A GOVERNANÇA PRIVADA DA INFORMAÇÃO: *ACCOUNTABILITY* E CONFIANÇA

Private Information Governance: Accountability and Trust

Humberto Eustáquio César Mota Filho[1]

SUMÁRIO 1. Introdução; 2. A lógica da *accountability*: informações transparentes; 3. Políticas corporativas para informações mais transparentes; 4. Informações seguras: a lógica da confiança; 5. Políticas corporativas para informações seguras; 6. Conclusão; Referências bibliográficas.

RESUMO Este artigo examina a literatura da governança da informação de forma a buscar respostas para a seguinte indagação: como tratar dados com transparência e segurança jurídica? Para tanto, aborda preliminarmente as lógicas da *accountability* e dos laços de confiança no setor privado, tendo como baliza alguns marcos legais e as boas práticas de mercado, os quais fornecem as normas, diretrizes e os controles de responsabilidade aplicáveis aos dados. Em seguida, recomenda quais seriam as melhores estratégias para desenvolver políticas corporativas que contribuam para o valor, a qualidade e o *compliance* das informações.

Palavras-chave: Governança da Informação. Transparência. *Accountability*.

ABSTRACT This study explores the information governance literature to seek answers to the following question: How to handle data transparency and legal certainty? To this end, it initially addresses the logics of accountability and trust in the private sector, with some legal frameworks and good market practices as guidelines, which provide the norms and controls applicable to data. From this, we suggest what would be the best strategies to develop corporate policies which contribute to information value, quality, and compliance.

Keywords: Information Governance. Transparency. Accountability.

[1] Doutor em Ciência Política pelo Instituto Universitário de Pesquisas do Rio de Janeiro (IUPERJ). Mestre em Direito pela Universidade Candido Mendes (UCAM). Pós-Graduado em Comércio Internacional pela Shanghai Business School. Pós-Graduado em Direito da Empresa e da Economia pela Fundação Getúlio Vargas (FGV). Pós-Graduado em Projetos Financeiros pela Universidade Estadual do Rio de Janeiro (UERJ). Bacharel em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Coordenador da Pós-Graduação Compliance Master da Escola de Negócios (IAG) da PUC-Rio. Professor Convidado da FGV Law Program. 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 Ordem dos Advogados do Brasil (OAB-RJ). Membro do Fórum da Justiça na Era Digital da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Consultor Jurídico do Banco Nacional de Desenvolvimento Econômico e Social (BNDES). Ex-Assessor Sênior da Presidência do BNDES. Ex-Conselheiro de Governança da Autoridade Pública Olímpica (APO).

1. INTRODUÇÃO

Conforme o International Data Corporation[2], os dados digitais criados, replicados e consumidos no mundo no período de um ano dobrarão de tamanho a cada dois anos e, em 2020, alcançarão 44 *zettabytes* (ou 44 trilhões de *gigabytes*). Novos marcos legais e a expansão do universo digital compelem as organizações a rever suas estratégias em relação à guarda e uso da informação. Empresas estão se tornando mais digitais, dependentes das novas tecnologias de comunicação e conectividade, em um cenário caracterizado pela expansão acentuada no volume e na complexidade dos dados. Nessa era do conhecimento, tanto as oportunidades quanto os desafios contemporâneos levam a seguinte pergunta: *como gerar valor para as organizações, a partir do gigantesco universo digital?*[3] Uma solução é investir na governança da informação.

Se a profusão de informação nas organizações propicia um grande potencial de desenvolvimento social e econômico, ela também oferece riscos operacionais e legais que necessitam ser geridos e minorados. É essencial investir em governança para criar estratégias, políticas e procedimentos em torno da distribuição da informação dentro e fora das empresas. Em linhas gerais, a governança da informação é o conjunto de normas, diretrizes e controles de responsabilidade desenvolvidos para assegurar o valor, a qualidade e o *compliance* das informações. Correlacionada a governança corporativa, a governança da informação está estreitamente associada aos princípios da transparência e da prestação de contas (*accountability*), pois tanto consumidores quanto executivos e acionistas 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. Logo se revela a importância de outra indagação presente em todas as corporações nos dias de hoje: *como tratar dados com transparência e segurança jurídica?*

Frequentemente o termo *dados* é empregado como um sinônimo da expressão *informação*, mas há também quem reconheça uma distinção semântica importante[4]. Ao se conceber essa distinção, o vocábulo *dado* ganha uma conotação mais fragmentada, sugerindo uma informação em estado potencial, antes de ser transmitida ou um estado de "pré-informação", anterior à interpretação e a um processo de elaboração, enquanto o termo *informação* alude a algo além da representação contida no dado, sendo capaz, por isso mesmo, de se revestir de sentido instrumental e

[2] INTERNATIONAL DATA CORPORATION. **The digital universe of opportunities**: rich data and the increasing value of the Internet of Things. Amsterdam: IDC, 2014. Disponível em: https://www.iotjournaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf. Acesso em: 20 out. 2022.

[3] FARIA, Fernando de Abreu; SYMPSON, Gladys. 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, 2013, p. 217-241.

[4] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014, p. 61-78.

fornecer conteúdo voltado a redução de incertezas. De qualquer maneira, em busca de um método para o tratamento de dados com transparência e segurança jurídica, é preciso ter em conta todo o ciclo de vida dos dados, significa dizer que a organização deve ser capaz de assegurar o valor, a qualidade e o *compliance* dos dados ou informações necessárias **à**s suas atividades ao longo do tempo, desde o momento da decisão em tratar determinado dado ou informação até quando da escolha em se eliminar certo dado ou informação de seus arquivos.

Consequentemente, cabe indagar quais são as melhores táticas para fazer avançar uma agenda de governança da informação, especialmente uma vez que não existe algo como uma receita única de sistema de governança ou de sistema de *compliance*[5].

Este artigo sugere um caminho que favoreça a busca dessa resposta, a partir de alguns marcos legais brasileiros e critérios objetivos que possam ser seguidos por empresas na governança de suas informações, em especial em coleta, tratamento, armazenamento e eliminação de documentos e dados. Em vista disso, são sugeridas quais as lógicas reitoras das políticas corporativas voltadas a essa modalidade de governança, no âmbito da transparência e da segurança da informação e são consideradas algumas de suas principais diretrizes, controles e responsabilidades.

Propõe-se que a governança da informação seja apreciada pelos elementos da transparência e da segurança da informação e são destacadas algumas medidas e práticas que podem favorecer seu avanço em nosso país, a partir de instrumentos legais específicos.

2. A LÓGICA DA *ACCOUNTABILITY*: INFORMAÇÕES TRANSPARENTES

Escândalos de corrupção e crises reputacionais, vazamentos de dados de consumidores, precarização dos serviços contratados e quebras de justas expectativas levam a um descontentamento generalizado com as corporações. As demandas por mais *accountability* desafiam as empresas. A *accountability* corporativa é um princípio fundamental, por meio do qual administradores e controladores prestam contas de suas ações aos cidadãos e ao mercado e podem ter seu comportamento autorizado, chancelado ou simplesmente sofrerem sanções em caso de mau desempenho, ineficiência, corrupção ou arbitrariedade no uso do poder econômico.

Há enormes variações no que se entende e no que implica a *accountability*. A *accountability* é ainda um conceito em evolução[6], o qual comporta uma nova reflexão sobre a ordem empresarial e um princípio de organização das relações entre

[5] MENZEL, Donald. Research on ethics and integrity in governance: a review and assessment. **Public Integrity**, New York, NY, v. 7, n. 2, p. 147-168, mar. 2005. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10999922.2005.11051272. Acesso em: 20 out. 2022.

[6] 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, fev./abr. 1990.

proprietários e não proprietários. Nessa evolução, vale observar que tal termo não parece se esgotar nas preocupações da administração tradicional, numa *accountability* de processos, restrita ao exame da conformidade das leis e normas procedimentais, a partir de um ponto de vista hierárquico e comprometido apenas com resultados operacionais, sem considerações adicionais.

Numa acepção mais abrangente, tal termo alude à responsabilidade perante alguém, a uma obrigação dos administradores ou controladores a explicarem e justificarem suas ações[7] – por exemplo, como mandatos e contratos foram tratados, como a autoridade e os recursos corporativos foram aplicados, e quais foram os resultados empresariais e seus impactos na sociedade e no meio ambiente.

Mais especificamente, a lógica da *accountability* corporativa corresponde a uma série de mecanismos pelos quais os agentes privados são obrigados a prestar contas por seu desempenho e suas atividades em relação aos cidadãos. Essa lógica demanda uma interação qualificada empresa-sociedade, baseada em: transparência, imputabilidade, controle, responsabilidade e responsividade[8] e dever de justificativa – *answerability*[9], similar a lógica da *accountability* pública.

Ao compreender essa lógica de uma interação mais qualificada, a definição clássica de O'Donnell de *accountabililty pública* horizontal para definir as relações entre atores nas diversas esferas de poder, sem a ideia de hierarquia e *accountabililty* vertical, para identificar a relação principal-agente ou mandante-mandatário, pela qual o titular originário das prerrogativas relacionadas ao exercício do poder as transfere para representantes dele incumbidos, se afigura insuficiente também na esfera privada. Assim, o controle do poder corporativo e de sua prestação de contas demanda uma mobilização, interlocução e articulação dos mais diversos atores públicos e privados na produção, no tratamento e na 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 *accountabililty* empresarial 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* desenvolvidos para assegurar *o valor,*

---

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

[8] KOPPELL, Jonathan. Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". **Public Administration Review**, Washington, DC, v. 65, n. 1, p. 94-108, jan./fev. 2005.

[9] SCHEDLER, Andreas Georg. Conceptualizing accountability. *In*: SCHEDLER, Andreas; DIAMOND, Larry; PLATTNER, Marc (ed.). **The self-restraining state**: power and accountability in new democracies. Boulder, CO: Lynne Rienner, 1999. p. 13-28; FIABANE, Danielle Fabian. **Controle social**: um novo *frame* nos movimentos sociais. 2011. Dissertação (Mestrado em Administração Pública e Governo) – Fundação Getúlio Vargas, São Paulo, 2011.

a qualidade e o compliance das informações. Para tanto, algumas políticas corporativas podem contribuir para o fluxo de informações mais transparentes.

3. POLÍTICAS CORPORATIVAS PARA INFORMAÇÕES MAIS TRANSPARENTES

Afinada com a governança corporativa e a governança de tecnologia da informação, a governança de informação pode assegurar transparência às empresas. Para que organizações privadas possam garantir o valor, a qualidade e o *compliance* de seu ambiente informacional e prosperar, elas devem possuir políticas corporativas transparentes que protejam seus clientes, seu modelo de negócios e preservem sua credibilidade e reputação.

No mundo corporativo, a agenda de governança das grandes empresas abertas, concentrada inicialmente em recuperar o poder de deliberação dos acionistas sobre o destino das empresas, foi uma reação as fragilidades demonstradas pelos casos de corrupção da Enron, WorldCom e Parmalat na década de 1990[10] e evolui para o campo da responsabilidade social corporativa, para além dos requisitos legais, principalmente naquelas empresas multinacionais, como tentativa de contrapor o vácuo regulatório na governança global[11]. A globalização de negócios, que afeta tanto as grandes quanto as pequenas e médias empresas, trouxe oportunidades de expansão e uma grande variedade de riscos regionais; não só as fraudes corporativas ainda experimentam tendência de alta, como muitos executivos evitam investir em determinados países em função desses riscos[12].

As boas práticas de governança corporativa, aí incluída a governança das informações, convertem princípios básicos em recomendações objetivas, a fim de preservar e otimizar o valor econômico de longo prazo da organização empresarial, envolvendo o relacionamento entre proprietários e não proprietários, com a facilitação de acesso a recursos, melhoria da qualidade da gestão da organização e contribuindo

[10] FONTES FILHO, Joaquim Rubens. O conceito e a prática de governança corporativa. *In*: VENTURA, Elvira Cruvinel Ferreira; FONTES FILHO, Joaquim Rubens; SOARES, Marden Marques (coord.). **Governança cooperativa**: diretrizes e mecanismos para fortalecimento da governança em cooperativas de crédito. Brasília, DF: Banco Central do Brasil, 2009, p. 31-48. Disponível em: https://www.bcb.gov.br/Pre/microFinancas/coopcar/pdf/livro_governanca_cooperativa_internet.pdf. Acesso em: 20 out. 2022.

[11] SCHERER, Andreas Georg; PALAZZO, Guido. The new political role of business in a globalized world: a review of a new perspective on CRS and its implications for the firm, governance and democracy. **Journal of Management Studies**, London, v. 48, n. 4, p. 899-931, Jun. 2011. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1467-6486.2010.00950.x. Acesso em: 20 out. 2022.

[12] KROLL. **Anti-bribery and corruption benchmarking report 2017**. New York, NY: Kroll, 2017. Disponível em: https://www.kroll.com/en/insights/publications/anti-bribery-and-corruption-benchmarking-report-2017. Acesso em: 20 out. 2022.

para sua longevidade e seu bem comum[13]. Assim, no âmbito empresarial, a governança das informações legitima a ação das empresas, ao incluir a transparência das informações nas políticas públicas.

De acordo com o Código das Melhores Práticas do Instituto Brasileiro Governança Corporativa[14], o princípio da transparência consiste na *decisão* de disponibilizar para as partes interessadas as informações que sejam de seu interesse, e não apenas aquelas impostas por disposições de leis ou regulamentos. Com base nesse princípio, tais informações não devem se restringir ao desempenho econômico-financeiro, abarcando também os elementos extra financeiros e os ativos intangíveis das empresas, de modo a preservar e otimizar o *valor* da organização. A transparência empresarial não se esgota no *compliance* operacional do cumprimento de obrigações de fornecimento de informações exigidas legalmente, também conhecido como *estar em compliance*, mas pode ser ampliada numa política corporativa estratégica de governança, direcionada para *ser compliance*, alinhada a princípios e comportamentos éticos[15]. A estratégia voltada ao *ser compliance* pode conferir mais *qualidade* às informações e preservar e agregar mais *valor* à organização empresarial, especialmente quando associada aos demais princípios básicos consagrados no âmbito do Código do IBGC.

Ainda no Código, tanto o preceito da transparência quanto os demais princípios básicos – equidade, prestação de contas e responsabilidade corporativa – procuram redirecionar as atividades das sociedades empresárias de forma responsável e sustentável, a fim de compatibilizar lucro e função social, mitigando externalidade negativas e potencializando as positivas em benefícios de todas as partes interessadas. Mais detidamente, o princípio da prestação de contas, bem entendido no âmbito mais amplo da *accountability*, no campo do setor privado, recomenda que os agentes de governança devem revelar de modo claro, conciso, compreensivo e tempestivo os motivos e os resultados de suas decisões corporativas, assumindo as consequências de seus atos ou omissões. Não por acaso, o princípio da equidade, caracterizado pelo dever de tratamento justo de todos os sócios e partes interessadas pelos administradores e o princípio da responsabilidade corporativa, qualificado pelo dever de zelo pela viabilidade econômico-financeira das organizações em bases sustentáveis, ao longo do tempo, são comunicados ao mercado por meio de informações transparentes. Tudo isso somado, compreende-se melhor por que só uma política corporativa de governança de informação transparente pode comunicar de modo efetivo

[13] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo: IBGC, 2015.

[14] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Compliance **à luz da governança corporativa**. São Paulo: IBGC, 2017. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=23486. Acesso em: 20 out. 2022.

[15] Ibidem.

a dinâmica de geração de valor das empresas, seus programas de integridade e seus compromissos éticos.

Em harmonia com esses princípios, Adam e Lachman[16] discernem características especiais das informações transparentes para a garantia de práticas de mercado equitativas: a) relevância, amplitude e fidedignidade dos dados; b) acesso fácil e linguagem simples e direta dos dados; c) agilidade na transmissão dos dados. Essas características podem ser sintetizadas no relato integrado.

O relato integrado visa promover uma abordagem mais coesa e eficiente ao processo de elaboração de relatos corporativos, visando melhorar a qualidade da informação disponível aos investidores. O objetivo principal de um relatório integrado é explicar aos provedores de capital financeiro como uma organização gera valor ao longo do tempo e, portanto, beneficia todas as partes que estejam interessadas na capacidade que uma organização tem de gerar valor, incluindo empregados, clientes, fornecedores, parceiros comerciais, comunidades locais, legisladores, reguladores e formuladores de políticas. Isto é possível, pois tal relato pretende explicar: a) quais são os recursos e os relacionamentos utilizados e afetados por uma organização; e b) como uma organização interage com o ambiente externo e como ela é gera valor no curto, médio e longo prazos com seus capitais.

Por tudo isso, o relato integrado aumenta a capacidade da organização em produzir informação de qualidade e em comunicar ao mercado como ela gera valor e permite o retorno financeiro aos seus investidores. Isto está relacionado ao valor gerado por uma organização para as partes interessadas e para a sociedade como um todo, por meio de uma ampla gama de atividades, interações e relacionamentos. Quando estes forem relevantes à capacidade de uma organização de gerar valor para si mesma, devem ser incluídos no relatório integrado[17].

Neste momento, as empresas privadas brasileiras não estão legalmente obrigadas a adotar o relato integral, mas talvez exatamente por isso aquelas que o fizerem podem comunicar de forma mais clara seus compromissos éticos. Nada impede o setor privado de avançar nessa agenda e fortalecer sua transparência e *accountability* corporativa.

Políticas corporativas podem favorecer a governança da informação nas empresas sempre que seus administradores incorporem em suas normas os princípios básicos da governança corporativa e forneçam aos seus proprietários, ao mercado e às partes interessadas, em geral, a prestação de contas de seus atos e dos resultados

[16] ADAM, Avshalom Madala; LACHMAN, Ran. The concept of information transparency: a spectrum in four dimensional spaces. **SSRN Papers**, Rochester, Jun. 2009. Disponível em: http://ssrn.com/abstract=1422637. Acesso em: 20 out. 2022.

[17] INTERNATIONAL INTEGRATED REPORTING COUNCIL. **A estrutura internacional para relato integrado**. Brasília, DF: Febraban, 2014. Disponível em: https://integratedreporting.org/wp-content/uploads/2015/03/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-Portugese-final-1.pdf. Acesso em: 20 out. 2022.

de suas atividades, com responsabilidade social (*accountability*), comunicando a capacidade das suas empresas em gerar valor no presente e no futuro. Indo mais além, a governança da informação corporativa terá mais legitimidade e credibilidade se o conjunto de suas normas e diretrizes assegurar a publicação e a disseminação de informações relevantes para o mercado e a sociedade e comunicar de forma clara e objetiva seu compromisso com o desenvolvimento sustentável, permitindo controles de responsabilidade mais efetivos[18].

4. INFORMAÇÕES SEGURAS: A LÓGICA DA CONFIANÇA

Segundo o dilema da confiança[19], explorado por Ovanessoff, Plastino e Faleiro[20], é preciso de confiança para cooperar; entretanto, também é preciso cooperar para ganhar confiança, seja na interação entre agentes públicos, agentes privados ou na interação entre agentes públicos e privados. E, de uma maneira geral, estudos apontam que a maioria dos brasileiros tem dificuldades no estabelecimento de novas relações de confiança[21] e que mesmo as empresas brasileiras 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.

Em pesquisas realizadas nos últimos anos, é revelador notar que nem organizações não governamentais (ONGs), empresas, mídia ou governo[22] alcançaram níveis satisfatórios de confiança entre os brasileiros. As ONGs e as empresas ao menos não despertaram a desconfiança entre os brasileiros, contudo a mídia e o governo não merecerem a confiança dos brasileiros. Essas pesquisas ainda revelaram que os brasileiros consideram suas fontes oficiais suspeitas. A maioria dos consultados considerou

[18] MOTA FILHO, Humberto Eustáquio César. *Compliance* e transparência: programas de integridade efetivos. *In*: CARNEIRO, Cláudio; MOTA FILHO, Humberto Eustáquio César (org.). Compliance: o estado da arte (regulações, práticas, experiências e propostas para o avanço da cultura da integridade no Brasil e no mundo). Curitiba: Instituto Memória, 2019, p. 69-85.

[19] MOTA FILHO, Humberto Eustáquio César. Como manter um ambiente ético nas empresas? A agenda positiva de governança e *compliance*. **Compliance Rio**, Rio de Janeiro, v. 1, n. 1, p. 30-37, out. 2018.

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

[21] CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. Retratos da sociedade brasileira: confiança interpessoal. **Indicadores CNI**, Brasília, DF, v. 6, n. 39, p. 1-3, jul. 2017. Disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/observatorio-nacional-da-familia/RetratosdaSociedadeBrasileiraConfianainterpessoal.pdf. Acesso em: 20 out. 2022.

[22] EDELMAN, Daniel. **Edelman trust barometer**: trust and the CEO: annual global study. Chicago, IL: Edelman, 2017. Disponível em: https://www.edelman.com/trust/2017-trust-barometer. Acesso em: 20 out. 2022.

que os indivíduos são mais confiáveis que as instituições e que as informações vazadas têm mais credibilidade que os comunicados das companhias para a imprensa.

Ainda que essa crise de confiança seja global, a chamada *era da economia da reputação*[23] parece intensificar suas consequências no ambiente empresarial brasileiro. Nessa nova economia da reputação, 84% do valor de mercado de uma empresa listada no S&P 500 dos EUA estão atrelados 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[24]. Sem sombra de dúvida, no meio empresarial a confiança é um ativo valioso e a falta de ética é um passivo fatal, 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 corporativa, ou seja, as soluções para o problema da confiança precisam ser legitimadas por uma agenda de mudança dos processos decisórios que incluam a sociedade desde o início das discussões. É preciso retomar níveis de confiança satisfatórios que permitam um ambiente propício ao debate público e ao desenvolvimento de mais negócios e investimentos em nosso país. É fundamental enfrentar o problema da confiança, com o diagnóstico e com as ferramentas certas.

Para avançar nessa agenda de mudança dos processos decisórios que fortalecem os laços de confiança sociais, a lógica da *accountability* é fundamental, mas não é suficiente. Uma estratégia efetiva para o avanço da governança da informação pede que junto com a transparência das informações esteja também associada sua segurança, assim será possível ganhar a *legitimidade* e a *credibilidade* necessárias para vencer o problema da confiança[25]. Políticas corporativas podem auxiliar a fortalecer a segurança das informações utilizadas pelas organizações.

5. POLÍTICAS CORPORATIVAS PARA INFORMAÇÕES SEGURAS

A informação pode ser entendida como um bem das organizações com finalidades econômicas, na medida em que ela é necessária para o planejamento e a implementação de estratégias empresariais, com a consequente realização dos negócios e a obtenção do lucro. Mas isto é apenas parte da história. Até recentemente, o mercado

[23] FAGUNDES, Suzana. Integridade como novo paradigma da reputação. **Revista de Governança e Compliance da Associação Comercial do Rio de Janeiro**, Rio de Janeiro, v. 1, n. 1, p. 30-34, dez. 2017.

[24] DELOITTE. **2014 global survey on reputation risk**: Reputation@Risk. London: 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: 20 out. 2022.

[25] MOTA FILHO, Humberto Eustáquio César. **Como manter um ambiente ético nas empresas? A agenda positiva de governança e *compliance***, 2018.

tratava os dados coletados como um ativo próprio, a ser livremente utilizado e comercializado por quem deles se apropriasse, sem maiores preocupações. Entretanto, na sociedade do conhecimento, essa perspectiva se alterou. Sob uma ótica mais cuidadosa e consciente da titularidade dos dados pessoais e das potenciais consequências de seu uso indevido houve recentemente uma mudança substancial na regulação do uso de dados pessoais nos negócios empresariais, sintetizada no marco legal da Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, os dados pessoais coletados pelas empresas privadas se revelam claramente como pertencentes às pessoas naturais às quais se referem, de modo que quem coleta os dados deve prestar contas de seu uso a seu titular, seja ele seu consumidor, seu empregado, seu acionista, ou quem quer que seja. Nessa linha, o uso de dados pessoais por empresas deve respeitar as bases legais da nova LGPD, sob pena de imposição de multas pesadas a seus infratores e risco de perdas reputacionais adicionais.

No mundo empresarial, uma estrutura de governança da informação deve atribuir responsabilidades claras pela custódia dos dados e seu fluxo de vida na corporação, integrando as áreas de negócio com as tecnologias existentes e com os projetos de tecnologias futuras, em bases jurídicas seguras. Não há um formato único para tal estrutura. As contingências às quais a organização está exposta, seja na relação com o ambiente externo, seja na conexão com a estrutura organizacional interna, certamente afetam sua configuração estrutural.

Apesar de não haver uma receita única para proteger dados nas organizações privadas, especialistas internacionais sugerem uma estratégia voltada ao desenvolvimento da segurança da informação, baseada na implementação de um conjunto de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*, a fim de assegurar que os objetivos do negócio sejam atendidos. A nova LGPD parece seguir essa mesma estratégia recomendada pelos especialistas[26] – nesse sentido, a segurança da informação compreende técnicas de tecnologia da informação, mas não se esgota nelas.

Pela LGPD, além da boa fé, as atividades de tratamento de dados pessoais devem seguir diversos princípios, dentre os quais se destaca aqui o princípio da segurança[27]. Assim sendo, tanto o controlador, responsável pelas decisões referentes ao tratamento desses dados, quanto o operador, responsável pelo tratamento dos dados em nome do controlador, **são legalmente designados como os agentes de tratamento de dados incumbidos de implementar a** *política* de proteção de dados de sua organização, ao adotarem as medidas de segurança técnicas e administrativas. As medidas técnicas se circunscrevem ao campo da tecnologia da informação, com o

[26] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: tecnologia da informação, técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

[27] Art. 6º, incisos VII, VIII e X da Lei nº 13.709/2018 (BRASIL, 2018c).

uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação, tais como ferramentas de autenticação de acesso a sistemas, recursos de criptografia e segregação de servidores. Já as medidas administrativas englobam medidas gerenciais e jurídicas, tais como as políticas corporativas para a proteção de dados, contratos de confidencialidade e políticas de privacidade[28].

Os *agentes* de tratamento de dados pessoais, no âmbito de suas competências, individualmente ou por meio de órgãos colegiados, poderão formular e implantar regras de boas práticas e de governança que estabeleçam as condições, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento dos dados, além das ações educativas, dos mecanismos internos de supervisão e de mitigação de riscos e de outros aspectos relacionados ao mapeamento e tratamento dos dados pessoais. Essas regras integrarão tanto a política de governança da informação quanto o programa de integridade da empresa, revelarão e documentarão seu grau de comprometimento com a proteção de dados pessoais e eventualmente excluirão ou reduzirão a aplicação das penalidades impostas às empresas pelos incidentes de segurança da informação e seus possíveis danos pela Autoridade Nacional de Proteção de Dados (ANPD)[29].

Ao impor aos agentes de tratamento o dever de adotar medidas de segurança aptas a resguardar os dados pessoais, a LGPD incorpora os mesmos pilares da segurança da informação expressos na Política Nacional de Segurança da Informação (PNSI)[30], assimilando a ideia de que tal segurança é uma questão que vai muito além da tecnologia e representa um verdadeiro desafio de governança e de política corporativa.

É preciso prevenir e ter condições de mitigar os casos de incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares das informações utilizadas pelo setor privado. Vale repetir que o controlador dos dados pessoais tem o dever de comunicar a ocorrência de incidentes de segurança para a ANPD e para o titular dos dados pessoais, sempre que o incidente de segurança "possa acarretar risco ou dano relevante aos titulares", em um prazo razoável. Então, sob a ótica jurídica,

[28] JIMENE, Camilla do Vale. Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 3. ed. São Paulo: Revista dos Tribunais, 2021, p. 339-341.

[29] Parte da inspiração para formular as regras de boas práticas e de governança pelos agentes de segurança pode vir da Norma Técnica ABNT NBR ISO/IEC 27002, da Associação Brasileira de Normas Técnicas, um verdadeiro código de boas práticas e melhores técnicas mundialmente reconhecidas para controles de segurança da informação.

[30] A PNSI instituída no âmbito da administração pública federal, tem por objetivo assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação a nível nacional e abrange os campos da segurança e defesa cibernética, segurança física e proteção de dados organizacionais. (BRASIL, 2018b).

para justificar sua comunicação, o incidente de segurança deve ser capaz de: a) possibilitar a ocorrência de um perigo ou sinistro causador de dano ou prejuízo, suscetível a acarretar a responsabilidade civil na sua reparação e; caso tal incidente se efetive, b) que os impactos negativos ou prejuízos sofridos sejam potencialmente expressivos, ao atingirem bens de ordem econômica ou moral.

No âmbito da LGPD, nem todo e qualquer incidente deve ser comunicado. No caso da perda de um *pen drive*, o furto de um *notebook* ou a interrupção de acesso a um sistema haverá um incidente de segurança do ponto de vista técnico, no âmbito da governança da tecnologia da informação, pois os dados corporativos estarão ameaçados de exposição, entretanto não necessariamente esse incidente será digno de notificação à ANPD ou aos titulares de dados, caso não se revele como uma potencial ameaça de dano aos titulares de dados pessoais, passível de reparação civil. Uma boa governança da informação conjugada com um programa de integridade efetivo deve ser capaz de mapear dentre os potenciais incidentes de segurança de informação aqueles mais relevantes e impactantes para a corporação e para os titulares dos dados pessoais envolvidos e suas possíveis consequências, com a confecção de planos preventivos e de contingência.

Seguindo a lógica da proteção jurídica no tratamento de dados, há regulamentações específicas para atividades intensivas no uso de dados pessoais, como a atividade bancária, com muitos riscos de incidentes de segurança potencialmente relevantes e volumoso tráfego de dados digitais, ao redor do mundo todo, ensejando possíveis danos de grande monta. As instituições financeiras (IFs) devem conhecer seus clientes para avaliar o risco de crédito de seus mutuários na concessão de financiamentos ou para evitar operações de lavagem de dinheiro, por exemplo. Para tanto, tais instituições devem seguir as regulamentações do Banco Central do Brasil, a autoridade responsável pelo sistema financeiro nacional, em especial os normativos que tratam da política de segurança cibernética (PSC) e sobre os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem[31].

Vale notar que essa PSC contempla: a) os procedimentos e os controles adotados para reduzir a vulnerabilidade das IFs aos incidentes; b) os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; c) o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição; e d) os mecanismos para disseminação da cultura de segurança cibernética nas IFs. A PSC vem confirmar que a manutenção da segurança da informação decorre de uma estratégia corporativa e de uma mudança de cultura, e não somente de investimentos em novas tecnologias, e oferece um roteiro para avançar na implementação

[31] Resolução nº 4.658/2018, do Banco Central do Brasil (BRASIL, 2018a).

dessa estratégia baseada no reconhecimento da importância da proteção de dados para a credibilidade do sistema financeiro como um todo, para a estabilidade dos negócios bancários e o desenvolvimento de novos modelos de negócios que favorecem o crescimento dessa atividade econômica.

Nessa linha, a PSC pode servir de inspiração para outros ramos de atividades econômicas que necessitem estar apoiados em sólidas medidas de segurança da informação. Em termos mais gerais, no âmbito da lógica da LGPD e de seus limites rígidos no tratamento de dados pessoais, as medidas de segurança serão mais efetivas quando observadas desde a concepção do produto ou do serviço próprio de cada atividade empresarial. Não por acaso, a LGPD acolhe a ideia de *privacy by design*[32], ou seja, o desenho e o desenvolvimento de novos produtos, serviços ou mesmo modelos de negócios precisam levar em conta a segurança e o sigilo dos dados como um elemento essencial de seus projetos corporativos, desde seu início. Isso permite a adoção de controles mais efetivos, favorece o mapeamento e a auditoria dos riscos e estimula uma mudança organizacional nas empresas com maior respeito à privacidade das pessoas naturais. Mais particularmente, a ideia de *privacy by design* pode assegurar não apenas o cumprimento de parâmetros regulatórios e o *compliance* da proteção de dados, mas servem para direcionar o agente de tratamento de dados rumo a políticas corporativas que efetivamente avaliem os impactos das atividades empresariais nos usuários de seus produtos e serviços e nos terceiros interessados. Tais políticas corporativas poderão transformar os processos de criação, desenvolvimento, aplicação e avaliação de produtos e serviços e, portanto, serão capazes de criar informações com mais *valor* internamente para a organização e externamente para o mercado. Informações mais seguras juridicamente tendem a diminuir a litigiosidade processual e reduzir os riscos reputacionais das atividades empresariais e, desse modo, será possível avaliar os benefícios concretos do avanço da governança da informação em tais empresas.

6. CONCLUSÃO

O emprego das lógicas da *accountability* e dos laços de *confiança* contribui para o tratamento de dados de forma transparente e segura para o setor privado. Os marcos legais e as boas práticas de mercado existentes já servem de guia para a identificação das normas, diretrizes e dos controles de responsabilidade aplicáveis aos dados. A partir daí, é fundamental traçar as estratégias para desenvolver e aplicar políticas corporativas que contribuam para o valor, a qualidade e o *compliance* das informações.

[32] CAVOUKIAN, Ann. **Privacy by design**: the 7 foundational principles. 2011. Ontario: Information and Privacy Commissioner of Ontario, 2011. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 20 out. 2022.

Políticas corporativas serão mais transparentes sempre que seus administradores incorporem em suas normas os princípios básicos da governança corporativa e forneçam aos proprietários, ao mercado e as partes interessadas, em geral, a prestação de contas dos seus atos, com responsabilidade social (*accountability corporativa*), comunicando claramente a capacidade de suas empresas em gerar valor no presente e no futuro. A transparência empresarial não se esgota no *compliance* operacional do cumprimento de obrigações de fornecimento de informações exigidas legalmente, também conhecido como *estar em compliance*, mas pode ser ampliada numa política corporativa estratégica de governança, direcionada para *ser compliance*, alinhada a princípios e comportamentos éticos. A estratégia voltada ao *ser compliance* pode conferir mais *qualidade* às informações e preservar e agregar mais *valor* à organização empresarial.

Políticas corporativas para proteger dados nas organizações privadas demandam uma estratégia voltada ao desenvolvimento da segurança da informação, baseada na implementação de um conjunto de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*, a fim de assegurar que os objetivos do negócio sejam atendidos. A segurança da informação compreende tecnologia, tal como a criptografia, mas não se esgota nelas. Tais políticas englobam além das medidas técnicas, a adoção de medidas administrativas, a fim de prover segurança jurídica em contratos de confidencialidade, políticas de privacidade e na caracterização de incidentes de segurança, por exemplo.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: tecnologia da informação, técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

ADAM, Avshalom Madala; LACHMAN, Ran. The concept of information transparency: a spectrum in four dimensional spaces. **SSRN Papers**, Rochester, jun. 2009. Disponível em: http://ssrn.com/abstract=1422637. Acesso em: 17 set. 2021.

BRASIL. Banco Central. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 26-28, 30 abr. 2018a. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 19 set. 2021.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, *caput*,

inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**: seção 1, Brasília, DF, p. 23, 27 dez. 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 20 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, p. 59, 15 ago. 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 set. 2021.

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, fev./abr. 1990.

CAVOUKIAN, Ann. **Privacy by design**: the 7 foundational principles. 2011. Ontario: Information and Privacy Commissioner of Ontario, 2011. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 20 out. 2022.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. Retratos da sociedade brasileira: confiança interpessoal. **Indicadores CNI**, Brasília, DF, v. 6, n. 39, p. 1-3, jul. 2017. Disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/observatorio-nacional-da-familia/RetratosdaSociedadeBrasileiraConfianainterpessoal.pdf. Acesso em: 20 out. 2022.

DELOITTE. **2014 global survey on reputation risk**: Reputation@Risk. London: 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: 20 out. 2022.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 61-78.

EDELMAN, Daniel. **Edelman trust barometer**: trust and the CEO: annual global study. Chicago, IL: Edelman, 2017. Disponível em: https://www.edelman.com/trust/2017-trust-barometer. Acesso em: 20 out. 2022.

FAGUNDES, Suzana. Integridade como novo paradigma da reputação. **Revista de Governança e Compliance da Associação Comercial do Rio de Janeiro**, Rio de Janeiro, v. 1, n. 1, p. 30-34, dez. 2017.

FARIA, Fernando de Abreu; SYMPSON, Gladys. 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, 2013. p. 217-241.

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

FONTES FILHO, Joaquim Rubens. O conceito e a prática de governança corporativa. *In*: VENTURA, Elvira Cruvinel Ferreira; FONTES FILHO, Joaquim Rubens; SOARES, Marden Marques (coord.). **Governança cooperativa**: diretrizes e mecanismos para fortalecimento da governança em cooperativas de crédito. Brasília, DF: Banco Central do Brasil, 2009. p. 31-48. Disponível em: https://www.bcb.gov.br/Pre/microFinancas/coopcar/pdf/livro_governanca_cooperativa_internet.pdf. Acesso em: 20 out. 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo: IBGC, 2015.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Compliance **à luz da governança corporativa**. São Paulo: IBGC, 2017. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=23486. Acesso em: 20 out. 2022.

INTERNATIONAL DATA CORPORATION. **The digital universe of opportunities**: rich data and the increasing value of the Internet of Things. Amsterdam: IDC, 2014. Disponível em: https://www.iotjournaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf. Acesso em: 19 set. 2021.

INTERNATIONAL INTEGRATED REPORTING COUNCIL. **A estrutura internacional para relato integrado**. Brasília, DF: Febraban, 2014. Disponível em: https://integratedreporting.org/wp-content/uploads/2015/03/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK--Portugese-final-1.pdf. Acesso em: 20 out. 2022.

JIMENE, Camilla do Vale. Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 339-341.

KOPPELL, Jonathan. Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". **Public Administration Review**, Washington, DC, v. 65, n. 1, p. 94-108, jan./fev. 2005.

KROLL. **Anti-bribery and corruption benchmarking report 2017**. New York, NY: Kroll, 2017. Disponível em: https://www.kroll.com/en/insights/publications/anti-bribery--and-corruption-benchmarking-report-2017. Acesso em: 20 set. 2021.

MENZEL, Donald. Research on ethics and integrity in governance: a review and assessment. **Public Integrity**, New York, NY, v. 7, n. 2, p. 147-168, mar. 2005. Disponível em: https://www.researchgate.net/publication/228343411_Research_on_Ethics_and_Integrity_in_Governance_A_Review_and_Assessment. Acesso em: 19 set. 2021.

MOTA FILHO, Humberto Eustáquio César. Como manter um ambiente ético nas empresas? A agenda positiva de governança e *compliance*. **Compliance Rio**, Rio de Janeiro, v. 1, n. 1, p. 30-37, out. 2018.

MOTA FILHO, Humberto Eustáquio César. *Compliance* e transparência: programas de integridade efetivos. *In*: CARNEIRO, Cláudio; MOTA FILHO, Humberto Eustáquio

César (org.). Compliance: o estado da arte (regulações, práticas, experiências e propostas para o avanço da cultura da integridade no Brasil e no mundo). Curitiba: Instituto Memória/Centro de Estudos da Contemporaneidade, 2019. p. 69-85.

OLSEN, Johan P. Accountability **democrática, ordem política e mudança**: explorando processos de *accountability* em uma era de transformação europeia. Tradução de 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.

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

SCHERER, Andreas Georg; PALAZZO, Guido. The new political role of business in a globalized world: a review of a new perspective on CRS and its implications for the firm, governance and democracy. **Journal of Management Studies**, London, v. 48, n. 4, p. 899-931, Jun. 2011. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1467-6486.2010.00950.x. Acesso em: 20 set. 2021.