XX ENANCIB
21 a 25 Outubro/2019 – Florianópolis
A Ciência da Informação e a era da Ciência de Dados

GT-4 – GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

HORIZONTES SOBRE OS DADOS PESSOAIS NO BRASIL: A LEI GERAL DE PROTEÇÃO E A AUTORIDADE NACIONAL DE DADOS EM QUESTÃO

HORIZONS ABOUT PERSONAL DATA IN BRAZIL: THE GENERAL PROTECTION ACT AND THE NATIONAL DATA AUTHORITY IN QUESTION

Lucia Maria Velloso de Oliveira (Universidade Federal Fluminense – UFF/Fundação Casa de Rui Barbosa)
Bianca Therezinha Carvalho Panisset (Universidade Federal Fluminense – UFF/Fundação Casa de Rui Barbosa)
José Antonio da Silva (Universidade Federal Fluminense – UFF/Fundação Casa de Rui Barbosa)

Modalidade: Trabalho Completo

Resumo: A presente pesquisa discute os horizontes dos dados pessoais no Brasil a partir da promulgação da Lei Geral de Dados Pessoais e a criação de uma Autoridade Nacional para a proteção, criação de normas e fiscalização de procedimentos sobre o uso de dados privados no país. Questionamos a efetividade da Lei Geral e de sua Autoridade Nacional em seu intento de controlar o mercado de dados particulares estabelecidos. Nesse sentido, nosso objetivo geral é o de analisar essas leis quanto às possibilidades efetivas de contribuírem para controlar o tráfico de dados ilegal que vem ocorrendo no país. Para isso, recorremos a uma análise documental, através da qual discutimos o enquadramento entre o texto dos referidos normativos legais e o contexto informacional brasileiro. Nossos resultados apontam para um avanço na política de dados pessoais no Brasil com a introdução da legislação dedicada ao tema. Contudo, a partir de uma análise crítica dos artigos que a fundamentam, constatamos algumas inconsistências em sua concepção.

Palavras-chave: Dados Pessoais; Lei Geral de Proteção; Autoridade Nacional.

Abstract: This research discusses the horizons of personal data in Brazil from the enactment of the General Personal Data Law and the creation of a National Authority for the protection, creation of rules and supervision of procedures on the use of private data in the country. We question the effectiveness of the General Law and its National Authority in its attempt to control the established private data market. In this sense, our general objective is to analyze these laws regarding the effective possibilities of contributing to control the illegal data traffic that has been occurring in the country. For this, we resort to a documentary analysis, through which we discuss the framing between the text of the referred legal norms and the Brazilian informational context. Our results point to an advance in the personal data policy in Brazil with the introduction of legislation dedicated to the subject. However, from a critical analysis of the articles that support it, we found some inconsistencies in its design.

Keywords: Personal Data; General Law of Protection; National Authority.

1 INTRODUÇÃO

A discussão sobre o uso de dados pessoais no mundo foi fomentada pelo escândalo envolvendo a empresa Cambridge Analytica. A referida organização foi acusada de extrair milhões de dados privados da rede social *Facebook*, sem a devida autorização dos proprietários, sendo processada nos Estados Unidos e no Reino Unido por sua conduta ilegal na obtenção das informações de cidadãos de diversos países, entre eles, o Brasil.

A mesma empresa foi apontada ainda por utilizar dados pessoais para orientar resultados de processos eleitorais recentes, entre eles, o plebiscito sobre o *Brexit* e a eleição norte americana do ano de 2016.

Para isto, a Cambridge Analytica utilizava-se do processo de mineração de dados, ou *data mining*, correspondendo à manipulação de dados pessoais com a finalidade de traçar perfis de personalidade e de consumo, além de tendências político-ideológicas e composição de informações sobre grupos de interesses, por meio de algoritmos.

No entanto, essa ação passa a ser criminosa quando o dado é utilizado sem o devido consentimento do indivíduo ao qual se refere. Adicionalmente ao uso desautorizado de dados, estão as questões que ferem a soberania das nações, e, concomitantemente, a democracia. Além disso, a questão perpassa o uso de dados com finalidade lucrativa: a venda de dados sensíveis a terceiros, apontando para um mercado de dados privados.

Nesse escopo, deparamo-nos, durante a pesquisa, com a notícia da representação do Ministério Público do Distrito Federal e Territórios (MPDFT) contra o Serviço Federal de Processamento de Dados (SERPRO) sobre o serviço *Datavalid*. Segundo o MPDFT, o *Datavalid* utiliza o banco de dados da Carteira Nacional de Habilitação (CNH), fornecendo informações pessoais, dados de cadastro biométrico e de reconhecimento facial. Mas esses fornecimentos não são autorizados pelo cidadão ao solicitar sua CNH (MPF, 2019).

A representação do MPDFT nos alerta para a urgência da discussão sobre a apropriação e uso de nossos dados pessoais, e que esse problema não está restrito às empresas privadas que utilizam, por exemplo, nossos dados extraídos de redes sociais.

Ainda no Brasil, o jornal *Correio Brasiliense*, em 16/07/2018, publicou notícia sobre a venda livre de dados no país, com a manchete: "*Dados pessoais de brasileiros são negociados livremente na internet - Enquanto o Legislativo e o Executivo discutem proteção a dados*

pessoais, informações de milhares de brasileiros são negociadas ilegalmente na internet, a preços irrisórios" (Correio Brasiliense, 2018).

No texto, além de apontar a ação de empresas e organizações privadas, o jornal menciona uma fonte que afirma que até mesmo as instituições públicas, por meio da ação de servidores públicos mal-intencionados, estariam vendendo dados pessoais.

Isso pode ser ratificado quando verificamos dois casos amplamente noticiados na mídia. O primeiro se refere a um site denominado *Tudo sobre todos*, que supostamente proporcionaria a venda ilegal de dados privados, sendo alvo de investigação por parte do Ministério Público Federal. Do mesmo modo, o segundo episódio diz respeito à já mencionada maior empresa pública de tecnologia da informação do mundo, o Serviço de Processamento de Dados (SERPRO), do governo federal brasileiro, que também vem sofrendo acusações de supostos esquemas de vendas de dados pessoais.

A situação é tão alarmante no mundo que, em Singapura, foram roubados aproximadamente 15 mil dados sobre portadores do vírus HIV no país, segundo a agência de notícias britânica Reuters. O vazamento desses dados permitiu o acesso desde o nome do cidadão ao seu endereço, representando uma exposição delicada sobre um assunto sensível aos indivíduos daquela nação (G1, 2018).

Lott e Cianconi, em estudo sobre vigilância e privacidade, publicado em 2018, na Revista Perspectivas em Ciência da Informação, afirmam que:

> o aproveitamento indevido de informações pessoais vem se tornando cada vez mais frequente, o que traz à tona discussões sobre os critérios de segurança dos bancos de dados e a transparência das políticas de privacidade que devem assegurar aos usuários a propriedade sobre seus dados (LOTT; CIANCONI, 2018, p.119).

O contexto, então, sinaliza que vivemos numa era de expansão informacional complexa, veloz, volumosa e variada, como propõe o conceito de *Big Data*, que diz respeito ao conjunto de dados que precisam ser geridos com a devida atenção ao seu processamento, armazenamento e segurança. Isto vai ao encontro do que se prevê para a boa gestão da informação e do conhecimento.

Amorim e Tomáel ratificam essa compreensão, ao afirmarem que "na sociedade contemporânea, a informação e o conhecimento estão sendo considerados fundamentais para as organizações que se encontram em ambientes ambíguos e de extrema incerteza" (AMORIM; TOMÁEL, 2011, p.2).

Diante desses cenários complexos, que não se esgotam aqui, o Brasil começa a criar mecanismos de proteção legais. Em 2018, o ex-presidente Michel Temer promulgou a Lei nº 13.709, de 14 de agosto, chamada *Lei de Proteção de Dados Pessoais*, com o "objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Já em julho de 2019, foi definida, pelo Poder Executivo, a estrutura da Autoridade Nacional de Proteção de Dados (ANPD), "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional", segundo a Lei Federal nº 13.853/2019. Tanto a Lei Geral de Proteção (LGPD) quanto a Autoridade Nacional de Dados (ANPD) denotam novos horizontes sobre a gestão dos dados privados no país, diante da situação alarmante provocada pela era do *Big Data*.

No entanto, questionamos a efetividade da LGPD como parte do arcabouço jurídico-legal brasileiro e da ANPD, em seu intento de controlar o mercado de dados estabelecidos, visto que estes instrumentos apontam algumas incongruências em sua concepção.

O fato de a Autoridade Nacional ficar subordinada diretamente ao presidente da República, por exemplo, deixa em dúvida a legitimidade do chefe do executivo para atuar com tanta proximidade a uma estatal que regulará o uso de dados privados no país, inviabilizando o caráter independente do órgão e possibilitando que, mais uma vez, dados pessoais possam ser utilizados para fins de controle político ou sem a devida autorização de seus produtores.

Ainda que a legislação preveja que, em momento oportuno, ela poderá virar uma agência autônoma, já é possível sinalizar as incoerências definidas na Lei para a proteção de dados, visto que a subordinação direta ao Poder Executivo também expõem, de algum modo, dados sensíveis de milhões de brasileiros.

Nesse sentido, este trabalho de pesquisa tem por objetivo analisar a Lei de Proteção de Dados Pessoais e apresentar a Autoridade Nacional quanto às possibilidades efetivas de contribuírem para controlar o tráfico ilegal de dados que vem ocorrendo no país.

Como objetivos específicos, pretendemos: a) apresentar a LGPD e a ANPD; b) discutir o enquadramento entre o texto da LGPD e o contexto informacional brasileiro; e c) contribuir para a reflexão acerca de medidas que possam ajudar na proteção de dados pessoais dos cidadãos brasileiros. Como metodologia, utilizaremos uma análise documental visando a análise da LGPD e uma suscinta discussão acerca da ANPD.

Assim, com base nas discussões sobre a lei e a literatura de referência, pretendemos responder à questão central de investigação, delineando os horizontes que se configuram para o país no que se diz respeito à segurança dos dados pessoais no Brasil.

2 DADOS PESSOAIS NO BRASIL: TRAJETÓRIA

A discussão sobre instrumentos de proteção de dados pessoais no Brasil ainda é pouco explorada. Em que pese esta situação, observamos que, antes da promulgação das duas leis que criaram a LGPD e a ANPD, a questão do dado privado encontrava-se pulverizada na Constituição Federal de 1988, no Código de Defesa do Consumidor, na Lei de Arquivos, no Código Civil, na Lei de Acesso à Informação, na Lei de Tipificação criminal de delitos informáticos, no Marco Civil da Internet e, mais recentemente, no Decreto de Dados Abertos.

Na Constituição Federal de 1988, a discussão sobre dados privados esteve, em certa medida, reduzida ao art. 5º, inciso XII, onde se preceitua:

> 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 (BRASIL, 1988, grifo nosso).

Embora o referido inciso constitucional estivesse, desde então, entre as garantias e inviolabilidades previstas pela Carta Magna em seu art. 5º, esta configuração não possibilitou que a questão sobre os dados fosse tratada de modo tímido.

Naturalmente, quando da promulgação do texto constitucional, o período histórico citado não tinha o fluxo de dados no país como nos dias de hoje. Logo, o referido trecho tinha tão somente por pressuposto assegurar um direito que não existia até então, em virtude do regime ditatorial vivenciado entre 1964 e 1985: a proteção de seus dados com finalidades persecutórias da ditatura militar.

O mesmo artigo previra o instituto do *habeas data*, cuja possibilidade de concessão, segundo a Carta Magna de 1988, seria para: a) "[...] assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público"; e b) "[...] a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (BRASIL, 1988).

Ainda no mesmo artigo 5º, em seu inciso XXXII, a Constituição previu que "o Estado promoverá, na forma da lei, a defesa do consumidor", sem, contudo, detalhar como isso se

daria. Na esteira dessa obrigação normativa constitucional, foi promulgada a Lei Federal nº 8.078, de setembro de 1990, conhecida como o *Código de Defesa do Consumidor* (CDC). Compreendia-se, então, como consumidor, "toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final", segundo a CDC.

Esta Lei, que inovava ao ditar regras para as relações de consumo, apontando a linha entre os direitos e deveres do consumidor e do fornecedor de produtos e serviços, abordava como direitos básicos do consumidor:

> Art. 6º São direitos básicos do consumidor: **I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;** II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; **IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;** V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas; **VI - a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos;** VII - o acesso aos órgãos judiciários e administrativos com vistas à prevenção ou reparação de danos patrimoniais e morais, individuais, coletivos ou difusos, assegurada a proteção jurídica, administrativa e técnica aos necessitados; VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências; IX - (Vetado); X - a adequada e eficaz prestação dos serviços públicos em geral (BRASIL, 1991, grifos nossos).

De início, o Código previu a "segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços (...)". E ainda menciona, nos incisos seguintes, "métodos comerciais coercitivos ou desleais" e a possibilidade de "reparação de danos", em casos de não atendimento aos preceitos daquela legislação.

Ainda que não tratando de dados pessoais em si, o *Código de Defesa do Consumidor* começa a esboçar as linhas gerais sobre o direito dos usuários de produtos e serviços ofertados pelo mercado. Este instrumento, em vigência atualmente, ainda que tacitamente, favorece a discussão de práticas que não trazem segurança aos consumidores diante da expansão e rapidez tecnológica, entre elas a transação de dados a partir de compras realizadas na internet.

Um exemplo mais contemporâneo pode ser mencionado quando qualquer indivíduo realiza uma determinada compra pela *web* e, então, passa a receber uma sequência de e-mails, mensagens de textos e até mesmo propagandas em redes sociais sobre produtos e serviços similares aos adquiridos recentemente.

Isso demonstra que nossos dados estão sendo, de algum modo, utilizados e sem nossa autorização, colocando em risco nossa segurança e, portanto, infringindo o disposto no inciso I do CDC.

Ainda no início dos anos 1991, a Lei nº 8.159, de 8 janeiro, denominada *Lei de Arquivos*, dá continuidade, ainda de modo incipiente, às discussões sobre dados pessoais, ao prever neste instrumento normativo federal a gestão de arquivos públicos e arquivos privados. Ainda que, mais uma vez, não se mencione o dado pessoal ou que este seja o assunto principal, esta Lei já demonstra a relevância do arquivo privado:

> Art. 11 - Consideram-se arquivos privados os conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, em decorrência de suas atividades. Art. 12 - Os arquivos privados podem ser identificados pelo Poder Público como de interesse público e social, desde que sejam considerados como conjuntos de fontes relevantes para a história e desenvolvimento científico nacional. Art. 13 - Os arquivos privados identificados como de interesse público e social não poderão ser alienados com dispersão ou perda da unidade documental, nem transferidos para o exterior. Parágrafo único - Na alienação desses arquivos o Poder Público exercerá preferência na aquisição. Art. 14 - O acesso aos documentos de arquivos privados identificados como de interesse público e social poderá ser franqueado mediante autorização de seu proprietário ou possuidor. Art. 15 - Os arquivos privados identificados como de interesse público e social poderão ser depositados a título revogável, ou doados a instituições arquivísticas públicas. Art. 16 - Os registros civis de arquivos de entidades religiosas produzidos anteriormente à vigência do Código Civil ficam identificados como de interesse público e social (BRASIL, 1991).

A Lei de Arquivos já denota que o documento produzido por uma pessoa pode ter relevância, representando o contexto de uma época, envolvendo hábitos, costumes e cultura de modo geral. No entanto, o acesso a esse conteúdo, se transformado de interesse público, necessitaria previamente de "autorização de seu proprietário ou possuidor", denotando que somente o produtor pode permitir que qualquer informação pessoal sobre sua vida esteja nas mãos de terceiros, mesmo que estes sejam da administração pública. A referida Lei aponta então a necessidade de protocolos mínimos para se lidar com o conteúdo documental advindo de ação privada, como norteiam as boas práticas para o zelo com as informações pessoais.

O Código Civil de 2002, promulgado pela Lei Federal nº 10.406, também previa alguma proteção à informação pessoal quando, no artigo 21, explicita: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002). Entretanto, continua sendo uma situação que não abarca a discussão sobre dados pessoal na profundidade que o caso requer.

A Lei de Acesso à Informação (LAI), dispositivo federal nº 12.527, promulgado em 2011, trouxe para o contexto brasileiro inovações com relação ao acesso à informação. Todavia, ainda assim, manteve-se tanto quanto silenciosa no que se referia ao dado pessoal. No referido dispositivo legal, o art. 4º elucida o conceito de "informação pessoal": "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011). No mais, embora o texto tenha promovido uma modificação nas discussões acerca do acesso, ele manteve a lacuna dos dispositivos legais que o antecederam no que diz respeito ao conteúdo de natureza privada.

A discussão sobre o dado pessoal ganha força a partir de uma ocorrência com a atriz brasileira Carolina Dieckman. A atriz teve seu computador acessado e arquivos privados subtraídos, envolvendo fotos de caráter íntimo que foram difundidas pelas redes sociais com amplo alcance. Diante da repercussão, a então presidente Dilma Rousseff submete ao Congresso e promulga uma lei que altera e tipifica, no Código Penal Brasileiro, a invasão de dispositivo informático:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa" (BRASIL, 2012; BRASIL, 1940).

Embora tenha sido considerada uma medida adequada, a mera definição da possibilidade do acesso indevido a dispositivos informáticos persistia em não promover uma discussão necessária ao uso, tramitação, segurança e gestão do dado pessoal por meio eletrônico. Precisava-se, então, de uma discussão que aprofundasse a gestão desse ambiente, o uso de sistemas e demais discussões sobre recursos informacionais na *web*.

Nesse sentido, alguns anos depois do episódio, o dado pessoal começa a ser discutido a partir do chamado *Marco Civil da Internet*, ou a Lei Federal nº 12.965, de 23 de abril de 2014,

que tinha por objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Pelo preâmbulo, é possível, de imediato, apontar que o Marco não tinha por objetivo enfrentar a gestão dos dados pessoais, mas, sim, regular as relações advindas do contexto eletrônico na *web*. Contudo, foi neste dispositivo que mais se mencionou o dado particular como objeto de interesse. O art. 3º disciplinara o uso da internet e propunha, entre seus princípios, a "proteção à privacidade". E, no artigo 8º, propunha: "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (BRASIL, 2014).

E, enfim, com mais especificidade ao tema deste artigo, aludia sobre o dado pessoal na seguinte perspectiva:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de **dados pessoais** ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à **privacidade, à proteção dos dados pessoais** e ao sigilo das comunicações privadas e dos registros (BRASIL, 2014, grifos nossos).

Além disso, dá os primeiros passos acerca de dados pessoais quando, no parágrafo terceiro do artigo supracitado, previu que:

> Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações (BRASIL, 2014).

Por fim, a regulamentação dos dados abertos no Brasil, consolidado pelo Decreto 8.777, de 11 de maio de 2016, menciona que a Política de Dados Abertos do Executivo federal seria coordenada pela Controladoria-Geral da União (CGU) utilizando-se a chamada Infraestrutura Nacional de Dados Abertos - INDA. A esta última, por sua vez, foi atribuída poderes para "(...) estabelecer normas complementares relacionadas com a elaboração do Plano de Dados Abertos, bem como relacionadas à **proteção de informações pessoais** na publicação de bases de dados abertos nos termos deste Decreto" (BRASIL, 2016, grifo nosso).

Diante dessa síntese do cenário do arcabouço jurídico brasileiro, podemos perceber que, até a promulgação da Lei Geral de Proteção de Dados, em 2018, (que entrará em vigor efetivamente apenas em agosto de 2020) e a efetiva criação de uma Autoridade Nacional para sua gestão, em 2019, a proteção aos dados privados não foi foco de interesse e dedicação do

Estado brasileiro. Configuração que, no campo científico foi bem diferente, pois muitas pesquisas, sobretudo no campo da Ciência da Informação, já discutiam a questão do dado pessoal no país.

Logo, o aprofundamento do debate, que agora começa a tomar forma legal, pode estar vindo tardiamente, tendo permitido que o silêncio da lei provocasse o uso indevido de dados de muitos brasileiros e possibilitasse que os cidadãos estivessem à mercê dos interesses econômicos advindos do desigual espaço ocupado por usuários de produtos e serviços e sua relação com o mercado e a avançada tecnologia.

Mesmo assim, entendemos que, com a chegada da Lei de Proteção de Dados e de sua Autoridade Nacional, esta discussão deve começar a ser ampliada no âmbito da Ciência da Informação, a fim de colaborar para evitar que a timidez estatal adotada sobre o tema durante as últimas décadas, do ponto de vista legal, possa continuar nas agendas de discussão da área. Sobretudo porque na questão do dado pessoal, abrangendo sua gestão, segurança e configuração, perpassa um problema de informação.

Saracevic (1996), ao discutir a ecologia informacional, propõe caminhos para discussões que se assemelhem à situação incipiente dos dados pessoais no Brasil. Menciona, então, o autor:

> Qualquer estudo sobre problemas específicos da informação e as tentativas de solução, para serem significativos e bem sucedidos, não podem ser desenvolvidos isoladamente dos demais atores e mecanismos da cadeia ecológica. Os princípios ecológicos devem ser invocados. Por exemplo, a otimização de um elemento ecológico não significa, necessariamente, um melhor funcionamento total da ecologia; ao contrário, algumas vezes pode representar o declínio do seu equilíbrio. Em outras palavras, o estudo e a solução de qualquer problema específico da informação exige, como regra, a consideração dos vários outros atores e mecanismos no conjunto maior da ecologia informacional (SARACEVIC, 1996, p.58).

Ainda que o silêncio estatal-legal dos últimos anos não tenha sido adequado, quando nos detemos à fala de Saracevic acima - através da qual ele destaca que “a otimização de um elemento ecológico não significa, necessariamente, um melhor funcionamento total da ecologia; ao contrário, algumas vezes pode representar o declínio do seu equilíbrio” -, passamos a questionar se a promulgação de dois importantes marcos legais para a gestão de dados pessoais no Brasil, dado o contexto político vivenciado nos últimos anos, reflete o caminho de ascensão de boas práticas ou o enfraquecimento, em algum grau, das intenções desse novo contexto normativo.

Esta avaliação, para ser respondida, envolve compreender os fundamentos das recém promulgadas leis acerca dos dados pessoais no país, com especial enfoque numa discussão sobre direitos humanos e ética.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E A AUTORIDADE NACIONAL: FUNDAMENTOS

A proteção à privacidade é uma questão tão relevante que esta segurança jurídica se faz presente em duas referências internacionais: a Convenção Europeia de Direitos Humanos e a Declaração Universal dos Direitos Humanos.

No Brasil, em um período da história recente no qual a frase "Direitos humanos para humanos direitos" vem sendo alardeada sem a menor culpa ou cerimônia por alguns grupos, discutir o tema das garantias individuais torna-se cada vez mais oportuno e conveniente. Entre eles**,** o direito à privacidade, ao direito à intimidade e o respeito às informações de natureza sensível. Segundo Magrani, na obra *Entre dados e robôs - ética e privacidade na era da conectividade*, o autor menciona que:

> o direito à privacidade, esfera do direito à vida privada, está intimamente conectado à proteção da dignidade e personalidade humanas, e pode ser extraído do reconhecimento constitucional dado à intimidade, à vida privada e à inviolabilidade de dados (MAGRANI, 2019, p.86).

Nesse sentido, no âmbito das discussões sobre a Ciência da Informação, compreender a dimensão ética do acesso ao dado pessoal como uma garantia fundamental à manutenção do Estado Democrático de Direito no Brasil contribui para que não nos esqueçamos os pressupostos do conceito de "direitos humanos" e busquemos reiterar a importância, dentre eles, do direito à privacidade.

Estes direitos fundamentam-se no respeito mínimo aos seres humanos e ao seu pleno exercício de uma vida digna, como moradia adequada, saúde para todos, educação, liberdade de expressão e tantas outras práticas que legitimam uma proposta realmente humanitária e equalizadora. Não fugindo deste escopo, portanto, o respeito à sua privacidade e intimidade.

Logo, o uso, obtenção, transmissão de quaisquer informações pessoais sem o consentimento prévio proporciona um desequilíbrio no pleno direito à privacidade, que deve estar amparado por critérios de segurança e de proteção à vida particular.

Estranha-se, então, que, passados quase 30 anos após a vigência da atual Constituição brasileira, somente no biênio 2018-2019 tenham sido promulgadas duas leis que tratam efetivamente o dado pessoal, a Lei Geral de Proteção de Dados (LGPD), Lei 13.709 de 14 de

agosto de 2018, e a lei de criação de uma Autoridade Nacional de Proteção de Dados (ANPD), a Lei nº 13.853, de 08 de julho de 2019.

Conforme o artigo 5º da LGPD, dado pessoal é "informação relacionada à pessoa natural identificada ou identificável". Essa definição é semelhante à de informação pessoal utilizada no art. 4° da LAI, onde considera "informação pessoal: aquela relacionada a pessoa natural identificada ou identificável". A própria definição de dado pessoal já designa o caráter privado ao qual ele se refere, sendo a questão da privacidade umas das mais sensíveis a se tratar quando da discussão sobre o assunto.

Paul M. Schwartz, especialista em legislação de proteção de dados e professor da *UC Berkeley School of Law*, da Universidade da Califórnia, em pesquisa publicada no ano de 2003, discutiu as questões de propriedade e privacidade em dados pessoais, sob a perspectiva do dado como *commodity* (mercadoria).

O autor supramencionado desenvolveu um modelo de propriedade de dados pessoais que preservasse a privacidade, a partir de cinco elementos críticos: limitações no direito do indivíduo de transferir a propriedade de suas informações pessoais; regras padrão que forçam a divulgação dos termos de troca (linguagem utilizada no comércio internacional para caracterizar a relação entre o valor das importações e o das exportações de um país em período de tempo determinado); um direito de saída para os participantes do mercado; o estabelecimento de danos para impedir abusos de mercado; e instituições para fiscalizar o mercado de informação pessoal e punir violações de privacidade (SCHWARTZ, 2003, p. 2056).

O artigo acima, produzido há dezesseis anos nos Estados Unidos, mantém-se atual na discussão da privacidade e da propriedade dos dados pessoais, situação bastante agravada desde que as redes sociais passaram a fazer parte do cotidiano de uma quantidade significativa de pessoas no mundo, onde inúmeros dados pessoais são voluntariamente divulgados pelos seus detentores. Tais dados abrangem informações sobre o bairro onde se reside, as escolas frequentadas, viagens, refeições, nomes de familiares e interesses de itens de consumo, isso sem contar a quantidade de informação pessoal que se fornece executando-se os mais variados tipos de teste de personalidade e o uso "gratuito" de aplicativos, que é condicionado ao fornecimento dos nossos dados, entre muitos outros.

Nesse contexto, o Brasil, no ano de 2018, publicou a sua Lei Geral de Proteção de Dados (LGPD). Outros países também caminham no mesmo sentido da proteção dos dados

pessoais dos indivíduos e publicaram suas legislações, como a União Europeia (de onde o Brasil se inspirou para produzir sua lei), Estados Unidos e México.

A LGPD é o instrumento normativo que disciplina a proteção e o tratamento dos dados pessoais no Brasil e entrará em vigor no país em 14 de agosto de 2020. O tratamento de dados pessoais com o qual a LGPD se envolve, de acordo com seu artigo 5º, refere-se a:

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A Autoridade Nacional de Proteção de Dados já estava prevista na LGPD de 2018, mas a Lei nº13.853/2019 a criou sem aumento de despesa, como órgão da administração pública federal, integrante da Presidência da República, de natureza jurídica transitória, podendo ser transformada em entidade da administração pública indireta. Sua finalidade é zelar, implementar e fiscalizar a aplicação da LGPD no Brasil. A este órgão compete ainda elaborar as diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

A ANPD possui autonomia técnica e decisória, garantida pela lei supramencionada. Entretanto, este órgão é subordinado à Presidência, sendo todos os membros de seu conselho diretor indicados pela maior autoridade do país, o que beira, em nossa visão, a uma possibilidade da adoção de métodos clientelistas para a ocupação das vagas.

Salientamos, então, alguns aspectos considerados relevantes a partir da promulgação da LGPD e da criação da ANPD: o tratamento dos dados pessoais, exigindo que haja o consentimento de seu titular; criação de informações sobre a utilização de dados pessoais de um titular; a caracterização de dados sensíveis (“[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, [...] à saúde ou à vida sexual, [...] genético ou biométrico”), a regulamentação do seu tratamento no artigo 11 e a vedação de seu uso para atividade econômica; a possibilidade do titular acessar, retirar e corrigir os seus dados do controlador, a quem competem as decisões referentes ao tratamento de dados pessoais; a tratativa da transferência internacional de dados pessoais; e a criação de uma Autoridade Nacional de Proteção de Dados que, dentre seus objetivos, compete-lhe: zelar pela proteção dos dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle

dos titulares sobre seus dados pessoais. Essas ações denotam, a princípio, um contexto que estabelece regras quanto às responsabilidades no uso de dados pessoais.

Rafael Capurro, em artigo intitulado *A liberdade na era digital* (2017), faz reflexão sobre a liberdade e as responsabilidades na era digital. Este é um aspecto que tangencia o tema do presente trabalho, pois o tratamento da segurança e da privacidade dos dados pessoais é consequência também de uma liberdade de comunicação nas redes sociais. Para ele:

> Os grandes monopólios da informação e da comunicação digitais exercem um controle mais sutil, porém não menos global que desvaloriza ou desvia, mediante um *by-pass* digital, não apenas a autonomia e privacidade de seus usuários individuais, mas também das instituições nacionais e internacionais baseadas em códigos técnicos, políticos, legais e morais. Isso cria de fato formas de inclusão, exclusão e manipulação que, embora costumem estar fundamentadas nas leis de seus respectivos países, se subtraem a elas em sua atividade global. Não existe até agora um acordo internacional a respeito disso, ou existe apenas uma Declaração de Princípios, como a proclamada na Cúpula Mundial sobre a Sociedade da Informação (CAPURRO, 2017, p.65).

Para Capurro, os grandes monopólios de informação exercem controle e manipulação de seus usuários e das instituições nacionais e internacionais, mencionando a importância de haver um acordo internacional sobre isso. Isso se dá porque os interesses de uso dos dados privados, fornecidos ou não pelos indivíduos na rede, são tão variados que é preciso ir além das exigências e do cumprimento das leis mencionadas no presente trabalho, motivo pelo qual propomos também uma reflexão ética em torno da privacidade. Nesse sentido, Fugazza e Saldanha afirmam que:

> A valorização da ideia de privacidade da ética informacional é caracteristicamente um valor moral que predomina nas culturas ocidentais, imbricada com os ideais democráticos que defendem os princípios de autonomia e liberdade. Quando adentramos as esferas políticas locais, percebemos o conjunto de problemas evocados pelo campo da ética no território das políticas de direito social e da participação cidadã crítica (FUGAZZA; SALDANHA, 2017, p.92).

Para os autores, esses princípios de liberdade e autonomia não poderiam caracterizar as experiências dos usuários na rede, porque as organizações responsáveis pelas plataformas onde essas experiências são disseminadas visam ao lucro. Logo, a informação pessoal transmitida nas redes é mercadoria, esteja essa informação sob a custódia de organizações públicas ou privadas.

Cabe a nós decidirmos o que faremos com elas, o quanto de nós será exposto voluntariamente em redes sociais e como fiscalizaremos o tratamento e uso dos nossos dados, exigindo transparência, e utilizando os mecanismos legais (como as recentes leis brasileiras) para obtermos dos órgãos controladores a prestação de contas sobre o que é feito com os nossos dados privados.

Nesse sentido, considerando toda a contextualização até aqui apresentada, passamos a discutir sobre dados pessoais na perspectiva de criação da LGPD e da ANPD, no intuito de evidenciarmos se, nestes instrumento, constam questões equivocadas sobre a gestão de dados pessoais no país.

4 LGPD E ANPD: REFLEXÕES INICIAIS NECESSÁRIAS

Pontuadas todas as considerações de caráter ético, humanístico e social que envolvem o dado pessoal, observamos que o tema necessita ser discutido e analisado com acuidade. É oportuno ressaltar que a LGPD prevê, em seu art. 6º, os princípios para o tratamento de dados pessoais, quais sejam:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

Entretanto, ainda que afirme observar a boa-fé, uma lei que trata de assunto sensível necessita ser investigada por meio de reflexão científica. Nesse sentido, passamos a seguir a analisar a recente legislação aplicada à "Proteção de Dados Pessoais" no Brasil, no intuito de levantar questões para que a finalidade do dispositivo legal seja atendida: a proteção dos dados pessoais em sua integralidade. Para isto, após uma leitura cuidadosa da LGPD, destacamos alguns trechos da Lei, sem a intenção de esgotá-los, elencando apenas aqueles que representam, em nossa visão, questões que merecem análise crítica no escopo da gestão do conhecimento e da informação.

Quadro 1: Análise crítica da Lei 13.709/2018 - Lei Geral de Proteção de Dados.

Texto Normativo	Análise Crítica
Art. 4º Esta Lei **não se aplica** ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) **segurança do Estado**; ou d) atividades de investigação e repressão de infrações penais; ou § 1º O tratamento de dados pessoais previsto no inciso III **será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.	A lei permite exceções que não estão muito claras: decretada a necessidade de **segurança do Estado**, a invasão de dados pessoais passa a ser permitida. Entretanto, não podemos deixar de destacar que o Estado, em seu sentido *stricto sensu*, denota um conjunto de instituições que perpassam os poderes Executivo, Legislativo e Judiciário nos mais diferentes níveis da federação. Porém, este mesmo ente coexiste sob a gestão de um governo que, dependendo da ideologia adotada, pode considerar "segurança nacional" questões que justifiquem o acesso a dados que não deveriam ser acessados. Logo, observamos que este artigo mantém uma lacuna um tanto quanto perigosa para possíveis posturas antidemocráticas travestidas de boas práticas no âmbito da governança pública acerca do dado pessoal.
Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] I - mediante o fornecimento de consentimento pelo titular; **IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;** § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.	O tratamento dos dados pessoais, conforme o artigo 7º, exige de seu titular consentimento por escrito ou por outro meio que o demonstre. Entretanto, se este tiver tornado público seu dado de forma voluntária, a exigência do consentimento é dispensada. Ora, se tomarmos como exemplo a atividade de *overposting* nas redes sociais, onde espontaneamente o usuário publica sua vida e distribui na rede um conjunto significativo de informações e dados pessoais, a LGPD, ao invés de proteger, concedeu ressalvas à proteção dos dados pessoais, ainda que proteja o cidadão
Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se	Controlador, conforme definição do artigo 5º, é "a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Este artigo elenca dois

limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.	incisos e 3 parágrafos, mas não explicita de forma clara quais seriam as finalidades concretas que dariam ao controlador o direito de tratar os dados pessoais. Questionamos, portanto, o que seria o "legítimo interesse"?
Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] **II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:** **a) cumprimento de obrigação legal ou regulatória pelo controlador;** **b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;** [...]	O normativo possibilita o uso de dados pessoais sensíveis, ou seja, aqueles que, segundo a União Europeia, referem-se a: "dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa". Compreendemos que, neste trecho da lei, há mais um equívoco, visto que as hipóteses que fundamentam essa possibilidade de acessar dados pessoais sensíveis, sem o prévio consentimento, podem proporcionar o acesso justificado por intenção diversa. A possibilidade, por exemplo, de uso de dados de portadores com vírus HIV por região, ainda que se justifique como política pública de saúde, se não for bem administrada, pode levar à insegurança de dados altamente prejudiciais aos interessados, conforme o caso de Singapura já mencionado neste trabalho.
Art. 11 - § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.	Sobre este parágrafo do artigo 11, entendemos ter sido um ponto positivo da Lei, visto que possibilita que não ocorram discriminações quando do direito do cidadão em contratar plano de saúde suplementar em virtude de prévio acesso das empresas ofertantes sobre os dados pessoais do interessado.
art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. **§ 2º Poderão ser igualmente considerados como**	O parágrafo segundo desse artigo é considerado positivo, na medida em que é um instrumento de controle dos dados pessoais coletados em enquetes de perfil de personalidade e comportamento, bastante utilizado em aplicativos e testes nas redes sociais.

dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.	
Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. **§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.**	O tratamento de dados pessoais de crianças e adolescentes causa novo estranhamento: o que corresponderia ao "melhor interesse", como propõe a lei?
Art. 16. Os **dados pessoais serão eliminados** após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.	Tratar da eliminação de dados significa prover e autorizar o apagamento. Entretanto, questionamos sob que perspectivas de controles esta ação estaria sendo regulada?
Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseados no legítimo interesse.	Consideramos que este controle permitirá a transparência, uma vez que a ciência sobre as operações que ocorrem acerca dos dados pessoais colabora para a segurança desses dados.
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá 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.	A exigência e a existência de documento arquivístico (relatório) do controlador à autoridade nacional, prestando contas sobre as ações realizadas no tratamento concedido aos dados pessoais, é considerada também ação de transparência e controle para a efetividade do cumprimento da legislação.
Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.	Cabe salientar que a documentação produzida pela autoridade nacional deverá ser preservada conforme as diretrizes e orientações técnicas do Conselho Nacional de Arquivos e assegurando o previsto na Lei de Arquivos (Lei 8.159/1991), em seu artigo 1º: "É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação".
Das Boas Práticas e da Governança Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as	Chama a atenção o fato de o Arquivo não ser mencionado nesse processo, uma vez que muitos dos padrões técnicos mencionados no artigo podem tangenciar a adequada gestão de documentos, atividade definida pela Lei de Arquivos.

condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.	

Fonte: Elaboração própria, com base na legislação analisada (LGPD).

A partir das análises críticas acima mencionadas, pretendeu-se contribuir, no seio de uma pesquisa científica, para a reflexão sobre a transparência, democracia e controle dos dados pessoais, tendo como campo empírico a recente legislação brasileira sobre esse tema.

Acerca da Lei nº 13.853/2019, que cria a Autoridade Nacional de Proteção de Dados Pessoais (ANDP), frisamos que o instrumento normativo apenas altera alguns incisos da Lei nº 13.709/2018 (LGPD) supramencionada, detalhando as finalidades e estruturas do novo órgão.

Nesse sentido, nosso questionamento sobre a referida autoridade centraliza-se na falta de sua independência em relação ao Poder Executivo, como já mencionado na pesquisa, e sobre a capacidade dela em gerir dados pessoais sem provocar vazamentos, como acusadas algumas instituições públicos federais, aqui também mencionadas.

Além disso, pontuamos que a ANPD não foi constituída plenamente – ainda não tem regimento interno, não possui definição da ocupação de cargos-chave de direção e outros requisitos de gestão –, o que a coloca em uma situação de fragilidade institucional dada sua importância para a implementação da nova política de Dados Pessoais.

Ao mesmo tempo, compreendemos que a ANPD tem importância para o marco civil sobre dados privados, uma vez que suas finalidades proporcionam, salvo melhor juízo, a adoção de boas práticas acerca da manipulação dos dados, entre elas o zelo no uso de dados por todo e qualquer agente, a adequada implementação e a fiscalização da Lei de Proteção de Dados Pessoais (LGPD) em todo o território nacional.

5 CONSIDERAÇÕES FINAIS

O presente trabalho pretendeu contribuir com reflexões acerca de medidas que possam ajudar na proteção de dados pessoais dos cidadãos brasileiros. A partir das análises realizadas no presente artigo, perguntamo-nos se a disponibilização dos dados pessoais na rede seria a mesma caso as políticas de privacidade dos aplicativos e provedores fossem transparentes e nos informassem os possíveis usos dos mesmos. Questionamos em que

medida o uso destes dados poderia favorecer a manipulação de nossos interesses e o nosso comportamento. Apontamos que o caminho para essa transparência ideal envolve conflitos de interesse que transitam entre governos, instituições públicas, organizações privadas e o próprio indivíduo. Embora a legislação responsabilize-os pelo uso inadequado, na prática, isso vem sendo ignorado sistematicamente. Parece-nos que o preço dessa "liberdade" digital é alto quando, por exemplo, observamos que a técnica de mineração de dados na rede permite produzir propagandas personalizadas. Isto nos leva a questionar até que ponto estamos pensando por nós mesmos ou estamos sendo orientados a pensar de acordo com os controladores de algoritmos da internet. Além disso, sinalizamos que a utilização de dados privados frustra o processo democrático, podendo levar ao poder, por manipulação de perfis, grupos políticos que, em um campo de disputa justo, não assumiriam protagonismo no cenário governamental. Essas abordagens perpassam a questão ética em torno da privacidade, cuja formação de uma consciência, traduzida em ações morais sobre o tratamento dos dados pessoais, transcendem a questão legal.

Nesse escopo, esta pesquisa traz questionamentos acerca da efetividade da LGPD e da ANPD como instrumentais para a gestão de dados pessoais no Brasil. A análise destes institutos permite inferir que eles representam a introdução de um controle melhor sobre o uso do dado pessoal no país.

Indicamos, portanto, como resultados positivos a vedação a seleção de riscos, por parte de operadoras de saúde; a implementação de controle dos dados pessoais coletados anonimamente; a determinação do registro das atividades dos controladores e operadores que tratam dados pessoais; e o benefício da previsão legal para confecção de relatório de impacto à proteção de dados pessoais, conferindo mais transparência ao processo.

Por outro lado, observamos que as essas recentes iniciativas apresentam inconsistências em sua concepção. Percebemos alguns pontos de fragilidades que possibilitam um horizonte de gestão estatal de dados pessoais controverso, como: as restrições à aplicação da LGPD sob o argumento da "segurança do Estado"; o não esclarecimento do significado de "legítimo interesse" e "melhor interesse"; o uso de dados sensíveis sem o consentimento do titular; a ausência de caráter regulatório sobre a eliminação de dados; e, por fim, o fato da Autoridade Nacional ter previsão legal, mas não estar em pleno funcionamento.

Diante do exposto, ainda que se reconheça que a LGPD e a ANPD representam avanços para a legislação sobre o tema, é possível observar algumas contradições que fragilizam a atual configuração normativa e institucional da política de controle sobre dados pessoais no Brasil.

REFERÊNCIAS

AMORIM, Fabiana Borelli. TOMAÉL, Maria Inês. Gestão da Informação e Gestão do Conhecimento na Prática Organizacional: análise de estudos e casos. In: **Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, v.8, n.2, p.01-22, jan./jun. 2011. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1931. Acesso em 22 set 2019.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Congresso Nacional, 1988.

BRASIL. **Código de Defesa do Consumidor**. Brasília: Congresso Nacional, 1990.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, 09 jan. 1991. Seção 1, p. 1.

BRASIL. **Código Civil.** Brasília: Congresso Nacional, 2002.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. Seção 1, p. 1, edição extra.

BRASIL. **Tipificação Criminal de Delitos Informáticos**. Brasília: Congresso Nacional, 2012.

BRASIL. **Decreto de Dados Abertos**. Brasília: Congresso Nacional, 2016.

BRASIL. **Marco Civil da Internet.** Brasília: Congresso Nacional, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial da República Federativa do Brasil**, Brasília, 15 ago. 2018.

BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, 09 jul. 2019.

CAPURRO, Rafael. A liberdade na era digital. *In*: GONZALEZ DE GOMEZ, Maria Nélida; DE BARROS CIANCONI, Regina (Orgs.). **Ética da Informação**. Niterói: PPGCI/UFF, 2017.

CORREIO BRASILIENSE. Dados pessoais de brasileiros são negociados livremente na internet. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2018/07/16/interna-brasil,695136/dados-pessoais-de-milhares-de-brasileiros-sao-negociados-na-internet.shtml. Acesso em: 01 ago. 2019.

FUGAZZA, Grace Quaresma; SALDANHA, Gustavo Silva. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, v.22, n.50, p.91-101, 2017.

G1. Dados de 14,2 mil portadores de HIV são roubados e expostos em Singapura. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/01/29/dados-de-142-mil-portadores-de-hiv-sao-roubados-e-expostos-em-singapura.ghtml. Acesso em: 01 ago. 2019.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. *In*: **Perspectivas em Ciência da Informação**, v.23, n.4, p.117-132, out./dez. 2018. Disponível em: http://www.scielo.br/pdf/pci/v23n4/1413-9936-pci-23-04-00117.pdf. Acesso em: 22 set. 2019.

MAGRANI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade. **Série Pautas em Direito**. Porto Alegre: Arquipélago Editorial, 2019.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL. Notícia contra o Serviço de Processamento de Dados Federal (SERPRO). Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10987-mpdft-representa-contra-o-serpro-no-tcu. Acesso em: 01 ago. 2019.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v.1, n.1, p.41-62, jan./jun. 1996. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235/22. Accesso em: 19 set 2019.

SCHWARTZ, Paul M. Property, privacy, and personal data. **Harv. L. Rev**., v.117, p.2056, 2003. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/hlr117&div=91&id=&page=. Acesso em: 09 ago 2019.

UNIÃO EUROPEIA. Conceito de Dados Sensíveis. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt. Acesso em: 09 ago 2019.