Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais

The accounting courts in the exercise of external control according to the new General Law on Personal Data Protection

Moises Maciel[1]

RESUMO

O exercício das funções que competem aos tribunais de contas exige acesso a informações para a fiscalização orçamentária dos demais órgãos públicos, em busca de controlar e combater atos de corrupção, protegendo os direitos e interesses da coletividade. Com a publicação da nova Lei de Proteção de Dados Pessoais, questionou-se a sua aplicabilidade às cortes de contas e se estas se encontravam, ou não, ao alcance da nova lei. Este estudo busca analisar o texto legal, a fim de verificar seu impacto nas funções atribuídas pela Constituição da República aos tribunais de contas no exercício do controle externo, de maneira a proteger o direito à privacidade do indivíduo sem comprometer o interesse público que, todos sabemos, deve ser priorizado diante de um conflito.

Palavras-chave: Controle. Fiscalização. Interesse Público. Proteção de Dados. Tribunais de Contas.

ABSTRACT

Court of accounts activities require access to information for the budget regulation of other public agencies in order to control and combat corruption, protecting the rights and interests of the community. With the publication of the Personal Data Protection Law', its applicability to audit courts was criticized with regard to whether or not these courts were within the scope of the new law. This study sought to analyze the new law document in order to verify its impact on the functions

1 Mestre e doutorando em Função Social do Direito pela Faculdade Autônoma de Direito (Fadisp). Exerce o cargo vitalício de Conselheiro Substituto do Tribunal de Contas do Estado de Mato Grosso (TCE/MT), mediante aprovação em concurso público de provas e títulos realizado em 2011, e atualmente também atua no Tribunal Pleno como Conselheiro Interino. É instrutor e palestrante da Escola Superior de Contas do TCE/MT. E-mail: mmaciel@tce.mt.gov.br

assigned by the Brazilian Constitution onto the courts of accounts in the exercise of External Control for the protection of the individual's right to privacy, without compromising the public interest, which must be prioritized during times of conflict.

Keywords: Courts of Accounts. Control. Data Protection. Inspection. Public Interest.

Recebido: 20-11-2019
Aprovado: 11-12-2019

1 INTRODUÇÃO

No exercício do controle e da fiscalização, a Administração Pública depara muitas vezes com um embate: o sigilo dos dados e a proteção à privacidade, prevista em nosso ordenamento jurídico. Como observar o direito fundamental ao bom governo, garantindo um direito da coletividade, sem ferir direitos individuais à privacidade? Como aproveitar os avanços tecnológicos e resguardar a segurança jurídico-social? Quais os limites legais para a tecnologia? Há limites legais? Muito se debateu para resolver o impasse entre o interesse público, a segurança jurídica e a proteção aos direitos fundamentais à privacidade. O exercício do poder de polícia e o direito da personalidade. O direito público e o direito privado.

De um lado, a evolução do tratamento e do armazenamento de dados, bem como a problemática atual decorrente disso (como o caso do vazamento de dados para fins políticos, do Facebook para a Cambridge Analytica, expondo cerca de 50 milhões de usuários, ocorrido em março de 2018), acirrou ainda mais as discussões acerca da necessidade premente de maior proteção desses dados, em face da inevitabilidade do crescimento e da evolução da era digital. Era preciso regulamentar, de maneira específica e eficiente, o uso desses dados, posto que se trata de um caminho sem volta e que cresce a passos rápidos, necessitando de limites e fronteiras bem definidos a fim de impedir abusos e invasões da tão sonhada (e paradoxalmente tão exposta) vida privada. Afinal, todos temos a garantia da privacidade como um direito inerente à personalidade humana. Direito, este, constitucionalmente previsto e consolidado.

Lado outro, por vezes a Administração Pública, no exercício do seu múnus

fiscalizatório, necessita ter acesso a dados pessoais, a fim de garantir a aplicabilidade correta e eficaz da legislação, evitando fraudes, corrupção, potencializando a arrecadação, aprimorando a qualidade dos gastos e despesas públicas e alçando melhores resultados no exercício de suas funções como gestor do interesse público.

A questão que insurge, neste momento, é: como conciliar a necessidade e a prioridade do interesse público com a proteção legal à privacidade do indivíduo e à sua vida pessoal? Como fiscalizar e acessar esses dados pessoais, de modo a evitar ou driblar possíveis fraudes e abusos, sem atingir a vida privada dos cidadãos? Como agir para garantir a eficácia da lei sem infringir a própria lei? Como proteger a segurança jurídica pública sem invadir a intimidade privada?

Nesta esteira de raciocínio e buscando refletir sobre tais questionamentos sem, contudo, a pretensão de responder a todos, este estudo busca fazer uma análise da nova Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018 alterada em 8 de julho de 2019 pela Lei nº 13.853), a fim de verificar seu impacto na fiscalização dos agentes públicos (especificamente dos detentores do exercício do controle externo, ou seja, os tribunais de contas), traçando um breve comparativo com as legislações estrangeiras a respeito. Para tanto, fará uso da metodologia dedutiva, partindo da lei para analisá-la diante de questões individuais que possam se concretizar além de dados bibliográficos, textos de lei e análises de casos concretos.

2 A DEMOCRATIZAÇÃO DO SABER E O DIREITO HUMANO AO SABER: A LIBERDADE DE INFORMAÇÃO

As necessidades do ser humano, em constante evolução e transformação, somadas ao rápido progresso científico e ao fenômeno atual de desenvolvimento tecnológico, têm causado diversos ciclos de transformações, tanto na área social quanto na econômica e cultural, acarretando a premência de adequação não apenas na seara privada, como na pública.

A revolução tecnológica é uma realidade crescente, da qual não se vislumbra um retorno e se requer uma adaptação constante. Vivemos, de fato, a Era Digital e vislumbramos, no dia a dia, o que já fora afirmado por Eric Schmidt e Jared Cohen (2013). Os autores pontuam que até 2025 toda uma geração, hoje sem quaisquer condições de acesso à informação, saltará para a disponibilidade

de todo conhecimento existente, ao seu rápido e fácil alcance, bastando ter um dispositivo, literalmente, na palma de sua mão. Segundo esses executivos, "se o ritmo atual da inovação tecnológica for mantido, a maioria da população da Terra, estimada em oito bilhões de pessoas, estará on-line" (SCHMIDT; COHEN, 2013, p. 12-13). Isso já é um fato!

O acesso à informação (antes restrito aos *campi* universitários e bibliotecas) encontra-se totalmente democratizado. Todos que têm acesso à internet têm acesso ao saber. As informações chegam rapidamente. Livros são disponibilizados, artigos, opiniões, notícias. A chamada Era Digital se tornou real e, de fato, democratizou o direito humano do saber.

Se antigamente alguns podiam gozar do direito do saber e, consequentemente, do poder que ele produz, como já ensinava o filósofo Paul-Michel Foucault (2013), hoje esse saber encontra-se amplamente disponível e a questão não se restringe mais ao seu acesso, mas ao que fazer com esse acesso tão democrático. Se o saber produz poder, a pergunta é: sabemos administrar esse poder? Até que ponto o exercício desse poder de saber é legítimo? Isso porque, se é fato que a internet possibilita, hoje, que milhões e milhões de pessoas tenham acesso ao conhecimento, em igual proporção (talvez até maior), também é notório o potencial ofensivo do seu uso para fins inadequados e escusos.

Schmidt e Cohen (2013) afirmam com razão que a internet é uma das poucas criações do ser humano que ele mesmo não consegue, ainda, compreender completamente. Segundo os autores, criada inicialmente como um sistema de transmissão eletrônica de informação, a internet se transformou rapidamente em uma espécie de válvula de escape onipresente e multifacetada. Algo intangível e que está em constante transformação, tornando-se, a cada segundo, mais complexa. Não é difícil perceber as qualidades e as vantagens que essa descoberta trouxe, e ainda vem trazendo para os indivíduos e para toda a sociedade mundial; todavia, seu devastador potencial para o mal também tem sido testemunhado no cenário global. Aduzem ainda que, a cada minuto centenas de milhões de pessoas se conectam, consumindo uma soma de conteúdo digital que não é passível de ser mensurada e, o que é mais preocupante, em um universo digital que ainda não conseguiu ser limitado por leis terrestres.

O poder produzido pelo saber mencionado por Foucault (2013) se encontra potencializado diante das facilidades de seu acesso e de sua apreensão. Basta refletir a respeito da quantidade de *websites* visitados, por cada um de nós, a

cada dia. Da quantidade de e-mails compartilhados, de artigos e opiniões on-line acessados e que são capazes de influenciar milhares de pessoas, tanto para o certo quanto para o errado. A quantidade de relações construídas à distância (porque é fato que a internet diminuiu a distância entre as nações e vem universalizando os idiomas que, hoje, não consistem mais em barreiras de interações e trocas de experiências) sofreu um aumento considerável. A internet consiste, hoje, sem dúvidas, no maior espaço sem governo no mundo, e toda essa tecnologia colocou por terra quaisquer limites geográficos, da mesma forma que se deu com os limites de linguagem e de conhecimento. Nunca tantas pessoas, de diversos países e continentes, costumes, religiões e opiniões, tiveram acesso tão fácil a tanto poder!

A progressão das tecnologias de comunicação se deu de maneira vertiginosa e seu acesso só tende a crescer, conforme o passar do tempo e os avanços científicos.

Em artigo publicado na obra *Acesso à informação como direito fundamental e dever estatal*, Carlos Molinaro e Ingo Sarlet (2016) aduzem que, hoje, é nítida a concepção de que a questão da informação como objeto de regulação legal encontra-se disposta, especificamente, nos atos de informar, se informar e, ainda, ser informado, assumindo, neste aspecto, uma dimensão puramente individual e independente do direito da coletividade. Lado outro, contudo, o direito de acesso à informação, seja no âmbito privado ou coletivo, acaba por atrair, via de consequência, a proteção dos direitos da personalidade, de modo a buscar definir e traçar os limites necessários ao acesso e à difusão das informações obtidas com base no princípio da paridade de armas, não apenas entre cidadãos, como também entre cidadãos e o Estado, na busca por materializar o direito à autodeterminação e à informação de modo legal e eficaz.

Importa recordar que, hoje, quando nos conectamos a uma rede social, esta coleta nossos dados que, por sua vez, ficam armazenados em um banco de dados que vai se tornando mais robusto a cada nova informação ou acesso realizado, de maneira que, com o tempo, conterá não apenas nome, e-mail, cidade, profissão, mas também gostos, amizades e interesses. Dados que acabam por definir tendências de consumo, de políticas, comportamentais e religiosas e que podem ser utilizados por qualquer um, seja qual for a sua intenção.

Consoante o disposto em nossa Carta Magna, artigo 5º, §1º, as normas que definem direitos fundamentais são de aplicabilidade imediata, de modo que a ausência de uma previsão legal no que tange, por exemplo, à garantia de acesso

à informação, não impediria o Judiciário de assegurar tal direito. A par disso, porém, uma normatização infraconstitucional se fazia necessária a fim de assegurar um procedimento adequado no exercício desses direitos, bem como a observância das garantias legais. Como resultado, foi publicada em 18 de novembro de 2011 a Lei nº 12.527 (regulada pelo Decreto nº 7.724/2012), que se tornou conhecida como Lei de Acesso à Informação, trazendo a regulamentação de instrumentos que viabilizam a pessoas físicas e jurídicas acesso a informações públicas sem a necessidade de motivos previamente apresentados, determinando que toda informação, seja produzida, seja custodiada por órgãos públicos, pode ser disponibilizada ao cidadão, ressalvados casos excepcionais, legalmente previstos, de proteção ao sigilo, à intimidade e à privacidade das pessoas naturais ou ao sigilo protegido por outras leis, como o fiscal e o bancário. De acordo com a Lei de Acesso à Informação, a disponibilização desse sigilo pode se dar por via ativa (quando o Estado, de modo proativo, concede informações de interesse geral por meio de divulgação pública) ou passiva (quando o Estado responde, fornecendo informações solicitadas por pessoas físicas ou jurídicas).

É imperioso, contudo, observar os limites não apenas legais, mas éticos e morais do uso democrático do saber, exercendo o poder dele decorrente com sabedoria e respeito pelos direitos individuais, reconhecidos universalmente como direitos da pessoa humana. Os fins não podem justificar os meios, contudo, é mister encontrar o ponto de equilíbrio entre o direito ao saber, ao conhecimento e, consequentemente, ao exercício do poder e, ainda, à proteção da vida privada e da intimidade do indivíduo, expressamente protegidas pela Convenção Americana de Direitos Humanos em seu artigo 11 (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969), bem como na Constituição brasileira, art. 5º, X e XII (BRASIL, 1988).

3 A GARANTIA DE ACESSO A INFORMAÇÕES: DIREITO A BOA ADMINISTRAÇÃO PÚBLICA OU DIREITO FUNDAMENTAL AO BOM GOVERNO

Toda essa gama de transformações que estamos passando é necessária e inevitável e não pode passar despercebida, nem por nós nem pela Administração Pública, em especial nos tempos atuais em que se faz reconhecido o direito fundamental ao bom governo como um direito humano.

Compete à Administração Pública entregar à coletividade resultados de qualidade, necessários para garantir serviços e políticas públicas adequados, em observância aos seus direitos como cidadãos. Essa transformação digital pode ensejar diversas oportunidades para a oferta desses serviços, de maneira eficaz e com menos recursos. Para tanto, porém, necessita ser bem aproveitada e isso requer limites claros e objetivos, posto que é indubitável que a evolução tecnológica muito pode agregar, no tocante a eficiência e, ainda mais, no que concerne à agilidade na prestação dos serviços públicos. No entanto não é demais recordar que são as instituições estatais que trabalham para que a Administração Pública esteja a serviço da sociedade e não o inverso. Afora isso, ainda precisamos reconhecer os riscos decorrentes do uso de dados para vigilância em massa. Tal qual tem acontecido em diversos países, como a China, onde foi criado um programa para identificar as pessoas por meio do seu andar. Nesses casos, o fim originário de garantir a segurança pública tem sido questionado e, para muitos, ignorado, atingindo direitos pessoais dos particulares (A CHINA…, 2018). Sem falar do acesso e do compartilhamento de informações nitidamente pessoais, sem a devida e prévia autorização de seus titulares. O poder público não necessita sempre de autorização prévia para coletar dados pessoais dos seus usuários, no entanto se faz mister que tal coleta tenha a finalidade de utilização para o bem público, especificamente para serviços essenciais, de modo que o seu resultado venha a ser revertido em proveito de toda a sociedade, para a melhoria dos serviços públicos. Ao menos é o que se espera. É preciso observar os princípios da necessidade e da proporcionalidade.

Ilustramos o disposto anteriormente com um caso ocorrido no metrô, em São Paulo, em abril de 2018, em que a Concessionária Linha-4 Amarela instalou um mecanismo de reconhecimento facial nas portas, com o fim de registrar (via imagem e som) o fluxo de passageiros para melhorar a qualidade do transporte, mas que camuflava um interesse publicitário, registrando a reação dos passageiros a cada publicidade apresentada a fim de ofertá-las conforme os registros obtidos, para potencializar o lucro almejado. Ou seja, a finalidade passou a ser estritamente publicitária, razão pela qual, em agosto do mesmo ano, o Instituto Brasileiro de Defesa do Consumidor (Idec) propôs ação civil pública contra a concessionária, mediante a alegação de que a coleta dos dados pessoais, nas chamadas portas interativas digitais, era ilegal e violava direitos básicos dos consumidores à informação, posto que o consumidor não tinha qualquer opção de recusar tal coleta, demonstrando uma perspectiva de abuso evidente. E esclareceu que não

se tratava de uma tentativa de impedir o uso da tecnologia, mas de adequá-la de modo que seu uso não viesse a ferir os direitos básicos do cidadão e os princípios da Administração Pública, como o direito de consentimento e, ainda, o princípio da transparência (JUSTIÇA…, 2018).

O uso de dados pelo poder público é real e vivenciado em nosso dia a dia. Sensores que detectam o fluxo do tráfego, a umidade do ar, o índice de poluição, a temperatura e a pressão atmosférica, dentre outros, já são considerados normais e sequer são percebidos pela sociedade, uma vez que, como não são dados pessoais, não há necessidade prévia de autorização para o seu uso. A questão em comento, contudo, vai mais além e busca analisar o uso de dados pessoais pelo poder público, aqueles capazes de identificar um indivíduo. Em regra, os modelos normativos vigentes não fazem distinção com relação ao uso desses dados pelo poder público ou privado. Como exemplo, citamos o Regulamento Geral sobre a Proteção de Dados (General Personal Data Protection – GPDR), aplicável na Europa, e o Marco Civil da Internet (Lei nº 12.965, de 2014), aqui no Brasil.

Portanto insta uma gestão de dados eficiente para ser eficaz, condizente com os direitos da personalidade (inerente a toda pessoa, física ou jurídica), a fim de servir como instrumento de facilidade, tempestividade e, principalmente, qualidade no cumprimento das atribuições estatais. Neste caminho, como explana Byrnes (2015), o uso de técnicas aprimoradas na análise de dados e o *big data*, a auditoria contínua e a detecção de fraudes seriam apenas os passos iniciais para uma reengenharia completa dos processos de fiscalização.

Impende também salientar que a necessidade de observância do princípio da legalidade por parte do poder público pode, muitas vezes, servir como instrumento dificultador de sua adaptação às novas realidades tecnológicas e digitais. Contudo não se pode olvidar que, para lograr êxito no seu papel de gestor dos interesses públicos, a administração pública em geral necessita acompanhar tais evoluções, a fim de interagir adequadamente com a sociedade, observando e atendendo os seus anseios e necessidades. Não se trata de opção, mas de um verdadeiro dever do Estado, em respeito à cidadania, aos direitos individuais e, obviamente, aos direitos fundamentais.

Hoje, o denominado Governo Digital é, se não o único, reconhecidamente importante caminho, que pode direcionar a administração pública em sua busca por excelência e efetividade no que concerne aos serviços prestados à sociedade, trazendo benefícios concretos a todos.

A evolução tecnológica e o tratamento de dados servem como incremento, auxiliando a transparência das informações e o acesso geral à prestação de contas e serviços públicos, bem como do andamento de políticas públicas. Isto favorece o exercício do controle interno, externo e, ainda, do controle social que, se bem utilizado, poderá restar fortalecido, cooperando para um grande salto na luta contra fraude e corrupção no poder público o que, por sua vez, favorece toda a sociedade. Para tanto impende o exercício de cautela e é imprescindível, ainda, que a privacidade dos indivíduos seja seriamente considerada, e que o uso de dados pela administração pública respeite as finalidades específicas, peculiares à prestação do serviço que se busca.

Porém é sabido que a mesma propriedade que serve de remédio também serve de veneno, dependendo da dosagem. Motivo este pelo qual, apesar de reconhecermos a importância da evolução, do uso e do tratamento dos dados digitais no exercício da administração e da gestão pública, também frisamos a necessidade imperiosa de regras limitadoras de sua atuação, com sanções específicas e adequadas para dificultar o uso indiscriminado e abusivo desses dados, garantindo seu escopo de servir como instrumento facilitador e que vem agregar na busca pela entrega e observância do direito fundamental ao bom governo.

4 A NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018) E O SEU IMPACTO NO ÂMBITO DO CONTROLE EXTERNO E DA FISCALIZAÇÃO

Nesta senda, como já salientado, a mudança ocasionada pelos avanços tecnológicos é inevitável e seu crescimento exponencial é um fato, contudo é possível exercer alguma espécie de controle em seus desdobramentos. Como bem salientam Schmidt e Cohen (2013), aquela conversa de que as máquinas assumirão o comando deve ser esquecida. O homem é o responsável por essa evolução vertiginosa, portanto o que acontecerá no futuro (bem próximo) é de total responsabilidade nossa. E o que nos cabe fazer? Traçar os delineamentos legais para dificultar o uso abusivo desses meios, possibilitando seu exercício com a finalidade adequada, de maneira a servir de verdadeiro instrumento para o exercício legal da democracia com ética e total respeito aos direitos humanos.

Com tal intento, foi publicada recentemente no Brasil, mais especifica-

mente em 15 de agosto de 2018, a nova Lei Geral de Proteção de Dados Pessoais, nº 13.709, de 2018 (alterada pela Lei nº 13.853, de 8 de julho de 2019), que veio dispor sobre a proteção desses dados, alterando a Lei nº 12.965 de 2014 (conhecida como Marco Civil da Internet), representando um grande avanço no que concerne a essa temática. Seu escopo reside no estabelecimento de regras sobre como as empresas e o poder público tratam os dados pessoais, seja em sua coleta, em seu armazenamento, nas negociações etc., de maneira e fixar-lhes limites rígidos e precisos.

Trazendo normas que regulamentam o modo pelo qual são coletadas as informações, bem como o seu tratamento, além de dispor dos direitos de seus titulares, a nova lei possui aplicação multisetorial, posto ser aplicada tanto nos setores públicos quanto nos privados e, também, extraterritorial, tendo em vista que a sua eficácia poderá se dar além dos nossos limites geográficos, alcançando outras regiões. Seus fundamentos residem no respeito à privacidade, na liberdade de expressão e de informação, na inviolabilidade da intimidade, da honra e da imagem, no desenvolvimento econômico e tecnológico, na inovação, na livre iniciativa, na livre concorrência e na defesa do consumidor, nos direitos humanos, no livre desenvolvimento da personalidade, na dignidade, dentre outros.

No que concerne ao tratamento dos dados pessoais e à sua utilização pelo poder público, a Lei Geral de Proteção de Dados Pessoais possui um capítulo específico para tal regularização, conferindo à administração pública algumas peculiaridades como, por exemplo, a observância de requisitos específicos.

Como já explicitado, a administração pública não necessita de prévio consentimento para tratamento e compartilhamento dos dados pessoais quando estes forem necessários, por exemplo, para a execução de políticas públicas (desde que previamente previstas em lei ou baseadas em contratos ou convênios) e, ainda assim, nesses casos, o tratamento dos dados deve ser realizado com estrita observância à sua finalidade pública e, especialmente, para a persecução do interesse público, mediante informações claras e atualizadas concernentes à finalidade, os procedimentos e demais práticas a serem utilizadas, em veículos de fácil acesso a toda a sociedade. Além disso, conforme disposição legal, se faz mister indicar um encarregado (pessoa física ou jurídica) para figurar como uma espécie de canal de comunicação entre o controlador, os titulares dos dados utilizados e, ainda, a autoridade nacional, de modo que o encarregado fique responsável pela execução do tratamento dos dados, conforme as informações que lhe forem fornecidas pelo controlador.

Importa salientar que a lei em comento não se aplica aos tratamentos de dados pessoais que forem realizados com a exclusiva finalidade de garantir a segurança pública, a defesa nacional, a segurança do Estado, bem como em atividades de investigação ou repressão de infrações penais, casos em que o tratamento dos dados deverá ser regido por legislação específica, conforme disposto expressamente em seu artigo 4º.

Consoante o disposto no texto legal, o compartilhamento de dados deverá ser mantido em formato "interoperável"[2] e estruturado visando a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelos cidadãos.

Ainda no que concerne ao compartilhamento dos dados pelo poder público, a Medida Provisória nº 869/2018 prevê a possibilidade de compartilhamento entidades privadas, desde que previamente previsto em lei, em contratos específicos ou convênios, mediante a nomeação de um encarregado, e também quando tal compartilhamento tiver o intuito de prevenir fraudes e irregularidades ou, ainda, proteger e resguardar a segurança e a integridade do titular dos dados. No tocante ao compartilhamento internacional, o texto legal permite, exclusivamente, para países que proporcionem o mesmo grau de proteção nele previstos e regulamentados, possibilitando inclusive requerimento à autoridade nacional, solicitando avaliação do nível de proteção legal conferido ao tratamento dos dados pessoais, pelo país ou organismo internacional. Outrossim, permite a transferência internacional, quando necessária à cooperação jurídica entre órgãos públicos de inteligência, investigação e persecução, quando resultar de compromisso assumido em acordo de cooperação internacional e, ainda, quando for necessário para fins de execução de política pública.

A lei prevê a responsabilização solidária dos agentes de tratamento, do operador e do controlador nos casos por ela especificados e mediante requisitos preestabelecidos, possibilitando que a autoridade nacional encaminhe informativos determinando, às entidades e aos órgãos públicos, as medidas necessárias cabíveis para fazer cessar a violação ao direito de privacidade em decorrência do tratamento dos dados pessoais. Além disso, possibilita o requerimento para a publicação de relatórios referentes aos impactos desses tratamentos na proteção dos dados, sugerindo boas práticas para tanto.

2 No site Governo Digital, do Ministério da Economia, encontramos informações sobre o que se compreende por interoperabilidade, segundo o qual se refere à capacidade de comunicabilidade transparente entre os sistemas, sejam eles informatizados ou não. Ou seja, significa a possibilidade de dois ou mais sistemas (similares ou não) trabalharem conjuntamente, possibilitando a troca de informações (não dados) (PADRÕES…, 2019).

As sanções previstas consistem em advertência, publicização da infração, bloqueio ou eliminação dos dados (objeto da infração), sem qualquer prejuízo à aplicação das sanções previstas no Estatuto do Servidor Público Federal, na Lei de Improbidade Administrativa e na Lei de acesso à Informação, bem como em outras legislações congêneres compatíveis. E não podemos olvidar, ainda, o que tem sido considerado ponto mais relevante da nova lei: a criação da Autoridade Nacional de Proteção de Dados (ANPD), uma entidade pública autônoma e independente, com a responsabilidade de fiscalizar e aplicar as sanções necessárias em casos de violação comprovada. Vetada inicialmente pelo ex-presidente Michel Temer, a ANPD foi criada por meio de edição da Medida Provisória de nº 869, no final do exercício de 2018.

Importa ainda destacar que a LGPD trouxe, em seu bojo, a obrigatoriedade de observância dos princípios *Privacy by design e Privacy by default*, por meio dos quais deverão ser adotadas as medidas de segurança, técnicas e administrativas que sejam idôneas para a proteção dos dados pessoais, desde a concepção do produto ou serviço até a sua execução, traduzindo uma verdadeira garantia de segurança com relação ao tratamento dos dados pessoais dos cidadãos, contribuindo, ainda, para o aprimoramento dos serviços e das políticas públicas. Além disso, o texto legal determina também que no tratamento dos dados pessoais deverão ser observados os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e da prestação de contas.

O consentimento para o tratamento de dados é requisito essencial, previsto em lei, por escrito ou por outro meio que possa demonstrar, de forma inequívoca, a manifestação de vontade do titular, ressalvados os casos de dados manifestamente públicos.

A lei proíbe expressamente o compartilhamento de dados pessoais entre controladores com fins de obter vantagens econômicas e determina que o término do tratamento dos dados pessoais se dará quando se verificar que a sua finalidade foi alcançada; quando terminar o período de tratamento; por meio de comunicação do titular (inclusive pela revogação do consentimento anteriormente fornecido); e por determinação da autoridade nacional, se constatada violação de dispositivo legal. Neste caso, os dados devem ser eliminados, ressalvadas as exceções expressamente previstas em lei.

No que concerne ao tratamento de dados pessoais pelo poder público, a LGPD prevê que deverão ser observados a finalidade pública e o interesse públi-

co, e ter como objetivo o cumprimento das atribuições legais do serviço público. Para tanto, deverão informar de maneira clara, transparente e acessível as hipóteses em que se realiza o tratamento desses dados, bem como sua finalidade, os procedimentos adotados e as práticas utilizadas para tanto; ainda deverá indicar um encarregado quando forem realizadas as operações de tratamento e, a respeito da transferência de dados para entidades privadas constantes na base de dados do Poder Público, há expressa vedação legal, com a devida ressalva para os casos de execução descentralizada de atividade pública que exija transferência para fim específico e determinado com observância ao disposto na Lei de Acesso à Informação (Lei nº 12.527/2011) e, ainda, nos casos em que os dados foram acessíveis publicamente.

A nova lei também traz regras expressas sobre a transferência internacional de dados, elencando os casos em que ela é permitida, por exemplo, "quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23" (BRASIL, 2018, n.p.).

A doutrina é unânime em reconhecer o grande avanço na elaboração e publicação da referida lei, cuja *vacatio* encerrará em 14 de janeiro de 2020, passando a viger no dia seguinte. Insta, portanto, fomentar essa nova geração de prestação de serviços públicos eficientes, mas sem eliminar as garantias fundamentais, pertinentes à privacidade dos indivíduos que compõem o Estado.

Realizadas as considerações necessárias, a questão que insurge é: a Constituição Federal determina, em seu artigo 70, que a fiscalização contábil, financeira, orçamentária, operacional e patrimonial é dever estatal, devendo ser realizado pelos entes federativos e pelas entidades da administração direta e indireta, quanto à legalidade, economicidade, aplicação das subvenções e renúncias de receitas. Diante do disposto neste artigo, podemos afirmar que a nova Lei de Proteção de Dados Pessoais se aplica, ou não, aos tribunais de contas? Estão os tribunais, devido ao exercício típico fiscalizatório e sancionatório, fora do alcance da lei?

Com a devida vênia aos posicionamentos diversos, entendemos que a lei se aplica a toda e qualquer pessoa, física ou jurídica, de direito privado ou público, posto ter como objetivo principal proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto em seu bojo (BRASIL, 2018). Esse é o fim e obviamente que, tal como acontece com os princípios, em geral eles deverão ser sopesados quando

de sua aplicabilidade de maneira que no exercício da sua função fiscalizatória e, consequentemente, sancionatória, as cortes de contas contarão com a ressalva expressa no art. 4º da própria legislação em comento, em seu inciso III:

> Art. 4º – Esta lei não se aplica ao tratamento de dados pessoais:
> (…)
> III – realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais (BRASIL, 2018).

Para que a atividade fiscalizatória da administração pública se dê de maneira eficaz, com qualidade e eficiência, são necessárias certas medidas, tais como o acesso desses órgãos de controle às informações de outros órgãos públicos por eles fiscalizados. As atividades desses órgãos de controle têm por objeto, na maioria das vezes, documentos e informações prestadas por outros órgãos e entidades, a fim de que eles possam observar as competências dispostas no artigo 71 da Constituição da República brasileira, de maneira que o compartilhamento dessas informações é de suma importância para assegurar interesses da coletividade.

A atividade fiscalizatória, típica dos tribunais de contas, no entanto, não o exclui das determinações constantes na LGPD, devendo resguardar os cuidados nela previstos com relação aos dados pessoais (constantes em seus bancos de dados). Necessário se faz ressaltar que, no exercício de sua missão institucional, os tribunais de contas possuem o poder e o dever de acessar todo e qualquer dado pertinente à execução orçamentária, ou seja, receitas ou despesas, independentemente de serem dados públicos ou privados. Qualquer medida contrária ensejaria um verdadeiro óbice às informações que essas cortes precisam para realizar com eficiência suas funções, prejudicando a sociedade inteira. Por esse motivo, é pacífico o entendimento de que aos órgãos de controle não se aplica o sigilo tributário, isso seria incongruência.

Em artigo escrito anteriormente para o III Congresso Hispano-Brasileiro de Direitos Humanos, explicitamos que o STF estabeleceu no Recurso Extraordinário nº 601.314/SP, com repercussão geral reconhecida, que o direito ao sigilo fiscal não se trata de um direito absoluto e que, apesar de gozar de proteção cons-

titucional especial, pode ser ponderado à luz do princípio da razoabilidade, diante de um aparente conflito de normas (BRASIL, 2016).

Isso não nos autoriza a concluir que as cortes de contas estão liberadas do dever de proteção dessas informações sigilosas; pelo contrário, cabe a elas o dever de guardar e proteger os dados pessoais; dever este que decorre de sua função de auditoria, cuja competência encontra-se disposta na Constituição da República. Esse sigilo, por sua vez, se estende a todos os que atuam em tais órgãos (membros, assessores, auditores e demais servidores) e manuseiam, de alguma forma, tais informações.

A par disso, porém, é pacífico que os sigilos bancário e fiscal não restringem a tais poderes. Neste sentido, Jorge Ulisses Jacoby Fernandes (2018, n.p.) diz:

> Não podemos vislumbrar controle sem acesso a tais informações, seja porque é possível resguardar a privacidade em uma investigação de controle, seja porque não se concebe controle de contas considerando-se apenas a despesa, sem se permitir o exame da receita, inclusive tributária.

Com base em tais afirmações, o autor salienta que dentre as limitações constitucionais estabelecidas às ações das cortes de contas, não se encontra qualquer menção ao sigilo fiscal e/ou bancário, tendo em vista não serem condizentes com a função dessas cortes. E o Tribunal de Contas da União (2018), inclusive, manifestou-se novamente no sentido de que o sigilo bancário constante da Lei Complementar nº 105 de 2001 não se aplica a informações que se refiram a contas específicas, abertas para movimentação de recursos descentralizados pela União, ou seja, não cabem quaisquer alegações de proteção ao sigilo bancário com intento de afastar o dever de prestar informações requeridas pelos tribunais de contas. Qualquer posicionamento contrário prejudicaria o exercício da fiscalização dessas cortes, favorecendo fraudes, abusos e corrupção.

Corroborando tal posicionamento, dentre as Normas de Auditoria Governamental (NAG) que abarcam diretrizes fundamentais para o cumprimento das auditorias contábeis, operacionais e de cumprimento, encontramos a NAG 3000, relativas aos profissionais de auditoria governamental. Especificamente:

> 3500 – Sigilo Profissional A informação obtida pelos profissionais de auditoria governamental na execução de seus trabalhos não deverá ser revelada a terceiros, nem oralmente nem por es-

> crito, salvo aos responsáveis pelo cumprimento de determinações legais, ou às EFs como parte dos procedimentos normais, ou em conformidade com a legislação pertinente.
> 3501 – O profissional de auditoria governamental deve manter, respeitar e assegurar o sigilo relativo às informações obtidas durante o seu trabalho, não divulgando, sob qualquer circunstância, para terceiros, sem autorização expressa do ente auditado, salvo quando houver obrigação legal ou judicial de fazê-lo. O dever de manter sigilo continua depois de terminados os trabalhos.
> 3502 – O sigilo profissional é regra mandatória no exercício da auditoria governamental. O profissional de auditoria governamental é obrigado a utilizar os dados e as informações do seu conhecimento exclusivamente na execução dos serviços que lhe foram confiados, salvo determinação legal ou judicial (BRASIL, 2011).

Por fim, em 26 de agosto de 2019, foi publicada a Lei nº 13.866 (com entrada em vigor no mesmo dia), com a finalidade de alterar a Lei nº 8.443, de 16 de julho de 1992 (Lei Orgânica do Tribunal de Contas da União), determinando expressamente (a fim de não deixar quaisquer dúvidas a respeito) que o art. 55 da Lei nº 8.443/1992 passe a vigorar acrescido do seguinte § 3º: "Ao decidir, caberá ao Tribunal manter o sigilo do objeto e da autoria da denúncia quando imprescindível à segurança da sociedade e do Estado" (BRASIL, 2019b, n.p.).

A nova Lei Geral de Proteção de Dados Pessoais veio proteger os direitos do indivíduo diante desse crescimento desenfreado dos relacionamentos digitais e do mundo virtual. Não possui, contudo, o condão de prejudicar ou obstaculizar a atuação fiscalizatória das cortes de contas no exercício do controle externo, mas apenas possibilitar e favorecer um controle límpido, ético, legítimo, focado em seus objetivos, sem, contudo, desrespeitar os interesses privados, assegurando o interesse de toda a coletividade que se sentirá segura e devidamente amparada. Ademais, é entendimento pacificado e consolidado que quando em conflito, o princípio da supremacia do interesse público acaba por limitar os efeitos do princípio da privacidade, já que o interesse coletivo deve estar acima dos interesses puramente privados.

Restará a todo o Estado e também a suas cortes de contas se adequar ao conteúdo da nova lei, investindo em questões de segurança digital e em treinamento e capacitação de pessoal, ciente de que o texto legislativo veio contribuir e

não prejudicar as atividades estatais, bem como o exercício da função fiscalizadora e sancionadora dos tribunais de contas.

5 A PROTEÇÃO DOS DADOS PESSOAIS E A FISCALIZAÇÃO NO MUNDO: DIREITO COMPARADO

Toda essa revolução tecnológica tem gerado e propagado, mundo afora, complexos desafios legais. Dia após dia novos negócios são estabelecidos como fruto do intenso uso do Big data. A inteligência artificial vem sendo um dos campos de maior disputa por hegemonia internacional, tendo os Estados Unidos como principal força desenvolvedora, mas que conta, atualmente, com o crescimento e a importância de outros atores. O principal desses atores é a China, que vem despontando como provável líder no desenvolvimento de novas aplicações de tecnologia de informação e de inteligência artificial, para fins de aproveitamento e armazenamento de dados pessoais. Cabe menção, ainda, à União Europeia, principalmente no que tange às questões regulatórias que, por sua vez, acabam impactando companhias americanas como o Google (MORENO, 2018).

O GPDR rege o uso de dados pessoais, a fim de proteger os interesses de todos os indivíduos da União Europeia, bem como o espaço econômico europeu, criado em 2018, regulamentando, ainda, a exportação de dados pessoais para fora desses espaços. Essa lei revoga a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE) e é aplicável a todas as empresas que operem no Espaço Econômico Europeu, independente do país de origem, e determina a "anonimização" completa dos dados, de maneira a impossibilitar sua disponibilização sem consentimento explícito. Aprovado em 15 de abril de 2016, após período de dois anos de transição, esse regulamento passou a viger em 25 de maio de 2018 e exerceu forte influência na legislação brasileira em comento.

A Europa já possuía legislação robusta a respeito do tratamento de dados pessoais desde 1995 e deu um grande passo no sentido de um regulamento mais abrangente, que garante maior proteção aos direitos dos cidadãos.

Segundo dados da revista *Valor Econômico* (MACHADO MEYER ADVOGADOS, 2019), no primeiro ano de vigência da GPDR, as queixas referentes a supostas infrações legais chegaram ao número de 144.376 e as violações comprovadas resultaram em 89.271 notificações e em multas de, aproximadamente,

56 milhões de euros. Essas mudanças vêm afetando fortemente a rotina das empresas que negociam com os países da União Europeia e, portanto, são obrigadas a se adequar ao regulamento.

Na Espanha, especificamente, o Senado aprovou em novembro de 2018 a *Ley de protección de datos y garantias de derechosdigitales*, a fim de se adequar à reforma provocada pelo GPDR e, dentre as inovações trazidas consta um artigo polêmico, o artigo 58, que modifica a Lei Orgânica do Regime Eleitoral, permitindo que partidos políticos consultem e registrem o conteúdo divulgado por usuários em suas redes sociais, assim como seus dados pessoais, para obter informações com fins eleitorais, criando uma verdadeira exceção à regra de proteção de dados pessoais para uso eleitoral. E para blindar tal ação das restrições impostas pelo GPDR, informa a normativa que o caráter dessas mensagens não é de atividade comercial, afirmação não muito condizente.

A Agência Espanhola de Proteção de Dados, por sua vez, divulgou um comunicado informando que a nova legislação não permite o envio de propaganda eleitoral com base em informações obtidas em perfis disponibilizados nas redes sociais. Tais propagandas devem ressaltar sua finalidade eleitoral possibilitando que o cidadão exerça o seu direito de se opor. No entanto, não é o que consta no texto da lei, denominada pela imprensa espanhola como lei espiã (SÁNCHEZ, 2018) e considerada, até mesmo, como legalização do Cambridge Analytica espanhol (CASTILLO; SARABIA, 2018), refletindo a preocupação da opinião pública no que concerne à insegurança jurídica gerada pela lei que se encontra em provável posição de infração das normas constantes da União Europeia, que poderá acarretar na sua revogação (CARVALHO; VERÍSSIMO, 2018).

Nos Estados Unidos ganhou destaque, no ano passado, a declaração do CEO da Apple, Tim Cook (SALINAS; MEREDITH, 2018), em uma conferência sobre privacidade em Bruxelas. Segundo ele as grandes empresas de tecnologia estavam criando um complexo industrial de dados, utilizando dados pessoais com o que chamou de eficiência militar, alegando que, se levado ao extremo, possibilita que seja criado um perfil digital duradouro dos indivíduos que permitirá que as empresas venham a conhecer tais indivíduos melhor do que eles próprios e usou esse argumento para defender a criação de uma lei federal americana com vistas a proteger as pessoas contra essas ameaças. Uma legislação, segundo as suas próprias palavras, similar ao novo regulamento europeu, a GPDR (REINALDO FILHO, 2018). Palavras que demonstram o reconhecimento das empresas de tec-

nologia de que a aprovação de normas robustas de proteção dos dados pessoais é uma tendência em todo mundo, e que não se vislumbra quaisquer possibilidades de reversão.

No final de 2018 o senador Ron Wyden, um democrata do Estado de Oregon, apresentou um projeto de lei com sanções rigorosas para empresas que violem a privacidade dos usuários, que recebeu o nome de Consumer Data Protection Act e, segundo previsões expressas, se aprovado se aplicará a empresas com faturamento superior a 50 milhões de dólares e com mais de 1 milhão de usuários. Por não especificar regras sobre coleta e uso de dados e informações pessoais, não é considerada uma lei geral de proteção de dados pessoais, mas busca ampliar os poderes da Federal Trade Comission (FTC) de maneira a permitir à agência reguladora de defesa de interesses de consumidores servir como reguladora de assuntos ligados à privacidade. Uma de suas grandes inovações consiste na criação do cadastro *Do not track*, que permite que as pessoas manifestem a intenção de não ter seus dados pessoais repassados a terceiros. Uma boa prática cuja eficácia, porém, ainda é bastante questionada, visto que os últimos escândalos de vazamento de dados se deram por falhas de segurança ou por comportamento inadequado das empresas de tecnologia (REINALDO FILHO, 2018).

Em situação oposta, os dados pessoais são amplamente disponíveis na China, disponíveis em troca de centavos por companhias de seguro, bancos, agiotas e outras mais. No entanto, uma lei de segurança na internet entrou em vigor em junho de 2017, com o intuito de garantir a segurança nacional, impactando o modo como empresas estrangeiras negociam com a China. Uma das regras que tem sido causa de preocupação se refere à obrigação dos operadores de infraestruturas de informação chave a armazenar seus dados na China, devendo sujeitar tais dados a uma avaliação por parte das autoridades chinesas antes de poder transferi-los para fora do país. Muitos têm criticado tal normatização por considerá-la vaga em excesso e aberta a diferentes interpretações que poderiam, até mesmo, resultar em discriminações no mercado (THAM, 2018). A legislação chinesa proíbe os serviços on-line de recolher e vender dados individuais, dando direito de apagar tais dados em caso de abuso; todavia, confere amplos poderes ao governo. Reiteramos, a título de ilustração, o exemplo já citado, do uso de programas para reconhecimento dos indivíduos pela maneira de andar que, inicialmente criado como um instrumento fortalecedor do sistema de segurança, foi utilizado para controlar os cidadãos chineses atribuindo pontuação individual de bom comportamento.

O governo chinês alega que a finalidade da lei é a proteção do ciberespaço

chinês e o interesse público, bem como os direitos e os interesses do cidadão. Contudo, organizações de defesa dos direitos humanos têm afirmado que a legislação abre espaço para que as autoridades possam reprimir a liberdade de expressão e a privacidade dos indivíduos (CHINA IMPLEMENTA…, 2017).

Na Rússia, por sua vez, a regulamentação acerca da proteção de dados pessoais se dá por meio da Lei Federal nº 152-FZ, que traz a exigência de proteção dos dados recolhidos pelos operadores, e a multa pela inobservância dos dispositivos legais pode chegar a 295 mil rublos (pouco mais de 18 mil reais). Um dos casos envolvendo a legislação russa é o do LinkedIn, que decidiu não cumprir os requisitos impostos pelas autoridades russas e foi bloqueado no país pelo Serviço Federal de Supervisão na Esfera de Telecomunicações, Tecnologias da Informação e Comunicações de Massa (*Roskomnadzor* – que é o órgão do governo russo responsável pela regulação e proteção de dados e da internet) (GEVORGYAN, 2017). Todavia a Duma (parlamento russo) aprovou, em abril de 2019, um projeto que garante aos políticos russos o poder de isolar a Rússia do restante do mundo na internet. Conhecida pelo nome de internet soberana, o projeto propõe a criação de uma "*runet*", ou seja, uma estrutura de internet formulada com fins de conectar os sistemas da Rússia em servidores próprios, independentes de recursos externos. Com previsão de US$ 470 milhões de custos, o projeto tem sido considerado como um sistema de segurança, permitindo que o sistema russo continue a funcionar mesmo em caso de derrubada dos servidores dos demais países no mundo, como os Estados Unidos. A proposta, endossada por Vladimir Putin, é de criar uma versão russa do Firewall, usado pelo governo chinês para controle do tráfego da internet. A Rússia vive em constantes conflitos com seus países vizinhos em decorrência de supostos ataques cibernéticos provocados pelo seu povo.

Um fato atual, a título exemplificativo, refere-se ao aplicativo Face App, desenvolvido por uma empresa russa, que tinha a finalidade de tornar as pessoas "mais velhas" em fotos do Facebook. No entanto ninguém se atentou às políticas de privacidade do aplicativo, na qual constava que a empresa poderia monitorar a navegação dos usuários na *web* para acessar e entender seus hábitos, tendências, perfis de busca, além do fato de que, ao brincar de envelhecer suas fotos, os usuários cediam seus direitos de todas imagens geradas e publicadas por meio do aplicativo, possibilitando que ele detivesse um imenso banco de dados pessoais para comercializar com empresas de marketing digital.

A crítica vê o projeto como um atraso, pela possibilidade de redução da ve-

locidade da internet no país e, ainda, pela possibilidade de controle e censura dos cidadãos por parte do governo, por meio de remoção de postagens, por exemplo. Devido a isso alguns protestos ocorreram nas principais cidades do país, manifestando posicionamento contrário à aprovação do projeto, reunindo mais de 15 mil pessoas nas ruas de Moscou, em prol da liberdade na internet (SILVA, 2019).

Outros países vêm se movimentando em busca de regulamentar melhor o uso dos dados pessoais a fim de proteger os direitos fundamentais da pessoa humana; a eficácia de tais leis só poderá ser comprovada no tempo, no entanto, insta agir posto que evolução digital está a pleno vapor e sem qualquer pretensão de regredir.

6 CONSIDERAÇÕES FINAIS

A proposta inicial deste artigo tinha como escopo analisar de que maneira poderia ser observado o direito fundamental ao bom governo, a fim de garantir o direito da coletividade, mantendo o devido respeito à privacidade dos indivíduos que a compõem. Para tanto, partimos de alguns questionamentos: como aproveitar os avanços tecnológicos e, ao mesmo tempo, resguardar a segurança jurídica nacional? Como conciliar a necessidade e a prioridade do interesse público com a proteção legal à privacidade do indivíduo e à sua vida pessoal? Como fiscalizar e acessar esses dados pessoais, a fim de evitar ou driblar possíveis fraudes e abusos, sem atingir a vida privada dos cidadãos? Como garantir a eficácia da lei (protegendo a segurança jurídica e evitando fraudes), sem infringir a própria lei (invadindo a intimidade)?

Por se tratar de tema complexo e ainda recente, nosso objetivo não se fixou em encontrar, de imediato, as respostas para todos os questionamentos, mas por ora apenas em levantar o debate e provocar a reflexão necessária. De todo modo entendemos que, diante do princípio constitucional da supremacia do interesse público, a privacidade e a intimidade dos cidadãos devem ser sopesadas e, assim, mitigadas, em face da necessidade de proteção dos interesses coletivos.

Não adianta focar na proteção individual diante da possibilidade de abusos e fraudes que possam prejudicar interesses da sociedade inteira. Para tanto, precisaremos de limites que auxiliem e tracem os delineamentos necessários para que, em nome da coletividade, não se cometa abusos a direitos individuais.

É preciso capacitar, compreender, conhecer tais limites e agir com responsabilidade e consciência dos deveres impostos aos administradores e gestores

públicos, para bem usufruir de todo esse aparato tecnológico, dando a eles sua melhor utilidade para o bem-estar de toda a coletividade.

Muito ainda precisamos caminhar nessa busca pela compreensão e fixação dos parâmetros, necessários para o bom uso das tecnologias, sem desconsiderar os interesses individuais. A linha que os separa é tênue e precisamos avançar nos estudos, nas pesquisas, não para impedir ou vedar acessos, mas para conciliar as atividades possibilitando, dessa forma, que todos saiam ganhando, com responsabilidade e responsividade, ética, cautela e, principalmente, compromisso com a sociedade e com os indivíduos que a integram.

Neste passo, diante de tais avanços e da impossibilidade de contê-los, cabe aos países regulamentá-los, estabelecendo requisitos e pressupostos claros, objetivos e bem delimitados. Não se pode impedir a evolução digital e ela pode ser extremamente útil se bem utilizada, para tanto, impende investir em treinamento, em capacitação e, principalmente, em conscientização, no sentido de que a utilização dos dados pessoais deve ser realizada para o bem da coletividade e, excetuando os casos em que o interesse público sobreleva o privado (como se dá nas funções fiscalizatórias e sancionadoras dos tribunais de contas), deverá sempre requerer o prévio consentimento dos titulares dos dados pessoais, em respeito aos direitos fundamentais que protegem a intimidade e a privacidade do indivíduo. Qualquer utilização que não observe isso será abusiva, ultrapassando os fins legítimos.

No que concerne às cortes de contas, a nova Lei Geral de Proteção de Dados Pessoais brasileira não gera impactos negativos, sendo a eles aplicada, consoante o disposto em seu próprio texto legal que, por sua vez, já excetua da obrigatoriedade de observância normativa os casos de exercício das funções fiscalizadoras e sancionadoras, típicas (mas não únicas) dos tribunais de contas. Nesses casos, a lei prevê expressamente a sua inaplicabilidade no sentido de não ser obrigatório o consentimento prévio do titular dos dados pessoais, no entanto determina a observância dos princípios da finalidade, da necessidade, da proporcionalidade, de modo que devem utilizar tais dados com o intuito exclusivo de atender ao interesse público, limitando o seu compartilhamento para fins outros.

A finalidade da lei é protetiva e seu impacto perante o exercício das funções dos tribunais de contas se dá no sentido de determinar responsabilidade no tratamento dos dados pessoais, mitigando o direito à privacidade e à intimidade dos indivíduos, a fim de garantir algo maior, qual seja: o bem-estar social.

REFERÊNCIAS

A CHINA já pode identificar seus cidadãos só pela forma de andar. **El País**, Madri, 10 nov. 2018. Disponível em: https://bit.ly/2Rrkdkq. Acesso em: 23 ago. 2019.

ALENCAR, A. C.; MACIEL, M. O acesso à informação pelos órgãos de controle face ao direito à privacidade. *In*: VELLOZO, J. C. O.; ISHIKAWA, L.; FLORÊNCIO FILHO, M. A. (org.). **Direitos humanos**: diálogos ibero-americanos. Belo Horizonte: D' Plácido, 2019. p. 477-495.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://bit.ly/2Ro0qSD. Acesso em: 23 ago. 2019.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF: Presidência da República, 2001. Disponível em: https://bit.ly/30QwUrS. Acesso em: 24 ago. 2019.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: https://bit.ly/36oROzJ. Acesso em: 20 ago. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://bit.ly/3aIP2Zd. Acesso em: 20 ago. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 601.314/SP**. Plenário. Relator: Min. Edson Fachin, 24 de fevereiro de 2016. Brasília, DF: Supremo Tribunal Federal, 2016. Disponível em: https://bit.ly/37xukcW. Acesso em: 24 ago. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Da-

dos Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://bit.ly/2RoYzgI. Acesso em: 20 ago. 2019.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019a. Disponível em: https://bit.ly/2TXy3fR. Acesso em: 20 ago. 2019.

BRASIL. **Lei nº 13.866, de 26 de agosto de 2019**. Altera a Lei nº 8.443, de 16 de julho de 1992, que dispõe sobre a Lei Orgânica do Tribunal de Contas da União, para tratar do sigilo das denúncias formuladas ao Tribunal de Contas da União. Brasília, DF: Presidência da República, 2019b. Disponível em: https://bit.ly/2O3TnNb. Acesso em: 20 ago. 2019.

BYRNES, P. E.; CRISTE, T.; STEWART, T.; VASARHELYI, M. Reimagining Auditing in a Wired World. *In*: AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS. **Audit Analytics and Continuous Audit**: Looking Toward the Future. New York: AICPA, 2015. p. 87-102. Disponível em: https://bit.ly/36lOpBp. Acesso em: 20 ago. 2019.

CARVALHO, A. M. C.; VERÍSSIMO, L. B. O. O spam eleitoral na Espanha e a proteção de dados: exemplo para o Brasil? **Jota**, São Paulo, 6 dez. 2018. Disponível em: https://bit.ly/2t5UWmq. Acesso em: 27 jan. 2020.

CASTILLO, C.; SARABIA, D. Aprobada la ley que permitirá a los partidos hacer spam electoral y propaganda personalizada en Internet con los votos de PP, PSOE y Ciudadanos. **El Diario**, Madrid, 21 nov. 2018. Disponível em: https://bit.ly/2tRrNf5. Acesso em: 24 jan. 2020.

CHINA implementa nova lei de proteção de dados. **Euronews**, [s. l.], 29 maio 2017. Disponível em: https://bit.ly/2RmrMJ0. Acesso em: 23 ago. 2019.

FERNANDES, J. U. J. O sigilo bancário e as limitações à atuação do TCU. **Jusbrasil**, [s. l.], 16 jul. 2018. Disponível em: https://bit.ly/311taUN. Acesso em: 24 ago. 2019.

FOUCAULT, M. **A arqueologia do saber**. Rio de Janeiro: Forense Universitária, 2013.

GEVORGYAN, L. Regulamentação sobre proteção de dados na Rússia. Tradução de Luiza Brandão. **Iris**, Belo Horizonte, 24 jul. 2017. Disponível em: https://bit.ly/2TS7fxC. Acesso em: 22 ago. 2019.
INSTITUTO RUI BARBOSA. **Normas de Auditoria Governamental – NAGS**. Curitiba: IRB, 2011.

JUSTIÇA impede uso de câmera que coleta dados faciais em metrô em SP. **Instituto Brasileiro de Defesa do Consumidor**, São Paulo, 18 set. 2018. Disponível em: https://bit.ly/2TTkUV7. Acesso em: 23 ago. 2019.

MACHADO MEYER ADVOGADOS. Regulamento de proteção de dados pessoais europeu é alerta ao Brasil. **Valor Econômico**, São Paulo, 24 jun. 2019. Disponível em: https://glo.bo/2tC6T3z. Acesso em: 23 ago. 2019.

MOLINARO, C. A.; SARLET, I. W. O direito à informação na ordem constitucional brasileira: breves apontamentos. In: SARLET, I. W.; MARTOS, J. A. M.; RUARO, R. L. (coord.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016. p. 11-26.

MORENO, M. Proteção de dados pessoais: o cenário mundial e a regulamentação brasileira. **Consultor Jurídico**, São Paulo, 31 ago. 2018. Disponível em: https://bit.ly/2uwP2uI. Acesso em: 23 ago. 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana de Direitos Humanos – 1969 (Pacto San Jose da Costa Rica)**. San Jose: OEA, 1969. Disponível em: https://bit.ly/38A2rRA. Acesso em: 23 ago. 2019.

PADRÕES de Interoperabilidade. **Governo Federal**, Brasília, DF, 28 nov. 2019. Disponível em: http://bit.ly/31Kueww. Acesso em: 23 ago. 2019.

REINALDO FILHO, D. EUA se preparam para aprovar lei sobre proteção de

dados pessoais semelhante à europeia? **Juristas**, [s. l.], 8 nov. 2018. Disponível em: https://bit.ly/2O1UKMj. Acesso em: 27 jan. 2020.

SALINAS, S.; MEREDITH, S. Apple CEO Tim Cook: Personal Data Is Being "'Weaponized Against Us With Military Efficiency'. **Technocracy**, [s. l.], 24 out. 2018.

SÁNCHEZ, J. M. Llega la ley que «espía» tu ideología: los partidos podrán recopilar tus datos sin consentimiento. **Diario ABC**, Madrid, 7 dez. 2018. Disponível em: https://bit.ly/36lTKZt. Acesso em: 27 nov. 2018.

SCHMIDT, E.; COHEN, J. **A nova era digital**: como será o futuro das pessoas, das nações e dos negócios. Tradução de Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013.

SILVA, R. R. Lei aprovada na Rússia é o primeiro passo para isolar o país do resto do mundo. **Canaltech**, [s. l.], 12 abr. 2019. Disponível em: https://bit.ly/2RnWYr7. Acesso em: 23 ago. 2019.

TRIBUNAL DE CONTAS DA UNIÃO. **Boletim de Jurisprudência nº 224**. Brasília, DF: TCU, 19-20 jun. 2018. Disponível em: https://bit.ly/36vycd. Acesso em: 24 ago. 2019.

THAM, E. China vê aumento de comercialização de dados pessoais. **Terra**, Porto Alegre, 23 ago. 2018. Disponível em: https://bit.ly/30YpoLO. Acesso em: 23 ago. 2019.