FACULDADE MERIDIONAL – IMED
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO – PPGD
MESTRADO EM DIREITO

DIONIS JANNER LEAL

GOVERNANÇA NO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: *ACCOUNTABILITY* E *COMPLIANCE* COMO INSTRUMENTOS DE CONTROLE E GESTÃO

Passo Fundo, RS
2021

DIONIS JANNER LEAL

GOVERNANÇA NO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: *ACCOUNTABILITY* E *COMPLIANCE* COMO INSTRUMENTOS DE CONTROLE E GESTÃO

Dissertação apresentada ao Programa de Pós-graduação *Stricto Sensu* – Mestrado em Direito – da Faculdade Meridional – IMED, em sua área de concentração em Direito Democracia e Sustentabilidade, Linha de Pesquisa Efetividade do Direito, da Democracia e da Sustentabilidade.

Orientador: Drª Salete Oro Boff

Passo Fundo, RS
2021

CIP – Catalogação na Publicação

L435g LEAL, Dionis Janner

Governança no compartilhamento de dados pessoais entre órgãos da administração pública: accountability e compliance como instrumentos de controle e gestão / Dionis Janner Leal. – 2021.

83 f., il.; 30 cm.

Dissertação (Mestrado em Direito) – Faculdade IMED, Passo Fundo, 2021.

Orientadora: Dr.ª Salete Oro Boff.

1. Compliance. 2. Privacidade. 3. Poder público – Dados pessoais. I. BOFF, Salete Oro, orientadora. II. Título.

CDU: 342

Catalogação: Bibliotecária Angela Saadi Machado - CRB 10/1857

Autor: **Dionis Janner Leal**

Título: **GOVERNANÇA NO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA:** *ACCOUNTABILITY* E *COMPLIANCE* COMO INSTRUMENTOS DE CONTROLE E GESTÃO

Dissertação apresentada ao Programa de Pós-graduação *Stricto Sensu* – Mestrado em Direito – da Faculdade Meridional – IMED, como requisito para a obtenção do grau de Mestre em Direito.

Passo Fundo, RS, 30 de março de 2021.

Dra. Salete Oro Boff – Orientadora

Dra. Cinthia Obladen de Almendra Freitas - PPGD-PUC/PR – Membro

Dr. Neuro José Zambam - PPGD-IMED – Membro

Aos meus pais, Djalma Pires Leal e Tania Maria Janner

À minha esposa, Eliana Dornelles

RESUMO

Os dados pessoais e a privacidade possuem destaque no cenário de desenvolvimento tecnológico a partir da disponibilidade de informações e da ausência de critérios legais de controle no seu tratamento por organizações públicas e privadas. Nesse contexto, o presente estudo tem como objetivo abordar os limites do compartilhamento de dados pessoais pelos órgãos da Administração Pública a partir da governança e instrumentos de controle e gestão como a *accountability* e o *compliance*. O primeiro capítulo trata da proteção de dados e o seu uso pelo poder. No segundo capítulo trata a abordagem dos limites do compartilhamento de dados entre órgãos públicos na LGPD e a sua transparência, ao contemplar questões quanto à circulação de informações na organização pública. O terceiro capítulo aborda a necessidade do *compliance* e da *accountability*, na perspectiva de O'Donnell, como instrumentos de controle no compartilhamento de dados na Administração Pública em razão dos princípios normativos expressos na LGPD. A partir de pesquisa bibliográfica de natureza exploratória e qualitativa, e utilizando o método hipotético-dedutivo e técnica monográfica, conclui-se que a Administração Pública tem o dever de assegurar a proteção e tratamento de dados pessoais, inclusive no compartilhamento perante outros órgãos públicos para os fins de atender a políticas públicas e institucionais, nos limites legais. Para tanto, deverá valer-se de instrumentos de controle e gestão disponíveis no mercado privado, como a gestão de riscos e a *compliance*, as boas práticas utilizadas por outras organizações somadas ao reforço da implementação da *accountability* pelas instituições públicas, ensejando-lhes, legalmente, prerrogativas de supervisão, de prestação de contas, de responsabilização e de sanção perante outros órgãos públicos que venham transgredir a legislação e as normativas no tratamento de dados pessoais. O tratamento adequado dos dados pessoais é dever institucional e direito dos seus titulares, o que visa assegurar o direito à privacidade.

Palavras-chave: *Accountability; Compliance;* Dados pessoais; Poder Público; Privacidade.

ABSTRACT

Personal data and privacy are highlighted in the technological development scenario based on the availability of information and the absence of legal control criteria in their treatment by public and private organizations. In this context, the present study aims to address the limits of the sharing of personal data by Public Administration bodies based on governance and control and management instruments such as accountability and compliance. The first chapter deals with data protection and its use by power. The second chapter deals with the approach to the limits of data sharing between public bodies in the LGPD and its transparency, when contemplating issues regarding the circulation of information in the public organization. The third chapter addresses the need for compliance and accountability, in O'Donnell's perspective, as control instruments in data sharing in Public Administration due to the normative principles expressed in the LGPD. From bibliographic research of exploratory and qualitative nature, and using the hypothetical-deductive method and monographic technique, it is concluded that the Public Administration has a duty to ensure the protection and treatment of personal data, including sharing with other public bodies for the purposes of complying with public and institutional policies, within the legal limits. To this end, it should make use of control and management instruments available in the private market, such as risk management and compliance, the good practices used by other organizations in addition to the strengthening of the implementation of accountability by public institutions, enabling them, legally , prerogatives of supervision, accountability, accountability and sanction before other public bodies that may violate legislation and regulations in the processing of personal data. The proper treatment of personal data is an institutional duty and the right of its holders, which aims to ensure the right to privacy.
Keywords: Accountability; Compliance; Personal data; Public Power; Privacy.

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

AH – *Accountability* horizontal

AS – *Accountability* social

ANPD – Autoridade Nacional de Proteção de Dados

CF – Constituição da República Federativa do Brasil

CGU – Controladoria-Geral da União

ERM - *Enterprise Risk Management*

GDPR – *General Data Protection Regulation*

IBGC – Instituto Brasileiro de Governança Corporativa

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

MP – Ministério do Planejamento

NBR – Norma Brasileira

IN – Instrução Normativa

INMETRO – Instituto Nacional de Metrologia, Qualidade e Tecnologia

ISO – Organização Internacional de Padronização

ONU – Organização das Nações Unidas

TCU – Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO

A privacidade passou nas últimas décadas por um processo de normatização unitária no direito brasileiro, com melhor clareza em sua tutela a partir da sua inserção na Constituição Federal de 1988 (privacidade, intimidade, honra) e, ultimamente, pelo legislador infraconstitucional por intermédio das Leis de Acesso à Informação (Lei n° 12.527/2011), Marco Civil da Internet (Lei n° 12.965/2014) e de Proteção de Dados Pessoais (Lei n° 13.709/2018).

Nesse cenário houve uma "institucionalização" e protagonismo do Estado em fazer cumprir – por ele mesmo – e exigir seu cumprimento perante as demais organizações acerca dos cuidados que se deve ter com dados e informações das pessoas, os quais lhes são inerentes e não podem ser violadas ou invadidas pelo alvedrio de quem quer que seja, inclusive o próprio Poder Público, sem que haja anuência do seu titular ou previsão normativa e, ainda, nos limites delineados pela importância constitucional que se deve ao tema.

Esse protagonismo do Estado em dar melhor atenção e proteção a um direito fundamental é legitimado pelo simples fato desses dados e informações estarem desde sempre sob sua guarda e uso, sem regulação e regulamentação a nível infraconstitucional, o que até então não atenderia de forma satisfatória à exigência constitucional de inviolabilidade da vida privada de seus cidadãos.

Apesar de reconhecer a importância do direito à privacidade (dados e informações) para a pessoa, por lhe dizer respeito à intimidade, o legislador constitucional relativizou sua proteção, mediante determinação judicial (art. 5°, XII, CF), e, a par disso, a legislação infraconstitucional dispensou o tratamento de dados quando o Estado estiver exercendo suas funções de tutela do bem comum, como segurança pública, defesa nacional, infrações e investigações penais, por exemplo.

A partir dessas constatações, o presente estudo trata do tema da governança pública no compartilhamento de dados pela Administração Pública e o controle e gestão a partir dos instrumentos de *accountability* e *compliance.*

Nesse ponto, o Poder Público é dispensado de atender à Lei Geral de Proteção de Dados Pessoais (LGPD) quando faz uso dos dados pessoais para fins de compartilhamento entre órgãos da Administração Pública nas atividades de investigação e repressão de infrações penais (artigo 4°, III, *d*, da LGPD), a exemplo de crimes como lavagem de dinheiro ou

organização criminosa, exceção dada quanto ao compartilhamento de dados para execução de políticas públicas (artigo 7°, III, da LGPD).

Nesse contexto, há necessidade ou não de ser dispensável (ou dispensado?) o consentimento do titular do dado protegido pelo direito à privacidade, ou que em razão de disposição legal expressa em legislação esparsa, inclusive de autorização judicial para atender às finalidades institucionais ou legais da organização estatal, é válida enquanto ausente legislação específica (artigo 4°, § 1°, da LGPD)? Quais são os limites impostos pela legislação para o compartilhamento de dados pessoais pela Administração Pública?

Como hipótese, a partir dos princípios que norteiam a LGPD, a figura do *accountability* (artigo 6°, X, da LGPD) torna-se instrumento capaz de garantir as finalidades pelas quais os dados pessoais foram originalmente coletados, dando-lhes destinação de acordo com a finalidade, a adequação, a segurança e a prevenção, as quais são princípios de observância obrigatória na execução da LGPD, que toma o *compliance* (artigo 46, § 1° c/c artigo 49, ambos da LGPD) como seu mecanismo de governança, aptos a resguardar o direito à privacidade enquanto não promulgada a legislação específica (artigo 4°, § 1°, da LGPD) e de observância obrigatória quando da sua regulamentação.

A privacidade tem fomentada a ideia de poder, de um tipo de controle pelo Estado, não em razão da privacidade em si, mas do denso conteúdo nela existente que são compartilhados por seus titulares, voluntária ou involuntariamente e que são registrados e guardados por terceiros. Não se pode olvidar em registrar que o Poder Público foi o primeiro a utilizar de forma ampla as informações pessoais, cujos motivos era a Administração Pública ser eficiente, tendo conhecimento de dados da população, ao passo que se utiliza para ativar controles sociais, típico de Estado de regime totalitário.

Os contornos que a noção de privacidade aflora, inerente à ideia de não intervenção de terceiros – inclusive o Estado –, não dispensam trazer para questões como o biopoder e a psicopolítica, que são técnicas de poder, conforme Foucault e Han.

Ao lado desse controle pelo poder, o compartilhamento de dados pessoais pelo Poder Público para os fins previstos na LGPD, em razão do princípio da publicidade esculpido no artigo 37, *caput* da Constituição Federal, é dever do ente governamental comunicar o titular dos dados pessoais que foram coletados e/ou tratados para fins diversos daqueles previamente autorizados (com ou sem consentimento) em virtude de lei ou em razão de prerrogativas de competências inerentes às suas respectivas funções públicas, sob pena de, em tese, serem

considerados nulos os atos, procedimentos e/ou processos administrativos que se valeram de dados pessoais.

Todavia, o Poder Público possui a prerrogativa legal de dispensa do consentimento do titular no uso e compartilhamento de seus dados para fins os quais deve desenvolver suas atividades e atribuições que lhes foram incumbidas por lei, a exemplo de atividades investigativas de infrações penais, como preferiu o legislador ao deixar expresso sua vontade na lei.

A premissa é que não obstante o privilégio legal conferido ao Estado no controle de informações de cidadãos que estejam sob sua jurisdição, o próprio legislador condicionou essa exceção à aplicação da lei mediante promulgação de legislação específica (lei regulamentadora), sem descurar da observância de princípios tratados pela própria LGPD, bem como princípios constitucionais como o devido processo legal.

Nesse ponto, contribui o legislador nacional com a internalização de instrumentos utilizados em legislação estrangeira como o relatório de impacto que visa avaliar os riscos gerados às liberdades e aos direitos fundamentais dos titulares dos dados, valendo-se como exemplo de controle e prestação de contas (*accountability)*, exigida pela LGPD por intermédio da ANPD para às exceções de tratamento de dados pessoais previstas na lei.

No exemplo Europeu, Regulamento n° 2016/679, em seu artigo 35, exige o relatório de impacto e comunicação aos órgãos fiscalizadores somente quando houver alto risco aos direitos tutelados – mensurados subjetivamente pelo controlador –, no mesmo sentido, pela LGPD, exige-se nos casos de alto risco (artigo 55-J, XIII), sob a competência da ANPD, apesar de não especificar em qual o momento do tratamento, e exigível pela Autoridade Nacional de Proteção de Dados (ANPD), isto é, *a posteriori*.

Nesse sentido, a justificativa para a realização deste estudo corresponde à consideração que a ausência (*a priori*) de transparência e *accountability* afrontam o direito à privacidade e à informação do titular dos dados pessoais tratados pelos órgãos públicos, para os fins de execução de suas competências, infringindo os ditames principiológicos da Constituição Federal de transparência e publicidade, além do direito fundamental à privacidade.

Ao mesmo tempo, considera-se que a privacidade da pessoa humana se tornou uma questão de Estado, com o fim de que este possa garantir proteção ao direito personalíssimo da pessoa humana, onde o acesso ilimitado às informações pessoais se tornou moeda de troca, isto é, com potencial econômico, que floresceu – ou se intensificou – por decorrência do

desenvolvimento tecnológico vivenciado nos últimos tempos o qual permitiu e facilitou a disponibilidade irrestrita e exponencial de dados de pessoas e organizações sem quaisquer autorização de seus titulares para livre utilização e, não rara às vezes, com "sede" dos usuários do meio digital pela "liberdade" sem quaisquer medos ou receios ou ausência de riscos e consequências dessa liberdade exposta ao mundo digital.

Ademais, existe a possibilidade de corporações privadas, inclusive o próprio Estado – por ausência de autocontrole ou *accountability* – de exercer um poder sobre as pessoas em razão do tratamento dos dados por eles fornecidos, o que enseja, consequentemente e ao mesmo tempo, controle e responsabilidades mútuas, além de se exigir inerentemente uma transparência. A transparência que se exige e aqui será tratada, deve ser analisada sob a óptica – possibilidade – da anuência do usuário ou da sua simples comunicação de que determinados dados pessoais foram coletados para os fins a que lhe compete um ou outro órgão nas suas respectivas atribuições ou, ainda, pela existência de instrumento de controle eficientes.

Destaca-se a importância da pesquisa que se pretende estabelecer a partir de pretextos do alcance do interesse público e para os fins institucionais de órgãos públicos é que se fundamentam a violação à privacidade garantida constitucionalmente, chancelada por decisões judicias de cortes superiores nesse mesmo sentido, sem, contudo, ensejar publicidade – transparência – a que se deve na coleta de dados pessoais.

A partir disso, a responsabilidade por uso de informações alheias passou a ser tema de debates no judiciário e, consequentemente, o poder legislativo das nações do mundo passaram a regulamentar seu uso e tratamento.

Não obstante a responsabilização pelo uso indevido de informações privadas, compete ao Estado, inclusive, criar mecanismos de conformidade a fim de se adequar às normas por ele próprio editadas – o que se confirma por intermédio do *compliance*.

Todavia, não está claro a forma como esses dados serão tratados pelo Poder Público, quando se trata de informações coletadas de usuários ou beneficiários dos serviços públicos e/ou quando tenham com particulares um vínculo contratual.

O objetivo geral do estudo é analisar os instrumentos de governança existentes na LGPD para o tratamento de dados pessoais e garantir a proteção à privacidade no compartilhamento desses dados entre órgãos da Administração Pública.

Seus objetivos específicos são compreender a evolução e as definições de privacidade e dados pessoais, as características e conceitos de *accountability* e *compliance* e definir os

limites do compartilhamento de dados entre órgãos do Poder Público e exemplificar as boas práticas necessárias para garantir o seu tratamento adequado pela Administração Pública.

O primeiro capítulo, com base nos objetivos apresentados, trata da proteção de dados e da privacidade no Brasil, a sua inserção enquanto proteção constitucional, o seu conceito normativo, suas inter-relações com outras normas jurídicas e o uso de dados pelo poder.

No segundo capítulo trata a abordagem dos limites do compartilhamento de dados entre órgãos públicos na LGPD e a sua transparência, ao contemplar questões quanto à circulação de informações na organização pública, em que o compartilhamento de dados entre órgãos públicos é permitido, bem como destacar os princípios que lhe são inerentes e o uso de normas técnicas como auxiliares nas finalidades da proteção de dados pessoais.

O terceiro capítulo aborda a necessidade – e o uso compulsório – do *compliance* e da *accountability*, na perspectiva de O'Donnell, como instrumentos de controle no compartilhamento de dados na Administração Pública em razão dos princípios normativos expressos na LGPD.

A metodologia do estudo é a pesquisa e coleta de informações teóricas a partir do levantamento bibliográfico. Aplica-se o desenvolvimento do texto por intermédio do método hipotético-dedutivo e monográfico. A investigação tem como objetivo desafiador a discussão da produção acadêmica no campo jurídico do conhecimento, buscando examinar os aspectos e dimensões provenientes desses materiais e de suas abordagens, relacionando-os à área jurídico-científica.

No caso desse estudo, a busca é orientada no âmbito das ciências jurídicas, em especial do direito administrativo, direito constitucional e da ciência política, quando for o caso, abordando o tema de forma qualitativa.

Pode-se afirmar que os instrumentos da governança como a *accountability* e o *compliance* estão presentes na LGPD e devem ser aplicados no compartilhamento de dados pessoais pela Administração Pública, a qual deverá adequar-se e reorganizar-se para atender as disposições legais e as melhores práticas no tratamento de dados pessoais dos cidadãos.

2 PROTEÇÃO DE DADOS E PRIVACIDADE NO BRASIL

Num contexto histórico, o ordenamento jurídico brasileiro positivou o direito à privacidade, quando inicialmente a tratou como tutela de inviolabilidade de domicílio e de correspondências.

A Constituição de 1988 trouxe a proteção da privacidade por via reflexa, por intermédio da proteção à dignidade humana, e, por via direta, como na proteção da imagem, da vida privada, da honra e da intimidade (MAURMO, 2017, p. 124), esculpida no inciso X, do artigo 5°, sem olvidar o seu inciso XII, acerca da inviolabilidade do sigilo das correspondências e comunicações telegráficas.

Existem outros diplomas legais no Brasil como o Código Civil, Código de Processo Penal e o Código de Defesa do Consumidor que tratam acerca da proteção à privacidade, sendo que este último equiparou os registros de dados de consumidores de qualquer gênero às entidades de caráter público (FORTES, 2015, p. 102).

Nesse contexto, os contornos que a noção de privacidade aflora, inerente à ideia de não intervenção de terceiros, como o Estado, não dispensam trazer noções de biopoder e a psicopolítica, que são técnicas de poder, tratados por Michel Foucault e Byung-Chul Han, bem como poder ser inerente à pessoa ser, *prima facie*, um direito fundamental.

Com este propósito o presente capítulo se propõe a apresentar o conceito normativo de dados pessoais – delineado pela LGPD – (2.1), os dados pessoais, em busca de um conceito normativo, (2.2), a proteção de dados pessoais e privacidade como direito fundamental (2.3), a LGPD e a LAI e suas inter-relações normativas na privacidade, e (2.4), o controle de dados pelo poder.

2.1 Dados pessoais: em busca de um conceito normativo

A fim de delimitar o presente estudo, é imperioso destacar preliminarmente que privacidade é gênero donde advém os dados pessoais. Assim, "os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade"[1] (BIONI, 2019, p. 100).

Por outro lado, a quem, como Rodotà (2008) trata a tutela dos dados pessoais como um novo formato da privacidade, no sentido de "aderir a uma concepção fundada na

[1] Ainda, Bioni justifica que: "O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão [...]" (2019, p. 100).

autodeterminação sobre as próprias informações em razão de novas questões geradas pela realidade dos sistemas informativos atuais" (MASILI, 2018, p. 29).

> O autor reconhece, porém, um direito de acesso a informações não como derivação da privacidade, mas da liberdade de informação. Tal direito, sim, é desvinculado por Rodotá (2008) de questões de intimidade ou privacidade, e relacionado apenas ao direito à informação, como forma de ligar tecnologia e democracia. Assim, em vez de separar privacidade e direito sobre os dados pessoais, a separação dá-se entre privacidade e direito à informação (2018, p. 30).

Enquanto direito da pessoa, a privacidade foi definida na área jurídica e tida como marco inicial no artigo de Samuel Warren e Louis Brandeis, de 1890, conhecido como direito de ser deixado só (WARREN, BRANDEIS, 1890, p. 86), passando a ser concebido como "direito de manter o controle sobre as próprias informações" (RODOTÀ, 2008, p. 92).

O conceito de privacidade foi emergido na jurisprudência norteamericana como "*el derecho a ser dejado solo*" e que posteriormente foi apresentado por Warren e Brandeis (1890), a definição de privacidade nesses termos (TRAVIESO, 2014, p. 9).

No âmbito da legislação internacional, a Declaração Universal dos Direitos Humanos (DUDH), em seu artigo 12[2], dispõe que não haverá intromissão arbitrária na vida privada da pessoa, e contra essa violação haverá o direito à proteção da lei. A necessidade de medidas de controle e direito de acesso a informações pessoais tornam-se indispensáveis a fim de não ser violado o direito à privacidade e, consequentemente, o abuso no uso das informações coletadas por terceiros, com ou sem o consentimento do titular, inclusive o Estado.

Importante observar que, acerca da DUDH, a análise dever ser realizada a partir da interpretação evolutiva dos direitos humanos, em especial quando se refere a termos cujos conteúdos são indeterminados, a exemplo de "interesse público", "privacidade", "devido processo legal", que podem variar no decorrer do tempo (RAMOS, 2016, p. 149).

No ordenamento jurídico brasileiro, pode-se dizer que desde as primeiras Constituições o legislador nacional fez referência à proteção do direito à privacidade, arrolando-a "por meio da tutela à inviolabilidade do domicílio e das correspondências" (MAURMO, 2017, p. 107).

A privacidade está presente na Constituição de 1824[3] a partir da inviolabilidade do domicílio; na Constituição de 1891[4] no sigilo de correspondência; na Constituição de 1934

---

[2] Assim estabelece o artigo 12 (XII) da DUDH: Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[3] Art. 179. A inviolabilidade dos Direitos Civis, e Politicos dos Cidadãos Brazileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte. [...] VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella,

nos direitos de inviolabilidade do domicílio e de correspondência, a qual foi mantida na Constituição de 1937 e suspensa, posteriormente, a inviolabilidade pelo Decreto n° 10.358/1942; na Constituição de 1946 os direitos individuais referidos nas Constituições anteriores foram mantidos e, na Constituição de 1967 houve a inclusão, além daqueles direitos, as comunicações telegráficas e telefônicas, resultantes da modernidade das comunicações, na época.

A proteção constitucional da privacidade pode ser analisada sob duas ópticas distintas no panorama normativo nacional, uma sem a compreensão jurídica da internet e outra com a sua internalização. Sob o primeiro prisma, a proteção da privacidade não era reconhecida em relação a banco de dados informáticos, mas a ordem jurídica já reconhecia que o instituto do *habeas data* era o que mais se aproximava de uma proteção legal, mas se limitava à esfera de órgãos e entidades governamentais (FORTES, 2015, p. 102).

Para o autor, "as mencionadas normas jurídicas brasileiras mantêm distanciamento de situações vinculadas aos novos fenômenos proporcionados pela internet, na sociedade da informação", o que vem a permitir "metadados anônimos e até mesmo protegidos por normas de sigilo bancário, tal como prevê a lei brasileira, tornam-se dados pessoais vulneráveis", arrematando o autor a necessidade de uma melhor compreensão da internet na seara jurídica a fim de contribuir para com a eficácia da proteção constitucional exigível (FORTES, 2015, p. 104).

Tal análise sob essas duas ópticas (com e sem compreensão jurídica da internet) quanto à proteção à privacidade no âmbito constitucional, conclui-se que o entendimento adotado por Fortes (2015) é aquele versado por Rodotà (2008), qual seja, a proteção de dados como uma variante da privacidade.

Apesar da abordagem se limitar ao ordenamento jurídico nacional, não se pode deixar de registrar que no cenário internacional no âmbito da América do Sul, por exemplo, de acordo com Travieso, os direitos humanos vêm historicamente contribuindo para o tratamento adequado dos dados pessoais, sendo o meio para encarar a luta entre o direito e a tecnologia, não sendo alheio à proteção da privacidade, promulgando diplomas e regulamentos. Como exemplos, a Declaração Universal de Direitos Humanos (DUDH) de 1948, a Convenção 108

---

senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar.

[4] Art.72 - A Constituição assegura a brasileiros e a estrangeiros residentes no paiz a inviolabilidade dos direitos concernentes á liberdade, á segurança individual e á propriedade, nos termos seguintes: [...] § 11. A casa é o asylo inviolavel do individuo; ninguem póde ahi penetrar, de noite, sem consentimento do morador, senão para acudir a victimas de crimes, ou desastres, nem de dia, senão nos casos e pela fórma prescriptos na lei. [...] § 18. É inviolavekl o sigillo da correspondencia.

do Conselho da Europa de 1981 que trata da proteção das pessoas com respeito ao tratamento automatizado de dados e foram ratificados por todos os membros europeus, e em 2009 com a entrada em vigor do Tratado de Lisboa vinculou juridicamente os países membros à Carta dos Direitos Fundamentais da União Europeia à proteção de dados pessoais (TRAVIESO, 2013, p. 72).

Por sua vez, a doutrina nacional tentou exprimir distinção, seja em relação a conceito normativo constitucional ou infraconstitucional de privacidade sob uma óptica abrangente, seja compreendendo privacidade, dados e informações como sinônimos para fins de aplicação da lei.

Para Maurmo[5], a privacidade é gênero, cujas espécies contemplam-se a vida privada e a intimidade (2014, p. 35), assim como para Cunha Júnior, abrangendo além da intimidade e da vida privada, a honra e a imagem (2010, p. 37).

Contudo, a doutrina distingue os termos privacidade, vida privada, intimidade e dados pessoais, arrolando outros adjetivos como sigilo e segredo, ao considerar a expressa autonomia que o legislador constitucional determinou no artigo 5°, inciso X, da Constituição Federal. Assim, para Doneda prescreve que:

> Ao se tratar da privacidade, há de se fazer antes de tudo um esclarecimento inicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representá-la, propriamente ou não, é considerável; além de "privacidade" propriamente dita, podem ser mencionados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como "privatividade" e "privaticidade", por exemplo. O fato de a doutrina estrangeira apontar igualmente para várias nomenclaturas certamente contribui, induzindo juristas brasileiros a experimentar alternativas. (2020, p. 26).

Ademais, o próprio Doneda entende ser desnecessário buscar um conceito que faça emergir diferenças ou conotações entre as expressões privacidade e intimidade, a qual deve ser aplicada no caso concreto quando na análise dos direitos fundamentais, ao prescrever que deve "ser lida em razão do contexto no qual se encontram os direitos fundamentais que visa proteger" (2020, p. 27).

Para o presente trabalho, segue-se a concepção de Doneda (2020), considera-se a expressão *privacidade* como a mais adequada, a qual contempla expressões como *dados*, *informações,* bem como *intimidade* e *vida privada*, não num sentido genérico, mas de tutela jurídica da inviolabilidade dos *dados* ou *informações* que são inerentes à cada pessoa e que apenas a ela dizem respeito.

---

[5] Considerando que este estudo não visa esgotar e trabalhar a privacidade e seus conceitos, sugere-se a leitura de Maurmo (2014).

Verifica-se, desse modo, que inexiste um conceito normativo específico definido pelo legislador brasileiro de privacidade. A doutrina nacional não é uníssona ao afirmar de forma segura suas distinções, mas pode-se afirmar que *dados* e *informações* são expressões que dizem respeito à privacidade da pessoa e que são objeto de tutela jurídica em face de terceiros, inclusive o Estado.

No Brasil, de acordo com Cueva, o Superior Tribunal de Justiça (STJ) em 1995, no julgamento do REsp. 22.337-8/RS, antes de haver legislação específica acerca do tema, já decidia acerca da "privacidade como exclusão de terceiros" e aludia ao "direito fundamental à autodeterminação informativa", na medida em que a coleta e armazenamento de informações pessoais sem o consentimento do titular invadia a sua esfera privada (2019, p. 88).

Foi a partir de uma lei ordinária, o Código de Defesa do Consumidor (CDC), em seu artigo 43[6], que se estabeleceu como um marco infraconstitucional acerca de se pensar em alimentar um conceito jurisprudencial de privacidade. Ainda, a jurisprudência do STJ passou por evolução conceitual, abrangendo a tutela da privacidade para outros direitos, no REsp. 306.570, da 2ª Turma da Corte, em que a Ministra Eliana Calmon reconheceu o direito do "contribuinte ou o titular de conta bancária tem direito à privacidade em relação aos seus dados pessoais" (STJ, 2001).

Por outro lado, o Supremo Tribunal Federal, em 2006[7], proferiu decisão negando o reconhecimento da existência de um direito à inviolabilidade de dados pessoais armazenados em computador, ao seguir doutrina de Tércio Sampaio Ferraz Júnior, que possui o entendimento de que a tutela de sigilo corresponde à comunicação, mas não a dados pessoais:

> [...] o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-los! (FERRAZ JR, 1993, p. 447).

Em recente decisão de 2020[8], a 5ª Turma do STJ mantém o entendimento do STF o qual dispõe que os dados contidos na agenda eletrônica do aparelho telefônico móvel não estão abrangidos pela proteção do sigilo de dados telemáticos. Nesta decisão o STJ

[6] Lei n° 8.078/1990. Artigo 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
[7] Recurso Extraordinário 418-416-8/SC, Dje 04.04.2006.
[8] Recurso Especial 1782386, Dje 18.12.2020.

rememorou outra decisão[9], também da 5ª Turma, de relatoria do Ministrio Reynaldo Soares da Fonseca, que faz a distinção entre aqueles dados que são acessados a partir de mensagem de texto e conversas por meio de aplicativos, sem autorização judicial, considerando-o como ilícitos, daqueles outros dados oriundos da agenda do aparelho celular e aos registros telefônicos, sem autorização, que são considerados lícitos.

Com o advento de Leis como a de Acesso à Informação (LAI, Lei n° 12.527/2011,), Marco Civil da Internet (MCI, Lei n° 12.965/2014) e de Proteção de Dados Pessoais (LGPD, Lei n° 13.709/2018), optou por uma tentativa de conceituar o legislador nacional a privacidade no ordenamento jurídico.

Inicialmente, por ordem cronológica, a LAI definiu em seu artigo 4°, inciso I, o que é informação [10] , o MCI não conceituou dados pessoais, mas o fez em sua norma regulamentadora, ao definir dado pessoal e tratamento de dados no artigo 14, do Decreto n° 8.771/2016[11] e, por fim, a LGPD trouxe, em seu artigo 4°[12], uma definição de informação.

A promulgação da LGPD, objetivou sistematizar o tratamento de dados pessoais como eixo estruturante em relação às demais normativas – como norma geral – e apresentou novos elementos que causaram impactos, como princípios de proteção de dados, conceitos próprios, um novo enfoque de tutela de direitos dos titulares proporcionado pelas regras de *accountability* (DONEDA, 2021, s.p).

Tem-se, pois, como norma central de proteção de dados pessoais a LGPD, que em cooperação com outras normas legais, fortalecerão a tutela da proteção de dados e o direito à privacidade, confirmando sua inserção como direto fundamental.

2.2 Proteção de dados pessoais e privacidade como direito fundamental

O direito constitucional brasileiro adotou a terminologia direitos e garantias fundamentais como gênero das demais espécies de direitos, não afastamento outras

[9] Recurso Especial 1853702, Dje 30.06.2020.
[10] Art. 4º Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
[11] Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - tratamento de dados pessoais - 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.
[12] Art. 4º Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

expressões como direitos humanos, direitos do homem, direitos individuais ou direitos humanos fundamentais para corresponder a categoria de direitos mais limitada daquele mais complexo representado pelos direitos fundamentais, apesar de no plano internacional a expressão utilizada é *direitos humanos* (SARLET, 2017, p. 331).

Para o presente trabalho, utiliza-se a expressão *direitos fundamentais* seguindo [13], na medida em que se limitará o estudo à ordem constitucional no que diz respeito à privacidade do homem, conforme expressa o inciso X, do artigo 5° da Constituição da República Federativa do Brasil[14].

Nas constituições democráticas, os direitos fundamentais atuam como limitação e direção do Estado (ALEXY, 2011, p. 721). Nessa linha, pode-se afirmar que a privacidade no ordenamento jurídico brasileiro é um direito fundamental da pessoa que implica na não intervenção de terceiros, inclusive do Estado.

Segundo Sarlet, os direitos fundamentais na ordem constitucional brasileira compreendem "todas as posições jurídicas concernentes à pessoa (naturais ou jurídicas…) [...]", que foram "integradas à constituição e retiradas da esfera de disponibilidade dos poderes constituídos", refletindo "a dupla fundamentalidade formal e material" e contempla a "noção de uma abertura material do catálogo de direitos fundamentais" (2017, p. 350).

Os direitos fundamentais do cidadão estão esculpidos nas diversas passagens da Constituição Federal, e não apenas no seu Título II, no artigo 5°e seus vários incisos. A doutrina de Sarlet o classifica como direitos fundamentais expressamente positivados, não apenas na Constituição, mas também em diplomas jurídicos de natureza constitucional, como os tratados internacionais de direitos humanos (2017, p. 354).

O aludido autor ainda conceitua os direitos fundamentais na ordem constitucional brasileira como "todas as posições jurídicas concernentes à pessoa (naturais ou jurídicas)...", que foram "integradas à constituição e retiradas da esfera de disponibilidade dos poderes constituídos", refletindo "a dupla fundamentalidade formal e material" e contempla a "noção de uma abertura material do catálogo de direitos fundamentais" (SARLET, 2017, p. 350).

A privacidade é tida como direito fundamental e tem sua relevância acentuada na vinculação à dignidade humana, bem como na relação com a intimidade, a inviolabilidade do

---

[13] Para o autor, "atribuímos às expressões 'direitos humanos' (ou direitos humanos fundamentais), compreendidos como direitos da pessoa humana reconhecidos pela ordem jurídica internacional e com pretensão de validade universal, e "direitos fundamentais", concebidos como aqueles direitos (dentre os quais se destacam os direitos humanos) reconhecidos e positivados na esfera do direito constitucional." (, 2017, p. 333).

[14] Art. 5°. [...] 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.

domicílio, tratado pelo ordenamento constitucional brasileiro como bens tutelados de forma autônoma (SARLET, 2017, p. 487-88).

Considerando-se a proteção constitucional da inviolabilidade da vida privada, isto é, da privacidade e os direitos dela decorrentes, com direito fundamental, por consequência terá a proteção do Poder Público, inclusive impondo limites sobre a sua atuação. Do mesmo modo, não se limitando à atuação do Poder Judiciário como interventor quando motivado, mas de observância obrigatória – e preventiva – por todos os órgãos e entidades da Administração Pública quando do exercício de suas atribuições legais, de acordo com os princípios esculpidos no artigo 37, da Constituição Federal, em especial o da legalidade.

Nesse cenário é que a inclusão do Poder Público na abrangência da LGPD foi – no anteprojeto – e é primordial, tendo em vista dois fundamentos que se entende como relevantes: primeiro, o Estado é detentor de massivos dados e informações de seus cidadãos, usuários de serviços públicos e agentes públicos; segundo, sua obrigação constitucional de tutela de direitos fundamentais o insere como guardião – de si próprio – de violação da privacidade por intermédio de dados pessoais.

Percebe-se, pois, que a não inserção do Estado no rol da LGPD ofenderia direitos fundamentais, como corrobora Pacheco Júnior, ao prescrever que [...] “omitir da Lei a tutela dos direitos à proteção dos dados pessoais tratados pela administração pública, seria uma violação aos próprios direitos constitucionais basilares” (2020, s.p).

A LGPD em seu artigo 5°, inciso X, prescreve que o tratamento de dados diz respeito à atividade de “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”, o que contempla um rol imensurável de possibilidades em seu tratamento.

Observe-se, todavia, que inexiste expressa previsão como direitos humanos – plano internacional – de proteção de dados, seja no ONU, nas Convenções Interamericana e Europeia, mas apenas no âmbito dos órgãos judiciários na aplicação de tratados é possível o direito de proteção de dados como direitos humanos (SARLET, 2021, s.p).

O direito à proteção de dados pessoais é fundamental (no sentido material) por servir à proteção de princípios e direitos, como o princípio da dignidade da pessoa humana e o direito à privacidade, e no sentido formal, uma vez que mesmo inexistindo previsão expressa na Constituição Federal, ele tem *status* equivalente na hierarquia normativa, exigindo-se atuação estatal para sua garantia (SARLET, 2021, s.p).

A tutela de proteção de dados vai além da tutela da privacidade, considerando-se "um direito fundamental autônomo, diretamente vinculado à proteção da personalidade" (SARLET, 2021, s.p) e que não pode ser "reduzido a uma mera evolução do direito à privacidade" (BIONI, 2019, p. 95).

O direito à privacidade é um direito de proteção estática, negativa, ao passo que a proteção de dados estabelece regras que legitimam o titular a tomar iniciativas, medidas de controle sobre seus dados (RODOTÀ, 2008, p. 17).

Por seu turno, Zuboff contribui entendendo a privacidade como gênero de dados ao prescrever que "os direitos de privacidade conferem, assim, direitos de decisão; a privacidade permite uma decisão sobre onde se quer estar no espectro entre sigilo e transparência em cada situação" (2018, p. 47).

Inobstante essa observação e inserção da privacidade e a proteção de dados como direitos fundamentais, os dados podem ser utilizados como instrumento de controle pelo poder por quem o detém, em especial por parte do Estado, o maior guardião de dados pessoais.

2.3 Lei Geral de Proteção de Dados e Lei de Acesso à Informação: inter-relações normativas na privacidade

A tutela constitucional da privacidade ramifica-se, como visto na primeira parte deste estudo, na legislação infraconstitucional, assim como nos princípios do direito, em especial os arrolados nas leis do MCI, LGPD e LAI, as quais visam, em segundo plano, o princípio da transparência.

A Constituição Federal, em seu artigo 5°, inciso XXXIII, arrolou a transparência como direito fundamental, ao prescrever que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular" [...] que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". O sigilo, portanto, é a exceção no que diz respeito à segurança que o Estado deve tutelar.

Tendo como regra a transparência, alguns dados não podem ficar abertos ao público de modo irrestrito, sendo necessária a utilização dos princípios da proporcionalidade e da ponderação[15]. Nessa linha, Canhadas assim prescreve:

[15] Ver a catalogação acerca dos princípios da LGPD no item 3.2 deste trabalho.

> [...] a transparência é a regra e as informações detidas pelo poder público devem ser acessadas de maneira ampla, fácil e rápida. Contudo, *a depender do resultado da ponderação* entre os direitos conflitantes, há *hipóteses em que a transparência pode ser não obrigatória, mas permitida* (quando o seu detentor tem o direito de abrir o acesso à informação, mas pode não fazê-lo por questões de conveniência e oportunidade) e *também há hipóteses em que a transparência é em verdade proibida*, justamente porque o acesso à determinada informação pelo público pode significar a violação de outro direito fundamental ainda mais relevante para o ordenamento jurídico. (2020, s.p.) [grifo do autor].

Ao lado da LGPD, a LAI pode ser examinada como a sua outra face (CANHADAS, 2020, s.p.), pois, se de um lado tem o Estado o dever de transparência, por outro, deve zelar pela privacidade dos dados pessoais. E entre as duas faces há uma linha tênue, pouco observada pela doutrina e que vem à tona no presente estudo, que diz respeito ao compartilhamento ou transferência de dados entre órgãos públicos para atingir os fins públicos. Entre o dever de transparência e a proteção da privacidade existe um limbo do compartilhamento de informações, que não estão abertos ao público (transparência) tampouco o titular dos dados tem garantida à privacidade por lhe faltar a anuência e/ou comunicação.

A LAI assim como a LGPD, nos seus termos, arrola vedações à transparência e à privacidade, respectivamente, as quais servem como freios e contrapesos entre o sigilo e a transparência.

As informações do Poder Público são demasiadas e estão disponíveis em portais de transparência, cujos dados são acessíveis a qualquer cidadão, contudo, apenas há informações, cujos conteúdos (processos e procedimentos) permanecem no âmbito dos órgãos públicos e serão acessíveis apenas quando solicitado de forma expressa por aquele que interessado for. Inexiste, portanto, transparência espontânea, mas expectativa de direito de acesso a informações que serão exteriorizadas a partir da manifestação do requerente.

Nessa busca de concretude e efetividade, uma lei necessita de impulsos, como condutas comportamentais das pessoas e organismos privados que sejam proativos e não estejam à mercê de ingerências. Veja-se:

> […] temos de buscar uma combinação de iniciativas que incluam a reforma dos sistemas de administração e de investigação, alterando a estrutura de incentivos, a realização de reformas legais adequadas, reduzindo a tolerância social da desonestidade financeira e expandindo o uso de disposições já codificadas na Lei do Direito à Informação e em legislações relacionadas, e o estabelecimento de um jornalismo investigativo que vise relatar, de forma sistemática, o mau comportamento do qual não se presta conta (SEN, 2015, p. 171).

Contudo, essa possível efetividade da lei é dificultada a partir do momento em que se exige, como requisito, a identificação do requerente (LAI, art. 10), indo de encontro com a impessoalidade e à proteção daquele que não pretende se identificar no acesso de informações públicas. Nesse ponto, a LAI exige identificação daquele que pretende acessar um dado público, que pode estar sob sigilo em razão da proteção à privacidade. Eis a conversação implícita entre privacidade e transparência.

Partindo-se da ideia de que, como regra, as informações protegidas pelo Poder Público são públicas, a obrigatoriedade da identificação do usuário que pretende acessar informações – que são públicas, frise-se – deixa de garantir proteção da identidade do requerente, o qual é passível de intimidação ou retaliação por agentes do órgão estatal, comumente em comunidades pequenas onde todas as pessoas têm conhecimento de quem é cada morador, onde labora ou reside.

Por outro lado, é óbvio que a identificação do usuário requerente das informações de atos de governo – inclusive procedimentos e processos – que estão guarnecidas pelo Poder Público serve mais para resposta ao destinatário da solicitação do que a identificação do solicitante em si.

Em trabalho empírico, corroborando com essa percepção de fragilidade e limitação da LAI, a organização internacional Artigo 19 contribui com a seguinte passagem:

> Os reflexos dessa "cultura do sigilo" adquirem características especialmente preocupantes no nível municipal, onde a pessoalidade frequentemente permeia as relações entre sociedade e servidores públicos, de modo que a identificação gera constantemente constrangimentos em relações de trabalho e tratamento diferenciado em respostas a demandas por informação. Em trabalho de campo realizado pela ARTIGO 19 em municípios pequenos, por exemplo, notou-se o receio da população quanto à realização de pedidos de informação. Temia-se que a prática pudesse colocar em risco serviços básicos providos por autoridades locais e a própria integridade física dos requerentes, uma vez que muitos já haviam sido ameaçados (ARTIGO 19, 2018, p. 9).

Ora, a proteção de dados pessoais (identificação) inexiste daqueles requerentes de acesso a informações perante o Poder Público de forma expressa na LGPD, o que gera "entrave à efetividade do seu exercício, já que a exigência pode colocar em risco não só o próprio conteúdo da informação apresentada como também o próprio solicitante" (SIGARINI; SANTOS, 2020).

Uma alternativa plausível – autorizada pela própria LAI – é a supressão de identificadores (endereço, idade, cadastro pessoal de pessoa física – CPF) do requerente a fim de não o tornar facilmente identificável, que são classificados por Bioni como conceito expansionista, "pelo qual do dado pessoal equivale a uma informação que, direta ou

indiretamente, identifica um sujeito" abrangendo "mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota" (2019, s.p.).

Percebe-se que a inter-relação entre as duas normas (LGPD e LAI) que visam ao mesmo tempo por um lado proteger a privacidade e por outro garantir a transparência possuem um conflito aparente. Para encaminhar esta situação de colisão, a ponderação e a proporcionalidade[16] são requisitos exigíveis daqueles que operam na praxe administrativa do Poder Público, os quais devem zelar pelos direitos que possam ser violados.

2.4 Dados pessoais e poder

Importante relacionar o uso e a manipulação dos dados com o poder, uma vez que este pode corromper-se, a fim de oportunizar finalidades outras que não aquelas originalmente estipuladas, controlando-os, ou, ainda, concebendo instrumentos de controle de dados em face do próprio poder, controlando-o.

As formas de manifestação de poder sobre dados são objeto da presente análise, partindo-se de concepções de teóricos no contexto da proteção de dados pessoais.

2.4.1 Controle de dados pelo Poder

Para toda e qualquer manipulação – coerção ou intervenção, direta ou indireta – na vida das pessoas, existe um 'poder' que emana sobre ela. Nesse sentido, para Foucault, o poder sobre a população dá-se por meio de 'técnicas ou tecnologias de poder' que, nos séculos XVII e XVIII, eram centrados no corpo individual das pessoas, e denominadas de tecnologia disciplinar do trabalho (hierarquia, inspeção e relatórios) (2010, p. 203).

Ainda no final do século XVIII, floresceu uma nova tecnologia de poder, a qual Foucault denominou de biopolítica – ou biopoder –, que diz respeito a fatores externos do corpo do homem, atingindo universalmente a espécie humana, como as adversidades da vida, a exemplo de saúde pública, taxa de natalidade, mortalidade e longevidade. No início do século XIX, concebeu-se instituições estatais de assistência e outros mecanismos de cunho privado como seguridade e poupança financeira a fim de atender às necessidades do homem na velhice e na saúde (FOUCAULT, 2010, p. 205).

[16] Sobre o tema ver: MORAIS, Fausto Santos de. Ponderação e arbitrariedade: a inadequada recepção de Alexy pelo STF. 2. ed. Salvador: Juspodivm, 2018.

O biopoder, na concepção do autor, exerce o controle e a vigilância (administração) da população, produzindo forças e deixando-as crescer e a organizar-se ao invés de aniquilá-la ou coibi-las – o que difere, desde o século XVII do poder da morte (intervenção nas leis biológicas – vida – da população). O controle biopolítico – ou biopoder – limita-se a fatores externos, não adentrando na mente do homem, na psique da população.

Além da existência dessa tecnologia de poder, há outra que adentrará na psique humana e, consequentemente, na privacidade de cada indivíduo. Essa nova tecnologia de poder, surgida no final do século XX e mais evidente no século XXI, é denominada por Han como psicopoder – ou psicopolítica –, a qual, "está em posição para, com ajuda da vigilância digital, ler e controlar pensamentos", capaz de intervir nos processos psicológicos da população. A partir do *Big Data* há possibilidade de prever comportamentos dando margem ao surgimento da nova tecnologia do poder, a 'psicopolítica' (HAN, 2018, p. 131-132).

É a era da vigilância ativa, do controle, o que pode ser chamado de psicopolítica digital, na qual a negatividade de uma decisão livre abre espaço para a positividade do 'estado de coisas', onde o *Big Data* dita as regras e comportamentos pessoais (HAN, 2014, p. 26).

Logo, ao transformarem-se em *pessoas transparentes* ("livro aberto"), tornamo-nos *coisa* – os dados, as informações –, a qual é controlável e manipulável. É essa face do Estado, cuja transparência para com ele se impõe (compulsória) e em prejuízo da privacidade, que se utiliza para fomentar sua faceta autoritária (controle), sob o argumento de que está agindo no interesse público, na segurança nacional ou do próprio Estado (eficiência). [grifos do autor]

Nessa linha, de acordo com Doneda (2020, p. 3), o Estado foi o primeiro a utilizar de forma ampla as informações pessoais, cujos motivos era – e ainda o são – a Administração Pública ser eficiente, tendo conhecimento de dados da população, ao passo que se utiliza do controle para ativar controles sociais, típico de Estado de regime totalitário.

Para Han o *Big Data* é o instrumento poderoso da psicopolítica, pois se desloca da vigilância passiva para o controle ativo, "*nos precipita a una crisis de la libertad con mayor alcance, pues ahora afecta a la misma voluntad libre*." Por meio do *Big Data* é possível *"adquirir un conocimiento integral de la dinámica inherente a la sociedad de la comunicación. Se trata de un conocimiento de dominación que permite intervenir en la psique y condicionarla a un nivel reflexivo."* (2014, p. 25). Han adverte para uma nova forma de evolução:

> [...] incluso como una forma de mutación del capitalismo, no se ocupa primeramente de lo «biológico, somático, corporal». Por el contrario, descubre la *psique* como fuerza productiva. Este giro a la psique, y con ello a la psicopolítica, está

> relacionado con la forma de producción del capitalismo actual, puesto que este último está determinado por formas de producción inmateriales e incorpóreas. No se producen objetos físicos, sino objetos no-físicos como informaciones y programas. El cuerpo como fuerza productiva ya no es tan central como en la sociedad disciplinaria biopolítica. Para incrementar la productividad, no se *superan* resistencias corporales, sino que se *optimizan* procesos psíquicos y mentales. El *disciplinamento corporal* cede ante la *optimización mental*. Así, el *neuro-enhancement** se distingue fundamentalmente de las técnicas disciplinarias psiquiátricas. (2014, p. 42). [grifo do autor]

Desse modo, a biopolítica "*impede un acceso sutil a la psique. La psicopolítica digital, por el contrario, es capaz de llegar a procesos psíquicos de manera prospectiva. Es quizá mucho más rápida que la voluntad libre*" (HAN, 2014, p. 95). Chega-se ao entendimento de que a privacidade é – e sempre foi – objeto de interesses econômicos, agora acelerada e potencializada pelo auxílio das tecnologias de informação e de comunicação (TICs) que oportunizam a otimização e compilação de quaisquer informações pessoais. Caracteriza-se a era do totalitarismo digital, onde os dados são meios de transparência e o dataísmo é uma ideologia em si (HAN, 2014, p. 88).

É nesse cenário que o Estado com acesso livre a banco de dados por ele geridos (e não tratados?) tem meios de monitorar e controlar seus cidadãos, uma vez que "a liberdade e a comunicação ilimitadas se transformaram em monitoramento e controle total" (HAN, 2018, p. 19).

Não é diferente, pois, que leis que visam ser instrumentos de proteção dos cidadãos face o "poder" do Estado, como os institutos do *habeas data* e da Lei de Acesso à Informação (LAI), contribuem para uma transparência no agir do Poder Público, em especial quando diz respeito a tratamento das informações de caráter pessoal de seus cidadãos. É o que determina a LAI em seu artigo 31, onde que, além da transparência, o Estado deve observar outros direitos, como a intimidade, a privacidade, a honra, a imagem, as liberdades e garantias individuais das pessoas, apesar de, a própria lei relativizar esse zelo às informações pessoais, quando se tratar de questões inerentes a irregularidades, por exemplo[17].

Tem-se, portanto, pelo menos ventilada a hipótese de, sem controle ou *accountability*, valer-se o Estado de informações e dados de seus cidadãos e deles utilizar-se na "busca do interesse público", de suas políticas públicas e investigações criminais sem que haja quaisquer

[17] Art. 31. 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. [...]
§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

tipos de tratamentos ou anuência do titular desses dados é no mínimo temerário, além de afrontar direitos fundamentais sob a égide da busca do interesse público.

2.4.2 Prerrogativa estatal no controle de dados pessoais: a biopolítica e a psicopolítica como técnicas de poder

Conquanto a LGPD seja um marco regulador do tratamento de informações pessoais no ordenamento jurídico nacional, tendo como objeto da proteção de direitos fundamentais (liberdade, privacidade e o livre desenvolvimento da personalidade), estabeleceu-se apenas em face da pessoa natural, no teor do artigo 1° da Lei[18], o que rechaça, de imediato, a ideia de proteção de dados da pessoa jurídica, como documentos sigilosos, segredos de negócios, as quais dizem respeito a leis esparsas – como direito de propriedade intelectual e direito civil –, o que vai de encontro ao defendido por Richard Posner, para o qual a proteção de dados empresariais – ou privacidade comercial – traz maiores benefícios sociais do que a de dados pessoais (2010, p. 293).

Não quer isso dizer, entretanto, que estão livres de proteção os registros inerentes às pessoas jurídicas, mas não há um 'código' ou compilação de normas que tratam especificamente dessa proteção como o faz a LGPD para as pessoas naturais. Quando o Estado atua nos seus interesses 'particulares' – valendo-se de informações das pessoas (naturais) para os fins que a lei lhe autoriza, parece que está a controlar informações de seus cidadãos, as quais, *a priori,* passam desreguladas ou sem controle sobre si mesmo – sem um *accountability* no Estado.

Todavia, a lei traz uma possível solução para essa 'ausência' de controle aparente, ao estabelecer, em seu artigo 40, que o Estado, por intermédio da autoridade nacional – Autoridade Nacional de Proteção de Dados (ANPD) –, "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". Como o Poder Público por intermédio de seu aparelho estatal possui a atribuição de fiscalizador e também de regulador da lei, tem-se presente a psicopolítica tratada por Han, considerando a ausência de *accountability*[19] (prestação de contas e responsabilidade).

---

[18] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[19] *Accountability* será tratado em tópico específico neste trabalho.

Nessa relação de transparência (liberdade e comunicação ilimitadas) de caráter unilateral do cidadão para com o Estado, viabiliza-se o acesso irrestrito e sem controle (aparente) pelos organismos estatais, nos quais não se estaria diante de um 'panóptico' digital na perspectiva de Han, mas de biopolítica. Explique-se.

Os inseridos no panóptico digital "comunicam-se intensivamente e expõem-se por vontade própria", participando ativamente da sua construção. Nesse ambiente, a "sociedade digital de controle faz uso intensivo da liberdade", possível em razão da autoexposição voluntária, cuja "entrega dos dados não acontece por coação, mas a partir de uma necessidade interna", em que "reside a eficiência do panóptico digital" (HAN, 2018, p. 19).

Em contraponto, para Zuboff, inexiste panóptico, pois há o "surgimento de uma nova arquitetura universal", denominada de *Big Other*, que se configura como "um ubíquo regime institucional em rede que registra, modifica e mercantiliza a experiência cotidiana" [...] "é o poder soberano de um futuro próximo que aniquila a liberdade alcançada pelo Estado de direito" (2018, p. 44). Ademais, o panóptico de Bentham "é prosaico em comparação com essa nova arquitetura", que focava a um único ponto de observação (2018, p. 44).

Quando o Estado colhe informações pessoais de seus cidadãos para lhes garantir direitos, como acesso à educação (matrícula escolar), saúde (cadastro no Sistema Único de Saúde – SUS) ou assistência social (benefício prestacional), o faz sem coação, tampouco por voluntarismo, mas por necessidade intrínseca (ou interna, como prefere Han) criado pelo biopoder – e pelo psicopoder ou psicopolítica –, isto é, pelo controle de ensejar e potencializar necessidade de acesso a bens essenciais (ou primários) que são disponibilizados somente a partir de uma contrapartida pelo cidadão, como identificação, qualificação e localização, por exemplo, a fim de aferir se tem ou não direito ao acesso a determinados bens, como matrícula em instituição de ensino público, tratamento de saúde no SUS, benefício assistencial ou previdenciário, e até mesmo para fins eleitorais, como endereço de domicílio de votação que vinculam e identificam a territorialidade do cidadão.

Longe está neste ponto, como afirma Han, "caminhando para a era da psicopolítica digital" (HAN, 2018, p. 23), porque presente está ambas as técnicas de poder (biopolítica e psicopolítica), inclusive arrisca-se em denominar de "biopolítica digital" quando ocorre utilização da estrutura do Estado para controlar o acesso a bens primários pelos cidadãos e com isso extrair por meio de coação indireta (ou voluntarismo forçado) dados pessoais. Estes, por sua vez, estão inseridos na pscipolítica digital, por serem eles coisas imateriais de uma pessoa controlada por terceiro (Estado) quando este faz uso para fins outros que não aqueles

conscientemente e originalmente concedidos outrora em razão da "necessidade humana" (biopolítica) e exigência estatal.

A ideia do poder emanado pelo Estado nesses dados é garantir tutela frente a novas tecnologias e infrações penais modernas, em que a intervenção mínima do direito penal (sistema garantista), abre espaço a fim de tutelar "novos bens jurídicos de natureza coletiva, pelo predomínio dos tipos penais abstratos em detrimento de figuras delitivas de resultado", em razão da necessidade de antecipar a intervenção penal e prevenir o dano (MAYA, 2017, p. 64).

Apesar do interesse em tutelar tais direitos frente a infrações penais, como visto alhures quanto à dispensa de tratamento de dados em face da LGPD, Lopes Jr traz importante contribuição quanto à legitimidade desse poder de intervir do Estado nas liberdades individuais do cidadão sob a óptica constitucional.

O Estado deve justificar e se legitimar para intervir na liberdade individual[20] da pessoa, e não o oposto, isto é, não a liberdade individual deve ser legitimada, pois ela já o é naturalmente, porque não pode "resultar de uma autoatribuição do Estado (autolegitimação, que conduza a uma situação autopoiética, portanto)"[21] (LOPES JÚNIOR, 2020, p. 37). Não pode, portanto, o Poder Público se valer ou lhe reservar a prerrogativa de intervir em liberdades individuais – como a privacidade – por sua própria condição de Estado, legitimando-se em face de uma tutela natural que lhe foi incumbida pelo Estado Democrático de Direito.

No cenário do mundo digital, as Tecnologias da Informação e Comunicação (TIC's) possuem "impacto no Estado informacional, no qual a gestão pública é operada, basicamente, a partir de dispositivos eletrônicos, os quais facilitam ao governo a coleta e o processamento de informações sobre os cidadãos" (BOFF, 2018, p. 26). Nessa lógica, o Estado torna-se o próprio *Big Data* que tudo vê, uma vez que a partir do momento que possui e conserva infinitas informações dos seus cidadãos – mesmo que por suas ramificações e aparelhos estatais – e lança mão da forma que melhor lhe aprouver para utilizá-las, inclusive justificando-se sobre tutela de bens jurídicos penais e/ou de interesse público, é imperioso a inserção de mecanismos de *accountability,* a fim de garantir proteção dos direitos

[20] Aqui se entende a expressão "liberdade individual" o conjunto de direitos de liberdade da pessoa, como a privacidade, a intimidade, a honra, a imagem, etc.

[21] LOPES JUNIOR, Aury. Fundamentos do processo penal. 6. ed. São Paulo: Saraiva Educação, 2020, p. 37.

fundamentais – como a liberdade e a privacidade – do próprio Estado sob a égide do interesse coletivo.

É de se observar, contudo, que o panóptico eletrônico ou digital estará presente apenas quando os dados ou informações não estejam disponíveis de forma fragmentada, distribuídos em vários dispositivos e bancos digitais, mas que, posteriormente, sejam reunidos e tratados por alguma organização quando coletados. Nesse ponto nasce, para o titular do dado ou informação coletada disponível de forma fragmentada em vários ambientes (físico ou digital), o direito de que as suas informações passem pelo exame da LGPD, com a observância dos princípios gerais de proteção.

Diz-se isso uma vez que, se o dado está fragmentado e sem a centralização deles é impossível passar um mínimo de informação que identifique ou relacione uma pessoa, não se estaria diante de violação da privacidade. Contudo, Doneda argumenta que:

> Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. [...] Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza (2020, p. 1).

Essa lógica de que dado e informação são distintos ao ponto de inviabilizar a extração de algo que possa identificar ou relacionar um fato à uma pessoa parece equívoca, uma vez que a LGPD e a LAI desconhecem essa distinção[22]. Todavia, mesmo assim pode-se manter a ideia de panóptico digital – apesar da óptica de Zuboff em outra passagem – por estarem eles (dados ou informações) distribuídas e fragmentadas em locais (físicos ou digitais), mas somente a partir do momento em que é possível a sua reunião para relacionar a uma pessoa natural identificada ou identificável.

Conveniente esclarecer que a sociedade da transparência decorre sociedade da informação, entretanto nem sempre as informações e comunicações demasiadas ensejam transparência, pois a massificação de informações não gera verdade e, quanto mais informações liberadas, mais falta de transparência e desinformação o que leva a afirmar que "a hiperinformação e a hiercomunicação não trazem luz à escuridão" (HAN, 2017, p. 95-96).

---

[22] A LGPD, artigo 5°, I, e a Lei de Acesso à Informação, artigo 4°, I, dispõem, respectivamente: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Essa crítica de Han desperta atenção para a transparência. Na sua análise, "transparência e poder não se coadunam muito bem", pois o poder prefere andar no oculto ao passo que a transparência é que derruba a esfera oculta do poder, e que uma transparência recíproca só haveria por meio de uma supervisão permanente (2017, p. 110). Diz-se isso uma vez que a "confiança só é possível em uma situação que conjuga saber e não saber. Confiança significa edificar uma boa relação positiva com o outro, apesar de não saber dele; possibilita ação, apesar da falta de saber." A transparência remete a "um estado no qual se elimina todo e qualquer não saber, pois onde impera a transparência já não há espaço para a confiança" (2017, p. 111).

Para o Estado ou organização pública, enquanto controlador dessas informações e também detentor de dados pessoais (art. 7°, III, da Lei nº 13.709/2018), há ausência de relação de confiança, pois eles já têm as informações de seus cidadãos e usuários. Desse modo, todos estão incluídos em "um único panóptico" (panóptico digital[23] como prefere HAN), porque as redes sociais e empresas de tecnologia – como o Google – "se apresentam como espaços de liberdades, estão adotando cada vez mais formas panópticas". Hodiernamente, as pessoas se auto expõem de forma livre e espontânea ao olho panóptico (HAN, 2017, p. 115), e que elas preferem "manipular o mundo à sua volta, escolhendo quais informações revelarão sobre si mesmas" (POSNER. 2010, p. 275).

Portanto, no âmbito da relação entre cidadãos e o Estado, em especial na relação de concessão de informações e dados pessoais para permitir acesso a bens primários ou essenciais disponibilizados pelo Poder Público, que se dá por intermédio de uma via unilateral "compulsória", isto é, desprovida de voluntarismo do titular ou ausência de coerção direta do ente estatal, a ideia de panóptico digital de Han não se aplica, por lhe carecer requisitos mínimos como o voluntarismo e ausência de coerção plena na anuência e disponibilização de dados pessoais pelos cidadãos ao Estado. Por outro lado, é certo que há uso de tecnologia de poder pelo Estado sem um mínimo de transparência, tampouco anuência do titular dos dados, legitimado a partir da concretização de interesses públicos.

As previsões constitucional e legal de direitos de proteção à privacidade e a dados pessoais foram concebidas em razão da negativa à intervenção do Estado – e das técnicas de poder – no uso e na manipulação de informações inerentes às pessoas, prática que pode acarretar algum dano à dignidade humana, impondo limites ao poder estatal nas transações de

[23] BOFF se valeu da expressão "panóptico eletrônico" para representar a forma de controle por uso das TIC's (2018, p. 26).

dados pessoais, a fim de garantir a privacidade ao passo que desempenha suas funções em busca do interesse público.

É imperioso, portanto, buscar entender os limites que o compartilhamento de dados na LGPD se impõe para o Estado como pretexto na busca de alcançar seus objetivos institucionais. O próximo capítulo procurará apresentar os limites do Estado no compartilhamento de dados pessoais no ambiente estatal.

REFERÊNCIAS

ALEXY, Robert. Direitos fundamentais, ponderação e racionalidade. In: **Direito constitucional: teoria geral da constituição.** CLÈVE, Clèmerson Merlin; BARROSO, Luís Roberto (Org). São Paulo: Revista dos Tribunais, 2011.

ARTIGO 19. **Identidade revelada:** entraves na busca por informação pública no Brasil. Maio 2018. Disponível em: https://artigo19.org/?p=13806. Acesso em: 21 de ago. 2020.

ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. Nações Unidas, 1948. Disponível em: https://www.ohchr.org/en/udhr/documents/udhr_translations/por.pdf. Acesso em: 21 ago. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013.** Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em: 17 nov. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013.** Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306580. Acesso em 17 nov. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019.** Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=437612. Acesso em 10 mar 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Gestão de Riscos**. Disponível em: http://www.abnt.org.br/imprensa/releases/5753-lancada-a-nova-versao-da-norma-iso-31000-gestao-de-riscos Acesso em: 14 set. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000:2009**. Gestão de riscos: princípios e diretrizes. Rio de Janeiro: 2009.

ÁVILA, Humberto. **Teoria dos princípios**: da definição à aplicação dos princípios jurídicos. 16ª ed. São Paulo: Malheiros, 2015.

BECK, Ulrich, **A metamorfose do mundo:** novos conceitos para uma nova realidade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro Zahar, 2018.

BOFF, Salete Oro; LEAL, Dionis Janner. Exigibilidade Constitucional da Sustentabilidade nas Contratações Públicas: normas técnicas e gestão de riscos como instrumento de eficiência. **Revista de Direito Administrativo e Gestão Pública**, 6 (1), 98-118, 2020.

BOTTI, Flávia Bomtempo; RESENDE, Marta Elizabeth de Souza Mendes. A gestão do *compliance* como tecnologia promissora para concretização do princípio da eficiência no setor público brasileiro. **Revista dos Tribunais**. vol. 1002, abr 2019, p. 65-84.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988.

BRASIL. **Constituição Política do Império do Brazil**. Rio de Janeiro, 1824.

BRASIL. **Constituição da República dos Estados Unidos do Brasil.** Rio de Janeiro, 1891.

BRASIL. **Constituição da República dos Estados Unidos do Brasil.** Rio de Janeiro, 1934.

BRASIL. **Constituição da República dos Estados Unidos do Brasil.** Rio de Janeiro, 1937.

BRASIL. **Constituição da República dos Estados Unidos do Brasil.** Rio de Janeiro, 1946.

BRASIL. **Constituição da República Federativa do Brasil.** Congresso Nacional, 1967.

BRASIL. **Decreto n° 10.358/1942**. Declara o estado de guerra em todo o território nacional. Rio de Janeiro, 1942.

BRASIL. **Lei n° 12.850/2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.

BRASIL. **Lei n° 8.666/1993.** Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8666cons.htm.

BRASIL. **Lei n° 4.150/1962.** Institui o regime obrigatório de preparo e observância das normas técnicas nos contratos de obras e compras do serviço público de execução direta, concedida, autárquica ou de economia mista, através da Associação Brasileira de Normas Técnicas e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/1950-1969/l4150.htm#:~:text=LEI%20N%C2%BA%204.150%2C%20DE%2021,T%C3%A9cnicas%20e%20d%C3%A1%20outras%20provid%C3%AAncias.

BRASIL. **Lei n° 5.966/1973.** Institui o Sistema Nacional de Metrologia, Normalização e Qualidade Industrial, e dá outras providências. http://www.planalto.gov.br/ccivil_03/leis/l5966.htm

BRASIL. Lei n° 13.709/2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 12 set. 2020.

BRASIL. **Lei n° 12.846/2013.** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

BRASIL. **Lei n° 12.527/2011**. 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 13 set. 2020.

BRASIL. **Lei n° 12.965/2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Decreto n° 9.203/2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm. Acesso em 12 set. 2020.

BRASIL. Casa Civil da Presidência da República. **Guia da política de governança pública**. Brasília: Casa Civil da Presidência da República, 2018. Disponível em: https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica. Acesso em 12 set. 2020.

BRASIL. Controladoria-Geral da União. **Instrução normativa conjunta n° 1, de 10 de maio de 2016**. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em 12 set. 2020.

BRASIL. Ministério do Planejamento Orçamento e Gestão. **Instrução normativa n° 05, de 26 de maio de 2017**. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/20239255/do1-2017-05-26-instrucao-normativa-n-5-de-26-de-maio-de-2017-20237783. Acesso em 13 set. 2020.

BRASIL. **Guia de Transparência Ativa (GTA) para os órgãos e entidades do Poder Executivo Federal.** 6ª. ed. 2019. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/46643/1/gta_6_versao_2019.pdf. Acesso em 16 nov. 2020.

BRASIL. Controladoria Geral da União. **Guia técnico de regulamentação da Lei de Acesso à Informação em Municípios e check list**. Brasílis, 2013. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/transparencia-publica/brasil-transparente/arquivos/guia_checklist.pdf. Acesso em 16 nov. 2020.

BRASIL. **Lei n° 8.078/1990.** Dispõe sobre a proteção do consumidor e dá outras providências.

BRASIL. Superior Tribunal de Justiça. **REsp. 22.337-8/RS**. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/RevSTJ/article/download/6345/6471

BRASIL. Superior Tribunal de Justiça. **Resp. 306570/SP.** Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200100235255&dt_publicacao=18/02/2002

BRASIL. Superior Tribunal de Justiça. **Resp. 1782386/RJ.** Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201803152161&dt_publicacao=18/12/2020

BRASIL. Superior Tribunal de Justiça. **Resp. 1853702/RS.** Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903748407&dt_publicacao=30/06/2020

BRASIL. Superior Tribunal de Justiça. **REsp 1.102.578-MG**. Disponível em: https://ww2.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=@cod=%270411%27.

BRASIL. Superior Tribunal de Justiça. **HC 349945/PE.** Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201600498873&dt_publicacao=02/02/2017

BRASIL. Supremo Tribunal Federal. **RE. 418-416-8/SC.** Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur90028/false.

BRASIL. Supremo Tribunal Federal. **RE. 105591/SP**. Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5213056&numeroProcesso=1055941&classeProcesso=RE&numeroTema=990

BRASIL. **Decreto n° 8.771/2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm.

BRASIL. **Decreto n° 10.046/2019.** Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm

BRITTO, Carlos Ayres. Distinção entre "Controle social do poder" e "Participação popular". **Revista Trim'estral de Direito Público – RTDP**, Belo Horizonte, n. 61, 2015. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=239182>. Acesso em: 22 nov. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRITTO, Carlos Ayres. Distinção entre "controle social do poder" e "participação popular". **Revista de Direito Administrativo.** Jul/set. 1992, Rio de Janeiro. Acesso em 20 jan. 2020. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45286/47723.

CABRAL, Flávio Garcia. Os fundamentos políticos da prestação de contas estatal. **Revista de Direito Administrativo**. Belo Horizonte, n. 270, set – dez 2015. Acesso em: 13 set. 2020.

CABRAL, Flávio Garcia; CABRAL, Dafne Reichel. O Tribunal de Contas da União (TCU) e seu papel para um accountability horizontal efetiva. **Revista de Direito Administrativo e Infraestrutura**, São Paulo, vol. 6/2018, p. 143 – 164, Jul - Set 2018. Online. Acesso em: 13 set 2020.

CANHADAS, Fernando Augusto Martins. A lei de acesso à informação e a lei geral de proteção de dados: a transparência proibida. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Org.) **LGPD e administração pública:** uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

CASTRO, Rodrigo Pironti Aguirre de; GONÇALVES, Francine Silva Pacheco. ***Compliance* e gestão de riscos nas empresas estatais**. Belo Horizonte: Fórum, 2018.

CASTRO, Rodrigo Pironti Aguirre de; ZILIOTTO, Mirela Miró. ***Compliance* nas contratações públicas:** exigência e critérios normativos. Belo Horizonte: Fórum, 2019.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de *compliance* digital na administração pública: contribuições da LGPD para a integridade governamental. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coord.). **LGPD e administração pública** [livro eletrônico]: uma análise ampla dos impactos. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

CELLA, José Renato Gaziero; COPPETTI, Rafael (2017). Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. **Revista de Direito, Governança e Novas Tecnologias**. v. 3. p. 39. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0049/2017.v3i2.2471. Acessado em 01/11/2020.

CONTROLADORIA-GERAL DA UNIÃO. **Programa de integridade. Diretrizes para empresas privadas**. Brasília: CGU, 2015. Disponível em: https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf . Acesso em: 12 set. 2020.

CONTROLADORIA-GERAL DA UNIÃO. **Instrução normativa conjunta n° 1, de 10 de maio de 2016**. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em 12 set. 2020.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo, OLIVA, Milena Donato (Coord). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

CUNHA JÚNIOR, Dirley da; NOVELINO, Marcelo. **Constituição Federal para concursos**. Salvador: Juspodivm, 2010.

DALLARI, Adilson Abreu. Privatização, eficiência e responsabilidade. **Revista Eletrônica de Direito Administrativo Econômico**. Salvador, Instituto de Direito Público da Bahia, n° 5, dev/mar/abr de 2006. Disponível em: www.direitodoestado.com.br. Acesso em 01 mar 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo : Thomson Reuters Brasil, 2020.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. DONEDA, Danilo; , Ingo Wolfgang; MENDES, Laura Scherltel, [et. al] (Coord). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 33. ed. Rio de Janeiro: Forense, 2020.

FARIA, Edimur Ferreira de; DAMASCENO, Luíza Mascarenhas. Governança Corporativa na Administração Pública. **Revista de Direito Administrativo e Infraestrutura**, São Paulo, vol. 8/2019, p. 153 – 169, Jan - Mar 2019. Acesso em: 10 set. 2020.

FERRAZ JR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizado do Estado. In: **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993. Disponível em https://www.revistas.usp.br/rfdusp/article/view/67231/69841.

FORTES, VINICIUS BORGES. **O direito fundamental à privacidade:** uma proposta conceitual para a regulamentação da proteção de dados pessoais na internet no Brasil. 2015. 225 f. Tese (Doutorado em Direito Instituição de Ensino) – Universidade Estácio de Sá, Rio de Janeiro, 2015.

FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2. ed. São Paulo: WMF Martins Fontes, 2010.

FREITAS, Juarez. **O controle dos atos administrativos e os princípios fundamentais.** 5. ed. São Paulo: Malheiros, 2013.

FRYDMAN, Benoit. **O fim do estado de direito:** governar para standards e indicadores. 2. ed. Porto Alegre: Livraria do Advogado, 2018.

GIOVANINI, Wagner. ***Compliance*:** a excelência na prática. São Paulo: [s.e], 2014.

HAN, Byung-Chul. **Psicopolítica.** Barcelona-ES: Herder Editorial S.L., 2014.

HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis, RJ: Vozes, 2017.

HAN, Byung-Chul. **Psicopolítica**. Tradução de Maurício Liesen. Belo Horizonte: Ayné, 2018.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. ***Compliance* à Luz da Governança Corporativa**. São Paulo: IBGC, 2017. Disponível em: https://www.legiscompliance.com.br/images/pdf/ibgc_orienta_compliance_a_luz_da_governanca.pdf. Acesso em 16 fev. 2021.

KARL, Éryta Dallete Fernandes. *Compliance* e LGPD: uma exigência também para a Administração Pública. In: ZENKNER, Marcelo; CASTRO, Rodrigo Pironti Aguirre de (Coord.) ***Compliance* no setor público.** Belo Horizonte: Fórum, 2020.

KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer. Compartilhamento de dados pessoais no âmbito da administração pública sob a égide da lei geral de proteção de dados. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Org.) **LGPD e administração pública: uma análise ampla dos impactos.** São Paulo: Thomson Reuters Brasil, 2020.

LEAL, Dionis Janner Leal; BOFF, Salete Oro. O uso da *accountability* e *compliance* como formas de mitigar a responsabilidade pelos danos causados pela inteligência artificial. In Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fabiano Hartmann Peixoto; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2020. Disponível em: http://conpedi.danilolr.info/publicacoes/nl6180k3/m4tcws6j/8J0j3hOCne6YBKkw.pdf.

LEAL, Dionis Janner. *Accountability* no setor público sobre a perspectiva de Amartya Sen: do estado eficiente ao estado de controle e gestão de riscos. In: LUCAS, Doglas Cesar et al (Orgs.). **Direitos Humanos e Democracia em tempos de crise: a proteção jurídica das minorias.** Vol. 2. p. 544-558. Porto Alegre, RS: Editora Fi, 2019. Disponível em: https://3c290742-53df-4d6f-b12f-6b135a606bc7.filesusr.com/ugd/48d206_2da4445f97c94b8b9f8074df4630c076.pdf. Acesso em 12 set. 2020.

LOPES JUNIOR, Aury. **Fundamentos do processo penal.** 6. ed. São Paulo: Saraiva Educação, 2020.

MAIOLINO, Eurico Zecchin. *Accountability* popular e os sistemas de governo. **Revista dos Tribunais**, vol. 990, p. 41-54, abr 2018. Acesso em: 13 set. 2020.

MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. **Cadernos de direito constitucional e ciência política**, São Paulo, v. 25, n. 101, p. 105-124., mai./jun. 2017. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=138663. Acesso em: 4 fev. 2020.

MAURMO, Júlia Gomes Pereira. A distinção conceitual entre privacidade, intimidade, vida privada, honra e imagem. **Revista de Direito Privado.** São Paulo, v. 57, p. 33-52., jan-mar. 2014. Disponível em: https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000173d5badcf6a4d2fe98&docguid=I1240bb90bfa811e39d90010000000000&hitguid=I1240bb90bfa811e39d90010000000000&spos=2&epos=2&td=5&context=167&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em: 09 ago. 2020.

MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo.** Dissertação de Mestrado (Direito). Universidade de Brasília: Brasília, 2018.

MAYA, André Machado. Conservação e acesso a dados públicos e privados para fins penais: a normativa legal brasileira examinada desde a perspectiva da jurisprudência do Tribunal de Justiça da Comunidade Europeia. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 25, n. 138, p. 61-87, dez.. 2017. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=139661. Acesso em: 26 jul. 2020.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo.** 17ª ed. São Paulo: Malheiros, 2004.

MODESTO, Paulo. Notas para um debate sobre o princípio da eficiência. **Interesse Público**, Belo Horizonte, v. 51, n. 2, p. 107-121, abr./jun. 2000. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=51586>. Acesso em: 23 ago. 2019.

MORAIS, Fausto Santos de. **Ponderação e arbitrariedade:** a inadequada recepção de Alexy pelo STF. 2. ed. Salvador: Juspodivm, 2018.

NASCIMENTO, Juliana Oliveira. Panorama internacional e brasileiro da governança, riscos, controles internos e compliance no setor público. PAULA, Marco Aurélio Borges de; CASTRO, Rodrigo Pironti de (Coord.). ***Compliance*, gestão de riscos e combate à corrupção: integridade para o desenvolvimento.** Belo Horizonte: Fórum, 2018.

NEVES, Marcelo. **Transconstitucionalismo**. São Paulo: WMF Martins Fontes, 2009.

RAMOS, André de Carvalho. **Teoria geral dos direitos humanos na ordem internacional.** 6. ed. São Paulo: Saraiva, 2016.

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

ROPSA, Aline Martins. **Decripitando as reformas do Poder Judiciário brasileiro motivadas pelo pluralismo transnacional: o império *standards* e indicadores.** Santa Maria: UFSM (Dissertação – Direito), 2018. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/13985/DIS_PPGDIREITO_2018_ROSPA_ALINE.pdf?sequence=1&isAllowed=y. Acesso em 17 ago. 2020.

ROSA, Alexandre Morais da. **Guia do processo penal conforme a teoria dos jogos.** 6. ed. ver., atual., e ampl. Florianópolis: EMais, 2020.

O'DONNELL, Guilhermo A. **Dissonâncias:** crítica democráticas à democracia. Tradução de Marta Maria Assumpção Rodrigues. Rio de Janeiro: UFRJ, 2017.

O'DONNELL, Guilhermo A. *Accountability* horizontal e novas poliarquias. Lua Nova: **Revista de Cultura e Política**, n° 44, p. 27-54. Disponível em: https://www.scielo.br/pdf/ln/n44/a03n44.pdf

PACHECO JUNIOR, Francisco Gabriel. O tratamento de dados pessoais pelo setor público e o alcance da LGPD. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Org.). **LGPD e administração pública:** uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Org.) **LGPD e administração pública:** uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

POSNER, Richard A. **A Economia da Justiça.** Tradução de Evandro Ferreira e Silva. São Paulo: WMF Martins Fontes, 2010.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; e MITIDIERO, Daniel. **Curso de direito constitucional.** 6. ed. São Paulo: Saraiva, 2017.

SARLET, Ingo Wolfgang. Panorama histórico da proteção de dados pessoais. DONEDA, Danilo; , Ingo Wolfgang; MENDES, Laura Scherltel, [et. al] (Coord). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

SCHRAMM, Fernanda Santos. ***Compliance*** **nas contratações públicas**. Belo Horizonte: Fórum, 2019.

SEN, Amartya; DRÈZE, Jean. **Glória incerta:** a Índia e suas contradições. Tradução de Ricardo Doninelli Mendes Laila Coutinho. São Paulo: Companhia das Letras, 2015.

SEN, Amartya. **Desigualdade reexaminada.** Tradução: Ricardo Doninelli Mendes. São Paulo: Record, 2001, p. 127.

SIGARINI, Danilo Cavalcante; SANTOS, Fábio de Sousa. A obrigatoriedade de identificação do solicitante da informação como obstáculo para garantia do direito de acesso à informação. **Revista de Direito Administrativo e Infraestrutura** | vol. 13/2020 | p. 129 - 144 | Abr - Jun / 2020 [eletrônica].

SILVA, Felipe Bezerra. Considerações a respeito da ABNT NBR ISO 31000:2009 (gestão de riscos) e sua aplicabilidade na Administração Pública direta e indireta. PAULA, Marco Aurélio Borges de; CASTRO, Rodrigo Pironti de (Coord.). **Compliance, gestão de riscos e combate à corrupção: integridade para o desenvolvimento.** Belo Horizonte: Fórum, 2018.

SIMÃO, Valdir Moysés. *Compliance* na administração pública direta: a perspectiva do cidadão. In: ZENKNER, Marcelo; CASTRO, Rodrigo Pironti Aguirre de (Coord.) ***Compliance*** **no setor público.** Belo Horizonte: Fórum, 2020.

STAFFEN, Márcio Ricardo; OLIVIERO, Maurizio. Transparência enquanto pretensão jurídica global. *A&C* – **Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 15, n. 61, jul./set. 2015. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=238032>. Acesso em: 22 nov. 2020.

TASSO, Fernando Antonio. Compartilhamento de dados entre o setor público e privado: possibilidades e limites. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 107-116, nov.. 2019. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=155162. Acesso em: 27 out. 2020.

TRAVIESO, Juan Antonio. Derecho Internacional de Los Derechos Humanos: clásico y futuro 3.0. In: ALDEGANI, Gustavo Roberto. **Régimen juíridico de los datos personales**. v. 1. 1. ed. Ciudad Autónoma de Buenos Aires: Abeledo Perrot, 2014.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em: warren-brandeis.pdf (cornell.edu). Acesso em 10 fev. 2021.

WILLEMAN, Marianna Montebello. ***Accountability* democrática e o desenho institucional dos Tribunais de Contas no Brasil.** 2. ed. Belo Horizonte: Fórum, 2020.

ZAMBAM, Neuro José. Bases informacionais transparentes: vitalidade da democracia e da justiça social. **Revista Novos Estudos Jurídicos.** v. 22, n. 2, 2017, p. 512-543.

ZIELINSKI, Dioleno Zella. **Controle social da administração pública:** A lei de acesso à infor-mação na perspectiva da dimensão da *accountability* societal. Dissertação (Mestrado em Di-reito). Programa de Pós-Graduação em Direito, Setor de Ciências Jurídicas, da Universidade Federal do Paraná. Curitiba, p. 130, 2015. Disponível em: https://sucupira.capes.gov.br/sucu-pira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?po-pup=true&id_trabalho=2367351. Acesso em: 13 set. 2020.

ZUBOFF, Shoshana. *Big Other*: capitalismo de vigilância e perspectivas para uma civilização de informação. BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta (et. al.). **Tecnopolíticas da vigilância:** perspectivas da margem. Tradução de Heloísa Cardoso Mourão. São Paulo: Boitempo, 2018.