade foi se tornando mais complexa, os fluxos de informação mais importantes, e os interesses do Estado nos dados cada vez maiores a fim de buscar mais controle e eficiência em sua administração. Nesse contexto, surgiram os censos e pesquisas estatais, que, nos Estados Unidos, por exemplo, na década de 1960, passaram a coletar dados sobre as habitações privadas dos cidadãos norte-americanos, e nos anos 70, sobre o motivo do rompimento dos seus matrimônios, se fosse o caso. Havia, assim, coleta de dados sobre os detalhes íntimos e da vida privada dos cidadãos. "A hipótese que explica o porquê desta crescente forma de invasão é o fato de que simplesmente tornou-se factível, para a tecnologia da época, processar estas informações e delas extrair alguma utilidade – e o que era novo não era a utilidade, mas o fato de sua obtenção ter sido tornada possível"[192], situação a qual Doneda chama de "vontade da técnica".

ftn1 > Acesso em: 15 out. 2018.

[191] Sobre as 4 gerações das leis de proteção de dados pessoais, ver: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 183-217.

[192] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 9-10.

O caso ocorrido nos Estados Unidos é um dos paradigmas para o entendimento atual da proteção de dados pessoais no mundo. Em 1965, o *Bureau of Budget* (espécie de Departamento responsável pelo orçamento) propôs, em nome da eficiência e racionalização administrativa, a construção de uma central única de armazenamento de informações pessoais, o *National Data Center*, a fim de reunir todos os bancos de dados da administração federal em um único local. Esse banco de dados centralizado incluiria os dados do censo, trabalhistas, fiscais e da previdência.

A proposta alarmou diversos setores da sociedade apenas pela potencial ameaça de violação à privacidade; de um controle invisível, de uma concentração de poder nas mãos de poucos, de uma supervigilância estatal[193]. Assim, o Congresso Nacional realizou audiências para tratar do tema e se pronunciou contrariamente à proposta, tendo sido encerrado o projeto.

Na década de 70, diante da percepção de que os direitos e liberdades fundamentais estariam ameaçados em razão da coleta ilimitada de dados pessoais para a criação de grandes bancos de dados e seu controle *a posteriori* por órgãos públicos, surgiram as primeiras iniciativas legislativas para a tutela de dados pessoais (na Alemanha, Suécia e Estados Unidos). Trata-se da 1ª geração de leis sobre a matéria. Em geral, elas dispunham sobre o processamento dos dados e não sobre a privacidade propriamente dita. Assim, com a evolução tecnológica e a multiplicação dos centros de processamento de dados, elas rapidamente se tornaram obsoletas.

No final da década de 70, então, começaram a surgir as leis que visavam à proteção dos dados pessoais, chamadas leis de 2ª geração. Objetivando eliminar a insatisfação

---

193 Segundo Bolzan de Morais, o Estado de Direito superou a "era de acesso" (à informação), passando para a "era da quantificação" (de dados), edificada sob um "capitalismo de serviços baseado em plataformas", que contribui para a chamada ***new surveillance***. Essa moderna forma de *suverllaince*, a *dataveillance,* existente numa *"sociedade de sensores"* (que vai além da mera vigilância, pois abarca as novas formas de relações sociais permitidas com o uso da tecnologia, com características como a hiperconectividade, a chamada revolução 4.0, a alta capacidade de produção, armazenamento e tratamento de dados, observação monitorada, identificação e rastreamento, intervenção analítica e modulação de comportamentos), segundo o autor, foi realçada após o atentado de 11 de setembro (2001), nos Estados Unidos, com a ampliação da coleta de dados e o objetivo de garantir mais segurança à população. Nesse sentido, pode-se dizer que era feito um *trade-off* entre a segurança e a privacidade. As pessoas optaram por abrir mão de sua liberdade e privacidade, numa "servidão voluntária", em troca de uma aparente segurança. E essa situação, após as denúncias de Edward Snowden e do caso Facebook/Cambridge Analytica, tornou ainda mais evidente a *new surveillance.* Mais que isso, a nova estrutura arquitetural, além de afetar a *privacy*, é capaz de promover uma "espécie de *social sorting* ou, por outro viés, de *digital discrimination*" (BOLZAN DE MORAIS, Jose Luis. **O Estado de Direito "confrontado" pela Revolução da Internet!** Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, RS, v. 13, n. 3, p. 876-903, dez. 2018. ISSN 1981-3694. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/33021>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.5902/1981369433021, p. 885/887 e 891/892 e DE MENEZES NETO, Elias Jacob; DE MORAIS, Jose Luis Bolzan. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. Novos Estudos Jurídicos, [S.I], v. 23, n.3, p. 1129-1154, dez. 2018. ISSN 2175-0491. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/13769>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.14210/nej.v23n3.; p. 1132, 1136/1137)

dos cidadãos que não tinham mecanismos adequados para exercer seus direitos e tutelar seus interesses, elas continham uma estrutura baseada na privacidade como uma liberdade negativa, ou seja, que deveria ser exercida pelo próprio indivíduo (é o caso da França e da Áustria, por exemplo).

Ocorre que, já na década de 80, percebeu-se que apenas a tutela individual dos direitos previstos nas leis de 2ª geração não era suficiente. O fornecimento dos dados pessoais pelo indivíduo consistia em:

> requisito indispensável para a sua efetiva participação na vida social (…) e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão – ou seja, a atuação direta da 'liberdade' do cidadão de interromper o fluxo para o exterior de suas informações pessoais – implicava não raro a sua exclusão de algum aspecto da vida social, ou em algum tipo de prejuízo mensurável[194].

Assim, surgiram as leis de 3ª geração, nas quais a tutela continuava centrada no cidadão, porém, "proporcionando o efetivo e pleno exercício da autodeterminação informativa" (emendas às leis da Alemanha, Suécia, além da Noruega e Finlândia), com a participação ativa do cidadão não apenas no momento do fornecimento dos dados, mas durante todo o processo de tratamento. Mesmo com a inserção de ferramentas efetivas que visavam à autodeterminação informativa, era apenas uma minoria que optava e tinha condições de enfrentar os custos – tanto econômicos, quanto sociais - de exercer tais direitos.

Foi nesse período que ocorreu um caso paradigmático na Alemanha, quando, em 1983, o Tribunal Constitucional da Alemanha declarou parcialmente inconstitucional uma lei que disciplinava o censo populacional:

> Havia previsão de uma ampla coleta de dados na Alemanha. Aquele que se recusasse a responder a todas as perguntas teria de arcar com pesadas multas. Pretendia-se não apenas a elaboração de quadro estatístico e demográfico, mas também a formação de banco de dados para posterior confronto com outros já existentes em agências federais e estaduais, permitindo-se a correção de informações armazenadas anteriormente, bem como a utilização das novas informações para determinados objetivos, vinculados à natureza das agências.
>
> A possibilidade de utilização de dados, nessas circunstâncias, gerou, na opinião pública, o temor de que as informações fossem utilizadas para controlar a atividade e comportamento dos cidadãos,

[194] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 210.

> gerando provocação da Corte Constitucional, que, em provimento cautelar, suspendeu a execução do recenseamento. Após profundas considerações a respeito dos direitos da personalidade diante dos riscos da informática, decidiu-se que o indivíduo tinha direito de decidir sobre o uso e a cessão dos dados pessoais. A limitação do direito seria admissível diante de relevante interesse geral ou por norma clara que atendesse ao princípio da proporcionalidade[195].

Para sanar situações como estas, começaram a ser editadas as leis de proteção de dados pessoais de 4ª geracão, o que vem ocorrendo até os dias atuais. Elas buscam amparar mais a coletividade do que simplesmente fornecer mecanismos para uma mera escolha individual. Para isso: a) reconhecem a assimetria informacional entre os coletores de dados e o indivíduo, b) passam a disseminar o modelo de autoridades independentes para a atuação da lei, já que em algumas situações o indivíduo necessita de maior proteção do que simplesmente dar o seu consentimento, c) editam normas específicas para setores mais sensíveis de processamento de dados, como saúde ou crédito ao consumo[196].

A partir desse breve histórico, é possível perceber especialmente a evolução da proteção de dados pessoais como um dos direitos da personalidade. Isso ocorreu sobretudo no modelo europeu, que se apresenta diametralmente oposto ao modelo norte-americano.

Esses dois são os modelos mais consolidados e consagrados atualmente em termos de proteção de dados pessoais e sensíveis em nível mundial. São, portanto, utilizados como principais referências[197] para tratar das discussões para a regulamentação

---

195 BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de protecão ao crédito**. São Paulo: Revista dos Tribunais: 2003, p. 100.

196 No Brasil, é importante referenciar a Lei nº 12.414, de 09 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. A partir dela, não apenas os registros sobre inadimplemento de dívidas eram permitidos, mas, também, aqueles sobre o adimplemento das pessoas. Com isso, algumas empresas criaram o sistema de *credit bureau*, realizando "verdadeiras predições para o futuro". O tema foi debatido no REsp nº 1.419.697-RS, de 2013. E, em 2015, a Súmula 550 do STJ reconheceu a legalidade do sistema de avaliação de crédito e da dispensa do consentimendo do consumidor para tal. Sobre o assunto ver: OLIVEIRA, Carlos Eduardo Goettenauer de. **Credit scoring e big data no regime jurídico brasileiro**. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gama Prata de. (Coord.) Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240. O texto, entre outros temas, discute questões relacionadas ao princípio da boa-fé utilizado nas relações contratuais *versus* as restrições em relação à transparência do sistema de *credit scoring* devido, por exemplo, ao segredo empresarial que impossibilita o desenvolvimento de engenharia reversa para análise dos modelos criados para atribuição de peso a cada variável avaliado pelo sistema e às dificuldades em decorrência de os algoritmos serem considerados propriedade intelectual.

197 a) Guidi entende que a proteção de dados pessoais deve ser pensada sobretudo como uma política pública, fala ainda de um terceiro modelo, o uruguaio, o qual não será objeto do presente estudo. Segundo ele, o Uruguai segue o modelo europeu e "teve origem semelhante à brasileira, na medida em que ambas foram resultado de uma

da matéria. O modelo europeu tem uma abordagem personalista, confiando ao indivíduo a autodeterminação de sua esfera privada, enquanto o norte-americano, é primordialmente patrimonialista e contratualista, na qual o consentimento, por exemplo, acaba legitimando o uso dos dados pessoais pelo mercado, transformando-os em mercadorias (*commodities*)[198].

Na Europa, entende-se a proteção de dados como um direito da personalidade, ou seja, sob a ótica objetiva, ela é tida como um "conjunto de características e atributos da pessoa humana, considerada como objeto de proteção por parte do ordenamento jurídico"[199].

Inicialmente com a Convenção nº 108/1981, denominada Convenção de Estraburgo, a União Europeia deu um grande avanço em termos de proteção de dados pessoais. À época, foi editada a Diretiva nº 95/46/CE, mas ela ainda não contava com recursos tecnológicos como na atualidade, que permitem, por exemplo, a realização de computação em nuvem, análise preditiva com base na Big Data, marketing comportamental.

Cerca de duas décadas depois, o RGPD nº 679/2016[200], que entrou em vigor em 25 de maio de 2018, mas foi pensado e debatido desde 2010, substituiu a Diretiva e trouxe regras mais rigorosas para os setores governamental e empresarial, dando mais

---

tradição sul-americana de reafirmação e expansão de direitos fundamentais, após regimes ditatoriais que tiveram compilação de dados sobre seus cidadãos, principalmente aqueles de ideais incompatíveis com tais regimes, uma importante arma na repressão de movimentos democráticos". Destacam-se, no entanto, algumas diferenças do modelo europeu, como a existência do Habeas Data (de forma mais expandida que no caso brasileiro), por meio do qual se pode exigir, por exemplo, o conhecimento das finalidades para as quais os bancos de dados utilizam as informações pessoais, bem como a inexistência de competência jurisdicional ou de resolução de conflitos pela Autoridade de Proteção de Dados, restando forte atuação do Judiciário para dirimir as controvérsias. (GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf> . Acesso em: 20 out. 2017). b) Raminelli e Rodegheri também fazem referência à Lei de proteção de dados da Argentina, primeiro país latino-americano que editou uma lei sobre a matéria, no ano 2000, e foi certificada pela União Europeia quanto ao nível de segurança exigido para o tratamento das informações. Frisa-se que na lei argentina os dados sensíveis são elencados num rol taxativo e é obrigatório o registro de todos os "arquivos, registros bases ou banco de dados públicos ou privados destinados a fornecer informações" (No Brasil, apesar de também ser obrigatória a edição de um Catálogo de Interoperabilidade, informando todas as bases oficiais do Governo e respectivos serviços ofertados, esse trabalho ainda não foi feito por todos os órgãos do setor público). (RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil**: Análise de decisões proferidas pelo Supremo Tribunal Federal. Cadernos do Programa de Pós-graduação em Direito – Ppgdir./ufrgs, [s.l.], v. 11, n. 2, p.89-118, 31 dez. 2016. Universidade Federal do Rio Grande do Sul. http://dx.doi.org/10.22456/2317-8558.61960. Disponível em: <https://seer.ufrgs.br/ppgdir/article/view/61960>. Acesso em: 20 set. 2018.).

198 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 372.

199 SCHREIBER, Anderson. **Direitos da Personalidade**. Rio de Janeiro: Atlas, 2011. p. 6.

200 Diferentemente da Diretiva 95/46/EC, que estabelecia diretrizes para que cada Estado-Membro da União Europeia (UE) adotasse sua própria lei de proteção de dados pessoais, o RGPD buscou harmonizar a legislação, sendo aplicável a todos indivíduos e empresas da UE.

controle aos cidadãos sobre o uso, tratamento e destinação conferidos aos seus dados. A norma, pode-se dizer, como um pequeno código pormenorizado e sistematizado, teve por objetivo unificar os diferentes entendimentos que conviviam simultaneamente no cenário europeu, em decorrência das diferentes legislações nacionais[201].

O controle dos dados pelos cidadãos, no modelo europeu, envolve, entre outros fatores, o conhecimento do nome da empresa que realiza o tratamento dos dados; as finalidades para as quais serão utilizados; a base jurídica para o tratamento dos dados pessoais; o período de tempo em que eles serão guardados; o direito de retirar o consentimento a qualquer momento, o de solicitar a exclusão dos dados das bases da empresa, além de requisitar a portabilidade (transferência) destes para outra organização[202].

Para as empresas e órgãos públicos, destacam-se, também, a consolidação dos conceitos de *privacy by design* e *privacy by default* nos seus sistemas e estruturas tecnológicas. O primeiro consiste na incorporação de recursos que garantam a privacidade na própria infraestrutura e arquitetura dos sistemas durante todo o seu ciclo de vida[203]. O segundo indica que as regras mais rígidas de privacidade, quando liberadas ao público, por padrão (por definição), devem ser aplicadas sem a necessidade de intervenção do usuário. Além disso, a quantidade de dados que devem ser coletados por qualquer sistema ou aplicativo deve ser a menor possível.

---

201 Importante destacar que, apesar das diferenças normativas, o ordenamento jurídico dos diferentes países europeus possuíam contornos comuns, dentre os quais: a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (art. 8º "Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."). Conselho da Europa. **Convenção Europeia dos Direitos do Homem**. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 01 out. 2018.

202 O RGPD não se aplica ao tratamento de dados pessoais de pessoas falecidas ou de pessoas coletivas. Da mesma forma, não se aplica ao tratamento de dados por motivos exclusivamente pessoais ou domésticos, não podendo haver qualquer relação como exercício de atividades profissionais ou comerciais. Comissão Europeia. **Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)?** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt>. Acesso em: 01 out. 2018.

203 Esse entendimento também foi seguido pela LGPD, no art. 46, § 2º, onde consta a necessidade de observância das medidas segurança e do sigilo de dados desde a fase de concepção até a execução do produto ou do serviço, e no art. 49, a necessidade de estruturação dos sistemas de acordo com os requisitos de segurança e aos padrões de boas práticas. Há também, que se mencionar as discussões acerca do segredo empresarial, propriedade intelectual e inviabilidade técnica da engenharia reversa, por exemplo, nos serviços de *credit scoring*, o que, em tese, restringiria a transparência e impediria o controle e o entendimento acerca do uso conferido aos dados pessoais e sensíveis (Sobre o assunto ver: OLIVEIRA, Carlos Eduardo Goettenauer de. **Credit scoring e big data no regime jurídico brasileiro**. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gama Prata de. (Coord.) Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240.).

Por fim, destaca-se no Regulamento europeu a criação das Autoridades de Proteção de Dados, "cujas atribuições extrapolam o de uma simples agência reguladora, mas caracterizam um órgão que agrega funções fiscalizatórias, normativas e jurisdicionais, ainda que em uma instância administrativa"[204]. Segundo o Conselho Europeu, elas são "autoridades públicas independentes que acompanham e controlam, através de poderes de investigação e de correção, a aplicação da legislação relativa à proteção de dados"[205]. Também são responsáveis por fornecer aconselhamentos sobre o RGPD, tratar de reclamações apresentadas contra violações às normas de proteção de dados pessoais e impor sanções às organizações, incluindo a suspensão ou cessação do tratamento de dados e a aplicação de multa.

Em contraposição ao modelo europeu, afirma Barroso que o constitucionalismo norte-americano prioriza os direitos individuais e não comunitários. Além disso, a

> dignidade humana nunca foi considerada, na argumentação dos membros da Suprema Corte, como um direito fundamental particular ou autônomo, mas sim como um valor subjacente, tanto aos direitos expressos quanto aos não enumerados, como os direitos à privacidade e à igualdade, à proteção contra penas cruéis e incomuns e contra a autoincriminação, entre outros. Portanto, o papel da dignidade humana tem sido, principalmente, o de informar a interpretação de direitos constitucionais específicos.[206]

Diferentemente dos países europeus, para os Estados Unidos, o direito à privacidade está associado ao valor da liberdade e não ao da dignidade, entendida como honra (tanto objetiva, que se tem perante a sociedade; quanto subjetiva, relacionada à auto-estima). Lá, prefere-se deixar que a proteção dos dados pessoais, no caso do setor privado, ocorra por meio da autorregulação, não tendo, assim, uma lei geral de proteção de dados pessoais, mas apenas leis setoriais (nacionais ou estaduais) direcionadas a setores mais sensíveis (como as voltadas às crianças e adolescentes, à área da saúde e de finanças, por exemplo), especialmente para o setor público[207].

Para as atividades estatais exercidas pelas agências federais existe o *Privacy Act* de 1974 (inserido no contexto das leis de 1ª geração mencionadas anteriormente). No

---

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

[205] Comissão Europeia. **O que são autoridades de proteção de dados (APD)?** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_pt>. Acesso em: 01 out. 2018.

[206] BARROSO, Luis Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo:** A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 42.

[207] MENDES, Laura Schertel Mendes. **Privacidade, proteção de dados pessoais e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 48.

entanto, apesar de tais agências terem competências fiscalizatórias, sancionatórias e normativas, é o Judiciário quem tem de ser acionado para executar ou fazer cumprir certas obrigações[208].

Assim, mesmo diante da existência dessas normas específicas, o principal instrumento para fazer valer o direito do titular dos dados quanto à tutela à privacidade nos EUA é o contrato. E o consentimento, diferentemente do modelo europeu, visa mais à concordância do titular quanto à venda e respectiva monetização de informações pessoais do que a uma cessão temporária de direitos sobre os dados individuais[209].

> Relegar ao judiciário a garantia de direitos, sem criar outros mecanismos que garantam direitos ou busquem incentivar a adoção de certas práticas de bom tom no tratamento da privacidade dos indivíduos, instila no empreendedor e nas empresas em geral a ideia de que a garantia da privacidade de seus clientes ou futuros clientes é apenas um fator na análise de rentabilidade e viabilidade de um modelo de negócios, e não um valor que deve ser preservado.
>
> Do ponto de vista geral, essa abordagem privilegia a livre iniciativa e a inovação, permitindo que usos novos e não regulados da informação sejam descobertos e utilizados para gerar valor aos consumidores. Do ponto de vista da proteção de dados pessoais, no entanto, trata-se de um modelo ineficaz de regulação, que recorre apenas a um viés regulatório jurídico, ao invés de avaliar a conduta regulada em termos econômicos, sociais e de "arquitetura", como queria Lessig[210].

Nesse cenário, observa-se que o Brasil optou por seguir o modelo europeu. A proximidade entre as leis é substancial. Frisa-se, é claro, que essa escolha não foi apenas por conta da construção normativa que foi se consolidando no país, como mostrado anteriormente (apesar de ter sido decisiva, também), mas por que a entrada em vigor do RGPD europeu vinha forçando essa "predileção".

De fato, a não adoção de certas normas e parâmetros europeus por outros países teriam reflexo muito negativo nas políticas de dados de intercâmbio internacional, restringindo a competitividade e as oportunidades de negócios. Segundo o novo

---

208 GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais.** Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf> . Acesso em: 20 out. 2017.

209 Ibidem, p. 14.

210 GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais.** Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf> . Acesso em: 20 out. 2017. (OBS: Lawrence Lessig defendia que a regulação da internet deveria ser feita por meio do código - "Code is law" -, ou seja da arquitetura dos sistemas, em consonância com a cultura norte-americana).

Regulamento, empresas, ainda que situadas fora do território europeu, se tratarem dados de europeus ou oferecerem produtos ou serviços a europeus, estarão sujeitos ao Regulamento. Com isso, diversas organizações, invariavelmente, teriam de se adaptar às novas regras de privacidade.

Em termos governamentais, a ausência de uma lei de proteção de dados minimamente semelhante em termos de proteção à privacidade no Brasil também o deixaria de fora de possíveis compartilhamentos de dados e informações, comércio eletrônico e transferências internacionais com aqueles países, podendo, inclusive, limitar a cooperação internacional para fins de investigação de ilícitos. Na América do Sul, até o momento, apenas Uruguai e Argentina são reconhecidos pela União Europeia nesses quesitos.

> O Brasil, por não ter um marco legal de proteção de dados e uma autoridade reguladora, não é reconhecido pela UE para permitir as transferências internacionais. Isso significa que as transferências para o Brasil somente poderão ocorrer mediante o (i) consentimento dos usuários, (ii) a celebração de contratos e cláusulas-padrão (*model contracts ou model clauses*), (iii) normas corporativas vinculantes (*binding corporate rules*) ou (iv) acordos e tratados bilaterais. As empresas brasileiras já começaram a receber uma avalanche de contratos de seus parceiros comerciais estabelecidos na UE para que também se comprometam a cumprir as suas disposições. É aqui que o GDPR ganha em capilaridade e profusão, uma vez que as redes contratuais irão propagar entre parceiros privados ao redor do mundo as obrigações sobre proteção de dados pessoais. Como a UE e os Estados Unidos negociaram um novo acordo de transferência de dados (*privacy shield*) para substituir o anterior, os americanos não devem enfrentar num primeiro momento maiores problemas, a despeito da perspectiva diversa com que tratam de temas de privacidade. Pela perspectiva americana, *national cybersecurity* vem à frente de privacidade[211].

Por outro lado, algumas diferenças em relação ao regulamento europeu também podem ser observadas na nova lei brasileira. Em parte, essas distinções decorrem do momento político-econômico delicado e incerto que o Brasil atravessa, em razão, entre outros fatores, de uma contemporânea crise econômica e das eleições que aconteceram em 2018.

No que tange à criação de uma Autoridade Nacional de Proteção de Dados (ANPD), por exemplo, o então presidente brasileiro vetou a proposta sob o argumento de vício

[211] SOMBRA, Thiago Luís. **GDPR e proteção de dados pessoais**: uma agenda também brasileira. JOTA, Brasília, 25 mai. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/gdpr-agenda-brasileira-25052018>. Acesso em 15 jun. 2018.

de iniciativa, ainda que na proposta advinda das consultas públicas realizadas pelo Ministério da Justiça sua criação estivesse presente. Posteriormente, no último ato de seu governo, por meio da MP 869/2018, procedeu à criação da ANPD.

Outro dispositivo vetado, diferentemente da Europa que não faz distinção entre os setores público e privado, dizia respeito à obrigação de dar publicidade de dados pessoais compartilhados com entidades de direito público. Segundo o chefe do Executivo, essa publicidade poderia tornar inviável o exercício regular de alguns projetos ou ações públicas como as de fiscalização, controle e polícia administrativa. Igualmente, também foi vetado o dispositivo que visava proteger a identificação do indivíduo que requisita informações ao Poder Público por meio da LAI e o respectivo compartilhamento dessas informações com outras entidades do Poder Público ou com pessoas jurídicas de direito privado.

Outra diferença substancial refere-se às sanções. No RGPD, elas estão todas previamente especificadas na lei. Na lei brasileira, além de serem passíveis de ações posteriores na Justiça, houve veto às sanções administrativas de suspensão, parcial ou total, ou proibição do tratamento de dados pelas organizações que descumprissem a lei.

Segundo o presidente, o motivo do veto foi a insegurança que poderia causar aos responsáveis por essas informações, bem como a possibilidade de obstrução das atividades empresariais caso a atividade fosse essencial ao negócio, como no caso das instituições financeiras.

A multa no RGPD também é mais intensa que no Brasil (€20 milhões ou até 4% do volume global de negócios da empresa, no RGPD; e até 2% do faturamento da empresa no Brasil no seu último exercício, limitada, no total, a R$50 milhões por infração, na lei brasileira).

Algumas outras divergências também podem ser ressaltadas, mas merecem discussões separadas, tais como a ilicitude para o tratamento de dados de crianças que, no caso europeu tem seu limite aos 16 anos e, no Brasil, 12 anos; e a permissão, apenas no caso brasileiro, de comercialização de dados sensíveis para obter benefício econômico, se houver autorização da autoridade protetora.

Não se pode deixar de mencionar a crítica de Paul Ohm acerca desses dois modelos de regulamentação. Para ele, a quebra da premissa de que a privacidade estaria protegida com as ferramentas de anonimização e a possibilidade da fácil reidentificação de dados ("*easy*

reidentification result"[212]) deveriam desencadear uma mudança radical nas legislações. Em sua visão, todas as leis e regulamentos editados sob o pressuposto e a confiança na anonimização robusta deveriam ser reexaminadas: "At the very least, legislators must abandon the idea that we protect privacy when we do nothing more than identify and remove PII. The idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned."[213]

Segundo o autor, o foco dos debates centra-se, atualmente, na definição do que são dados pessoais, incluindo os dados pessoais identificáveis ("*personally identifiable information*" - PII)[214]. Entretanto, para ele, nenhum dado pode ser tornado perfeitamente anônimo, ou seja, a privacidade perfeita só poderia ser atingida quando não se publica nada[215].

Além do mais, as PII são uma categoria em constante expansão. "No matter how effectively regulators follow the latest reidentification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII will never stop growing until it includes everything."[216]

Na mesma esteira, Bolzan e Jacob Neto, ao analisarem o então PL nº 5.276/16, criticam, não apenas o fato de não inserir a igualdade (mas, tão somente, a privacidade e a liberdade) no seu art. 1º, como o fato de se basear na classificação de dados anônimos (ideia incluída, com pequenas modificações, na LGDP[217]). Em relação à ausência da igualdade, afirmam tratar-se

---

212 OHM, Paul. **Broken Promises of Privacy**: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: <https://ssrn.com/abstract=1450006>. Acesso em: 14 mar 2019. P. 1706.

213 Ibidem, p. 1732.

214 SCHWARTZ e SOLOVE, ao contrário de OHM que busca encontrar um paradigma novo para regular a privacidade, defendem que a lei não pode abandonar o conceito de PII., já que este que estabelece os limites na regulação da privacidade. Além disso, avaliar custo/benefício da coleta e divulgação dos dados *a priori* é muito difícil, Para eles, a PII deve ser baseada em norma (e não em regra) e devem ser feitas duas categorizações (dados identificados e dados identificáveis), utilizando um *continuum* de risco de identificação e estimulando as práticas justas de informação (*Fair Information Practices – FIP)*. À essa proposta dão o nome de PII 2.0. (SCHWARTZ, Paul M.; SOLOVE, Daniel J. **The PII Problem**: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, v. 86, 2011, p. 1814-1894. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs>. Acesso em 15 mar 2019.)

215 OHM, Paul. Op. cit., p. 1752.

216 OHM, Paul. Op. cit., p. 1742.

217 PL 5.276/16: art. 5º, inc. IV – dados anonimizados: dados relativos a um titular que não possa ser identificado; inc. XII - anonimização: qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. / Lei nº 13.709/18: art. 5º, inc. III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; inc. XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

> de uma abordagem limitada, porque, embora esses problemas continuem a ser relevantes, é cada vez mais claro que eles não contam a história completa sobre a *surveillance*, porque ela, nos dias de hoje, classifica pessoas em categorias de interesse ou risco com consequências reais nas suas vidas. Logo, a *surveillance* torna-se um instrumento de estratificação da discriminação, o que faz com que deixe de ser, apenas, um problema de privacidade individual, mas, especialmente, de justiça social.
>
> Ainda que a omissão do artigo 1º do PL 5276/2016 fosse considerada um mero "esquecimento", suas consequências para a proteção dos direitos humanos seriam igualmente prejudiciais, especialmente quando se percebe que a coleta massiva de dados é capaz de categorizar pessoas em grupos de risco ou de (des) interesse econômico e social[218].

Sobre a confiança na impossibilidade de reidentificação com base na anonimização, sustenta ser uma "classificação fantasiosa, especialmente dentro do contexto dos avançados algoritmos de extração — *data mining* — e análise massiva de dados e, especialmente, de metadados — *big data*"

> Assim, os dados não são, como quer a lei, "essencialmente" pessoais, sensíveis ou anônimos. São, apenas, dados, cujo sentido é atribuído no momento da aplicação do algoritmo. Como resultado, dados que foram "anonimizados" podem sofrer o processo inverso e tornarem-se identificáveis, revelando informações sensíveis sobre um indivíduo ou grupo de indivíduos.
>
> Quanto mais fontes anônimas de dados forem concatenadas, menos anônimos esses dados serão. Assim, a classificação proposta pelo PL 5276/2016 permite que seja dada baixa proteção ao conjunto de informações que podem ser utilizadas para afetar diretamente a vida das pessoas, violando uma série de direitos humanos. Desse estado da arte, a classificação equivocada entre dados pessoais, sensíveis e anônimos coloca em risco os direitos humanos, em especial a igualdade, uma vez que possibilitará a proteção deficiente de dados potencialmente sensíveis e de extrema relevância para a vida das pessoas[219].

Diante desse quadro, os autores sugerem que não se trata de uma falha do modelo estatal, mas da insuficiência do formato de organização política capaz de proteger,

---

[218] BOLZAN DE MORAIS, Jose Luis; JACOB NETO, E.; BEZERRA, Tiago José de Souza L. **O Projeto de Lei de Proteção de Dados Pessoais (PL 5276/2016) no mundo do Big Data**: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos Direitos Humanos. Revista Brasileira de Políticas Públicas, [S.I], v. 7, p. 184-198, 2018. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840>. Acesso em: 15 mar. 2019. http://dx.doi.org/10.5102/rbpp.v7i3.4840, p. 193/194.

[219] Ibidem, p. 194.

sozinho, os direitos humanos na era do *big data*. Ohm, igualmente, afirma que nenhum dos dois modelos atuais é suficiente sozinho. Para ele, a abordagem dos EUA é falha porque permite que organizações inteiras escapem da regulação ao considerar diversos dados inofensivos e não causadores de danos no caso de caírem nas mãos erradas. Por outro lado, a abordagem europeia é muito onerosa para as organizações:

> It might have made good sense to impose such strict requirements (notice, consent, disclosure, accountability) on data administrators when we still believed in the power of anonymization because the law left the administrators with a fair choice: Anonymize your data to escape these burdens or keep your data identifiable and comply. But as we have seen, easy reidentification has mostly taken away this choice, thereby broadening the reach of the Directive considerably[220].

Sua proposta é, então, realizar análises de avaliação de risco, de acordo com uma gradação que considera fatores e situações em que, na divulgação de determinado dado, há probabilidade do dano ocorrer e de superar os benefícios do fluxo de informações. Quando isso fosse verificado, seria necessário regular contexto e setores específicos.

3.3 O respeito à finalidade e à transparência para suprir a necessidade do consentimento no setor público

Associado à impessoalidade (art. 37, caput, da CF 88), o princípio da finalidade é basilar para a Administração Pública, a qual deve sempre visar atingir o objetivo fixado em lei. E este, em última instância, será sempre o interesse público. Na nova lei de proteção de dados pessoais, consta expressamente do art. 6º, inc. I, a necessidade de observância a esse princípio. Diz a lei que a finalidade significa a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

Frisa-se, aqui, que os dados, portanto, não podem ser coletados em vão. Ao contrário, a finalidade deve ser comunicada antes da coleta dos dados individuais, o que facilita valorar os critérios de razoabilidade para sua utilização, evitando assim abusos por parte da entidade coletora. Devem ser também observados outros requisitos como o consentimento[221] (art. 5º, inc. XII) e os princípios da adequação, da necessidade e da qualidade (art. 6º, inc. II, III e V, respectivamente).

---

220 OHM, Paul. Op. cit., p. 1763.

221 Na mesma linha do modelo europeu, a norma brasileira exige que o pedido de consentimento especifique quais dados serão coletados e sua destinação, devendo ser apresentado de forma clara e concisa, de modo a garantir uma fácil compreensão. O consentimento, que deve ser dado de livre vontade, por escrito ou outra forma que demonstre a manifestação de vontade do titular, também deve ser solicitado de forma apartada e distinta

Além disso, a norma prescreve que a finalidade deve ser específica, sendo consideradas nulas autorizações genéricas (art. 8º, §4º). Também é necessário comunicar ao titular as possíveis mudanças de finalidade, caso houver, de forma que haja novo consentimento ou possibilidade de revogá-lo (art. 9º, §2º).

Estritamente no caso do setor público, o tratamento dos dados pessoais deverá ser realizado para atender à finalidade pública referente ao órgão, com o fim de executar as competências ou atribuições legais estabelecidas para o serviço público (art. 23, caput). Para isso, deve haver transparência quanto à base normativa utilizada e ao uso, aos procedimentos e às finalidades para os quais os dados são coletados, tratados e utilizados (art. 23, inc. I).

A nova legislação também regula o compartilhamento de dados pessoais pelo Poder Público com fundamento no princípio da finalidade. De acordo com a norma, esse procedimento só poderá ocorrer se houver previsão para o atendimento "a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º" (art. 26).

A transferência para entidades privadas, em regra, é vedada. Só poderá ocorrer em casos de execução descentralizada de atividade pública que exijam a referida transferência e exclusivamente para fim específico e determinado ou nos casos em que os dados já forem acessíveis publicamente.[222]

Vale destacar que, apesar de haver necessidade de que o consentimento seja concedido de forma destacada para finalidades específicas no caso de uso de dados sensíveis (art.

---

das outras informações como os "termos e condições de uso", o que, atualmente, é chamado de consentimento granular, ou seja, as permissões dadas pelos usuários para a coleta ou tratamento dos dados acontece de forma fragmentada, permitindo evitar a lógica do tudo ou nada. Nesse sentido, diz-se que ele deve ser expresso, livre, específico, informado e inequívoco,bem como deve advir de uma atitude ativa e não passiva. Por fim, ele pode ser revogado expressamente a qualquer momento pelo titular. É importante frisar que, apesar de o Còdigo Civil, em seu art. 11, estatuir que os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo sofrer limitação voluntária (o que desabonaria qualquer espécie de consentimento), o entendimento atual é de que o titular dos direitos não pode renunciá-los de forma definitiva e permanente (Enunciado 4 da I Jornada de Direito Civil). Assim, tais direitos podem sofrer limitações, desde que para atender aos melhores interesses do titular do direito e para realização da dignidade da pessoa humana.

222 O inc. II do § 1º do art. 26 da Lei 13.709/18 foi vetado. Sua redação excepcionava a vedação a transferência de dados do Poder Público para entidades privadas: quando houvesse previsão legal e a transferência fosse respaldada em contratos, convênios ou instrumentos congêneres. Na mensagem presidencial constam as seguintes razões do veto: "A redação do dispositivo exige que haja, cumulativamente, previsão legal e respaldo em contratos, convênios ou instrumentos congêneres para o compartilhamento de dados pessoais entre o Poder Público e entidades privadas. A cumulatividade da exigência estabelecida no dispositivo inviabiliza o funcionamento da Administração Pública, já que diversos procedimentos relativos à transferência de dados pessoais encontram-se detalhados em atos normativos infralegais, a exemplo do processamento da folha de pagamento dos servidores públicos em instituições financeiras privadas, a arrecadação de taxas e tributos e o pagamento de benefícios previdenciários e sociais, dentre outros." **Mensagem n. 451, de 14 de agosto de 2018.** Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em 15 out. 2018.

11, inc. I), a LGPD dispensa esse consentimento para o "tratamento compartilhado de dados necessários à execução, pela administração pública, de **políticas públicas previstas em leis ou regulamentos**" (art. 11, al. b, grifo nosso), devendo ser dada ampla publicidade à dispensa e às razões que a ensejaram.

Além disso, "os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral" (art. 25).

Diante do exposto, num primeiro momento, parece ser possível afirmar que a nova lei não irá impactar de forma significativa os programas e ações do setor público, pois as ressalvas, previstas no art. 11 e 26, para dispensa de consentimento[223] – um dos institutos jurídicos mais fortes para o exercício da autodeterminação informativa - são passíveis de justificativa na maioria dos casos, já que o fim último da Administração Pública é o interesse público. Desse modo, as exceções inseridas para o setor acabam dando margem a uma interpretação extensiva da lei e abarcando um número considerável de situações. Consequentemente, eventuais questionamentos acerca do tratamento de dados pelo Poder Público acabarão sendo decididos em juízo.

Por outro lado, entende-se que, no caso da utilização de dados coletados por aplicativos governamentais (abordado no item 2.3.4), a exceção quanto ao consentimento prevista na LGPD não estaria valendo. Como visto, a coleta de dados realizada atualmente é feita sem o devido respeito aos propósitos específicos de cada aplicativo, desrespeitando o princípio da necessidade que prevê o limite mínimo de coleta de dados para alcançar a finalidade (art. 6º, inc. I e III, da LGPD). E, a despeito dos inúmeros benefícios que pode levar aos seus usuários, como a facilidade de acesso, poder-se-ia afirmar que os aplicativos não estariam incluídos nas hipóteses de dispensa do consentimento previstas no art. 11 da LGPD.

Em relação aos questionamentos acerca do compartilhamento de dados entre os diferentes órgãos e entidades da Administração e entre estes e entidades de direito privado por meio de decretos ou normas infralegais, as dúvidas também parecem ser

---

[223] Apesar de o consentimento ser dispensado para o setor público quando para a execução de políticas públicas ou da prestação de serviços públicos, não se pode deixar de mencionar as discussões acerca da inefetividade do consentimento: "*(1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties*". Sobre o assunto ver: SOLOVE, DJ (2013) **Privacy self-management and the consent dilemma**. Harvard Law Review 126: 1880– 1903. Disponível em: <https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf> Acesso em: 15 out. 2018.

sanadas com a nova lei. De fato, a LGPD deve acabar com essa discussão e legitimar seu uso quando as instituições estiverem e comprovarem estar atuando no cumprimento de suas competências legais e finalidades específicas de execução de políticas públicas previstas em leis ou regulamentos, com a dispensa, inclusive, do consentimento do titular (art. 11, al. "b"). Destaca-se que a lei não deixa de lado a obediência aos demais princípios de proteção de dados pessoais nela elencados. (art. 26 c/c art. 6º).

De acordo com os novos dispositivos, também será possível o compartilhamento de dados pessoais e sensíveis entre controladores com objetivo de obter vantagem econômica. Essa prática, no entanto, poderá ser objeto de vedação ou de regulamentação pela autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (art. 11, §3º).

O compartilhamento dos dados de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá do consentimento do titular (art. 27). Entretanto, um dos aspectos mais criticados entre os defensores da proteção de dados foi a exclusão, pela MP 869 (em discussão pelo Congresso Nacional), da obrigatoriedade de o Poder Público informar esse compartilhamento à autoridade nacional, tornando necessária apenas a publicidade acerca dessa prática (art. 27, inc. II c/c art. 23).

O impacto maior que pode ser observado, então, é a obrigação, para o Poder Público, de ser mais transparente. Isso envolve dar publicidade quanto à motivação, ao uso e à finalidade para a qual os dados foram coletados, conferindo maior controle ao cidadão sobre as ações adotadas, sendo, também, uma forma de *accountability*. Para isso, inclusive, a pessoa do encarregado, criado pela lei, será de grande valia.

Mais uma vez inspirada na legislação europeia, a LGPD também criou a figura do encarregado pelo tratamento dos dados pessoais (*data protection officer*). O encarregado é uma pessoa indicada pelo controlador para atuar como canal de comunicação entre aquele, os titulares dos dados e a autoridade nacional (art. 5º, inc. VIII c/c art. 41), prestando esclarecimentos, orientando funcionários, verificando a conformidade e adotando providências acerca das práticas do uso dos dados. Em geral, deve ser uma pessoa que possua tanto conhecimentos jurídicos, quanto de tecnologia. A autoridade, por sua vez, poderá prever hipóteses de dispensa da necessidade dessa figura a depender da natureza ou do porte da entidade ou, ainda, do volume de operações de tratamento de dados (o que não significa dizer que a entidade poderá deixar de adotar ações visando à transparência).

Em relação à transparência, no caso do setor público, é possível inferir da norma que os cidadãos terão o direito de ser informados caso as decisões sejam tomadas

de forma automatizada (art. 20), impactando, por exemplo, a inclusão ou não de determinado perfil em programas sociais e ações afirmativas. E, nesses casos, poderão contestar a decisão (ou política pública instituída) ou exigir que as decisões possam ser revistas por uma pessoa, por exemplo.

A segurança por parte dos indivíduos de que as empresas e órgãos governamentais realizam uma coleta responsável e transparente das informações pessoais ou sensíveis poderia superar parte das preocupações acerca do tratamento e do uso conferido a esses dados e da desconfiança da população nas ações do Estado. Essa situação seria, ainda, majorada caso fosse demonstrada e garantida a independência do órgão de controle autônomo (como a autoridade nacional), capaz de garantir que tais medidas sejam, de fato, observadas e colocadas em prática (*enforcement*).

3.4 A imperatividade da independência funcional da autoridade nacional de proteção de dados

Como assinalado anteriormente, o presidente da República vetou a criação da Autoridade Nacional de Proteção de Dados (ANPD), a qual, segundo o projeto de lei deveria ser "integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça" (art. 55), regida pela Lei nº 9.986/2000, que disciplina a gestão de recursos humanos das Agências Reguladoras.

Nesse modelo, ela deveria apresentar independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes, além de autonomia financeira. O projeto de lei trazia dispositivos, também vetados, acerca das atribuições da ANPD, da criação e competência de um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (art. 55 a 59), órgão auxiliar composto por integrantes do Poder Público, empresariado e sociedade.

Nas razões dos vetos, foi indicada afronta ao artigo 61, § 1º, inc. II, al. "e" (é de iniciativa privativa do Presidente da República leis que disponham sobre criação e extinção de órgãos da administração pública), cumulado com o artigo 37, XIX (somente por lei específica poderá ser criada autarquia), ambos da Constituição.

Segundo Schertel, entretanto, o modelo de regulação da proteção de dados pessoais por meio de uma lei geral é relevante pois constrói uma "arquitetura regulatória" que busca consolidar o tema com um setor de políticas públicas. E, necessariamente para

que isso aconteça, deve abranger, além de instrumentos estatutários e sancionatórios, um órgão administrativo responsável pela implementação e aplicação da legislação correlata.

> A experiência das últimas décadas dos órgãos administrativos de proteção de dados pessoais demonstrou que a existência desses órgãos é essencial para a implementação da legislação e da cultura da privacidade no país, conforme afirmam Bennett e Raab: 'A existência de autoridades supervisoras robustas tem sido considerada como condição *sine qua non* para a adequada proteção à privacidade, pois as leis não são autoimplementáveis e a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine'. [224]

Segundo o Conselho Europeu, nos países da União, as chamadas Autoridades de Proteção de Dados (APDs) devem possuir características próprias para garantir o *enforcement* da lei. Elas devem ser independentes, com poderes de investigação e de correção e aplicação da legislação correlata. Elas cuidam das reclamações apresentadas contra violações às normas sobre os temas e podem impor sanções às organizações, incluindo multa, suspensão ou cessação do tratamento pela empresa[225].

No caso brasileiro, houve discussão sobre a quem competiriam essas novas atribuições, se ao Ministério da Justiça (como constou do projeto de lei sancionado), ao Ministério da Ciência, Tecnologia, Inovações e Comunicações ou, até mesmo, ao Ministério Público, que possui poderes investigativos.

Críticas foram feitas à proposta de integrar o órgão à estrutura do Poder Executivo, o que poderia retirar sua autonomia funcional. Foi aventada, até mesmo, a possibilidade de criação da autoridade por medida provisória, subordinada ao Gabinete de Segurança Institucional da Presidência da República[226].

Apesar de, à época, ter sido vetado o capítulo IX da Lei nº 13.709/2019, que visava à criação da ANPD e do CNPD, havia sido mantido o art. 5º, inc. XIX, que previa a existência da autoridade nacional na estrutura da administração pública indireta, sendo "responsável por zelar, implementar e fiscalizar o cumprimento desta Lei".

---

[224] MENDES, Laura Schertel Mendes. **Privacidade, proteção de dados pessoais e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 49.

[225] COMISSÃO EUROPEIA. **O que são autoridades de proteção de dados (APD)?** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_pt>. Acesso em: 01 out. 2018.

[226] Projeto de proteção de dados pessoais aguarda sanção de Temer. **G1:** online. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2018/07/projeto-de-protecao-de-dados-pessoais-aguarda-sancao-de-temer.html>. 19/07/2018. Acesso em 10 out. 2018.

Ocorre que a Medida Provisória nº 869/2018[227] também alterou esse dispositivo, retirando do inciso a palavra "indireta". Assim, a autoridade nacional passou a poder integrar a Administração Direta. E esse fato apresenta grandes possibilidades de comprometimento da independência e autonomia orçamentária-funcional da Autoridade, apesar de a norma assegurar a autonomia técnica (art. 55-B).

Como afirma o coordenador da Comissão de Proteção dos Dados Pessoais do MPDFT, Frederico Meinberg Ceroy, a independência da autoridade em relação à administração pública evita a chamada teoria da cooptação, a qual sustenta que as agências reguladoras ou seus funcionários são capturados, no decorrer do tempo, por ameaças externas, como interesses privados de alguns grupos ou agentes em prejuízo da coletividade[228].

Mesmo diante dessas ressalvas, o governo criou a ANPD inserida na estrutura da APF, como integrante da Presidência da República. A fim de minimizar as possíveis censuras quanto à autonomia do órgão, foram inseridas cláusulas dispondo que, a despeito de os membros de seu Conselho Diretor serem designados pelo presidente, só haverá perda dos mandatos (de quatro anos) em decorrência de renúncia, condenação judicial transitada em julgado ou demissão, após processo administrativo disciplinar. (art. 55-E). Dispôs a Lei, também, que a ANPD fará articulações com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais. (art. 55-K).

Há de se ressaltar que, por mais que o país esteja vivenciando uma crise econômica e que, da forma como foi criada a ANPD, não haja o aumento de despesa (um dos argumentos do Governo para deixá-la na estrutura da APF), da maneira atual, pode, sim, haver problemas relacionados à independência na execução das políticas de proteção de dados. Os agentes públicos vinculados à Autoridade, obrigatoriamente, terão o dever de obediência ao órgão superior, já que há vínculo hierárquico com a Presidência da República.

Mais uma vez, apesar dos longos anos de discussão sobre o tema, não foi realizado (ou, ao menos, apresentado e divulgado) diagnóstico ex-ante sobre o impacto

---

227 Acentua-se que, apesar de produzir efeitos jurídicos imediatos, as Medidas Provisórias precisam ser apreciadas pelo Congresso Nacional para se converterem em leis. O prazo inicial de vigência é de 60 dias, prorrogado automaticamente por igual período, caso a votação não tenha sido concluída nas duas Casas. Se não for votada em até 45 dias, contados de sua publicação, entra em regime de urgência na Casa em que se encontrar, ficando sobrestadas todas as demais deliberações legislativas até que se termine a votação em que estiver tramitando (art. 62, da CF88).

228 PRADO, Jean. Qual é a polêmica em torno da lei de proteção de dados pessoais no Brasil. **Tecnoblog.** Disponível em: <https://tecnoblog.net/251604/polemica-lei-protecao-dados-pessoais/>. Acesso em 05 nov. 2018.

orçamentário-financeiro para criação dessa nova política pública, caso tivesse sido feita a opção por criar esse novo órgão autônomo. A análise ex-ante visa estabelecer mais racionalidade às decisões, abrangendo a investigação, dentre outros fatores, da relação custo-benefício e a verificação acerca da disponibilidade de recursos do Poder Público para o financiamento do projeto, sem prejudicar o equilíbrio fiscal[229].

Por último, a parte referente à criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade entrou em vigor em 28 de dezembro de 2018 e os demais dispositivos, como já mencionado, com a publicação da Medida Provisória, foi ampliado para 24 meses.

3.5 A utilização dos dados pessoais e sensíveis para fins penais, de controle e de fiscalização

Em sintonia com o RGPD, a Lei brasileira protege os dados pessoais e sensíveis, sendo proibido, como regra geral, seu tratamento e compartilhamento (art. 11). Algumas hipóteses de incidência acabam por permitir seu uso, como no caso de o titular tornar esses dados manifestamente públicos, quando dá seu consentimento de forma explícita ou, ainda, para o cumprimento de obrigação legal ou regulatória pelo controlador ou para a proteção da vida ou tutela da saúde, entre outros.

Uma discussão interessante gira em torno da requisição de dados pessoais ou sensíveis para fins de fiscalização e controle por órgãos como o Ministério Público e Tribunal de Contas. O tema é, de fato, controverso, alcançando o Supremo Tribunal Federal em casos em que se discute a abertura de dados pessoais para cumprimento de outros direitos.

Um deles, por exemplo, são os censos populacionais, para os quais existem leis específicas, baseiam-se em interesse público e contém salvaguardas destinadas a proteger os dados sensíveis da pessoa, como a restrição de acesso apenas àqueles que trabalharão com o tratamento estatístico.

Em 2012, o Ministério Público Federal ajuizou ação civil pública, com pedido de liminar, requisitando o afastamento do sigilo de dados estatísticos coletados pelo IBGE, pretendendo a identificação de 45 crianças da área urbana do município de Bauru, São Paulo, que não tiveram seu nascimento regularmente registrados, conforme dados do

[229] BRASIL. Casa Civil da Presidência da República, Instituto de Pesquisa Econômica Aplicada. **Avaliação de Políticas Públicas Guia Prático de Análise Ex Ante.** Brasília: Ipea, 2018. V. 1. Disponível em: <http://www.cgu.gov.br/Publicacoes/auditoria-e-fiscalizacao/arquivos/guia-analise-ex-ante.pdf>. Acesso em 05 nov. 2018.

Censo Demográfico de 2010. A partir da análise das decisões dos magistrados, verifica-se uma colisão entre princípios que dizem respeito à proteção especial do Estado às crianças e aos adolescentes, de um lado, e à proteção ao sigilo estatístico necessário à fidelidade dos dados e da formulação de políticas públicas, de outro.

Para isso, o *Parquet* solicitou, também, a não-recepção constitucional de normas específicas[230] que asseguram o sigilo estatístico ao IBGE quando tratarem de requisições do Ministério Público e do Poder Judiciário referentes a crianças e adolescentes, pois, nesses casos, estariam em jogo "*valores de maior densidade e dimensão*".

Em 1ª instância, o juiz determinou[231] que o Instituto fornecesse os dados. Entretanto, após contestação, o juiz substituto julgou improcedente[232] o pedido por reconhecer que afastar o sigilo de dados do recenseamento prejudicaria a finalidade do Instituto. Julgou, também, inadequada a via utilizada para exame da recepção ou não das normas, extinguindo a ação no que tange a essa parte.

Já no Tribunal Regional Federal da 3ª Região[233], a 4ª Turma, por unanimidade, determinou o fornecimento dos dados requeridos, sob pena de multa diária. Segundo os magistrados, a decisão se justificaria na medida em que, no processo de sopesamento entre princípios colidentes, a ausência de registro das crianças as deixa sem qualquer proteção do Estado e da sociedade. Após recurso ao STF, a ministra Cármem Lúcia (por meio da Suspensão de Liminar nº 1.103), reverteu a decisão, suspendendo os efeitos da decisão proferida pelo TRF-3, com as seguintes considerações:

> o exame preliminar e superficial da causa conduz a reconhecer que o afastamento do sigilo estatístico imposto pela decisão contrastada dispõe de potencialidade lesiva à ordem pública, por abalar a confiança daqueles que prestam as informações aos entrevistadores do IBGE, comprometendo a fidelidade e veracidade dos dados fornecidos e, por conseguinte, a própria finalidade daquele Instituto, a subsidiar a elaboração de políticas públicas em benefício da sociedade[234].

---

230 Decreto-lei nº 161, de 13 de fevereiro de 1967, que "autoriza o Poder Executivo a instituir a 'Fundação Instituto Brasileiro de Geografia e Estatística' e dá outras providências" e Lei nº 5.534, de 14 de novembro de 1968, que "dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências".

231 BAURU/SP. 1ª Vara da 8ª Subseção Judiciária. Sentença. Relator: Juiz Federal Roberto Lemos dos Santos Filho. Bauru, SP, 26 de setembro de 2012. Disponível em: <http://www.jfsp.jus.br/assets/Uploads/administrativo/NUCS/decisoes/2012/120926sigiloigbe.pdf>. Acesso em: 26 jun. 2017.

232 BAURU/SP. 1ª Vara da 8ª Subseção Judiciária. Sentença. Relator: Juiz Federal Substituto Marcelo Freiberger Zandavali. Bauru, SP, 26 de novembro de 2012. Disponível em: <http://www.jfsp.jus.br/assets/Uploads/administrativo/NUCS/decisoes/2012/121123ibgebauru.pdf>. Acesso em 26 jun. 2017.

233 SÃO PAULO. Tribunal Regional de Justiça da 3ª Região. Acórdão nº 18862/2017. Relator: Desembargador Federal Marcelo Saraiva. São Paulo, SP, 07 de dezembro de 2016. Disponível em: <http://web.trf3.jus.br/acordaos/Acordao/BuscarDocumentoGedpro/5308630>. Acesso em: 26 jun. 2017.

234 BRASIL. Supremo Tribunal Federal. Media Cautelar na Suspensão de Liminar 1.103 São Paulo. Relator:

Após nova manifestação da Procuradoria Geral da República, contrária à suspensão da liminar, o assunto ainda será levado a julgamento de mérito pelo colegiado da Suprema Corte. No mesmo sentido do STF, instituições internacionais que coletam dados estatísticos oficiais fundamentam suas ações e asseguram o sigilo dos dados com base em princípios constitucionais, na legislação vigente e em códigos de conduta que garantem a confidencialidade (sejam os dados fornecidos obrigatória ou facultativamente; tenham natureza autodeclaratória ou não)[235]. Segundo o Código de Boas Práticas das Estatísticas do IBGE:

> Uma das maiores preocupações nesses casos é asseverar que, ao publicar microdados desidentificados ou informações estatísticas decorrentes das análises dos dados coletados, estes não sejam identificados ou identificáveis. Além disso, a legislação também deve dar a "*garantia de que* [os dados] *são usados, exclusivamente, para fins estatísticos, e que* ***não podem ser usados para fins comerciais, de tributação fiscal, de investigação judicial e outros***"[236] (grifo nosso)

A eventual quebra de sigilo pode ocorrer pelas mais diversas razões, seja por vazamento, por hackeamento ou por situações excepcionais de requisição de dados pelo Ministério Público ou do Poder Judiciário. Porém, cabe aos órgãos oficiais de estatística zelar e buscar, ao máximo, resguardar a confidencialidade.

Ministra Presidente Cármem Lúcia. Brasília, DF, 05 de maio de 2017. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=311747237&tipoApp=.pdf>. Acesso em: 26 jun. 2017.

235 Ver *United Nations Fundamental Principles of Official Statistics* disponível em*:* https://unstats.un.org/unsd/dnss/gp/Implementation_Guidelines_FINAL_without_edit.pdf; Código de Conduta das Estatísticas Europeias, disponível em http://ec.europa.eu/eurostat/documents/3859598/5922361/10425-PT-PT.PDF, Código de Boas Práticas das Estatísticas do IBGE, disponível em ftp://ftp.ibge.gov.br/Informacoes_Gerais_e_Referencia/Cartilha_Codigo_de_Boas_Praticas_das_Estatisticas_do_IBGE.pdf , *Handbook on European data protection Law,* disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> , por exemplo.

236 BRASIL. Instituto Brasileiro de Geografia e Estatística. **Código de Boas Práticas das Estatísticas do IBGE**. 2014. Disponível em: <ftp://ftp.ibge.gov.br/Informacoes_Gerais_e_Referencia/Cartilha_Codigo_de_Boas_Praticas_das_Estatisticas_do_IBGE.pdf>. Acesso em: 26 jun. 2017.

Sabe-se, também, que não existem direitos absolutos[237] e, de fato, a relativização do direito ao sigilo estatístico deve ter caráter excepcional e ser analisada à luz dos princípios colidentes no exame do caso concreto, de tal forma que o intérprete chegue à solução mais adequada. Porém, o sigilo dos dados parece preponderar sobre os demais. Observa-se que relativizar a confidencialidade dos dados pode trazer enormes efeitos negativos, gerando repercussões danosas e irreparáveis.

Especialmente em relação ao Poder Público, uma possível identificação e/ou revelação de dados pessoais pode ocasionar o descrédito da população nas instituições governamentais, como já aludido. Existe, nesses casos, além da observância ao princípio da finalidade, o atendimento à legítima expectativa e confiança de que os dados serão sigilosos e guardados com segurança[238].

Para fins penais[239], o acesso a dados pessoais e sensíveis também tem sido objeto de controvérsias, conforme se pode observar. Mesmo correndo em segredo de justiça, observa-se da ementa a seguir que, a partir do sopesamento feito entre a privacidade, que abrange a proteção de dados pessoais, e o interesse público, no acompanhamento de uma execução penal, prevaleceu a privacidade. Isso porque, além da falta da devida motivação, entendeu-se que o pedido era desproporcional e desnecessário.

---

[237] Esse é o entendimento adotado pela moderna teoria constitucional, que considera que, mesmo sendo básicos, os direitos fundamentais são relativizados em determinadas situações. Mendes e Gonet Branco comentam que a ideia de os direitos fundamentais serem absolutos tem como premissa "o pressuposto jusnaturalista de que o Estado existe para proteger direitos naturais, como a vida, a liberdade e a propriedade". Porém, segundo eles, até mesmo o elementar direito à vida tem limitação, quando é autorizada a pena de morte no caso de guerra declarada, conforme previsto no art. 5º, inc. XLVII, al. "a", CF88 (MENDES, Gilmar Ferrreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, São Paulo; Saraiva, 2017. p. 133). Na Suprema Corte, o entendimento já é pacificado: "Na contemporaneidade, não se reconhece a presença de direitos absolutos, mesmo de estatura de direitos fundamentais previstos no art. 5º, da Constituição Federal, e em textos de Tratados e Convenções Internacionais em matéria de direitos humanos. Os critérios e métodos da razoabilidade e da proporcionalidade se afiguram fundamentais neste contexto, de modo a não permitir que haja prevalência de determinado direito ou interesse sobre outro de igual ou maior estatura jurídico-valorativa. (HC 93250, Relator(a): Min. ELLEN GRACIE, Segunda Turma, julgado em 10/06/2008, DJe-117 DIVULG 26-06-2008 PUBLIC 27-06-2008 EMENT VOL-02325-04 PP-00644). Por fim, em relação a esse debate e, especificamente quanto ao conceito da dignidade humana, Barroso adverte: "Um choque de absolutos não tem solução. O que pode ser dito é que a dignidade humana, como um princípio e valor fundamental, deve ter precedência na maior parte dos casos, mas não necessariamente em todos. Uma vez que a dignidade é tida como o alicerce último de todos os direitos verdadeiramente fundamentais e como fonte de parte do seu conteúdo essencial, seria contraditório considerá-la como um direito em si, já que ela é parte de diferentes direitos. Além disso, se a dignidade humana fosse considerada um direito fundamental específico ela necessariamente iria ter que ser ponderada com outros direitos fundamentais, o que a colocaria em uma posição mais fraca do que ela teria caso fosse utilizada como um parâmetro externo" (BARROSO, Luis Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 9-87).

[238] No caso específico da requisição dos dados identificados das 45 crianças do município de Bauru, há que se destacar que a demora no julgamento da ação pode tornar prejudicada a pretensão devido à perda do objeto, uma vez que as crianças já poderão estar devidamente registradas.

[239] Ver art. 4º, inc. III, al,.d, da LGDP: "Esta Lei não se aplica ao tratamento de dados pessoais:III – realizado para fins **exclusivos** de: d) atividades de investigação e repressão de infrações penais". Esse tema deverá ser objeto de lei específica.

> RECURSO ESPECIAL. EXECUÇÃO. PRESTAÇÃO DE SERVIÇOS À COMUNIDADE. DILIGÊNCIAS PARA VERIFICAR O REGULAR CUMPRIMENTO DA PENA. DECISÃO DESPROVIDA DE FUNDAMENTAÇÃO. 1. Embora não sejam absolutas as restrições de acesso à privacidade e aos dados pessoais do cidadão, e mesmo considerado o interesse público no acompanhamento da execução penal, imprescindível é a qualquer decisão judicial a explicitação de seus motivos (art. 93, IX, da Constituição Federal). 2. Diligências invasivas de acesso a dados (bancários, telefônicos e de empresa de transporte aéreo) deferidas sem qualquer menção à necessidade e proporcionalidade dessas medidas investigatórias, não propriamente de crime, mas de regular cumprimento de pena imposta. Nulidade reconhecida. 3. Recurso especial parcialmente provido. (REsp 1133877/PR, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 19/08/2014, DJe 02/09/2014)

No Supremo Tribunal Federal, essa discussão do acesso e do compartilhamento de dados para fins penais já alçou o status de repercussão geral:

> Ementa Constitucional. Processual Penal. Compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pelo Fisco no legítimo exercício de seu dever de fiscalizar, sem a intermediação do Poder Judiciário. Transferência de informações em face da proteção constitucional da intimidade e do sigilo de dados. Art. 5º, incisos X e XII, da Constituição Federal. Questão eminentemente constitucional. Matéria passível de repetição em inúmeros processos, a repercutir na esfera do interesse público. Tema com repercussão geral. (RE 1055941 RG, RELATOR(A): MIN. DIAS TOFFOLI, JULGADO EM 12/04/2018, DJE-083 DIVULG 27-04-2018 PUBLIC 30-04-2018)

Outra situação controversa e questionada por alguns órgãos é a requisição, pelo Tribunal de Contas da União, dos diversos bancos de dados da Administração Pública Federal. Órgão auxiliar do Poder Legislativo e responsável pelo Controle Externo, além de outras competências, é encarregado de julgar as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos e fiscalizar a aplicação dos recursos da União. Para realizar suas atribuições, o Tribunal realiza inspeções e auditorias para avaliar aspectos operacionais, de legalidade, conformidade e gestão da Administração Pública, bem como é responsável por aplicar sanções e determinar a correção de ilegalidades e irregularidades em atos e contratos.

Em entrevista com o secretário de Gestão de Informações para o Controle Externo do TCU, Wesley Vaz Silva, ele defende uma base única para análise de dados na

Administração Federal. Para ele, há uma visão equivocada de que informação é poder. Em sua opinião, é o uso que se dá à informação que confere poder. Além disso, para ele, não haveria que se falar em recusa, pela Administração Pública, do fornecimento dos dados para os órgãos de controle. Isso porque ela não é dona dos dados, mas apenas sua custodiante. Nesse sentido, seria importante valorizar a informação como um patrimônio público.

Nesse cenário, o TCU criou, para fins de controle externo, o Laboratório de Informações e Controle (LabContas), plataforma digital colaborativa, espécie de repositório de bases de dados da Administração Pública Federal e estaduais utilizados para fins de fiscalização, que atualmente conta com mais de 90 bases e conecta cerca de 55 órgãos de controle do Brasil com desenvolvedores desses órgãos. Com quatro níveis de acesso, concedido para o usuário de acordo com a natureza da informação que vai acessar, visa otimizar o uso e a análise dos dados. Por meio do LabContas é possível ter acesso a mais de 1 milhão de Cadastros Nacionais de Pessoas Jurídicas (CNPJ) e 2,5 milhões de Cadastros Nacionais de Pessoas Físicas (CPFs) e cruzar informações para, por exemplo, detectar diversos tipos de fraudes e assim auxiliar no combate à corrupção.

De acordo com o secretário, a fase de integração física das bases já passou; o momento é de integração lógica, semântica. "No LabContas, não há bases integradas. É colocar todas no mesmo lugar e analisar de forma integrada, o que é bastante diferente". Além disso, para ele, a questão da proteção aos dados pessoais não é um problema, sendo de pouca aplicabilidade nesse caso, pois o fim da atividade de controle não é investigar a pessoa individualmente, mas a possível irregularidade ou a ineficiência da política pública. "Ainda assim, há situações em que o acesso é restrito por conta das regras que o LabContas tem".

Mesmo tendo conhecimento dessas informações (de que a plataforma é utilizada exclusivamente para fins de controle não individualizado e de que há diferentes níveis de acesso), diante da nova lei de proteção de dados pessoais, porém, há de se perquirir se os princípios da finalidade (desde a coleta dos dados) e da transparência estão sendo obedecidos uma vez que as bases, muitas vezes, são repassadas aos órgãos de controle contendo dados pessoais e sensíveis. Releva-se, ainda, que a nova lei não excepcionou a sua aplicabilidade nos casos de fiscalização e controle externo e, entende-se que essas atividades não são consideradas políticas públicas para as quais é dispensado o consentimento e incentivado o uso compartilhado[240].

[240] Vale destacar que, conforme art. 4º da LGPD não se aplica ao tratamento de dados pessoais a) realizado por

É importante também verificar como se dará o tratamento e o uso dos dados pessoais nas parcerias realizadas entre o TCU e outros órgãos, com o Conselho Nacional do Ministério Público (CNMP)[241], a Polícia Federal[242], o Conselho Superior da Justiça do Trabalho (CSJT)[243], as Controladorias Gerais do Poder Executivo (a exemplo da Controladoria do Município do Recife - PE[244]), a Procuradoria Geral da Fazenda Nacional etc. para acesso ao LabContas.

No caso do acordo com o CNMP, em relação ao princípio da finalidade, questiona-se, também, o fornecimento ao Tribunal das "bases de informações estruturadas **contendo dados de interesse fiscalizatório, notadamente aqueles relativos às ações de investigação de pessoas físicas e jurídicas** no âmbito do Ministério Público brasileiro **em razão da prática de improbidade administrativa**" (cláusula primeira, grifo nosso).

Por outro lado, elogia-se a inserção do parágrafo terceiro da cláusula terceira que prevê que a necessidade da "utilização dos conhecimentos compartilhados como prova ou evidência de ilícito será realizada de forma indireta, mediante a juntada de documentos de validação obtidos junto às respectivas fontes primárias".

Por sua vez, no acordo com a União, por intermédio do então Ministério da Justiça e Segurança Pública, com a interveniência da Polícia Federal, está previsto o fornecimento ao TCU "dos **campos que indiquem relações de parentesco** da base de dados do Sistema Nacional de Passaportes – SINPA". A cláusula sexta trata da reserva de competência e dispõe que não serão objeto de repasse pela Polícia Federal informações protegidas pelo sigilo previsto no art. 20 do Código de Processo Penal.

Já o Plano de Trabalho do acordo firmado com o CSJT estabelece a disponibilização ao TCU das "informações constantes das seguintes bases: de processos judiciais eletrônicos da justiça do trabalho, do banco nacional de devedores trabalhistas, de dados do Cadastro de Clientes do Sistema Financeiro Nacional (CCS) que mantenham vínculos com órgãos

---

pessoas naturais para fins exclusivamente particulares e não econômicos, b) para fins exclusivamente jornalístico e artístico, acadêmicos, de segurança pública, defesa nacional ou segurança do Estado, c) para atividades de investigação e repressão de infrações penais, d) provenientes de fora do território nacional e que não sejam objeto de comunicação/uso compartilhado.

241 Acordo de Cooperação Técnica TCU/CNMP. Disponível em: <http://www.cnmp.mp.br/portal/images/Termosdecooperacao/TCU/Acordo_de_Coopera%C3%A7%C3%A3o_CNMP-TCU_LabContas.pdf>. Acesso em 01 nov. 2018.

242 Acordo de Cooperação Técnica TCU/MJSP. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A25DAA01ED015DECBF60F60713&inline=1>. Acesso em 01 nov. 2018.

243 Acordo de Cooperação Técnica TCU/CSJT. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A25E877EBE015EA63F0DCA7A65&inline=1>. Acesso em 01 nov. 2018.

244 PERNAMBUCO. Prefeitura do Recife. **Prefeitura do Recife firma parceria inédita com o TCU para troca de informações**. Disponível em: <http://www2.recife.pe.gov.br/noticias/09/03/2018/prefeitura-do-recife-firma-parceria-inedita-com-o-tcu-para-troca-de-informacoes>. 09/03/82018. Acesso em 05 nov. 2018.

e entidades da administração pública, de bens penhorados pela justiça do trabalho, e, posteriormente, conforme andamento de desenvolvimento de solução computacional específica, do RENAVAM - Registro Nacional de Veículos Automotores e do RENACH - Registro Nacional de Carteira de Habilitação, observadas as limitações técnicas e legais".

Não obstante os questionamentos levantados, é relevante destacar que houve certa preocupação em manter a segurança, o sigilo e a confidencialidade dos dados, tendo sido inseridas cláusulas obrigacionais padrão nesses acordos, exigindo, inclusive, a assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS) ou documento equivalente, nos moldes do Decreto nº 7.845/2012[245].

A mais recente contenda judicial sobre o tema está sendo analisada pelo STF no Mandado de Segurança - MS 36150, cujas partes são o Inep e o TCU. O ministro Luís Roberto Barroso, em 10 dezembro de 2018, concedeu liminar suspendendo a decisão constante de Acórdão 2609, do TCU, de 14 de novembro de 2018, que determinava ao Inep a entrega de microdados individualizados do Censo da Educação Básica e do Exame Nacional do Ensino Médio (Enem), de 2013 a 2016, para auditoria operacional do Programa Bolsa Família, sob pena de aplicação de multa e afastamento temporário do responsável,[246].

O Inep, ao recusar-se a entregar os dados pessoais ao órgão de controle, alega que eles são sigilosos e sua entrega violaria o art. 5º, inc. X, XIV e XXXIII, da CF/88, o art. 23 da LAI, bem como o art. 6º do Decreto nº 6.425/2008, que dispõe sobre o sigilo dos dados do censo educacional, além de resolução da ONU que trata sobre o sigilo estatístico. Além do mais, no momento da coleta dos dados, os estudantes são informados sobre os objetivos para os quais eles serão utilizados, sob a garantia de sigilo das informações pessoais. Nesse sentido, deve-se obedecer o princípio da finalidade.

---

245 Nesse sentido, a Portaria – TCU nº 434, de 26 de setembro de 2017, estabelece critérios para o compartilhamento de informações, documentos e conhecimentos técnicos, no âmbito dos trabalhos em parceria com órgãos de fiscalização e controle. Em seu art. 2º, inc. III, regula: "as informações e os documentos protegidos por sigilo constitucional ou legal somente poderão ser repassados aos órgãos de controle e fiscalização parceiros, bem como deles obtidos, manuseados e inseridos em processos de controle externo, **mediante autorização judicial para seu compartilhamento**". (grifo nosso)

246 Segundo o TCU, esta auditoria teve início com o cruzamento dos dados do Cadastro Único, Folha de Pagamentos do Bolsa Família e RAIS, bases já disponíveis no TCU, visando analisar o impacto do programa Bolsa Família em relação ao acesso ao mercado formal de trabalho pelos jovens integrantes das famílias beneficiárias, com idade em torno de 18 anos. Para complementar a análise, foi necessária a obtenção das bases de dados identificadas do Enem e do Censo Escolar. Apesar de o Inep ter oferecido o acesso identificado aos dados por meio do Sedap, o TCU afirmou que a internalização das bases no próprio órgão é imprescindível, pois o cruzamento dos dados nas dependências do Instituto inviabilizaria a operação. Alega, por fim, o TCU que "apesar dos dados de identificação dos jovens (CPF, Nome, Nome da Mãe) serem necessários para a etapa prévia de cruzamento com outras bases de dados, a exemplo do próprio Cadastro Único, todas as análises econométricas previstas, acontecem de forma agregada, não sendo possível a identificação individual dos jovens, quando da divulgação dos resultados." (trecho do Acórdão 2609/2018 – TCU Plenário).

O TCU, por sua vez, alega que o fornecimento de dados sigilosos ao TCU não configura quebra de sigilo, mas, tão somente, a transferência do dever de confidencialidade das informações ao órgão, uma vez que o art. 31, § 1º, inciso I, da LAI[247] confere ao auditor a possibilidade de acesso às informações pessoais, mesmo que restritas. Além disso, a Lei Orgânica do Tribunal impõe a seus servidores o dever do sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções. Assim, o Inep não poderia restringir informações ao TCU "em razão de suas prerrogativas para o exercício pleno da atividade de controle externo" de programas governamentais.

Barroso, na análise da medida cautelar, entendeu que, não apenas a matéria é sujeita à reserva de jurisdição, "não cabendo ao órgão de controle externo decidir sobre a caracterização de ofensa à garantia constitucional", como "é plausível a alegação de que a transmissão desses dados para finalidade diversa: (i) subverte a autorização daqueles que concordaram em prestar as declarações; e (ii) coloca em risco a capacidade do INEP de pesquisar e monitorar políticas públicas".

Assim, deferiu a liminar tendo sido demonstrado o *periculum in mora* e o *fumus boni iuris,* já que o fornecimento dos dados esvaziaria o objeto da impetração e a iminência da aplicação de multa e de sanções impostas pelo TCU comprovam o dano. O TCU foi notificado para prestar informações e a Procuradoria-Geral da República, para emitir parecer, nos termos da Lei nº 12.016, de 7 de agosto de 2009, que disciplina o Mandado de Segurança.

Cabe, também, salientar a possibilidade que vem sendo aventada de utilização de "salas seguras" (nos moldes das salas de sigilo mencionadas no item 2.2, porém, não para fins de pesquisa[248]) para atividades de controle e fiscalização. Caso específico refere-se à iniciativa, de mais de 20 anos, do TCU de buscar mecanismos para viabilizar seu acesso a dados e informações protegidas por sigilo fiscal e custodiados pela Secretaria da Receita Federal (SRF) para realização de determinados trabalhos de fiscalização na área tributária e aduaneira.

Em agosto de 2018, após reuniões dos grupos de trabalhos formados para discutir "os requisitos técnicos, jurídicos e tecnológicos mínimos para garantir ao mesmo tempo a auditabilidade da administração tributária e a preservação do sigilo fiscal",

---

247 Art. 31, § 1º, inciso I, da Lei nº 12.527/2011: As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem.

248 Ver N.R. 226.

a SRF apresentou ao TCU um plano de ação para tentar implementar um ambiente seguro para acesso aos dados[249].

Por fim, a respeito desse tema, parece ser interessante fazer um alerta quanto à possível interpretação do art. 26, inc. V, da LGDP, incluído pela MP 869/2018. Respeitados os princípios de proteção de dados pessoais, o dispositivo excepciona o uso compartilhado desses dados pelo Poder Público, inclusive possibilitando sua transferência a entidades privadas, na hipótese de esta "objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados". Ora, se até mesmo entidades privadas poderão ter acesso a dados pessoais quando para prevenção de fraudes e irregularidades, mais ainda poder-se-ia falar dos órgãos públicos. Assim, é possível que tal dispositivo sirva de mais um argumento para que órgãos de fiscalização e controle tenham acesso aos dados pessoais para suas atividades finalísticas, mudando alguns dos entendimentos do Judiciário, apresentados nesse item.

3.6 A responsabilização com a eventual divulgação indevida e as dificuldades inerentes ao arbitramento do valor do dano

A violação, o eventual mau uso, bem como os incidentes de segurança com dados pessoais podem acarretar erros ou injustiças aos seus titulares. Qualquer um desses atos pode ofender a um ou mais direitos da personalidade e, em decorrência disso, pode ensejar responsabilização por danos patrimoniais e/ou morais[250]. O Código Civil, no art. 12. prescreve: "Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei".

No modelo europeu, "uma violação de dados pessoais ocorre quando existe uma violação da segurança que provoque, **de modo acidental ou ilícito**, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais tratados"[251]. Segundo o princípio da responsabilização, a organização que trata os dados de outrem é responsável pelos danos que causar e as sanções podem chegar até 20 (vinte) milhões de euros ou até 4% (quatro por cento) do volume de negócios anual

[249] BRASIL. Tribunal de Contas da União. Ambiente seguro dará acesso a dados fiscais sigilosos para auditoria do TCU. **TCU**. 12 set. 2018. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/ambiente-seguro-dara-acesso-a-dados-fiscais-sigilosos-para-auditoria-do-tcu.htm>. Acesso em: 5 mar. 2019.

[250] Súmula 37 do STJ: são cumuláveis as indenizações por dano material e dano moral oriundos do mesmo fato.

[251] COMISSÃO EUROEIA. **O que acontece se os dados partilhados por mim forem violados?**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/what-happens-if-data-i-have-shared-leaked_pt>. Acesso em: 10 out. 2018.

da empresa em nível mundial (art. 83, do RGPD), a depender do grau de severidade das violações. Nesse caso, a organização deve notificar a autoridade de controle (*data breach notification*) e, caso o risco decorrente da violação seja elevado, o titular dos dados também deverá ser informado (art. 33 e 34, do RGPD). Não há diferenciação entre as regras sancionatórias para o setor público ou privado.

Na Europa, havendo a violação dos dados, o cidadão poderá apresentar reclamação à autoridade de proteção de dados, ingressar com ação judicial contra a organização[252] ou contra a própria APD, caso entenda que esta não procedeu corretamente com a reclamação apresentada. As duas primeiras opções podem ocorrer de forma simultânea (arts. 77 a 79, do RGPD).

No caso brasileiro, assim como na norma europeia, a autoridade nacional de dados pode aplicar sanções administrativas aos agentes de tratamento de dados, porém, o valor da multa é inferior ao estipulado na norma europeia: até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado no último exercício ou até R$ 50 milhões de reais por infração (art. 52 a 54 da LGPD).

Para o setor público, há dispositivos específicos para tratar da responsabilidade dos órgãos públicos quando houver infração à Lei (art. 31 e 32, LGPD). Os artigos conferem à autoridade nacional a atribuição de enviar informe com as medidas cabíveis para cessar a violação no tratamento dos dados. E, ainda, a possibilidade de solicitar a publicação de relatórios de impacto e sugerir a adoção de padrões e de boas práticas para o tratamento dos dados.

O p. ún. do art. 38, ao dispor sobre os agentes de tratamento de dados pessoais, prescreve que os relatórios deverão conter, "no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

Importante também dar destaque ao art. 44 da LGPD. Segundo o dispositivo, o tratamento de dados pessoais será considerado irregular: a) quando a legislação não for observada ou b) quando não houver a segurança esperada pelo titular, o que pode abranger o modo, o resultado e os riscos esperados e as técnicas de tratamento disponíveis à época.

[252] Caso a empresa atue em diversos Estados-membros da União Europeia, as APD's desses Estados atuam em cooperação com as demais, num sistema de janela única (ou balcão único), como explicado no capítulo anterior.

Tal qual o modelo europeu, na norma brasileira há necessidade de o controlador de dados comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano ao indivíduo. O prazo de notificação será estabelecido pela ANPD.

Ainda no caso específico do setor público, à exceção da multa - já que, segundo a jurispridência, devido à natureza da Administração Pública, esta implicaria sanção à própria sociedade -, a ANPD poderá aplicar as seguintes sanções administrativas: a) advertência, b) publicização da infração, c) bloqueio dos dados pessoais a que se refere a infração até a sua regularização e d) a eliminação dos dados pessoais a que se refere a infração (art. 52, § 3º). Além disso, as sanções podem ser aplicadas sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)[253].

A maior dificuldade prática, no entanto, ocorre no momento do arbitramento do dano moral sofrido pelo titular dos dados pessoais. No Brasil, o *quantum* indenizatório é medido por sua extensão. Porém, esse cálculo é muito difícil: como quantificar a dor, como diferenciá-la do mero aborrecimento? E os danos morais reflexos ou por ricochete daqueles que tiveram seus dados divulgados indevidamente? Segundo Bessa,

> o caráter extrapatrimonial do direito à vida privada, além de significar que ele não possui valor pecuniário - não integrando, portanto, o patrimônio material do titular - evidencia que as tentativas jurídicas de protegê-lo devem conferir especial ênfase a prevenção. (…) A indenização por dano moral é aceita não como resposta adequada, mas por inexistir outro meio que possa realizar a reparação do bem jurídico[254].

Nessa perspectiva, a tutela inibitória (preventiva) não se confunde com a tutela ressarcitória (ou reparatória), pois aquela não visa à reparação do dano, mas ao impedimento ou repetição da prática do ilícito.

Ainda, por carecer de critérios objetivos, discute-se a ocorrência ou não do dano moral presumido ou *in re ipsa*[255]. O tema é controverso. Atualmente, a jurisprudência

---

253 Destaca-se o art. 34 da LAI: Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso. Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso à informação sigilosa ou pessoal e a submeta a tratamento indevido.

254 BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de protecão ao crédito**. São Paulo: Revista dos Tribunais: 2003.

255 Dano moral *in re ipsa* significa que a força dos fatos, por si, só já demonstra o prejuízo moral que alguém

considera que a inscrição ou a manutenção indevida[256] de nome no SPC, Serasa ou Cadin (Cadastro Informativo de Créditos) configuram danos morais presumidos.

Na mesma lógica, ao analisar julgado do Tribunal Regional do Trabalho da 15ª Região, além de ser possível observar a adoção do dano moral presumido, também verifica-se a necessidade do consentimento e da limitação e controle na utilização de dados pessoais por órgãos públicos para evitar abusos no compartilhamento:

> Ementa. OBTENÇÃO DE INFORMAÇÕES DO TRABALHADORJUNTOACADASTROSINFORMATIZADOS SEM SUA EXPRESSA AUTORIZAÇÃO. DANO MORAL CARACTERIZADO. **O mero acesso aos dados informatizados do cadastro mantido pelo DETRAN ou por qualquer outro órgão, sem a ciência e autorização específica do trabalhador, invade sua intimidade e causa prejuízo à sua honra, ensejando dano moral que deve ser reparado.** (TRT-15–RO: 410220145150044 SP 089934/2014 – PATR, Relator: MARIA INÊS CORREA DE CERQUEIRA CESAR TARGA, Data de Publicação: 28/11/2014, grifo nosso)

Um dos argumentos utilizados pelo autor da ação é de que consta do site do Detran de São Paulo o seguinte alerta: "O cadastro/login para acesso aos Serviços Online no portal Detran/SP é de uso exclusivo e restrito ao titular do documento ou por pessoa por ele autorizada. O uso indevido de informações pessoais é CRIME, que incorre em sanções previstas nos artigos 299 e 307 do Código Penal (falsidade ideológica e falsa identidade) ".

Diante disso, a desembargadora considerou a iniciativa do empregador desarrazoada, uma vez que ele poderia ter pedido diretamente autorização do trabalhador para acessar o site ou ter solicitado que as informações lhe fossem entregues pessoalmente. Condenou, então, o órgão público ao pagamento de R$ 3 mil reais a título de danos morais:

> A fixação do valor da indenização, à míngua de parâmetros objetivos, deve ser fixado de acordo com a condição econômica das partes, o grau de culpa do empregador e a gravidade da ofensa, com observância do princípio da razoabilidade. Não deve, então, ser fixado em valor irrisório ou em montante que importe no enriquecimento injustificado da vítima ou na ruína do empregador. Considerados tais critérios, arbitro à indenização o montante global de R$ 3.000,00, o qual atende ao **caráter pedagógico da pena** infligida ao empregador,

diz ter sofrido, ou seja, não já necessidade de apresentação de provas.

256 Ver, por exemplo REsp 994253 / RS – Relator(a) Ministra Nancy Andrigui – DJ: 15/05/2008.

> bem como guarda proporcionalidade com o prejuízo sofrido pelo demandante, **atendendo adequadamente aos requisitos punitivo e educativo, que visam impedir futuras condutas do mesmo modo pelo empregador**[257]. (grifo nosso)

Em outras situações, no entanto, como no julgado abaixo, a alegação de dano moral presumido não foi aceita. Nesse caso, teria sido necessário, para configurar dano moral, a comprovação de três requisitos: a conduta, o dano e o nexo de causalidade entre eles.

> (…) 5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. (…) II – CASO CONCRETO (…) 4) **Acolhimento da alegação de inocorrência de dano moral "in re ipsa"**. 5) **Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie**. (STJ - REsp 1419697/RS, 2013/0386285-0 Rel. Ministro PAULO DE TARSO SANSEVERINO, Data de julgamento: 12/11/2014, S2 – SEGUNDA SEÇÃO, Data de Publicação: Dje 17/11/2014, grifo nosso)

Nota-se, desse modo, que o arbitramento da indenização por dano moral é um tema de grande relevância, porém, ainda controvertido, no que se refere aos direitos da personalidade no Poder Judiciário. Por outro lado, a possibilidade de aplicação de sanções administrativas trazida pela LGDP, ainda que segundo parâmetros e critérios não tão objetivos, já que de difícil mensuração - tais como a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator e o grau do dano -; e de outros mais claros e objetivos - como a vantagem auferida ou pretendida pelo infrator, a sua cooperação e condição econômica, a reincidência da infração e a adoção reiterada e demonstrada de mecanismos e procedimentos capazes de minimizar o dano (art. 52, § 1º) [258] - devem reduzir a judiciliazação das querelas.

---

[257] Não se adentrará neste trabalho nas discussões doutrinárias e jurisprudenciais acerca da possibilidade de utilização do instituto do "*punitive damages*" pelo ordenamento jurídico brasileiro. A indenização punitiva tem função diferente do caráter compensatório da indenização extrapatrimonial e visa à aplicação de penalidade num montante expressivo com caráter preventivo de desestimular o cometimento de danos futuros.

[258] Na União Europeia, historicamente, vários desses parâmetros já eram utilizados. Para saber se a informação era privada nos julgamentos de delitos contra a privacidade, com informações pessoais divulgadas, era necessário conhecer se o requerente "possuía uma razoável expectativa de privacidade". Atualmente, as compensações por uso indevido de informações confidenciais e por violação à obrigação de proteção de dados têm sido uniformizadas. Alguns parâmetros são utilizados para estabelecer o quantum indenizatório para compensar o sofrimento:

Conclusão

A proteção de dados pessoais e sensíveis é, certamente, um dos temas mais delicados da atualidade. A globalização, a modernização tecnológica e as inúmeras possibilidades de inovação decorrentes da abundância de dados e informações coletados tanto pelo setor público quanto privado geram problemas relativos à ética do uso dos dados, bem como à privacidade dos indivíduos. São exemplos desses problemas a perfilagem comportamental, o estabelecimento de sistemas preditivos, a discriminação estatística, além de discussões como vigilância em massa e controle do cidadão.

O Direito tem papel essencial na conformação dessa situação, devendo atuar como vocalizador de demandas e nos arranjos institucionais, por exemplo. No caso da política pública de proteção de dados pessoais e sensíveis, percebemos que o problema já era identificado há algumas décadas. Porém, apenas em 2015 foi pautado na agenda governamental brasileira em razão do mau uso e do vazamento de dados de autoridades governamentais e da entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia, que exige parâmetros mínimos equivalentes de proteção de dados entre os países para que haja transferências internacionais.

Assim, após três anos de intensos debates, inclusive com participação popular, foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), que vem suprir a ausência de uma norma única e específica para tratar do tema. A Lei, aplicável ao âmbito público e privado, para o ambiente online e off-line, era uma demanda reprimida da sociedade e deve trazer diversos benefícios. Assim, ainda que só entre em vigor em 2020, empresas privadas e órgãos governamentais precisam se adequar para atender às novas regras.

No caso do setor público, objeto do presente estudo e maior detentor de dados e informações dos cidadãos, o compartilhamento e cruzamento de dados, se usados com o devido respeito à privacidade e garantia de segurança, podem auxiliar de

a) a natureza da informação (ex: dados médicos, que são considerados sensíveis); questões financeiras privadas; repetidas intrusões; entre outras ; b) a extensão e o propósito do uso indevido; c) as consequências do uso indevido; d) se houve perda financeira ao autor ou se a ação gerou ganho financeiro ao réu; e) quaisquer considerações políticas relevantes; f) quaisquer fatores atenuantes ou agravantes. "A indenização apropriada dependerá da natureza da informação, da sua importância como informação privada e do efeito na vítima da sua divulgação. Um efeito de curta duração baseado em constrangimento irá atrair menos compensações do que uma intrusão que mudará vidas…" Sobre o assundo, ver: ATKINSON, Steve. **Privacy and data protection cases: quantifying damages for distress.** Disponível em: <https://www.brownejacobson.com/training-and-resources/resources/legal-updates/2017/02/privacy-and-data-protection-cases-quantifying-damages-for-distress>. Acesso em 05 nov. 2018.

forma distintiva as políticas públicas e melhorar o exercício da cidadania, buscando concretizar os direitos fundamentais e evitando a discriminação.

Nesse sentido, a Administração tem se empenhado em aprimorar os serviços públicos centrados no cidadão, por meio de ações que buscam a simplificação do atendimento ao público, o compartilhamento de dados, a promoção de dados abertos, a transparência para os pedidos de acesso a dados, entre outros.

Entretanto, também é possível observar algumas dificuldades em decorrência de interpretações diversas, por vezes errôneas, dadas pelos gestores públicos às normas de conteúdo aberto. Ações precipitadas pela Administração Pública, apesar de muitas vezes bem-intencionadas, que visam ao atendimento dos princípios da transparência e da publicidade, também podem ferir os direitos da personalidade, uma vez que podem permitir o acesso a terceiros ou tornar públicos dados pessoais ou tornados sensíveis pelo cruzamento entre diferentes bases de dados.

Essa problemática está presente no caso específico do acesso a dados disponibilizados pela Administração Pública para fins de pesquisa, como no caso do IBGE, Inep e Ipea. As instituições possuem regras e níveis diferenciados de segurança da informação, o que, em alguns casos, pode acarretar falhas, divulgação indevida e consequente necessidade de responsabilização dos gestores pelo mau uso dos dados.

No caso do compartilhamento de dados entre os diferentes órgãos governamentais, o trabalho também pretendeu demonstrar, apoiado em julgados do TCU e investigações que vêm sendo empreendidas pelo Ministério Público que é preciso atenção quanto à eficiência do modelo de gestão de dados adotado pelo setor público. Numa breve avaliação, parece ser possível afirmar que o modelo descentralizado, por meio de empresas públicas como o Serpro e Dataprev, não tem sido eficiente. Para além disso, destaca-se o fato de o Serpro ser objeto de investigação pela possível comercialização dos dados pessoais e sensíveis.

Ainda sobre a governança de dados, as informações coletadas no estudo demonstraram que iniciativas de interoperabilidade como E-Ping tiveram baixa adesão. Além disso, documentos como o Catálogo e o Dicionário de Dados, apesar de constar das normas que todos os órgãos e entidades da APF deveriam produzir e favorecer diversas ações públicas, não são de exigência obrigatória e, portanto, não foram por eles priorizados.

Há que se ressaltar, por outro lado, as boas iniciativas da Administração na adoção de iniciativas como o modelo de janelas únicas, o uso de repositórios de dados (*Data Lake*) e o desenvolvimento de aplicativos para o cruzamento e a mineração de dados,

visando promover políticas públicas e gerar benefícios concretos para os cidadãos. Ao mesmo tempo, é questionável a utilização de normas infralegais sem o devido respaldo, a inobservância ao princípio da finalidade, a coleta excessiva de dados e a ausência do consentimento livre, expresso e informado em algumas dessas situações.

Acredita-se, no entanto, que, quando da entrada em vigor da LGDP alguns desses problemas serão supridos, já que, para o Poder Público, diferentemente do regime europeu, a norma prescreveu diversas exceções. Entre elas, a exigência do consentimento para o tratamento compartilhado de dados necessários à execução de políticas públicas. A norma também prevê que os dados deverão ser mantidos em formato interoperável e estruturado para uso compartilhado, o que abre brechas para a continuidade das ações de compartilhamento dos dados da forma como ocorre hoje.

A pesquisa buscou, também, discutir a requisição e a utilização de dados pessoais ou sensíveis para fins de fiscalização e controle. Temas ainda controvertidos e que já são objeto de análise pelas Cortes Judiciárias e que podem afetar a coleta dos dados pela Administração e aumentar a desconfiança da população no Estado.

Além disso, mesmo tendo como referência a norma europeia que considera os dados pessoais como espécie dos direitos da personalidade e projeção da dignidade humana, diferentemente desta, a LGDP foi sancionada com alguns vetos importantes. Destaca-se, nesse quesito, a criação da Autoridade Nacional de Proteção de Dados, que é órgão essencial para garantir a aplicação da Lei e, inicialmente, foi vetada por vício de iniciativa. Porém, mesmo tendo sido criada em dezembro de 2018, por meio de Medida Provisória optou-se por deixá-la vinculada à Presidência da República, havendo, então, questionamentos acerca de sua autonomia e independência para realizar as funções fiscalizatórias e normativas e não ser cooptada pelos interesses de grandes empresas ou mesmo do próprio governo devido à vinculação hierárquica.

Por fim, tendo em vista a dignidade humana, foram ressaltadas as problemáticas relacionadas à ofensa aos direitos da personalidade em decorrência do mau uso ou uso indevido dos dados. Uma das principais dificuldades, nesse caso, é o arbitramento do valor do dano.

Nesse cenário, ainda que também tenha sido possível observar diversos problemas quanto à gestão de dados pela APF, como deficiências no quadro técnico, baixo índice de planejamento e ausência de política de segurança da informação em grande parte das instituições governamentais, além de problemas relacionados à legalidade de algumas práticas, é de se acreditar que essa situação tende a melhorar com a vigência

da nova Lei, por exemplo, com a necessidade de incorporar recursos que garantam a privacidade dos titulares desde a concepção, na própria infraestrutura e arquitetura dos sistemas. Além disso, almeja-se que a Autoridade Nacional de Proteção de Dados seja capaz de garantir o *enforcement* na aplicação da Lei.

O presente estudo visou atestar, então, que, de fato, a tutela aos direitos pessoais no Brasil, quando se trata das grandes bases geridas pelo governo ainda são deficientes. Apesar de imperioso reconhecer que diversas iniciativas têm contribuído de forma substancial para promover um novo modelo democrático e participativo, bem como para possibilitar o exercício pleno da cidadania, as práticas demonstram que diversos requisitos de privacidade não estão sendo atendidos. Nesse sentido, e em face das exceções concedidas à APF, a transparência passa a ser o principal mecanismo de controle dos dados pelos cidadãos e o principal desafio para a Administração Pública para garantir a confiabilidade e credibilidade de suas ações perante os cidadãos.

Assim, como novos estudos, sugere-se o monitoramento das ações preparatórias pelo Poder Público até a entrada em vigor da norma. E, a partir de 2020, a investigação da efetividade de sua aplicação.

Também merece ser objeto de acompanhamento a atuação judiciária para averiguar as possíveis mudanças de entendimento a partir da nova legislação e os impactos dessas decisões nas políticas públicas executadas pelo Governo.

Sugere-se, por fim, que seja feito estudo comparado no intuito de verificar as melhores práticas internacionais no que tange à proteção de dados pessoais e sensíveis e, com isso, buscar o aprimoramento do modelo brasileiro atual.

Referências

ABREU, Jacqueline de Souza. **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016>. Acesso em: 10 jan. 2018.

ABREU, Jacqueline de Souza; LAGO, Lucas; MASSARO, Heloísa. **ESPECIAL: Por que se preocupar com o que o Estado faz com nossos dados pessoais.** InternetLab, 21 mai. 2018. Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo//>. Acesso em: 3 ago. 2018.

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.

ATKINSON, Steve. **Privacy and data protection cases: quantifying damages for distress.** Disponível em: <https://www.brownejacobson.com/training-and-resources/resources/legal-updates/2017/02/privacy-and-data-protection-cases-quantifying-damages-for-distress>. Acesso em 05 nov. 2018.

BAIRD, Stacy A., **Government Role and the Interoperability Ecosystem** (Summer 2009). Journal of Law and Policy for the Information Society, Vol. 5, No. 2, p. 219, Summer 2009. Disponível em: <https://ssrn.com/abstract=1482752>. Acesso em: 13 nov. 2016.

BAMBAUER, Derek E. **Privacy Versus Security**. *The Journal of Criminal Law & Criminology*, v. 103, n. 3, 2013, p. 667 – 684.

BARROSO, Luis Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016.

BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de protecão ao crédito.** São Paulo: Revista dos Tribunais: 2003.

BOLZAN DE MORAIS, Jose Luis. **O Estado de Direito "confrontado" pela Revolução da Internet!** Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, RS, v. 13, n. 3, p. 876-903, dez. 2018. ISSN 1981-3694. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/33021>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.5902/1981369433021.

BOLZAN DE MORAIS, Jose Luis; JACOB NETO, E.; BEZERRA, Tiago José de Souza L. **O Projeto de Lei de Proteção de Dados Pessoais (PL 5276/2016) no mundo do Big Data:** o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos Direitos Humanos. Revista Brasileira de Políticas Públicas, [S.I], v. 7, p. 184-198,

2018. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840>. Acesso em: 15 mar. 2019. http://dx.doi.org/10.5102/rbpp.v7i3.4840.

BOURDIEU, Pierra. **A produção da crença***:* contribuição para uma economia dos bens simbólicos. São Paulo: Zouk, 2a Ed., 2004.

Brasil é o país mais vunerável a vazamento de informações, diz pesquisador**. AGÊNCIA O GLOBO.** Disponível em: <http://revistapegn.globo.com/Tecnologia/noticia/2017/09/brasil-e-o-pais-mais-vulneravel-vazamento-de-informacoes-diz-pesquisador.html . Acesso em: 10 jan. 2018.

BRASIL. 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.

BRASIL. Casa Civil da Presidência da República, Instituto de Pesquisa Econômica Aplicada. Avaliação de Políticas Públicas **Guia Prático de Análise Ex Ante.** Brasília: Ipea, 2018. V. 1. Disponível em: <http://www.cgu.gov.br/Publicacoes/auditoria-e-fiscalizacao/arquivos/guia-analise-ex-ante.pdf>. Acesso em 05 nov. 2018.

BRASIL. **Conheça o e-Social.** Disponível em: <http://portal. e-Social.gov.br/institucional/conheca-o>. Acesso em: 10 jan. 2018.

BRASIL. Instituto Brasileiro de Geografia e Estatística. **Projeção da população do Brasil e das Unidades da Federação.** Disponível em: <http://www.ibge.gov.br/apps/populacao/projecao/>. Acesso em: 20 jun. 2018.

BRASIL. Instituto Brasileiro de Geografia e Estatística. . **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal: 2015.** Rio de Janeiro: IBGE, 2016. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/livros/liv99054.pdf>. Acesso em: 21 ago. 2017.

BRASIL. Instituto Brasileiro de Geografia e Estatística. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal: 2015.** Rio de Janeiro: IBGE, 2016. p. 49 Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/livros/liv99054.pdf>. Acesso em: 21 ago. 2017.

BRASIL. Instituto Brasileiro de Geografia e Estatística. **Código de Boas Práticas das Estatísticas do IBGE**. 2014. Disponível em: <ftp://ftp.ibge.gov.br/Informacoes_Gerais_e_Referencia/Cartilha_Codigo_de_Boas_Praticas_das_Estatisticas_do_IBGE.pdf>. Acesso em: 26 jun. 2017.

BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Texeira. **Serviço de Acesso a Dados Protegidos - Sedap:** Solicitação de acesso. Disponível em: <http://portal.inep.gov.br/dados/sedap/solicitacao-de-acesso>. Acesso em: 01 ago. 2018.

BRASIL. Ministério da Educação, Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Serviço de Acesso a Dados Protegidos (Sedap):** Guia do Usuário - versão 1.0. Brasília: Inep, 2019. Disponível em: <http://inep.gov.br/documents/186968/0/Guia+do+usu%C3%A1rio+-+Servi%C3%A7o+de+Acesso+a+Dados+Protegidos+%28Sedap%29/bc9e1642-e937-430a-b5b4-b360bfa6f176?version=1.2>. Acesso em 02 mar. 2019.

BRASIL. Ministério da Justiça. **Pensando o Direito:** Proteção de Dados Pessoais. Disponível em: <http://pensando.mj.gov.br/dadospessoais/> . Acesso em: 09 ago. 2018.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Acesso à Informação:** Busca de pedidos e respostas. Disponível em: <http://www.consultaesic.cgu.gov.br/busca>. Acesso em: 06 ago. 2018.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **E-SIC:** Relatório de pedidos de acesso à informação e solicitantes. Disponível em: <https://esic.cgu.gov.br/sistema/Relatorios/Anual/RelatorioAnualPedidos.aspx>. Acesso em: 09 ago. 2018.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **E-SIC:** sistema eletrônico do Serviço de Informação ao Cidadão. Disponível em: <https://esic.cgu.gov.br/sistema/site/index.aspx>. Acesso em: 09 ago. 2018.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **GovData**: Perguntas Frequentes. Disponível em: <http://govdata.gov.br/>. Acesso em 01 ago. 2018.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Governo Eletrônico.** Disponível em: <https://www.governodigital.gov.br/EGD/historico-1/historico>. Acesso em 01 out. 2018.

BRASIL. Ministério dos Transportes, Portos e Aviação Civil. **Porto sem Papel.** Disponível em: <http://www.portosdobrasil.gov.br/assuntos-1/inteligencia-logistica/porto-sem-papel-psp>. Acesso em: 10 jan. 2018.

BRASIL. **Padrões de Interoperabilidade de Governo Eletrônico – ePING** (versão 2018). Disponível em: <http://eping.governoeletronico.gov.br/> . Acesso em 10 ago. 2018.

BRASIL. Portal do SISP. **Catálogo de Interoperabilidade.** Disponível em: <http://www.sisp.gov.br/faq_interoperabilidade/one-faq?faq_id=13997087>. Acesso em 10 ago. 2018.

BRASIL. Serviço de Processamento de Dados. **Nota à imprensa:** Serpro assegura compromisso com o sigilo de dados dos cidadãos brasileiros. Disponível em: <http://serpro.gov.br/menu/imprensa/notas-a-imprensa-1/nota-oficial-01-06-2018> Acesso em 03 ago. 2018.

BRASIL. Serviço Federal de Processamento de Dados. **API Serpro.** Disponível em: https://servicos.serpro.gov.br/api-serpro/. Acesso em: 03 ago. 2018.

BRASIL. Tribunal de Contas da União. Ambiente seguro dará acesso a dados fiscais sigilosos para auditoria do TCU. **TCU.** 12 set. 2018. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/ambiente-seguro-dara-acesso-a-dados-fiscais-sigilosos-para-auditoria-do-tcu.htm>. Acesso em: 5 mar. 2019.

BRASIL. Tribunal de Contas da União. **Levantamento de Governança de TI.** Brasília: TCU, 2014. Disponível em: < https://portal.tcu.gov.br/comunidades/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/ >. Acesso em: 10 ago. 2018.

BRASIL. Tribunal de Contas da União. **Relatório sistêmico de fiscalização de tecnologia da informação.** Brasília: TCU, 2015. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/sumario-relatorio-sistemico-de-fiscalizacao-de-tecnologia-da-informacao-fiscti.htm>. Acesso em: 10 ago. 2018.

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.

BRESCIANINI, Carlos Penna. **Com revogação de decreto, senadores arquivam projeto sobre sigilo de informações.** Senadonotícias, 27 fev. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/02/27/com-revogacao-de-decreto-senadores-arquivam-o-texto-que-anularia-mudanca-na-lei-de-acesso-a-informacao>. Acesso em 05 mar. 2019.

BRESSER PEREIRA, Luiz Carlos. **Reforma do Estado para a Cidadania**: a reforma gerencial brasileira na perspectiva internaciona. Brasília: ENAP; São Paulo: Editora 34, 1998.

BRITTO, Carlos Ayres. **O humanismo como categoria constitucional**. Belo Horizonte: Fórum, 2012.

BUCCI, Maria Paula Dallari. **O conceito de política pública em direito**. In Políticas Públicas: Reflexões sobre o Conceito Jurídico (Maria Paula Dallari Bucci, org.) São Paulo: Saraiva, 2006.

CASTELLS, Manuel. **Redes de indignação e esperança**: movimentos sociais na era da internet. Rio de Janeiro: Jorge Zahar Editor Ltda., 2013.

CEROY, Frederico Meinberg. **Audiência Pública Interativa:** A oferta de serviços de extração de base de dados de CPF e de CNPJ pelo Serviço Federal de Processamento de Dados (Serpro) para órgãos da Administração Pública, mediante remuneração. 13 jun. 2018. 30 slides. Diponível em: https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=13787> Acesso em: 03 ago. 2018.

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.

COMISSÃO EUROPEIA. **Proteção de Dados**: regras para a proteção de dados pessoais dentro e fora da EU. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection_pt>. Acesso em: 10 out. 2018.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 01 out. 2018.

COSTA, Gilberto. Governo pretende unificar documentos em base digital. **Agência Brasil**, Brasília, 14 jan. 2019. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/governo-pretende-unificar-documentos-em-base-digital>. Acesso em: 25 fev. 2019.

COSTODIO FILHO, Ubirajara. **A Emenda Constitucional 19/98 e o Princípio da Eficiência na Administração Pública**. In : Cadernos de Direito Constitucional e Ciência Política, São Paulo : Revista dos Tribunais, n. 27, p. 210-217, abr./jul. 1999.

COUNCIL OF EUROPE. **Handbook on European data protection Law**. 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Acesso em: 01 ago. 2018.

COUTINHO, Diogo R. **O direito nas políticas públicas.** Disponível em: <http://www.fd.unb.br/images/Pos-Graduacao/Processo_Seletivo/Processo_Seletivo_2016/Prova_de_Conteudo/14_05_12_15O_direito_nas_politicas_publicas_FINAL.pdf>. Acesso em: 10 jun. 2018.

COUTINHO, Marcelo James Vasconcelos. Administração pública voltada para o cidadão: quadro teórico-conceitual. **Revista do Serviço Público,** Brasília, Ano 51, n. 3, p.40-73, jul/set 2000. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/331/337>. Acesso em: 10 jan. 2018.

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

DALLARI, Dalmo de Abreu. **O habeas data no sistema jurídico brasileiro.** Revista da Faculdade de Direito, Universidade de São Paulo, *97,* 2002, 239-253. Disponível em: <https://doi.org/10.11606/issn.2318-8235.v97i0p239-253>. Acesso em: 25 set. 2018.

DALLARI, Dalmo de Abreu. **Ser cidadão**. Revista Lua Nova, São Paulo, vol.1, n.2, p.61-64, jul/set 1984.

DEMARTINI. Felipe. **Apps do governo estão invadido privacidade dos usuários, diz estudo.** Canatech, 28 mai. 2018. Disponível em: <https://canaltech.com.br/seguranca/apps-do-governo-estao-invadindo-privacidade-dos-usuarios-diz-estudo-114680/>. Acesso em: 03ago. 2018.

DE MENEZES NETO, Elias Jacob; DE MORAIS, Jose Luis Bolzan. **Análises computacionais preditivas como um novo biopoder:** modificações do tempo na sociedade dos sensores. Novos Estudos Jurídicos, [S.I], v. 23, n.3, p. 1129-1154, dez. 2018. ISSN 2175-0491. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/13769>. Acesso em: 15 mar. 2019. doi:http://dx.doi.org/10.14210/nej.v23n3.p1129-1154.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** 27. ed. São Paulo: Atlas, 2014.

DONEDA, Danilo Cesar. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Disponivel em http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm#_ftn1> Acesso em: 15 out. 2018.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p.91-108, jul/dez 2012. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658>. Acesso em: 30 mai. 2018.

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

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.

DONEDA, Danilo. **Proteção de Dados Pessoais e LAI.** [13 jun. 2017] Brasília, CGU. Entrevista concedida ao site Governo Aberto – CGU. Disponível em: <http://www.governoaberto.cgu.gov.br/noticias/2017/protecao-de-dados-pessoais-e-lai.> . Acesso em: 05 ago. 2018.

EDELMAN. **2018 Edelman Trust Barometer: Global Report**. Disponível em: <https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf>. Acesso em 07 ago. 2018.

EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. **G1**: online. Disponível em: <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. 04/07/2015. Acesso em: 05 nov. 2018.

EUROSTAT. **Código de Conduta das Estatísticas Europeias**. Disponível em: <http://ec.europa.eu/eurostat/documents/3859598/5922361/10425-PT-PT.PDF>. Acesso em: 20 jul. 2018.

FARIA, José Eduardo. **Sociologia Jurídica**: direito e conjuntura. 2 ed. São Paulo: Saraiva, 2010.

FREITAS, Christiana Soares de. Mecanismos de dominação simbólica nas redes de participação política digital. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso (orgs.). **Democracia Digital, Comunicação Política e Redes:** Teoria e Prática. Rio de Janeiro: Folio Digital: Letra e Imagem, 2016. p. 110-135. Disponível em: <http://livro.democraciadigital.org.br/files/2017/05/Democracia-Digital.pdf>. Acesso em: 25 ago. 2017.

GOMES, Helton Simões. Bancos e lojas pagam até R$ 4,70 por acesso a dados do seu rosto**. UOL**, 06 ago. 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/08/06/bancos-e-lojas-pagam-ate-r-47-para-acessar-dado-do-rosto-de-brasileiros.htm>. Acesso em: 20 set.. 2018.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D.. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito GV**, [S.l.], v. 14, n. 2, p. 513-536, set. 2018. ISSN 2317-6172. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/77110/73916>. Acesso em: 15 mar. 2019.

GOVERNO DO ESTADO DA BAHIA. Secretaria da Segurança Pública. Reconhecimento Facial impede entrada de homicida em circuito. **SSP/BA.** Disponível em: < http://www.ssp.ba.gov.br/2019/03/5310/Reconhecimento-facial-impede-entrada-de-homicida-em-circuito-.html>. Acesso em 06 mar. 2019.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf> . Acesso em: 20 out. 2017.

HARARI, Yuval Noah. **Homo Deus**: Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

HESSEL, Rosana. **Governo altera Lei de Acesso à Informação e aumenta sigilo em dados.** Correio Braziliense, 24 jan. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/politica/2019/01/24/interna_politica,732627/governo-altera-lei-de-acesso-a-informacao-e-aumenta-sigilo-em-dados.shtml. Acesso em 25 fev. 2019.

HOWE, Jeff. **The Rise of Crowdsourcing.** Disponível em: <https://www.wired.com/2006/06/crowds/>. Acesso em: 23 ago. 2017.

HUBLI, K. Scott. **The Legislative Openness Movement**. Disponível em: <https://www.ndi.org/sites/default/files/TheLegislativeOpennessMovement-030917-final.pdf>. Acesso em: 10 jan. 2018.

Justiça de SP proíbe uso de câmeras de reconhecimento facial em painel do Metrô. **G1**: online. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2018/09/14/justica-de-sp-proibe-uso-de-cameras-de-reconhecimento-facial-em-painel-do-metro-de-sp.ghtml>. 14/09/2018. Acesso em 16 out. 2018.

JUSTICE INFORMATION SHARING. **Privacy Act of 1974.** Disponível em: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>. Acesso em: 28 jul. 2018.

KODAMA, Roberto. **Tratamento dos dados pessoais no acesso a informações públicas:** a honra relegada na sociedade da informação. 2018. 224 f. Dissertação (Mestrado) - Curso de Direito, Uniceub, Brasília, 2018.

KUNEVA, Meglena. **Keynote Speech**: Roundtable on Online Data Collection, Targeting and Profiling European Consumer Commissioner. European Comission, Bruxelas, 31 mar. 2009. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>. Acesso em 25 mai. 2018.

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

MARQUES, Marília. Grupo fraudava empréstimos de até R$ 500 mil com dados de servidores federais no DF; três foram presos. G1, Brasília, 09 jan. 2019. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2019/01/09/grupo-fraudava-emprestimos-de-ate-r-500-mil-com-dados-de-servidores-federais-no-df-tres-foram-presos.ghtml> . Acesso em 25 fev. 2019.

MARQUES, Marília. MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro. **G1**, Brasília, 01 jun. 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml>. Acesso em: 15 jun. 2018.

MAWAD, Marie; FOUQUET Helene; GRANT, Nico; Li, Dandan. Venda de dados pessoais é o próximo passo da revolução de big data. **Bloomberg**, 08 jun. 2018.Disponível em: <https://www.bloomberg.com.br/blog/venda-de-dados-pessoais-e-proximo-passo-da-revolucao-de-big-data/>. Acesso em: 15 jun. 2018.

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.

MENDES, Gilmar Ferrreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo; Saraiva, 2017.

MENDES, Laura Schertel Mendes. **Privacidade, proteção de dados pessoais e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertell. **A Tutela da Privacidade do Consumidor na Internet:** Uma Análise à Luz do Marco Civil da Internet e do Código de Defesa do Consumidor. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coordenadores). Direito & Internet III – Tomo I: Marco Civil da Internet (Lei 12.965/2014). São Paulo: Quartier Latin do Brasil, 2015.

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.

OHM, Paul. **Broken Promises of Privacy**: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: <https://ssrn.com/abstract=1450006>. Acesso em: 14 mar 2019.

OLIVEIRA, Carlos Eduardo Goettenauer de. **Credit scoring e big data no regime jurídico brasileiro**. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gama Prata de. (Coord.) Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia – 2017. Belo Horizonte: Fórum, 2018, p. 223-240.

PARLAMENTO EUROPEU, **Diretiva 95/46/CE**. Disponível em: <http://www.wipo.int/wipolex/en/text.jsp?file_id=313012>. Acesso em: 28 jul. 2018.

PERNAMBUCO. Prefeitura do Recife. **Prefeitura do Recife firma parceria inédita com o TCU para troca de informações.** Disponível em: <http://www2.recife.pe.gov.br/noticias/09/03/2018/prefeitura-do-recife-firma-parceria-inedita-com-o-tcu-para-troca-de-informacoes>. 09/03/82018. Acesso em 05 nov. 2018.

PIOVESAN, Flávia. **Temas de Direitos Humanos**. 5 ed. São Paulo: Saraiva, 2012.

PIRES, Maria Coeli Simões. **Esgotamento do modelo de desenvolvimento excludente no Brasil e 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.

PRADO, Jean. Qual é a polêmica em torno da lei de proteção de dados pessoais no Brasil. **Tecnoblog**: online. Disponível em: <https://tecnoblog.net/251604/polemica-lei-protecao-dados-pessoais/>. Acesso em 05 nov. 2018.

PRESCOTT, Roberta. PGR defende criação de uma autoridade nacional de proteção de dados. **Associação Brasileira de Internet**, 24 ago. 2016. Disponível em: <http://www.abranet.org.br/Noticias/PGR-defende-criacao-de-uma-autoridade-nacional-de-protecao-de-dados-1179.html#.WCnjudIrKM9>. Acesso em: 30 mai. 2018.

Projeto de proteção de dados pessoais aguarda sanção de Temer. **G1**: online. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2018/07/projeto-de-protecao-de-dados-pessoais-aguarda-sancao-de-temer.html>. 19/07/2018. Acesso em 10 out. 2018.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A Proteção de Dados Pessoais na Internet no Brasil**: Análise de decisões proferidas pelo Supremo Tribunal Federal. Cadernos do Programa de Pós-graduação em Direito – Ppgdir./ufrgs, [s.l.], v. 11, n. 2, p.89-118, 31 dez. 2016. Universidade Federal do Rio Grande do Sul. http://dx.doi.org/10.22456/2317-8558.61960. Disponível em: <https://seer.ufrgs.br/ppgdir/article/view/61960>. Acesso em: 20 set. 2018.

Recomendação do MPF/DF visa assegurar acesso da Polícia Rodoviária Federal a sistemas do Denatran**. Assessoria de Comunicação da Procuradoria da República no Distrito Federal.** Disponível em: <http://www.mpf.mp.br/df/sala-de-imprensa/noticias-df/recomendacao-do-mpf-df-visa-assegurar-acesso-da-policia-rodoviaria-federal-a-sistemas-do-denatran>. Acesso em: 25 fev. 2019.

RICHARDS, Neil M.; KING, Jonathan H. **Big Data Ethics.** *Wake Forest Law Review*, 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**. RDA: Revista de Direito Administrativo, Rio de Janeiro, v. 266, p.89-123, mai/ago 2014.

RODRIGUES, José Honório. **A pesquisa histórica no Brasil.** 3. ed. São Paulo: Nacional, 1978. p. 133. Disponível em: <http://www.brasiliana.com.br/obras/a-pesquisa-historica-no-brasil/pagina/133/texto>. Acesso em: 16 out. 2018.

ROUVROY, Antoinette. **"Of Data and Men":** Fundamental Rights and Freedoms in a World of Big Data. Bepress. 2016. Disponível em: < https://works.bepress.com/antoinette_rouvroy/64/>. Acesso em: 05 set. 2018.

ROUVROY, Antoinette; STIEGLER, Bernard. **Le régime de vérité numérique:** De la gouvernementalité algorithmique à un nouvel État de droit. Socio, 4, 2015, p. 113-140. Disponível em: <http://journals.openedition.org/socio/1251>. Acesso em: 05 set. 2018.

SANDOVAL-ALMAZÁN, Rodrigo. Open government and transparency: building a conceptual framework. **Convergencia Revista de Ciencias Sociales,** México, v. 68, p.1-24, mai/ago. 2015. Disponível em: <http://convergencia.uaemex.mx/article/viewFile/3660/2613>. Acesso em: 12 nov. 2016.

SANTOS, Maria da Glória Guimarães dos. **Audiência Pública Interativa: A o**ferta de serviços de extração de base de dados de CPF e de CNPJ pelo Serviço Federal de Processamento de Dados (Serpro) para órgãos da Administração Pública, mediante remuneração. 13 jun. 2018. 30 slides. Diponível em: https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=13787> Acesso em: 03 ago. 2018.

SCHREIBER, Anderson. **Direitos da Personalidade**. Rio de Janeiro: Atlas, 2011.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. **The PII Problem**: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, v. 86, 2011, p. 1814-1894. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs>. Acesso em 15 mar 2019.

SECCHI, Leonardo. **Políticas Públicas: conceitos, esquemas de análise, casos práticos.** São Paulo: Cengage Learning, 2012.

SEIFERT, Jeffrey W. **Data mining and homeland security**: an overview. 2008. Prepared for Members and Comittes of Congress - Congressional Research Service. Disponível em: <https://fas.org/sgp/crs/homesec/RL31798.pdf> . Acesso em: 13 nov. 2016.

SILVA, Leandro Augusto da; PERES, Sarajane Marques; BOSCARIOLI, Clodis. **Introdução à mineração de dados:** com aplicações em R. Rio de Janeiro: Elsevier, 2016.

SILVEIRA, Marco Antônio Karam. **Lei de Acesso a Informações Públicas (Lei nº 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.

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.

SOLANAS, Facundo. **La ley de educacion superior en Argentina: un analisis en terminos de referenciales de la accion publica.** Disponível em: <http://publicaciones.anuies.mx/pdfs/revista/Revista149_S4A2ES.pdf>. Acesso em: 25 ago. 2017.

SOLOVE, DJ (2013) **Privacy self-management and the consent dilemma.** Harvard Law Review 126: 1880– 1903. Disponível em: <https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf> Acesso em: 15 out. 2018.

SOMBRA, Thiago Luís. GDPR e proteção de dados pessoais: uma agenda também brasileira. **JOTA**: online, Brasília, 25 mai. 2018. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/gdpr-agenda-brasileira-25052018>. Acesso em 15 jun. 2018.

TEPEDINO, Gustavo. **Temas de direito civil.** Renovar: Rio de Janeiro, 2004.

TSE firma acordo para repassar dados de eleitores à Serasa. **G1**, Brasília, 07 ago. 2013. Disponível em : <http://g1.globo.com/politica/noticia/2013/08/tse-firma-acordo-para-repassar-dados-de-eleitores-serasa.html>. Acesso em: 20 jul. 2018.

UNITED NATIONS DEVELOPMENT PROGRAMME (UNDP). **Human Development Report 2016.** Washington, Dc, USA: Communications Development Incorporated, 2016. Disponível em: <http://www.br.undp.org/content/dam/brazil/docs/RelatoriosDesenvolvimento/undp-br-2016-human-development-report-2017.pdf>. Acesso em: 21 ago. 2017.

UNITED NATIONS. **United Nations Fundamental Principles of Official Statistics**: implementation guidelines. 2015. Disponível em*:* <https://unstats.un.org/unsd/dnss/gp/Implementation_Guidelines_FINAL_without_edit.pdf>. Acesso em*:* 20 jun. 2018.

URIBE, Gustavo. **Para Mourão, mudança de regra sobre sigilo de dados não afeta transparência.** Folha de S. Paulo, 24 jan. 2019. Disponível em: https://www1.folha.uol.com.br/poder/2019/01/para-mourao-mudanca-de-regra-sobre-sigilo-de-dados-nao-afeta-transparencia.shtml. Acesso em 25 fev. 2019.

VARELLA, Marcelo D.; OLIVEIRA, Clarice G.; MOESCH, Frederico. **Salto digital nas políticas públicas**: oportunidades e desafios. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, p. 560-583, 2017. ISSN 2236-1677. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4808/0>. Acesso em:15 mar. 2019. DOI: http://dx.doi.org/10.5102/rbpp.v7i3.4808.

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

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 28 jul. 2018.

WARSMANN, Jean-luc. **Simplifions nos lois pour guérir un mal français***:* rapport au Premier ministre. 2008. Disponível em: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000276.pdf>. Acesso em: 16 jul. 2016.

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: <https://artigos.ibge.gov.br/artigos-home/estatistica/8050-aperfeicoamentos-no-processo-de-acesso-a-microdados-restritos-no-ibge.html>. Acesso em: 16 mai. 2016.