A GOVERNANÇA PÚBLICA DA INFORMAÇÃO: TRANSPARÊNCIA E SEGURANÇA JURÍDICA

*Humberto Eustáquio César Mota Filho**

RESUMO

Este artigo explora a literatura da governança pública da informação buscando respostas para a seguinte pergunta: como tratar dados com transparência e segurança jurídica? Para tanto, aborda inicialmente as lógicas da *accountability* e dos laços de confiança no setor público, tendo como baliza alguns marcos legais e as boas práticas que fornecem as normas, diretrizes e os controles de responsabilidade aplicáveis aos dados. Com efeito, apontam-se quais seriam as melhores estratégias para desenvolver políticas públicas que contribuam para o valor, a qualidade e o *compliance* das informações.

Palavras-chave: Governança pública. Transparência. Segurança jurídica. Proteção de dados.

* Advogado do BNDES. Doutor em Ciência Política (Iuperj). Mestre em Direito (Ucam). Pós-graduado em Comércio Internacional (Shanghai Business School), Direito da Empresa e da Economia (FGV) e em Projetos Financeiros (UERJ). Bacharel em Direito (PUC/Rio). Coordenador da Pós-Graduação Master Compliance do IAG/PUC. Presidente do Conselho Empresarial de Governança e Compliance da Associação Comercial do Rio de Janeiro (ACRJ). Presidente da Comissão de Estudos da Transparência Pública da OAB/RJ. Consultor jurídico e professor. Membro do Fórum da Justiça na Era Digital da Escola da Magistratura do Rio de Janeiro (Emerj). Autor de livros e artigos jurídicos e palestrante em eventos nacionais e internacionais. Ex-Conselheiro de Governança da Autoridade Pública Olímpica (APO). O conteúdo desse trabalho é de exclusiva responsabilidade do autor, não refletindo, necessariamente, a opinião do BNDES.

INTRODUÇÃO

Em 2014, o International Data Corporation (IDC) estimou que os dados digitais criados, replicados e consumidos no mundo no período de um ano dobrariam de tamanho a cada dois anos, alcançando 44 zettabytes (ou 44 trilhões de gigabytes) em 2020 (IDC, 2014). Novos marcos legais e a expansão do universo digital obrigam as organizações a reavaliar suas estratégias em relação à guarda e ao uso da informação. Governos, empresas e indústrias estão se tornando mais digitais, dependentes das novas tecnologias de comunicação e conectividade, em um contexto caracterizado pelo crescimento acentuado do volume e da complexidade dos dados. Nessa sociedade do conhecimento, tanto as novas oportunidades quanto os novos desafios levam à seguinte pergunta: como gerar valor para as organizações a partir do gigantesco universo digital (FARIA; SYMPSON, 2014)? Uma possível resposta é investir na governança da informação.

Se a abundância de informação nas organizações oferece um grande potencial de desenvolvimento social e econômico, ela também traz riscos operacionais e legais que precisam ser geridos e mitigados. É fundamental, portanto, investir em governança para criar estratégias, políticas e procedimentos em torno da distribuição da informação dentro e fora das organizações. Em termos gerais, é possível afirmar que a governança da informação é o conjunto de normas, diretrizes e controles de responsabilidade desenvolvido para assegurar o valor, a qualidade e o *compliance* das informações.

Associada tanto à governança pública quanto à governança corporativa, a governança da informação está intimamente relacionada aos princípios da transparência e da prestação de contas (*accountability*). Isso porque tanto cidadãos quanto executivos e governantes necessitam de informações confiáveis para a tomada de decisões e para assegurar que seus dados estão protegidos e não foram adulterados, corrompidos, destruídos, descartados ou tratados e armazenados de forma indevida. Daí se revela a importância de outra indagação presente em todas as organizações atualmente: como tratar dados com transparência e segurança jurídica?

O termo "dados" costuma ser utilizado como sinônimo de informação, mas há também quem reconheça uma distinção semântica importante entre os dois (DONEDA, 2020). Ao se fazer essa distinção, o termo ganha conotação mais fragmentada, sugerindo uma informação em estado potencial, antes de ser transmitida, ou um estado de "pré-informação", anterior à interpretação e ao processo de elaboração, enquanto o vocábulo "informação" alude a algo além da representação contida no dado, sendo capaz, por isso mesmo, de se revestir de sentido instrumental e fornecer conteúdo voltado à redução de incertezas. De todo modo, é preciso ter em mente todo o ciclo de vida dos dados ao se buscar uma estratégia para tratá-los com transparência e segurança jurídica. Isso significa que a organização deve ser capaz de assegurar o valor, a qualidade e o *compliance* dos dados ou informações necessários às suas atividades ao longo do tempo, desde o momento da decisão de tratar determinado dado ou informação até a escolha de eliminá-lo de seus arquivos.

Então, cabe indagar quais são as melhores estratégias para fazer avançar uma agenda de governança da informação, especialmente porque não existe algo como uma receita única de sistema de governança ou de *compliance* (MENZEL, 2005).

Este artigo sugere um caminho que favoreça a busca por essa resposta partindo de marcos legais brasileiros e critérios objetivos que possam ser seguidos por governos e empresas públicas na governança de suas informações – em especial na coleta, no tratamento, armazenamento e eliminação de documentos e dados. Nesse sentido, são sugeridas quais as lógicas reitoras das políticas públicas voltadas a essa modalidade de governança no campo da transparência e da segurança da informação e são destacadas algumas de suas principais diretrizes, controles e responsabilidades.

Em outras palavras, propõe-se que a governança pública da informação seja aferida, em boa medida, pelos elementos da transparência e da segurança da informação, e são apontadas algumas

medidas e práticas que podem contribuir para o seu avanço em nosso país a partir de dispositivos legais específicos.

I. INFORMAÇÕES TRANSPARENTES: A LÓGICA DA *ACCOUNTABILITY*

Crises de confiança nas instituições, crises econômicas, precarização do bem-estar social e problemas em serviços públicos levam a um descontentamento generalizado com o Estado e com as corporações empresariais. As demandas por mais *accountability* desafiam as ordens políticas vigentes, já que esta é um princípio fundamental das democracias por meio do qual governantes e administradores prestam contas de suas ações aos cidadãos e ao mercado, podendo ter seu comportamento autorizado, chancelado ou simplesmente sofrer sanções em caso de mau desempenho, ineficiência, corrupção ou arbitrariedade no uso do poder.

De fato, a noção de *accountability* sugere um processo abrangente, envolvendo não apenas instituições representativas, mas também organizações da burocracia e outras com atores não eleitos (OLSEN, 2018). Há enormes variações no que se entende por e no que implica a *accountability*, pois é ainda um conceito em evolução (CAMPOS, 1990) que comporta uma nova reflexão sobre a ordem política e um princípio de organização das relações entre governados e governantes, proprietários e não proprietários.

Nessa evolução, é importante notar que o termo não parece se esgotar nas preocupações da administração pública tradicional, em uma *accountability* de processos, restrita ao exame da conformidade das leis e normas procedimentais, a partir de um ponto de vista hierárquico e descomprometido com resultados. Em uma acepção mais abrangente, *accountability* alude à responsabilidade perante alguém, a uma obrigação dos governantes ou administradores de explicarem e justificarem suas ações – por exemplo, como mandatos e contratos foram tratados, como a autoridade e os recursos foram aplicados e quais foram os resultados (OLSEN, 2018).

Mais especificamente, a lógica da *accountability* democrática corresponde a uma série de mecanismos pelos quais os agentes públicos são obrigados a prestar contas por seu desempenho e suas atividades em relação aos cidadãos (ABRUCIO; LOUREIRO, 2005). Essa lógica demanda uma interação qualificada Estado-sociedade, baseada em transparência, imputabilidade, controle, responsabilidade e responsividade (KOPPELL, 2005) e dever de justificativa – *answerability* (FIABANE, 2011; SCHEDLER, 1999).

Ao compreender essa lógica de uma interação mais qualificada, a definição de O'Donnell de *accountability* horizontal para as relações entre atores estatais das diversas esferas de poder, sem a ideia de hierarquia, e de *accountability* vertical para identificar a relação principal-agente ou mandante-mandatário, pela qual o titular originário das prerrogativas relacionadas ao exercício do poder político as transfere para representantes dele incumbidos, afigura-se insuficiente. Assim, o controle do poder público e da prestação de serviços públicos demanda mobilização, interlocução e articulação dos mais diversos atores públicos e privados na produção, tratamento e disponibilização de informações destinadas aos órgãos de controle estatal e aos cidadãos diretamente.

Numa dinâmica de "círculo virtuoso", informações transparentes tendem a favorecer a lógica da *accountability* democrática e estimular uma interação mais qualificada entre atores públicos e privados. É possível criar e manter um fluxo de informações transparentes a partir de um conjunto dado de normas, diretrizes e controles de responsabilidade desenvolvido para assegurar o valor, a qualidade e o *compliance* das informações, para o qual algumas políticas públicas podem contribuir.

A. POLÍTICAS PÚBLICAS PARA INFORMAÇÕES MAIS TRANSPARENTES

A governança da informação relaciona-se com questões públicas fundamentais. Na ótica da governança pública, sua boa execução requer transparência dos atos de governo – ou seja, a prestação de contas pela produção e divulgação sistemática de informações (MOTA FILHO; ALFRADIQUE, 2018) – e objetiva a geração de benefícios sociais. Nessa visão normativa de governança pública, a prestação de contas dos administradores públicos é compreendida como um bem básico da democracia – a *accountability* democrática (DIAMOND, 1999). Tanto é assim que, para os próprios conselheiros de administração das estatais federais, o maior avanço da Lei das Estatais (Lei 13.303, de 30 de junho de 2016) consistiu na determinação de mais transparência na divulgação das informações relevantes (SARDENBERG, 2018, p. 14).

A publicidade dos atos de governo é uma das bases do estado democrático de direito consagrado pela constituinte de 1988. Segundo os próprios constituintes, o acesso às informações dos órgãos públicos é fundamental para o aperfeiçoamento da máquina de governo, para a correção de eventuais abusos, para o combate à corrupção e para o exercício pleno da cidadania. Por essas razões, o direito à informação está inscrito no rol de direitos e garantias fundamentais da nossa Constituição Federal (BRASIL, 1988, art. 5º, XIV e XXXIII).

Em busca de mais legitimidade e da recuperação da confiança de seus cidadãos, governos democráticos investem na transparência e na divulgação de seus atos e políticas públicas, tal como as empresas em relação aos consumidores e ao público em geral. Assim o fazem por acreditarem que, ao se tornarem mais conhecidos e compreendidos, a confiança do público em suas ações será recuperada ou aumentará, então, as políticas públicas e as políticas corporativas terão mais chances de avançar e obter melhores resultados se contarem com mais credibilidade e apoio.

O conceito de transparência na gestão pública se divide em duas vertentes: a ativa e passiva. A primeira é caracterizada pela publicação e disseminação de forma proativa, pelo poder público, de informações essenciais sobre suas políticas e ações – em portais da transparência, por exemplo –, sem necessidade de pedidos prévios. Já na transparência passiva, o poder público fornece informações mediante solicitações e pedidos realizados pela sociedade civil organizada, por empresas ou por qualquer cidadão, atuando de forma reativa.

Políticas de dados abertos (PDA) tendem a qualificar o diálogo público-privado e agregam credibilidade às informações públicas repassadas, permitindo que as políticas públicas sejam concebidas, implementadas e avaliadas com base em melhores critérios e que se aumente a participação social em todas as fases de seu ciclo de desenvolvimento. Nessa lógica, o Governo Federal brasileiro regulamentou recentemente uma PDA (Decreto 8.777, de 11 de maio de 2016) contendo princípios orientadores e objetivos, dentre os quais destacam-se: (i) promover a publicação de dados da administração pública federal; (ii) aprimorar a cultura de transparência pública; (iii) franquear aos cidadãos o acesso aos dados produzidos ou acumulados pelo Poder Executivo federal sobre os quais não recaia vedação expressa de acesso; (iv) facilitar o intercâmbio de dados entre a administração pública federal e as diferentes esferas da federação; e (v) fomentar o controle social e o desenvolvimento de novas tecnologias destinadas à construção de ambiente de gestão pública participativa e democrática e à melhor oferta de serviços públicos para o cidadão.

Segundo a PDA, dados abertos são aqueles "acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte" (BRASIL, 2016a, art. 2º, III). Complementando tal definição, vale notar que os dados considerados acessíveis ao público são aqueles gerados ou acumulados pelo Governo Federal que não estejam sob sigilo ou sob restrição de acesso nos termos da Lei de Acesso à Informação. Então, geralmente, é responsabilidade dos órgãos e entidades públicas assegurar a gestão

transparente da informação, propiciando amplo acesso e divulgação, vedando o acesso do público apenas em casos excepcionais (BRASIL, 2011, art. 6º, I).

Entre suas responsabilidades, a Controladoria Geral da União (CGU) – órgão de controle interno do Governo Federal – deve zelar pelo incremento da transparência da gestão pública. Para tanto, conta com um portal de dados abertos, no qual estão disponíveis informações sobre auditorias realizadas, empresas inidôneas e suspensas e processos disciplinares, em linha com os objetivos expressos na PDA.

Mas é possível ir além para o avanço da governança da informação no âmbito da transparência pública, especialmente na questão da qualidade da informação, ao tratar os dados para demonstrar como uma organização pública gera valor. Lançado em 2014 pelo Conselho Internacional para Relato Integrado (International Intregrated Reporting Council – IIRC) – uma coalizão global de reguladores, investidores, empresas, organismos de normatização, entidades contábeis e organizações não governamentais (ONG) –, o relato integrado tem exatamente o objetivo de articular informações financeiras e não financeiras, de forma concisa, para demonstrar como uma organização gera valor para seus públicos de relacionamento.

Já existem alguns exemplos de promoção do relato integrado em nosso país. Em geral, a adoção do modelo pelo setor privado é voluntária, mas iniciativas do governo começam a tornar sua utilização obrigatória para alguns entes públicos. As empresas públicas e as sociedades de economia mista, por exemplo, devem divulgar anualmente relatório integrado ou de sustentabilidade (BRASIL, 2016b, art. 8º). Recentemente, o Tribunal de Contas da União (TCU) promoveu mudanças no processo de prestação de contas anuais da administração pública federal, incluindo a adoção do modelo do relato integrado para o relatório de gestão (TCU, 2018). Com essa exigência válida para todos os órgãos e entidades da administração pública, as mais de 1,1 mil unidades que prestam contas ao TCU deverão adotar esse modelo.

Políticas públicas podem favorecer uma boa governança da informação sempre que fornecerem os meios para que a transparência ativa e passiva esteja a serviço da prestação de contas dos administradores públicos (*accountability* democrática). Dito de outro modo, a governança da informação pública terá mais legitimidade e credibilidade se o conjunto de suas normas, diretrizes e controles de responsabilidade assegurar os valores da prestação de contas e da informação pública, a qualidade da informação (pela adoção das boas práticas organizacionais e de gestão documental) e o *compliance* das informações (pela forma correta de coleta, tratamento, armazenamento e eliminação de dados pessoais e coletivos dos cidadãos), necessários ao desenvolvimento das políticas públicas. Alguns desses temas serão abordados mais adiante, ao tratar-se da segurança da informação.

II. INFORMAÇÕES SEGURAS: A LÓGICA DA CONFIANÇA

Segundo o dilema da confiança (MOTA FILHO, 2018), explorado por Ovanessoff, Plastino e Faleiro (2015), é preciso confiança para cooperar, entretanto, também é preciso cooperar para ganhar confiança, seja na interação de agentes públicos, de agentes privados ou entre agentes públicos e privados. De maneira geral, estudos apontam que a maioria dos brasileiros tem dificuldades para estabelecer novas relações de confiança (CNI, 2014), e que mesmo as empresas do país consideradas inovadoras colaboram menos com outras organizações nacionais ou internacionais do que as empresas de grande parte dos países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Essas lacunas na confiança social acabam por comprometer a colaboração necessária nas relações negociais. Por seu turno, nas relações público-privadas, não há razão para supor que o quadro é muito melhor.

Mais recentemente, foi feita uma pesquisa nacional a fim de investigar qual é o nível de confiança dos brasileiros em suas instituições, especificamente entre as ONGs, empresas, mídia e governo

(EDELMAN, 2017), e é revelador notar que nenhuma dessas organizações atingiu resultados satisfatórios. As ONGs e as empresas ao menos não despertaram a desconfiança entre os brasileiros, enquanto a mídia e o governo não mereceram confiança. O levantamento ainda revelou que a população do país considera suas fontes oficiais suspeitas, já que a maioria dos consultados considerou os indivíduos mais confiáveis do que as instituições e as informações vazadas como tendo mais credibilidade do que os comunicados das companhias para a imprensa.

Ainda que essa crise de confiança seja global, a chamada era da economia da reputação (FAGUNDES, 2017) parece intensificar suas consequências no ambiente empresarial brasileiro. Nessa nova economia da reputação, 84% do valor de mercado de uma empresa listada no índice Standard & Poor's 500 (S&P 500) dos Estados Unidos está atrelado a valores intangíveis, como a reputação, e o Brasil não parece fugir dessa tendência. Os riscos reputacionais estão no topo das preocupações dos membros dos conselhos de administração e, segundo pesquisas internacionais, as principais causas da perda de reputação são os comportamentos à margem da ética e da integridade (DELOITTE, 2014). Sem sombra de dúvida, no meio empresarial, a confiança é um ativo valioso e a falta de ética é um passivo fatal. Assim, um ambiente geral de baixa confiança social, como no caso brasileiro, afeta negativamente a sociedade, os negócios e o governo.

Todos esses dados indicam a necessidade de mais governança pública, ou seja, as soluções para o problema da confiança precisam ser legitimadas por uma agenda de mudança dos processos decisórios que inclua a sociedade desde o início das discussões. É preciso retomar níveis de confiança satisfatórios que permitam criar um ambiente propício ao debate público e ao desenvolvimento de mais negócios e investimentos em nosso país. Portanto, é fundamental enfrentar o problema da confiança com o diagnóstico e as ferramentas certas.

Para avançar nessa agenda de forma a fortalecer os laços de confiança sociais, a lógica da *accountability* é fundamental, mas não suficiente. Uma estratégia efetiva para o avanço da governança da informação demanda que, junto com a transparência das informações, seja garantida a sua segurança, pois assim será possível ganhar a legitimidade e a credibilidade necessárias para vencer o problema da confiança (MOTA FILHO, 2018). Nesse sentido, políticas públicas podem ajudar a fortalecer a segurança das informações utilizadas pelas organizações.

A. POLÍTICAS PÚBLICAS PARA INFORMAÇÕES MAIS SEGURAS

Na governança pública, a informação é um bem público, na medida em que atende a demandas públicas e se converte em direito constitucional dos cidadãos, conforme nosso ordenamento jurídico. O emprego de informações incorretas, corrompidas ou indevidas pode acarretar prejuízos substanciais às políticas públicas e tornar suas ações ineficazes ou contraproducentes.

Ninguém dúvida que as organizações governamentais armazenam e criam uma quantidade de informações cada vez maior a cada dia. Entretanto, essas informações nem sempre geram valor para as organizações, já que muitas vezes não têm a qualidade desejada nem estão em conformidade com as leis e seus regulamentos. Problemas com a governança da informação são cada vez mais frequentes nas organizações, sejam eles referentes a vazamentos de dados privilegiados, prejuízos decorrentes de ataques cibernéticos ou sistemas contábeis e controles bancários corrompidos, chegando até mesmo a casos de processos fraudulentos automatizados pelos sistemas de certos bancos (LAJARA, 2013).

Na sociedade do conhecimento, a segurança é um dos elementos característicos e essenciais da governança da informação (WILLIAMS, 2008). Em termos gerais, o conceito de segurança da informação envolve a proteção da confidencialidade, integridade e disponibilidade (acessibilidade) da informação (POSTHUMUS; VON SOLMS, 2004). Mais especificamente, segundo esses três pilares

norteadores, a segurança da informação deve garantir que ela: esteja acessível quando necessária para o funcionamento da organização e realização de seus fins (disponibilidade); seja acessada e utilizada exclusivamente por quem é devidamente autorizado para tal (confidencialidade); seja verídica e não esteja corrompida (integridade) (FONTES, 2000).[1]

Precisamente nessa linha, a Política Nacional de Segurança da Informação (PNSI), instituída no âmbito da Administração Pública Federal pelo Decreto 9.637, de 26 de dezembro de 2018, tem como objetivo assegurar a disponibilidade, integridade, confidencialidade e autenticidade[2] da informação a nível nacional. A PNSI abrange os campos da segurança e defesa cibernética, segurança física e proteção de dados organizacionais. Sob a ótica dessa política, a governança da informação encontra, em termos gerais, as principais diretrizes desenvolvidas para assegurar a proteção de dados dessas organizações. Aqui vale ressaltar que é responsabilidade dos órgãos de governo, em todos os níveis, a proteção da informação custodiada por eles, garantindo sua disponibilidade, autenticidade e integridade, e a proteção da informação sigilosa e da informação pessoal (BRASIL, 2011, art. 6º, II e III).

Mas antes mesmo da edição da PNSI, a Lei 12.682, de 9 de julho de 2012, já consagrava legalmente esses pilares ao dispor sobre o processo de digitalização, ou seja, "sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos" (BRASIL, 2012). Nesse sentido, nosso sistema legal já reconhecia que tal processo deveria ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).[3] Assim, por regra, para que haja validade jurídica ou valor probatório de uma cópia ou reprodução de um documento original, é preciso que alguém investido de fé pública[4] ateste, com segurança, que verificou os elementos de autoria e integridade do original em cotejo com a cópia apresentada naquele ato. Portanto, esses procedimentos também devem ser incluídos no rol de uma política de governança da informação.

Na seara da proteção de dados, vale recordar que tal matéria é disciplinada na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet. Contudo, a nova Lei Geral de Proteção de Dados (LGPD) singulariza-se por sua abrangência, enunciando princípios, direitos, responsabilidades e demais aplicações decorrentes do tratamento de dados pessoais. Portanto, vale concentrar nossa análise nesse marco regulatório em especial, pois ele estabelece as diretrizes para o tratamento dos dados pessoais, inclusive nos meios digitais, por pessoas físicas ou jurídicas, de direito público ou privado.

Tendo em conta esse histórico, resta claro que a LGPD está inserida num sistema legal de proteção de dados mais amplo, não detendo a exclusividade do tratamento legislativo sobre a proteção de dados pessoais. Ela certamente se aplica ao tratamento de dados por pessoa jurídica de direito público e impacta a governança pública ao buscar a proteção de direitos e garantias fundamentais da pessoa natural. Assim, na ocorrência de infrações à LGPD, em especial no caso de incidentes de segurança da informação, a autoridade regulatória avaliará a boa-fé do infrator, a implementação de políticas de

1 Conceitos técnico-legais de disponibilidade, autenticidade e integridade podem ser encontrados no art. 4º, incisos VI, VII e VIII, da Lei 12.527, de 18 de novembro de 2011 (BRASIL, 2011).

2 Aqui vale recordar que a autenticidade é uma qualidade do documento, ou seja, significa que aquele documento é o que diz ser, livre de qualquer adulteração e corrupção. Já a autenticação é uma declaração dessa qualidade, quer dizer, é uma manifestação sobre um documento, num determinado momento, por uma pessoa física ou jurídica investida de autoridade para fazer tal declaração (servidor público, notário ou autoridade certificadora). Portanto, procedimentos que visam a certificação de conferência com o original, por exemplo, tratam da questão da autenticação de uma cópia. A observância desses procedimentos é importante, pois afeta diretamente a segurança das informações.

3 "Art. 1º A digitalização, o armazenamento em meio eletrônico, óptico ou equivalente e a reprodução de documentos públicos e privados serão regulados pelo disposto nesta Lei" (BRASIL, 2012).

4 Fé pública é o crédito que se deve dar a documentos emanados de autoridades públicas ou serventuários da justiça em virtude da função ou ofício exercido.

boas práticas e de governança e a pronta tomada de medidas corretivas, entre outros critérios (BRASIL, 2018b, art. 52, § 1º). Portanto, destaca-se a importância da adoção de uma política de governança da informação para a proteção de dados pessoais também no âmbito do setor público.

A LGPD aplica-se a qualquer órgão ou entidade pública, a empresas públicas e sociedades de economia mista, especialmente quando há utilização dos dados dos cidadãos para a elaboração e execução de políticas públicas e prestação de serviços públicos. Dessa forma, a implementação da LGPD no setor público exige a revisão de todos os processos que envolvam dados pessoais e sensíveis,[5] com o desenvolvimento de uma política de governança para o mapeamento e tratamento dessas informações em conformidade com a legislação. Essa nova lei dedicou todo um capítulo ao tratamento de dados pessoais pelo poder público em busca de estabelecer um equilíbrio entre o acesso à informação nas mãos da administração pública e a proteção dos dados pessoais dos cidadãos, fazendo ainda expressas menções à Lei de Acesso à Informação.[6]

É preciso cuidado especial nos casos de incidentes de segurança que possam acarretar riscos ou danos relevantes aos cidadãos, titulares das informações utilizadas pelo setor público. Vale recordar que diversos órgãos e entidades públicas lidam com dados pessoais tanto de contribuintes quanto de servidores e empregados públicos, por exemplo, sendo que muitos se enquadram na definição de dado pessoal sensível. Na ocorrência de incidente de segurança, é imprescindível comunicá-lo à Autoridade Nacional de Proteção de Dados[7] e ao titular dos dados, via órgão público, entidade pública, empresa pública ou sociedade de economia mista que desempenhar o papel de controlador, em um prazo razoável, sempre que o incidente de segurança puder acarretar risco ou dano relevante aos titulares.[8]

A segurança das informações também é impactada diretamente pela gestão da documentação governamental, que é regulada pela própria Constituição Federal (BRASIL, 1988, art. 216, § 2º), a qual determina que cabe à administração pública, na forma da lei, gerir e franquear a consulta dos arquivos públicos pela sociedade. Nessa esteira, foi promulgada a Lei 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados (PNAPP).

A PNAPP compreende a definição e adoção de um conjunto de normas e procedimentos técnicos e administrativos para disciplinar as atividades relativas aos serviços arquivísticos da administração pública, visando a melhoria desses arquivos no âmbito de um processo de reestruturação da própria administração. Nesse sentido, a política adota como objetivos do programa de gestão de documentos o controle sobre a produção documental e a racionalização de seu fluxo (BRASIL, 2002, art. 1º e art. 13, I-IV) para permitir, com isso, que os arquivos públicos cumpram sua função social,[9] aumen-

---

5 Dado pessoal é todo e qualquer dado que possa ser vinculado ou associado a uma determinada pessoa. Dados sensíveis são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

6 Várias regras foram criadas exclusivamente para órgãos e entidades públicos, como as relativas ao compartilhamento de dados pessoais à transparência e às bases autorizativas dos tratamentos de dados pessoais. Há previsão de diferentes sanções, a depender do regime concorrencial ou não da entidade pública, com impacto relevante para empresas públicas e sociedades de economia mista que ora atuam como entidades privadas, ora como gestoras ou executoras de políticas públicas.

7 O conteúdo dessa comunicação deve abarcar a descrição da natureza dos dados pessoais afetados; informações sobre os titulares envolvidos; indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; riscos relacionados ao incidente; motivos da demora, no caso de a comunicação não ter sido imediata; e medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. A Autoridade Nacional de Proteção de Dados, a depender da gravidade do incidente, pode determinar a adoção de outras providências, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

8 A ser definido pela Autoridade Nacional de Proteção de Dados. Na legislação europeia que trata do mesmo tema (General Data Protection Regulation – GDPR), o prazo definido foi de 72 horas.

9 A função social dos arquivos é revelada pelo registro documental, que tem a capacidade de "capturar os fatos, suas causas e consequências, de preservar e estender no tempo a memória e a evidência desses fatos", atestar "ações e transações, e [...] sua veracidade dependente das circunstâncias de sua criação" (DURANTI, 1994, p. 49-64).

tem sua eficácia e garantam o cumprimento dos direitos da cidadania,[10] dando suporte às decisões político-administrativas do Estado (BRASIL, 2001).

Apesar de elaborada no início da era digital, ao incidir sobre a gestão e o ciclo de vida dos documentos de interesse público, a PNAPP também pode orientar o desenvolvimento de informações mais seguras se harmonizada com os diplomas legais mais recentes da Política de Segurança da Informação e da LGPD, especialmente na questão da integridade e da eliminação dos documentos.

Para cumprir a PNAPP e os objetivos da gestão de documentos, foi organizado um código de classificação de documentos de arquivo para a administração pública aprovado pelo Conselho Nacional de Arquivos (Conarq), vinculado ao Arquivo Nacional. Mas os próprios representantes do Conarq reconhecem que as atividades da administração pública são dinâmicas e requerem alterações periódicas, a fim de garantir sua atualidade frente às constantes transformações desse setor (BRASIL, [2019]).

Assim sendo, a eliminação de documentos no setor público obedece a procedimentos previstos na legislação arquivística específica (BRASIL, 1996, art. 1º e 2), entre os quais estão a constituição de comissão permanente de avaliação de documentos, a elaboração de tabela de temporalidade e destinação de documentos e o cumprimento do disposto nas resoluções do Conarq que tratam da eliminação de documentos. No setor público, a eliminação deve ser precedida pela elaboração de listagem que, depois de aprovada pela instituição arquivística com esfera de competência específica, deverá ser publicada; quando for efetivada a eliminação, será lavrado o termo de eliminação de documentos, segundo a legislação vigente. Caso o original seja considerado de valor permanente, não poderá ser eliminado, conforme também determina a legislação. Nesse sentido, a observância da PNAPP pretende garantir segurança jurídica na eliminação dos documentos dos arquivos públicos.

Indo além, é fundamental incluir no planejamento de governança da informação do setor público a avaliação do alinhamento entre os prazos constantes na proposta de arquivamento de documentos[11] e os prazos prescricionais previstos no ordenamento jurídico para a defesa dos direitos reais e pessoais dessas entidades.

Afinal, o Poder Judiciário[12] entende que as ações de ressarcimento de danos ao erário, em determinadas hipóteses, são imprescritíveis. Ou seja, no limite, os órgãos e empresas públicas podem ser demandados a produzir, por tempo indeterminado, documentos relativos a condutas suspeitas de terem gerado dano ao erário público. Nesse contexto, recomenda-se especial cuidado na classificação, manutenção e eliminação de arquivos públicos que, por sua natureza, documentem operações com maiores riscos potenciais de caracterizar algum dano relevante.

CONSIDERAÇÕES FINAIS

O emprego das lógicas da *accountability* e dos laços de confiança contribui para o tratamento de dados de forma transparente e segura no setor público. Os marcos legais e as boas práticas de mercado existentes já servem de guia para a identificação das normas, diretrizes e controles de responsabilidade aplicáveis aos dados. A partir daí, é fundamental traçar as estratégias para

10 Na administração pública, graças à Constituição Federal de 1988, os arquivos estão associados à conquista de direitos civis e ao exercício pleno da cidadania. No capítulo sobre os direitos e garantias fundamentais, a Carta Magna assegurou a todos o direito ao acesso à informação e a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo geral (art. 5º, incisos XIV e XXIX), conferindo assim um papel de destaque à formulação de política pública de gestão de documentos, nos termos da Lei 8.159/1991, que regulamentou o artigo 216 da Constituição Federal.

11 Código de classificação e tabela de temporalidade e destinação de documentos de arquivo relativos às atividades-fim das entidades públicas previstos na PNAPP.

12 O Superior Tribunal Federal, em sede de repercussão geral, fixou a seguinte tese: "São imprescritíveis as ações de ressarcimento ao erário fundadas na prática de ato doloso tipificado na Lei de Improbidade Administrativa" (BRASIL, 2019).

desenvolver e aplicar políticas públicas que contribuam para o valor, a qualidade e o *compliance* das informações.

Políticas públicas mais transparentes devem estar a serviço da prestação de contas dos administradores públicos e dos resultados de suas ações e omissões (*accountability* democrática). Desse modo, as políticas públicas para proteção de dados devem fortalecer os três pilares que norteiam a segurança da informação: estar acessível quando necessária para o funcionamento da organização e realização de seus fins (disponibilidade); ser acessada e utilizada exclusivamente por quem é devidamente autorizado para tal (confidencialidade); e ser verídica e não estar corrompida (integridade).

A governança da informação pública terá mais legitimidade e credibilidade, portanto, se o conjunto de suas normas, diretrizes e controles de responsabilidade assegurar os valores da prestação de contas e da informação pública, bem como a qualidade da informação, pela adoção das boas práticas organizacionais e da gestão documental, e o *compliance* das informações, pela forma correta de coleta, tratamento, armazenamento e eliminação de dados pessoais e coletivos dos cidadãos – dados esses que são necessários ao desenvolvimento das políticas públicas.

REFERÊNCIAS

ABRUCIO, Fernando Luiz; LOUREIRO, Maria Rita. Finanças públicas, democracia e *accountability*: debate teórico e o caso brasileiro. *In:* ARVATE, Paulo Roberto; BIDERMAN, Ciro (org.). *Economia do setor público no Brasil*. Rio de Janeiro: Elsevier/Campos, 2005. p. 75-102.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 nov. 2021.

BRASIL. Arquivo Nacional. Conselho Nacional de Arquivos. *Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública*. Rio de Janeiro: Arquivo Nacional, 2001.

BRASIL. Arquivo Nacional. Conselho Nacional de Arquivos. Resolução n. 5, de 30 de setembro de 1996. Dispõe sobre a publicação de editais para Eliminação de Documentos nos Diários Oficiais da União, Distrito Federal, Estados e Municípios. *Diário Oficial da União*, Brasília, DF, p. 20558, 11 out. 1996.

BRASIL. Decreto n. 4.073, de 3 de janeiro de 2002. Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. *Diário Oficial da União*, Brasília, DF, p. 1, 3 jan. 2002.

BRASIL. Decreto n. 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo federal. *Diário Oficial da União*, Brasília, DF, p. 21, 12 maio 2016a.

BRASIL. Decreto n. 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação [...]. *Diário Oficial da União*, Brasília, DF, ed. 248, p. 23, 27 dez. 2018a.

BRASIL. Lei n. 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. *Diário Oficial da União*, Brasília, DF, p. 455, 9 jan. 1991.

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

BRASIL. Lei n. 12.682, de 9 de julho de 2012. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. *Diário Oficial da União*, Brasília, DF, p. 1, 10 jul. 2012.

BRASIL. Lei n. 13.303, de 30 de junho de 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. *Diário Oficial da União*, Brasília, DF, p. 1, 1 jul. 2016b.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*, Brasília, DF, ed. 157, p. 59, 15 ago. 2018b.

BRASIL. Ministério da Justiça e Segurança Pública. Perguntas mais frequentes. *Conarq*, Rio de Janeiro, [2019]. Disponível em: http://antigo.conarq.gov.br/documentos-eletronicos-ctde/perguntas-mais-frequentes.html. Acesso em: 16 jul. 2018.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 852.475/SP. Direito constitucional. Direito administrativo. Ressarcimento ao erário. Imprescritibilidade. Sentido e alcance do art. 37, § 5 °, da constituição [...]. Relator: Alexandre de Moraes. Relator do Acórdão: Edson Fachin, 8 de agosto de 2018. *Diário Eletrônico da Justiça*, São Paulo, n. 58, 25 mar. 2019.

CAMPOS, Anna Maria. Accountability: quando poderemos traduzi-la para o português? *Revista de Administração Pública*, Rio de Janeiro, v. 24, n. 2, p. 30-50, 1990.

CAVOUKIAN, Ann. *Privacy by design*: the 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario, 2011. Disponível em: www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 12 jun. 2018.

CNI – CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Pesquisa CNI-Ibope*: retratos da sociedade brasileira: confiança interpessoal, março de 2014. Brasília, DF: CNI, 2014.

DELOITTE. *2014 global survey on reputation risk*: Reputation@Risk. New York: Deloitte, 2014. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf. Acesso em: 12 jun. 2018.

DIAMOND, Larry. *Developing democracy*: toward consolidation. Baltimore: John Hopkins University Press, 1999.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (org). *Direito digital*: direito privado e internet. São Paulo: Foco, 2020. p. 33-51.

DURANTI, Luciana. Registros documentais contemporâneos como prova de ação. *Estudos Históricos*, Rio de Janeiro, v. 7, n. 13, p. 49-64, 1994.

EDELMAN. *2017 Edelman Trust Barometer*: trust and the CEO. Chicago: Edelman, 2017. Disponível em: https://www.ifac.org/system/files/uploads/Comms/Day%201%20-%20Trust%20Barometer%20-%20Justin%20Blake.pdf. Acesso em: 12 jun. 2018.

FAGUNDES, Suzana. Integridade como novo paradigma da reputação. *Revista Governança e Compliance da Associação Comercial do Rio de Janeiro*, Rio de Janeiro, v. 1, n. 1, p. 30-33, 2017.

FARIA, Fernando A.; SYMPSON, Gladys E. Bridging the gap between business and IT: an information governance perspective in the banking industry. *In:* BHANSALI, Neera. *Data governance*: creating value from information assets. Boca Raton: Taylor & Francis, 2014. p. 217-241.

FIABANE, Danielle Fabian. *Controle social*: um novo frame nos movimentos sociais. 2011. Dissertação (Mestrado em Administração Pública e Governo) – Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2011.

FONTES, Edison. *Vivendo a segurança da informação*: orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

IDC – INTERNATIONAL DATA CORPORATION. *The digital universe of opportunities*: rich data and the increasing value of the internet of things. Needham: IDC, 2014. Disponível em: https://www.iotjournaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf. Acesso em: 12 jun. 2018.

JIMENE, Camilla do Vale. Da segurança e das boas práticas. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 329-354.

KOPPELL, Jonathan G. S. Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review*, Hoboken, v. 65, n. 1, p. 94-108, 2005.

LAJARA, Tamara Tebaldi. *Governança da informação na perspectiva de valor, qualidade e compliance*: estudo de casos múltiplos. 2013. Dissertação (Mestrado em Administração) – Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013.

MENZEL, Donald C. Research on ethics and integrity in governance: a review and assessment. *Public Integrity*, Abingdon, v. 7, n. 2, p. 147-168, 2005.

MOTA FILHO, Humberto. Como manter um ambiente ético nas empresas? *Revista Compliance Rio*, Rio de Janeiro, v. 1, n. 1, p. 30-37, 2018.

MOTA FILHO, Humberto; ALFRADIQUE, Cláudio Nascimento. A governança e o controle da função pública: a transparência pública nos trinta anos da Constituição Cidadã. *In:* MONTEIRO, Geraldo Tadeu Moreira (org.).

Estado, democracia e direito no Brasil: trinta anos da constituição cidadã. Rio de Janeiro: Gramma, 2018. p. 413-436.

OLSEN, Johan P. *Accountability democrática, ordem política e mudança*: explorando processos de accountability em uma era de transformação europeia. Tradução: Eliane Rio Branco. Brasília, DF: Enap, 2018.

OVANESSOFF, Armen; PLASTINO, Eduardo; FALEIRO, Flaviano. *Por que o Brasil precisa aprender a confiar na inovação colaborativa.* São Paulo: Accenture, 2015.

POSTHUMUS, Shaun; VON SOLMS, Rossouw. A framework for the governance of information security. *Computers & Security*, Amsterdam, v. 23, n. 8, p. 638-646, 2004.

SARDENBERG, Dalton. *Integridade pública, regulação e controle social.* Seminário de Governança Privada e Integridade Pública da Associação Comercial do Rio de Janeiro, 7 jun. 2018.

SCHEDLER, Andreas. Conceptualizing accountability. *In*: SCHEDLER, Andreas; DIAMOND, Larry; PLATTNER, Marc F. (ed.). *The self-restraining state*: power and accountability in new democracies. Boulder: Lynne Rienner, 1999. p. 13-28.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. Decisão Normativa TCU n. 170, de 19 de setembro de 2018. Dispõe acerca das unidades cujos dirigentes máximos devem prestar contas de suas gestões ocorridas no exercício de 2018, especificando a forma, os conteúdos e os prazos de apresentação, nos termos do art. 3º da Instrução Normativa TCU 63, de 1º de setembro de 2010. *Diário Oficial da União*, Brasília, DF, ed. 187, p. 107, 24 set. 2018.

WILLIAMS, Patricia A. H. In a "trusting" environment everyone is responsible for information security. *Information Security Technical Report*, Amsterdam, v. 3, n. 4, p. 207-215, 2008.