DADOS PESSOAIS, PSICOPODER E RESPONSABILIZAÇÃO: ANÁLISE A PARTIR DA LEI BRASILEIRA DE PROTEÇÃO DE DADOS

PERSONAL DATA, PSYCHOPOWER AND ACCOUNTABILITY: ANALYSIS FROM THE BRAZILIAN DATA PROTECTION LAW

Salete Oro Boff;[1]

Dionis Janner Leal.[2]

Resumo: O desenvolvimento tecnológico, especialmente relacionado às tecnologias de informação e de comunicação – TICs –, permite e facilita a disponibilidade irrestrita e exponencial de dados pessoais (*Big Data*) e o acesso dos mesmos por organizações, com ou sem qualquer autorização de seus titulares. O acesso a dados pessoais, sem autorização, afronta o direito humano à privacidade, bem como permite exercer poder (vigilância/controle) sobre as pessoas em razão do tratamento dos dados por elas fornecidos, o que possibilita inclusive a intervenção em processos psicológicos da população. O tema despertou o interesse e o debate junto aos poderes instituídos e às legislações dos países que, gradativamente, vem regulamentando o uso e o tratamento de dados. O Brasil segue esta tendência e estabeleceu, em 2018, um diploma legal sobre a matéria (Lei nº 13.709/2018). O presente estudo desenvolve-se conceituando o direito à privacidade, na sequência apresenta regulamentação nacional acerca da proteção de dados pessoais e, por fim, a responsabilidade civil enquanto sanção e os meios de controle pelo uso indevido de informações de terceiros sem sua anuência, sob a ótica do Estado regulador. Verifica-se a dificuldade de conjugar a liberdade das pessoas no ambiente digital, com a proteção dos seus dados pessoais dispostos neste meio. Tem-se como encaminhamento viável a *accountability* na esfera privada corporativa e também em face do próprio governo. O método de pesquisa utilizado foi o dedutivo e a técnica de pesquisa bibliográfica.

Palavras-chave: Dados Pessoais. Estado Regulador. Privacidade. Psicopoder.

Abstract: Technological development, especially related to information and communication technologies - ICTs -, allows and facilitates the unrestricted and exponential availability of personal data (Big Data) and its access by organizations, with or without any authorization from their owners. Access to personal data, without authorization, violates the human right

[1] Professora permanente PPGD IMED. Pós-Doutora pela Universidade Federal de Santa Catarina (2008).

[2] Mestrando em Direito – PPGD – Faculdade Meridional. Especialista em Direito Público. Técnico Administrativo em Educação e Membro do Núcleo de Inovação e Transferência de Tecnologia, ambos no Instituto Federal de Educação, Ciência e Tecnologia Farroupilha. Mestrando em Direito e membro do Grupo de Estudos em Desenvolvimento, Inovação e Propriedade Intelectual-GEDIPI, ambos pela Faculdade Meridional de Passo Fundo - RS. Advogado.

Artigo recebido em 13/04/2020 e aprovado para publicação em 18/07/2021.

to privacy, and allows the exercise of power (surveillance / control) over people due to the processing of data provided by them, what makes it even possible to intervene in the psychological processes of the population. The topic aroused interest and debate together with the instituted powers and countries' the laws which, gradually, are regulating the use and treatment of data. Brazil follows this trend and established, in 2018, a legal diploma on the matter (Law No. 13,709/2018). The present study is developed by conceptualizing the right to privacy, then presenting national regulations regarding the protection of personal data and, finally, civil liability as a sanction and the means of control for the misuse of third party information without your consent, under the perspective of the regulatory state. There is a difficulty in combining people's freedom in the digital environment, with the protection of their personal data disposed in this medium. Accountability is a viable pathway in the private corporate sphere and also in the face of the government itself. The research method used was the deductive and the technique, bibliographical research.

Keywords: Privacy. Personal data. Regulatory state. Psychopower.

1 INTRODUÇÃO

O desenvolvimento das tecnologias de informação e de comunicação – TICs – criou um ambiente que permite e facilita a disponibilidade irrestrita e exponencial de dados de pessoas e organizações, sem qualquer autorização de seus titulares para livre utilização. A disponibilidade de dados é realizada quase que automaticamente pelos usuários, no intuito de ter acesso a "facilidades", sem quaisquer medos ou receios dos riscos e consequências dessa liberdade exposta ao mundo digital. O volume de dados pessoais disponibilizados no ambiente virtual possui potencial econômico e quem tem acesso e faz uso desses dados pode usufruir de benefícios privados e até estabelecer formas de indução e controles dissimulados.

Vários questionamentos surgem a partir dessa realidade, entre os quais: é possível proteger os dados pessoais disponíveis no ambiente virtual? que poder (vigilância/ controle/manipulação) a apropriação de dados pessoais pode gerar? quem poderá ser responsabilizado pelo uso ilegal dos dados pessoais?

Visando dar encaminhamento às questões postas, o presente estudo abordará inicialmente o conceito de privacidade e, sob a ótica econômica, a privacidade das informações na perspectiva de Posner. Na sequência, analisa-se a regulamentação nacional acerca da proteção de dados pessoais, o controle/influência do *Big Data* sobre as pessoas e o poder desses dados. Na terceira parte, expõe-se sobre a responsabilização enquanto sanção pelo uso indevido de informações de terceiros sem anuência, sob a ótica do Estado regulador. O estudo foi desenvolvido utilizando o método dedutivo e a técnica de pesquisa bibliográfica.

2 A PRIVACIDADE NO CONTEXTO DA PROTEÇÃO DE DADOS

Importante para o presente estudo o contexto histórico da privacidade, a fim de compreender a proteção de dados, que lhe é inerente, e verificar que não é de hoje que os dados pessoais são potencialmente violados.

É comum encontrar artigos ou trabalhos publicados acerca da privacidade ou proteção de dados com referência ao artigo *The Right to Privacy* (O Direito à Privacidade), de Warren e Brandeis (1890), o qual é o marco jurídico para o estudo privacidade frente à utilização de novas tecnologias (BOFF, 2018, p. 64). Entretanto, a expressão "privacidade" é mais remota do que a ofertada por Warren e Brandeis (1890) e chancelada por alguns estudiosos como marco jurídico – pode-se dizer que, em termos filosóficos, já foi idealizada por Aristóteles, o qual distinguiu a esfera pública e a esfera privada (doméstica), respectivamente denominadas *polis* e *oikos* (MALDONADO, 2019, p. 12). Para Saldaña (2012), parafraseado por Boff (2018, p. 66), o direito à privacidade garante proteção aos interesses imateriais (espirituais) da pessoa, ensejando o direito "individual de ser deixado em paz".

O ordenamento jurídico brasileiro positivou nas constituições acerca do direito à privacidade de seus cidadãos, quando inicialmente a tratou como tutela de inviolabilidade de domicílio e de correspondências e, hodiernamente, em razão da evolução da sociedade e das suas tecnologias, as conhecidas proteções seriam insuficientes para resguardar das novéis ingerências à vida íntima e privada dos cidadãos (MAURMO, 2017, p. 110).

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

Ainda sobre a proteção constitucional da privacidade, a abordagem de Fortes (2015) destaca o tema sob duas óticas 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).

Em atenção a essa peculiaridade brasileira, na República Argentina, o instituto do *habeas data* possui um alcance maior, abarcando organizações privadas, por expressa disposição do artigo 43 da Constituição da Nação Argentina, e que visam proteger os dados pessoais, cuja passagem merece transcrição:

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística. (ARGENTINA, 1994)

Para a doutrina argentina de Gozaíni, fazendo alusão à Lei nº 25.326/2000, que dispõe sobre a proteção de dados pessoais da Argentina, arrola os princípios dessa proteção e que o instituto do *habeas data* "otorga al individuo la posibilidad de concretar el cumplimiento de cualquiera de estos princípios" (GOZAÍNI, 2011, p. 106).

Todavia, no Brasil outros diplomas codificados como o Código Civil, Código de Processo Penal e o Código de Defesa do Consumidor versam nas suas esferas 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).

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).

Num contexto jurídico no qual a internet – e a sua utilização pelos usuários da rede – colaborou indiretamente para o aprimoramento das leis nacionais, a sociedade passa a conceber a privacidade na internet como direito fundamental amplo, abarcando "a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet" (FORTES, 2015, p. 188), contribuindo para um conceito transcendente da proteção constitucional à privacidade, para além da vida (dos

fatos) num contexto material, isto é, incluindo a mesma proteção à vida virtual, quando estivermos em nossa 'ágora digital'.

No cenário internacional, 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 de 1948, a Convenção 108 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 outro lado, Posner (2010, p. 274) traz uma explicação funcional (econômica) da informação privada das pessoas, uma vez que essa informação possa criar para outrem a oportunidade de tirar proveito – econômico ou não – quando da posse de informações alheias, estimulando a crescente intervenção na esfera privada e, consequentemente, o direito à ocultação de dados da vida pessoal pelo seu titular. Todavia, o autor adverte que, na sociedade moderna, não faz sentido afirmar que as pessoas têm o direto de não ser importunadas ou de ser deixado em paz, tendo em vista haver poucas pessoas que almejam a privacidade, pois preferem "manipular o mundo à sua volta, escolhendo quais informações revelarão sobre si mesmas" (POSNER, p. 275).

Pela análise econômica do direito, a privacidade das informações empresariais (ou da organização) deveria receber maior proteção que as informações na esfera privada das pessoas naturais, tendo em vista que, na esfera empresarial, o sigilo é importante por se apropriarem dos benefícios sociais que concebem, ao passo que, na vida privada (pessoal), a função do sigilo se resume à ocultação de informações pejorativas ou de demérito (POSNER, 2010, p. 293). Todavia, o próprio autor ao citar Greenawalt e Noam (1979), por entenderem de modo contrário a ele, pautam-se na ideia de que para o indivíduo (pessoa natural) a privacidade é um direito – à ocultação de informações, começar de novo (recomeço; nova chance) –, enquanto para as organizações são meros instrumentos utilitários.

Saindo da análise econômica do direito de Richard Posner, sem descurar o aspecto econômico das informações, importante trazer por outra ótica os contornos que a noção de

privacidade aflora, que é inerente à ideia de não intervenção de terceiros – como o Estado –, a exemplo do estado de vigilância permanente, o biopoder e a psicopolítica.

2.1 A PRIVACIDADE NO SÉCULO XXI: O CONTROLE DE DADOS E PODER

Para toda e qualquer manipulação – coerção ou intervenção, direta ou indireta – na vida das pessoas, existe um poder que emana sobre ele. Nesse sentido, para Foucault, o poder sobre a população dá-se por meio do que ele chama de 'técnicas ou tecnologias de poder' que, nos séculos XVII e XVIII, eram centrados no corpo individual das pessoas, o que denominava 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. E, já no início do século XIX, no que concerne à velhice, capacidades dos indivíduos, concebendo instituições estatais de assistência e outros mecanismos de cunho privado como seguridade e poupança financeira (FOUCAULT, 2010, p. 205).

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 – se limita a fatores externos, não adentrando na mente do homem, na psique da população. Todavia, há uma nova tecnologia do poder 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).

Assim, vivendo em estado de vigilância permanente, verifica-se que "a economia movida a dados e o capitalismo de vigilância são as duas faces da mesma moeda pois, quanto

maior a importância dos dados, maior será a coleta de dados". Diferentemente da coleta de dados relacionada por Warren e Brandeis, o *Big Data* e o *Big Analytics* trouxeram eficiência na obtenção, coleta, registro e acesso a dados alheios, na forma de mais "veracidade, velocidade, variedade e volume" – os chamados 4 V do *Big Data*. (FRAZÃO, 2019, p. 28.). É a era da vigilância ativa, do controle, o que pode ser chamado de psicopolítica digital, onde 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).

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. (HAN, 2014, p. 42).

Desse modo, a biopollítica "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 (e não econômicos, conforme Posner), agora acelerada e potencializada pelo auxílio das 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).

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS E A PSICOPOLÍTICA

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é o marco regulador do tratamento de informações pessoais. O art. 1° da Lei apresenta o objeto da proteção de direitos tidos como fundamentais (liberdade, privacidade e o livre desenvolvimento da personalidade) inerentes à pessoa natural, o que rechaça, de imediato, a ideia de proteção de dados da pessoa jurídica, documentos sigilosos, segredos de negócios, que dizem respeito a leis esparsas – como direito de propriedade intelectual e direito civil – contrariando o defendido por 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).

O legislador estabeleceu, como exceção, a não proteção de dados pessoais quando se trata, de questões relacionadas ao Estado (segurança pública, repressão e investigações de infrações penais) e quando tratado por pessoa natural para fins particulares e não econômicos (art. 4°, inciso I, da LGPD). Dessa regra pode-se extrair uma concepção econômica do direito emanado por Posner (2010) nesse dispositivo legal. O autor defende que numa relação real ou potencial, de negócios ou pessoal, há sempre uma oportunidade de tirar proveito (econômico ou não) quando da posse de informações de terceiros (POSNER, 2010, p. 274), que poderá ser utilizada (tratada) da forma que melhor lhe aprouver o detentor daquela informação em detrimento do seu titular, tendo em vista haver uma relação social entre pessoas naturais que, para o Estado, não lhe interessa proteger ou em razão do custo de sua proteção é maior que a informação ou dado a ser tratado.

Inserindo a teoria de Posner (2010) na exceção de proteção de dados pessoais ditada pela LGPD em comento, é dizer que esse direito fundamental, nas relações interpessoais e não econômicas, não vale o custo da proteção da informação. Dito de outro modo, "fazer valer o direito de propriedade sobre a informação implicaria, em muitos casos, custos desproporcionalmente elevados em relação ao valor da informação a ser protegida". Por exemplo, não compensaria proteger direito de propriedade intelectual sobre receitas de pratos ou atividades domésticas e outras tidas como comuns das pessoas, porque "os custos de investigação da origem de uma informação também inviabilizariam o recurso ao sistema de direitos de propriedade" e que "a violação dessas normas seria algo excessivamente abrangente e difícil de determinar" (POSNER, 2010, p. 288).

Assim, em consonância está o texto da lei brasileira ao silenciar no rol protetivo dos dados pessoais as relações entre pessoas naturais, uma vez que os valores sobre essas informações numa relação qualquer podem ser insignificantes – ou desinteressadas – e, por

outro lado, o custo da proteção para o aparato estatal ou das organizações privadas seriam superiores ao 'valor' arbitrado a tais dados pessoais. Para Posner, "quando a informação não é produto de investimento significativo, faz menos sentido defender sua proteção", como finalidade de proteção legal do sigilo (2010, p. 289).

Certamente, as informações pessoais de cunho não econômico mereceriam certa proteção, ou a sua violação deveria ser considerada fraude. Sobre a opção de não proteger, Posner argumenta que as pessoas, em geral, são racionais inclusive em comportamento não mercadológico (casamento, procriação, crime), e que, numa abordagem de "livre-mercado" – entre pessoas naturais – defendido pelo autor, "as pessoas devem ter liberdade para fazer suas próprias ponderações sobre os fatos desonrosos que os outros tentam esconder" e que de acordo com a análise econômica, a recusa em revelar determinado tipo de informação na seara privada deveria ser também considerada fraudulenta – considerada, pelo menos, anulável pelo direito (POSNER, 2010, p. 281).

Quando o Estado não garante proteção a dados pessoais nos casos exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais – que são inerentes a interesses "particulares" do Estado – valendo-se dessas informações para os fins que a lei lhe autoriza, parece que está a controlar as informações pessoais de seus cidadãos, as quais, *a priori*, passam desreguladas ou sem controle sobre si mesmo – sem *accountability* do Estado. O art. 40 da LGPD estabelece 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".

A competência instituída pela legislação brasileira à autoridade – ANPD - manter-se-á mesmo que o Poder Executivo opte por uma ou outra estrutura organizacional, apesar da estrutura organizacional original se manter como órgão hierarquicamente subordinado à Presidência da República. O art. 55-J da LGPD prevê as competências da ANPD.

Pelo exposto, a ANPD, *a priori*, terá caráter de instância de *compliance*, uma vez que instituirá diretrizes e procedimento para a conformidade da LGPD pelas pessoas jurídicas, de direito público e privado (III, VIII, XVIII), inclusive realizar ou determinar auditorias (XVI), além de deliberar acerca da interpretação da Lei. Em princípio, a centralização de várias atribuições pela ANPD fortalece o papel de uma instância de *compliance* de caráter

governamental ou *compliance* "externo", que é aquele que incumbido de "implantar as políticas de conformidade" (SCHRAMM, 2019, p. 170), porém com um viés não apenas fiscalizatório, mas também regulatório.[3]

Sob esse prisma, de que o poder público por intermédio de seu aparelho estatal – órgãos e entidades – possui a atribuição de fiscalizador e também de regulador, é que se tem presente a psicopolítica tratada por Han, considerando a ausência de *accountability* de *accountability*: ausência de controle sobre o controle – quem controla o Estado?

No contexto de uma sociedade de vigilância, o *Big Data* tudo vê, capturando todos os atos digitais dos usuários de tecnologias, utilizando-se dessas informações como poder para antecipar e decidir o futuro das pessoas e, nessa questão, não há devida transparência e *accountability*, tendo em vista que "os algoritmos utilizados por governos e grandes agentes empresariais são normalmente considerados segredos, respectivamente de Estado ou de negócios" (FRAZÃO, 2019, p. 38). Nesse sentido, "é urgente a necessidade de se introduzir mecanismos de transparência e *accountability* nas decisões algorítimicas", e é de saber, "entre o que não é conhecido, o que pode e deve ser conhecido, como pressuposto mínimo da proteção de direitos individuais e da própria democracia" e que "a transparência é pressuposto de inteligibilidade não apenas dos negócios, mas do próprio mundo" e que sem isso não será possível controlar os algoritmos. (FRAZÃO, 2019, p. 42-43).

Não se pode olvidar em esclarecer que a sociedade da transparência é uma sociedade da informação. Informações e comunicações demasiadas não ensejam transparência, ou seja, não lançam luz ao mundo, sendo que a massificação de informações não gera verdade, e quanto mais informações liberadas mais não transparente

[3] Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)
(...) III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; Incluído pela Lei nº 13.853, de 2019)
(...) VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)
(...) XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)
(...) XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

(intransparente) torna-se o mundo, logo, "a hiperinformação e a hiercomunicação não trazem luz à escuridão" (HAN, 2017, p. 95-96).

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). Conforme Frazão, "entre o que não é conhecido, o que pode e deve ser conhecido", vai de encontro com a proposta de transparência de Han, pois se tem algo que não é conhecido – não saber – há uma relação de confiança, e não de transparência. 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 as empresas e organizações privadas que detém os dados pessoais e para o Estado, enquanto controlador dessas informações e também detentor de dados pessoais (art. 7°, III, da Lei nº 13.709/2018), não há uma relação de confiança, pois eles já têm as informações. Desse modo, todos estão incluídos em "um único panóptico" (panóptico digital), 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).

2.3 A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, é o primeiro marco legal do Brasil que trata especificamente do modo como devem ser tratados os dados pessoais, inclusive os digitais, das pessoas física e jurídica, de personalidade jurídica de direito público ou privado, a fim de garantir proteção aos seus direitos fundamentais de liberdade e de privacidade. Apesar da Lei do Marco Civil da Internet já arrolar direitos alusivos à proteção de dados pessoais, ela foi alterada com o diploma legal, que visa dar efetividade a direitos

fundamentais inerentes aos dados das pessoas natural ou jurídica, abarcando os contornos e os efeitos da violação da privacidade e liberdades das pessoas no país.

A Lei do Marco Civil da Internet foi concebida como reação acerca da espionagem no Brasil. À época, havia um Projeto de Lei Azeredo (PL nº 2.160/2011), que tinha como ideia regulatória de legislação criminal para a internet, o que seria um retrocesso no ambiente regulatório. O projeto tornava crime condutas comuns dos cidadãos, o que engessava a pesquisa, a inovação e produção de novos serviços tecnológicos no país (LEMOS, 2014, p. 4).

Sob o prisma da responsabilidade civil, este diploma legal a fim de assegurar a liberdade de expressão e impedir a censura, estabeleceu em seu artigo 19 que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se não tomar providências oriundas de ordem judicial.

Ademais, como bem recordam Ruaro e Souza, a Lei 12.965/2014 é a primeira lei a nível infraconstitucional que regula a proteção de dados e prevê a responsabilização por danos em território brasileiro, mas não se aplica ou protege o usuário em território estrangeiro ou quando a lesão não ocorre na internet (RUARO; SOUZA, 2017, p. 211).

No outro lado do atlântico, a União Europeia já positivou seu novo marco de proteção de dados pessoais, aprovando em 2016 o Regulamento do Parlamento Europeu e do Conselho nº 2016/679 – em vigor a partir de 2018 –, revogando a Diretiva nº 95/46/CE (Regulamento Geral sobre a Proteção de Dados), levando em consideração o avanço das novas tecnologias da informação e comunicação, cujas questões não mais a diretiva regulava. O novo regulamento dispensa de legislação própria no Estado-Membro para a sua aplicação em âmbito nacional, bem como pode ter sua incidência implementada para além do território da União Europeia, bastando que a responsável tenha interesse econômico dentro da União Europeia, consoante disciplina o seu artigo 3º (RUARO; SOUZA, 2017, p. 206).

São importantes as alterações trazidas pelo novo regulamento europeu. As principais mudanças em relação à diretiva do final do século passado destacam-se: a inclusão de um único conjunto de regras de proteção de dados, com validade em todo o território da União Europeia; a maior responsabilidade e prestação de contas para o tratamento de dados pelas empresas; criação de uma autoridade que sujeite as organizações no país União Europeia onde estabelecida sua sede; garantia do cidadão de buscar a autoridade de proteção de dados no seu país, mesmo que seu dados sejam processados fora da UE; facilitação do cidadão de

acesso aos seus dados e possibilidade de sua transferência a outra organização (portabilidade); o direito ao esquecimento, com o fim de gerenciamento próprio de riscos de dados privados, sem olvidar de outras mudanças (ALVAREZ; TAVAREZ; 2017, p. 176).

Como visto, o novo diploma de proteção de dados europeu trouxe procedimentos simplificados para as organizações privadas, com vista a reforçar a proteção da privacidade do cidadão europeu (ALVAREZ; TAVAREZ; 2017, p. 176), o que o Brasil também está regulando a nível nacional.

Apesar de a iniciativa brasileira se inspirar em leis estrangeiras, como o regulamento da União Europeia, Regulamento (UE) nº 2016/679 do Parlamento Europeu, a legislação nacional exigiu que os dados, físicos ou digitais, sejam tratados pelo próprio poder público e pelas pessoas jurídicas de direito privado que tenham acesso, coletem ou utilizem essas informações de cunho pessoal, por motivos legais ou comerciais.

No âmbito das empresas privadas brasileiras, a lei inovou no ambiente cultural da organização para o tratamento de dados pessoais. A partir de agosto de 2020, todos aqueles que preenchem os requisitos legais deverão adotar mecanismos de controle, a fim de ensejar transparência nas relações que venham a utilizar as informações pessoais. Portanto, as pessoas jurídicas de direito público e privado necessitam adequar-se à lei, a fim de evitar as sanções nela previstas pela inadequada coleta, utilização ou armazenamento (tratamento) de informações de caráter pessoal dos clientes, colaboradores, empregados e quaisquer outros que tenham com ela alguma relação ou vínculo institucional, obrigacional, comercial ou legal.

O tratamento dado pela LGPD é diferente do que ocorre com o *compliance* anticorrupção disciplinado pela Lei n° 12.846/2013, onde os dirigentes ou administradores das pessoas jurídicas são responsáveis por atos ilícitos praticados pela empresa na medida de sua culpabilidade (Lei Anticorrupção, art. 3°, § 2°), ou seja, responsabilidade objetiva da empresa e subjetiva dos dirigentes, na LGPD a responsabilização recai sobre os agentes de tratamento de dados - operador e controlador - (LGPD, art. 42), o que descarta, *a priori*, a responsabilidade objetiva da empresa que coleta as informações pessoais de seus clientes ou colaboradores.

Por outro lado, a responsabilidade civil não se resume ao controlador e/ou operador, mesmo quando estes não forem empregados da empresa (LGPD, art. 5°, VI e VII) que realizam o tratamento das informações coletadas de seus usuários (clientes, colaboradores etc.), incluindo-se a responsabilidade da empresa em razão do seu funcionário que age em

desconformidade com o que determina a lei (LGPD, arts. 44 e 45). A responsabilidade da empresa que utiliza dados pessoais de consumidores, portanto, é objetiva e solidária e "qualquer fornecedor que estiver de posse de cadastros e dados pessoais de consumidores, sem suas expressas anuências, e utilizá-los para fazer oferta de produtos e serviços, deve responder e reparar pelos danos causados (...)" (NASSER FERREIRA, 2019).

Para otimizar e identificar melhor a responsabilização de cada agente da empresa responsável pelo tratamento de dados, sejam os agentes de tratamento ou funcionário encarregado, a gestão de riscos é uma medida de segurança a ser adotada. A implementação de um programa de conformidade digital ou *compliance* digital é uma medida para que se distribuam as responsabilidades, os papéis de cada encargo e dê efetividade aos ditames da nova lei no âmbito de cada organização.

Na legislação de proteção de dados brasileira está inserido o *accountability*[4], que é a prestação de contas atribuída também às organizações privadas no trato de dados pessoais pelos agentes responsáveis "adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais" (LGPD, art. 6°, X). Mesmo sem se enquadrar como agentes públicos, os operadores e controladores, no âmbito das organizações privadas, têm o dever de prestar contas à ANPD, conforme for disciplinado em suas diretrizes (LGPD, art. 55-J, III e XIV). Nasce, pois, o *compliance* empresarial em proteção de dados no âmbito nacional a partir do momento em que a ANPD estiver estruturada, as organizações públicas e privadas deverão a ela prestar contas (LGPD, art. 5° XIX c/c art. 10, § 3°e art. 27). Ao que parece não há um controle do próprio Estado, apesar de a ANPD enquanto poder público. O conceito de *accountability* "implica que os atores a serem controlados têm obrigações de agir de maneira consentânea com os *standards* aceitos de comportamento e que eles serão punidos pelo não cumprimento". (MAIOLINO, 2018).

De acordo com Amartya Sem, na Índia a legislação de acesso à informação impõe o dever de prestar contas à sociedade dos agentes públicos, uma vez que disponibiliza a qualquer cidadão não somente acesso a documentos, mas sim a pedidos de esclarecimento e

[4] A expressão *accountability* privilegia ideias de controle, responsabilidade e sanção, inerente à temática de prestação de contas (apesar de não haver uma tradução exata para o português do termo anglo-saxão). (CABRAL; CABRAL, 2018)

informações a respeito dos atos e procedimentos a serem executado pelo Poder Público (2015, p. 163).

No Brasil não é diferente, pois o acesso à informação, instituída pela Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), estabelece que qualquer cidadão (art. 10) poderá solicitar informações, documentos e direito de resposta a atos do governo (art. 7°), inclusive sobre processos, atos de gestão e o seu não atendimento pelos agentes públicos ensejam responsabilização administrativa e, *quiçá*, no crime de improbidade administrativa (art. 32, § 2°). Para Sen, a LAI tem como escopo combater a corrupção e promover a *accountability* (2015, 164) e o governo federal brasileiro deu um passo a mais, promulgando regulamento de governança pública visando incorporar a política de controle e responsabilidades em sua própria gestão pública.

No que tange à responsabilização prevista na LGPD nacional, o seu artigo 31 expressa que "a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação", quando identificar infração à lei, sem prejuízo do seu poder sancionatório aos órgãos jurisdicionados. Todavia, tal previsão serve mais para cientificar o responsável pelo órgão infrator na proteção de dados e levar em consideração no momento da tomada de decisão acerca da dosimetria da pena administrativa a ser imposta (TASSO, 2019, p. 288).

As sanções a serem impostas em razão da responsabilização daquele que deu causa à violação da lei estão arroladas no art. 52, prevendo a cumulatividade com outras sanções administrativas, civis e penais existentes em leis específicas. Quanto à responsabilidade de órgãos públicos, a autoridade nacional não pode enviar o mesmo informe previsto no artigo 31 a organizações privadas, pois esse dispositivo diz respeito à figura do autocontrole administrativo (TASSO, 2019, p. 288).

Quanto à responsabilização em nível internacional de dados pessoais, a legislação brasileira não é aplicável quando o tratamento de dados pessoais sejam provenientes de fora do território nacional ou de uso compartilhado de dados com agentes de tratamento brasileiros ou, ainda, objeto de transferência internacional de dados com outro país que não o de proveniência, condicionado que o país de proveniência proporcione grau de proteção de dados pessoais adequado à legislação brasileira (art. 4, IV, Lei nº 13.709/2018).

3 CONCLUSÃO

O novo diploma legal brasileiro acerca da proteção de dados pessoais trouxe inovações legislativas para o ordenamento jurídico e uma nova cultura no ambiente corporativo, seja ele público ou privado, a fim de dar tratamento adequado às informações pessoais coletadas dos usuários de seus serviços, além de normatizar a ideia de que os dados são privados e seus titulares podem fazer o que melhor lhes aprouver, contendo a usurpação por corporações empresariais, que se valem e apossam-se de direitos alheios, inclusive comercializando dados de terceiros.

A par disso, sob a ótica da economia do direito e do poder (biopoder/biopolítica e psicopoder/psicopolítica), a lei trouxe ao mesmo tempo a confirmação de que o Estado deve zelar pelas transações econômicas das informações privadas das pessoas naturais enquanto direito fundamental – inerente à pessoa como titular exclusivo de seus dados – e garantir que esses dados não sejam utilizados como manobra de massa ou indevidamente como forma de manipulação pelo poder (sobre as pessoas, seus comportamentos e pensamentos) – agora nas mãos também de organizações privadas – visando um controle e tratamento sobre essas informações. Criou-se uma colaboração mútua entre a ANPD e os agentes de tratamento de dados, que é uma 'corregulação' entre o público e privado a fim de somar esforços na construção de um tratamento de dados condizente com os direitos a que estão nele inclusos, como o da privacidade e inviolabilidade da liberdade de cada cidadão.

Todavia, ao mesmo tempo que ao Estado interessa regular o tratamento de dados pessoais ele cria um poder (psicopoder) sobre as pessoas – também compartilhado com a iniciativa privada –, mas não há de forma clara e direta – inclusive na própria lei – um mecanismo de controle pelos titulares desses dados em face do próprio Estado, como 'um controle sobre o controlador' (*accountability* sobre *accountability*).

Há, contudo, um encorajamento pelo Estado da criação de boas práticas de governança na seara pública e privada quanto a tratamento de dados e informações de cunho privado, o que de certa forma ensejará custos operacionais e de investimento para sua manutenção não previstos hodiernamente na iniciativa privada, assim como nos órgãos públicos com a capacitação de agentes para as novas atividades. Não há, todavia, proteção de direitos fundamentais como o da privacidade sem ônus para o Estado e, nesse caso, compartilhado com a iniciativa privada.

O *compliance* de dados é um novo procedimento criado pela LGPD a ser implementado em cada organização empresarial, agindo o Estado de modo indireto na

organização interna de cada empresa, incumbindo-lhe de responsabilidades com o trato de informações privadas a que até então eram comumente utilizadas sem respeito merecido aos direitos intrinsecamente envolvidos.

Em que pese haver uma governança pública sobre a própria Administração Pública – como o é o *compliance* na seara privada –, sente-se a ausência de um controle sobre a autoridade nacional (ANPD) pelos próprios titulares ou por meios de mecanismos ou instrumentos diretos como o *accountability*, o qual aparece como essencial e forma de garantir a transparência, uma vez que o Poder enseja transparência, mas não o contrário.

Logo, urge encontrar soluções, enquanto titulares de dados pessoais, de como implementar um *accountability* em face do poder público, em especial à ANPD, para garantir transparência, controle e responsabilidade do poder público sobre o tratamento de dados pessoais para evitar a invasão da esfera privada de seus cidadãos.

De todo o exposto, considerando a disponibilidade de dados pessoais sem controle ou conhecimento no *Big Data*, combinado com o interesse econômico das corporações privadas dos dados pessoais e a potencialidade de manipulação dos mesmos (inclusive dos dados dos titulares), ainda levando em conta o interesse do Estado de regular esse tratamento sem autocontrole e medindo forças com as organizações privadas para ter o poder de controlar essas informações, pode-se constatar que é tarefa árdua conjugar a liberdade das pessoas no ambiente digital. Aparentemente o encaminhamento viável parece levar a *accountability* na esfera privada corporativa e também em face do próprio governo.

REFERÊNCIAS

ALVAREZ, Bruna Acosta; TAVAREZ, Letícia Antunes. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA, Marcus Vinicius Kiyoshi; FILIPPO, Thiago Baldani Gomes de. *Brasil e EUA: temas de direito comparado.* São Paulo: Escola Paulista da Magistratura, 2017. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=94288. Acesso em: 04 fev 2020.

ARGENTINA. *Constitucion de la Nación Argen*tina. Disponível em: http://pdba.georgetown.edu/Parties/Argentina/Leyes/constitucion.pdf. Acesso em: 04 fev 2020.

BOFF, Salete Oro; FORTES, Vinícius Borges. Internet e proteção de dados pessoais: uma análise das normas jurídicas brasileiras a partir das repercussões do caso nsa vs. Edward

Snowden. *Cadernos do Programa de Pós-Graduação em Direito* - PPGDIR/UFRGS, v. 11, p. 340-370, 2016.

_____. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Sequência* (UFSC), v. 1, p. 109-127, 2014.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, C.P.A. *Proteção de Dados e Privacidade* - do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumem Juris, v. 1. 251p. 2018.

BORGES DA SILVA, Fabiani Oliveira. A responsabilidade do *compliance* officer na proteção de dados pessoais. *Revista de Direito e as Novas Tecnologias*, São Paulo, vol. 3, Abr-Jun 2019. Online. Acesso em: 24 nov. 2019.

BRASIL. Lei 13.709/2018. *Lei Geral de Proteção de Dados Pessoais* (LGPD).

_____. *Lei 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.

_____. *Lei 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.*

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.

FORTES, Vinícius Borges; BOFF, Salete Oro. An analysis of cybercrimes from a global perspective on penal law. *Revista Brasileira de Direito IMED*, v. 13, p. 7-24, 2017.

FORTES, Vinícius Borges; BOFF, Salete Oro; AYUDA, Fernando Galindo. The Fundamental Right to Privacy in Brazil And The Internet Privacy Rights in Regulating Personal Data Protection. *Revista Eletrônica do Curso de Direito da UFSM*, v. 11, p. 24, 2016.

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

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – noções introdutórias para a compreensão da importância da lei geral de proteção de dados. 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.

GOZAÍNI, Osvaldo Alfredo. *Derecho procesal constitucional*. Hábeas Data. Proteción de datos personales: doctrina y jurisprudencia. 2. ed. Santa Fé: Rubinzal-Culzoni, 2011.

HAN, Byung-Chul. *No enxame*: perspectivas do digital. Petrópolis, RJ: Vozes, 2018.

_____. *Psicopolítica*. Barcelona, ES: Herder Editorial S.L., 2014.

_____. *Estado de transparência*. Petrópolis, RJ: Vozes, 2017.

LEMOS, R. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, G.; LEMOS, R. (Eds.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.

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

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGDP – Lei Geral de Proteção de Dados Pessoais*: manual de implementação. São Paulo: Revista dos Tribunais, 2019.

MAURMO, Júlia Gomes Pereira. A tutela da privacidade nas constituições brasileiras. *Revista de Direito Constitucional e Internacional.* 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.

NASSER FERREIRA, Jussara Suzi Assis Borges. Fornecimento eletrônico de dados pessoais pelos consumidores: responsabilidade civil objetiva e solidária e o dano social. *Revista de Direito do Consumidor*, São Paulo, vol. 122/2019, p. 233-263, Mar-Abr 2019. Acesso em: 24 nov. 2019.

RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público* – IP, Belo Horizonte, ano 19, n. 103, p. 197-216, maio/jun. 2017. Disponível em: http://bidforum.com.br/bidBiblioteca_periodico_pdf.aspx?i=247799&p=16. Acesso em: 04 fev. 2020.

SEN, Amartya; DRÈZE, Jean. *Glória incerta*: a Índia e suas contradições. São Paulo: Companhia das Letras, 2015.

TASSO, Fernando Antonio. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Lei Geral de Proteção de Dados Comentada*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

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 EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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:32016R0679 Acesso em: 24 nov. 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 23 nov. 2019.

ZIELINSKI, Dioleno Zella. *Controle social da administração pública*: A lei de acesso à informação na perspectiva da dimensão da *accountability societal*. Dissertação (Mestrado em Direito). 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/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=2367351. Acesso em: 24 nov. 2019.