

**REVISTA SEMESTRAL DE
DIREITO EMPRESARIAL**

Nº 26

Publicação do Departamento de Direito Comercial e do Trabalho
da Faculdade de Direito da Universidade do Estado do Rio de Janeiro

Rio de Janeiro
Janeiro / Junho de 2020

REVISTA SEMESTRAL DE DIREITO EMPRESARIAL

Nº 26 Janeiro/Junho de 2020

Publicação do Departamento de Direito Comercial e do Trabalho da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (Prof. Alexandre Ferreira de Assumpção Alves, Prof. Eduardo Henrique Raymundo Von Adamovich, Prof. Enzo Baiocchi, Prof. Ivan Garcia, Prof. João Batista Berthier Leite Soares, Prof. José Carlos Vaz e Dias, Prof. José Gabriel Assis de Almeida, Prof. Leonardo da Silva Sant'Anna, Prof. Marcelo Leonardo Tavares, Prof. Mauricio Moreira Menezes, Prof. Rodrigo Lychowski e Prof. Sérgio Campinho).

EDITORES: Sérgio Campinho e Mauricio Moreira Menezes.

CONSELHO EDITORIAL: Alexandre Ferreira de Assumpção Alves (UERJ), Ana Frazão (UNB), António José Avelãs Nunes (Universidade de Coimbra), Carmen Tiburcio (UERJ), Fábio Ulhoa Coelho (PUC-SP), Jean E. Kalicki (Georgetown University Law School), John H. Rooney Jr. (University of Miami Law School), Jorge Manuel Coutinho de Abreu (Universidade de Coimbra), José de Oliveira Ascensão (Universidade Clássica de Lisboa), Luiz Edson Fachin (UFPR), Marie-Hélène Monsèrié-Bon (Université des Sciences Sociales de Toulouse), Paulo Fernando Campos Salles de Toledo (USP), Peter-Christian Müller-Graff (Ruprecht-Karls-Universität Heidelberg) e Werner Ebke (Ruprecht-Karls-Universität Heidelberg).

CONSELHO EXECUTIVO: Carlos Martins Neto e Mariana Pinto (coordenadores). Guilherme Vinseiro Martins, Leonardo da Silva Sant'Anna, Livia Ximenes Damasceno, Mariana Campinho, Mariana Pereira, Mauro Teixeira de Faria, Nicholas Furlan Di Biase e Rodrigo Cavalcante Moreira.

PARECERISTAS DESTE NÚMERO: Bruno Valladão Guimarães Ferreira (PUC-Rio), Caroline da Rosa Pinheiro (UFJF), Gerson Branco (UFRGS), José Gabriel Assis de Almeida (UERJ), Fabrício de Souza Oliveira (UFJF), Fernanda Valle Versiani (UFMG), Marcelo Féres (UFMG), Marcelo Lauar Leite (UFERSA), Milena Donato Oliva (UERJ), Pedro Wehrs do Vale Fernandes (UERJ), Samuel Max Gabbay (IFRJ), Sergio Negri (UFJF) e Unie Caminha (UNIFOR).

PATROCINADORES:



ISSN 1983-5264

CIP-Brasil. Catalogação-na-fonte
Sindicato Nacional dos Editores de Livros, RJ.

Revista semestral de direito empresarial. — n° 26 (janeiro/junho 2020)
. — Rio de Janeiro: Renovar, 2007-.

v.

UERJ
Campinho Advogados
Moreira Menezes, Martins Advogados

Semestral

1. Direito — Periódicos brasileiros e estrangeiros.

94-1416.

CDU — 236(104)

* Publicado no segundo semestre de 2021.

ACCOUNTABILITY E DEVIDA DILIGÊNCIA COMO VETORES DA GOVERNANÇA CORPORATIVA NOS MERCADOS RICOS EM DADOS¹

ACCOUNTABILITY AND DUE DILIGENCE AS VECTORS OF CORPORATE GOVERNANCE IN DATA-RICH MARKETS

*José Luiz de Moura Faleiros Júnior**

Resumo: Quando se pensa na governança de dados, o que se pretende destacar é um desdobramento natural da governança corporativa, cujas origens remontam ao século XX e ao início do fenômeno da globalização, em que as empresas passaram a se integrar dinamicamente em transações mais rápidas, exigindo sistematização de processos e o contato pela Rede Mundial de Computadores. A partir dessa premissa, o presente trabalho buscará esclarecer quais são as diretrizes adequadas para a implementação de políticas de proteção de dados pessoais que configurem o que a doutrina chama de governança de dados – considerada mais específica do que a governança corporativa, embora conexa a ela –, especialmente a partir de dois vetores, aqui tomados como hipótese da pesquisa proposta: o primeiro, a *accountability*, desdobrada da compreensão traçada quanto à governança e às boas práticas para a proteção de dados pessoais; a segunda, a devida diligência empresarial (*due diligence*), considerada importante elemento para a completa compreensão do princípio da prevenção. A pesquisa será realizada a partir do método dedutivo, com aportes bibliográficos. Ao final, uma conclusão será apresentada.

¹ Artigo recebido em 09.09.2021 e aceito em 11.10.2021.

* Doutorando em Direito Civil pela Universidade de São Paulo – USP/Largo de São Francisco. Doutorando em Direito, na área de estudo “Direito, Tecnologia e Inovação” pela Universidade Federal de Minas Gerais – UFMG. Mestre e Bacharel em Direito pela Universidade Federal de Uberlândia – UFU. Especialista em Direito Digital, Direito Civil e Empresarial. Advogado. E-mail: jfaleiros@usp.br

Palavras-chave: *Accountability*. Devida diligência. Governança corporativa. Mercados ricos em dados. Governança de dados.

Abstract: When thinking about data governance, what is intended to be highlighted is a natural offshoot of corporate governance, which dates back to the 20th century and the beginning of the phenomenon of globalization, in which companies began to dynamically integrate in faster transactions, demanding systematization of processes and contact by the World Wide Web. Based on this premise, this paper will seek to clarify which are the appropriate guidelines for the implementation of personal data protection policies that configure what the doctrine calls data governance — considered more specific than corporate governance, although connected to it — especially in light of two vectors, taken here as the hypothesis of the proposed research: the first, accountability, which unfolds from the understanding of governance and good practices for the protection of personal data; the second, corporate due diligence, considered an important element for the complete understanding of the principle of prevention. The research will be carried out using the deductive method, with bibliographic contributions. At the end, a conclusion will be presented.

Keywords: Accountability. Due diligence. Corporate governance. Data-rich markets. Data governance.

Sumário: Introdução. 1. Os mercados ricos em dados e sua preponderância na sociedade da informação. 2. *Accountability* como primeiro vetor: governança e boas práticas na proteção de dados pessoais. 3. A devida diligência como segundo vetor: um desdobramento virtuoso do princípio da prevenção. Conclusão.

Introdução.

A evolução da integração computacional e a facilitação do acesso dos cidadãos ao ambiente virtual vêm tornando cada vez

maior o volume de informações que circula pela rede, configurando o que se convencionou chamar de *Big Data*, o que contribui para o aumento dos riscos de responsabilização pela má curadoria de dados pessoais em decorrência do tratamento dispensado às informações coletadas de forma desordenada (cujos maus resultados são previsíveis), a configurar o tratamento irregular descrito no artigo 44, II, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Quando se pensa na governança de dados, o que se pretende destacar é um desdobramento natural da governança corporativa, cujas origens remontam ao século XX e ao início do fenômeno da globalização, em que as empresas passaram a se integrar dinamicamente em transações mais rápidas, exigindo sistematização de processos e o contato pela Rede Mundial de Computadores. Trata-se de reconhecer que as redes não são absolutamente seguras e que não bastam leis que resguardam a privacidade e a proteção de dados pessoais para que se tenha efetiva preservação de direitos.

Há interações de todos os níveis e em todos os segmentos, o que denota exatamente esse aspecto de fluidez da tecnologia e a relevância que este tema tem para a implementação da governança corporativa. Por isso, na sociedade hiperconectada, é preciso ir além da norma, pois já não restam dúvidas do virtuoso papel da governança, pautada em processos e na gestão de riscos relacionados às boas práticas relativas a dados. Nunca se falou tanto em *compliance*, e a principal razão possivelmente é decorrência dessa característica.

A implementação de políticas de governança de dados permite diagnosticar zonas de risco e prevenir responsabilidades quanto à gestão dos dados pessoais, notadamente em face do longo período que se leva até que um marco regulatório específico seja introjetado na sociedade. A partir dessa premissa, o presente trabalho buscará esclarecer quais são as diretrizes adequadas para a implementação de políticas de proteção de dados pessoais que configurem o que a doutrina chama de governança de dados, especialmente, com o objetivo de prevenir demandas e responsabilidades a partir da devida diligên-

cia empresarial (*due diligence*). Com fulcro nessa premissa e no objetivo de tecer considerações mais assertivas sobre o tema, proceder-se-á à análise comparativa, por meio de pesquisa bibliográfica, entre a governança corporativa (mais ampla) e a de dados (mais específica).

A hipótese da pesquisa almejada será estruturada a partir de dois vetores: o primeiro, a *accountability*, desdobrada da compreensão traçada quanto à governança e às boas práticas para a proteção de dados pessoais; a segunda, a devida diligência empresarial (*due diligence*), considerada importante elemento para a completa compreensão do princípio da prevenção. A pesquisa será realizada a partir do método dedutivo, com aportes bibliográficos. Ao final, uma conclusão será apresentada.

1. Os mercados ricos em dados e sua preponderância na sociedade da informação.

Quando os *shareholders* delegam ao administrador o poder de gestão da empresa, entendimentos distintos sobre os melhores procedimentos a serem adotados no zelo quanto ao desenvolvimento corporativo podem conduzir a distorções de interesses de vários outros envolvidos na estrutura corporativa (*stakeholders*). É exatamente isso que a governança corporativa procura superar, explicitando e até mesmo definindo regras cuja observância representa a conformidade (*compliance*) dos membros da corporação² a valores éticos que se introjetam nas rotinas e atividades.

2 Sobre a governança corporativa, Mariana Pargendler destaca seu valor e a proeminência do debate em torno de sua propagação: “Given the prominence of the corporate governance agenda in the academic and public spheres—and its resilience despite variations in the specific issues of the day—further appraisals of its normative implications are badly needed. There are two competing normative justifications for the obsession with corporate governance: whereas the first view is based on the relationship between corporate governance and shareholder value, the second conception assumes a direct effect of corporate governance practices on

Sobre o tema, convém ressaltar que o *compliance* – termo usualmente empregado como um conceito geral – advém do verbo inglês “*to comply*”, que, em tradução livre, sinaliza o ato de agir de acordo com as regras, englobando leis, marcos regulatórios infralegais e normativas internas e externas do mercado ou da própria corporação. Não obstante, algumas empresas focam em regulamentos internos sem alinhá-los com as questões jurídicas pertinentes, em especial aquelas que dizem respeito à inovação e às mudanças propiciadas por transformações no ambiente regulatório.

As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.³

Noutras palavras, pode-se dizer que governança corporativa é um conjunto de estratégias utilizadas para administrar a relação entre os acionistas, gestores, investidores, parceiros e que tem a função de parametrizar a direção estratégica e o desempenho das organizações. Apesar de ser assunto recorrente no século XXI, não se trata de tema muito antigo, com origens históricas que remontam ao famoso ‘Caso Watergate’, mas com estruturação mais recente, já que se considera que a publicação, em 1992, do Relatório Cadbury,

non-shareholder constituencies and social welfare more generally.” PARGENDLER, Mariana. The corporate governance obsession. *The Journal of Corporation Law*, Iowa City, v. 42, n. 2, p. 359-402, 2016, p. 395.

3 De acordo com André Luiz Carvalho da Silva, que cita entendimento adotado pela Comissão de Valores Mobiliários, pode-se conceituar a Governança Corporativa como: “[...] o conjunto de práticas que tem por finalidade melhorar o desempenho de uma companhia ao proteger todas as partes interessadas, por exemplo, investidores, empregados e credores, facilitando o acesso ao capital. Segundo essa definição, a análise das práticas de governança corporativa aplicada ao mercado de capitais envolve principalmente: a transparência, equidade, de tratamento dos acionistas e prestação de contas.” SILVA, André Luiz Carvalho da. *Governança corporativa e decisões financeiras no Brasil*. 2. ed. Rio de Janeiro: Mauad, 2005, p. 15.

foi o marco inicial do tema, sendo este o primeiro ‘código de boas práticas corporativas’.⁴

Por sua vez, a governança de Tecnologia da Informação (TI) contempla o conjunto de políticas, normas, métodos e procedimentos estipulados com a finalidade de permitir à administração o controle da utilização de Tecnologia da Informação, buscando uma eficiente utilização de recursos, minimização de riscos e o apoio aos processos da organização empresarial.⁵ Seu objetivo, portanto, é garantir que o uso da TI agregue valor ao negócio. Para o “*Information Technology Governance Institute*” – ITGI, trata-se de responsabilidade exigível dos executivos e da alta direção/administração,⁶ consistindo em aspectos de liderança, estrutura organizacional e processos que ga-

4 Em 1991, no Reino Unido, foi criado o Comitê Cadbury, presidido por Adrian Cadbury, com o objetivo de delinear os pilares da governança corporativa. As duas principais recomendações do Código eram: (i) que os conselhos de empresas de capital aberto incluíssem pelo menos três diretores não executivos; e (ii) que os cargos de CEO (*Chief Executive Officer*) e Presidente do Conselho dessas empresas deveriam ser ocupados por duas pessoas diferentes.

5 FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. *Implantando a Governança de T.I.: da estratégia à gestão dos processos e serviços*. 2. ed. Rio de Janeiro: Brasport, 2008, p. 23.

6 Partindo da ideia de que a cúpula estratégica da corporação está sujeita a erros, Michael Jensen e William Meckling escreveram seu emblemático artigo “Theory of the firm” (“Teoria da firma”, no português), publicado em 1976, no qual declararam a inexistência do “agente perfeito” em qualquer organização. Nos dizeres dos próprios autores: “While the literature of economics is replete with references to the “theory of the firm,” the material generally subsumed under that heading is not actually a theory of the firm but rather a theory of markets in which firms are important actors. The firm is a “black box” operated so as to meet the relevant marginal conditions with respect to inputs and outputs, thereby maximizing profits, or more accurately, present value. Except for a few recent and tentative steps, however, we have no theory which explains how the conflicting objectives of the individual participants are brought into equilibrium so as to yield this result. The limitations of this black box view of the firm have been cited by Adam Smith and Alfred Marshall, among others. More recently, popular and professional debates over the “social responsibility” of corporations, the separation of ownership and control, and the rash of reviews of the literature on the “theory of the firm” have evidenced continuing concern with these issues.” JENSEN, Michael; MECKLING, William H. Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, Nova York, v. 3, n. 4, p. 305-360, out. 1976, p. 308.

rantam que a área de TI da organização consiga suportar e aprimorar seus objetivos e estratégias.

O foco da governança corporativa é direcionar e monitorar a gestão da instituição⁷ ao passo que o foco da governança de TI é direcionar e monitorar as práticas de uso de TI de uma organização.⁸ É grande aliada da governança corporativa, com papel de destaque na estruturação de diretrizes, responsabilidades, competências e habilidades assumidas pelas organizações, objetivando controlar processos, garantir a segurança das informações, otimizar a utilização de recursos e dar suporte para a tomada de decisões alinhadas com os interesses de *stakeholders*.

Percebe-se que a governança de TI está dentro da governança corporativa, sendo parte indescutível dela neste modelo globalizado das corporações, em que a Internet se tornou instrumento preponderante das relações jurídicas.

Tem as seguintes áreas de foco: (i) estratégia: processos do negócio e os de tecnologia devem trabalhar conjuntamente; (ii) valor: acrescentar inovações ao negócio visando a um diferencial para eficiência e eficácia; (iii) riscos: visualização e gerenciamento de riscos, visando a minimizá-los, é também uma forma de agregar valor; (iv) recursos: neste caso, o papel da governança de TI é garantir que a gestão dos recursos humanos e tecnológicos da empresa seja a mais otimizada possível; (v) desempenho: deve auxiliar a visualizar os resultados do negócio mediante indicadores.⁹

7 Cf. ABREU, Jorge Manuel Coutinho de. *Governança das sociedades comerciais*. Coimbra: Almedina, 2010. p. 7-34; GILSON, Ronald. From corporate law to corporate governance. *ECGI Working Paper Series in Law*, Working Paper n. 324, set. 2016. Disponível em: http://ssrn.com/abstract_id=2819128. Acesso em: 09 set. 2021.

8 SELIG, Gad J.. IT Governance: an integrated framework and roadmap - how to plan, deploy and sustain for improved effectiveness. *Journal of International Technology and Information Management*, San Bernardino, v. 25, n. 1, p. 55-76, 2016, p. 59-60.

9 Pertinente, nesse contexto, a discussão sobre o valor do conhecimento para a corporação, que se inicia com os clássicos escritos de Fritz Machlup – que até mesmo revisitam a “Teoria

Como foi dito, uma nova estrutura econômica, política e cultural surgiu devido ao fenômeno da globalização, que se iniciou com a liberação ampla do comércio exterior e posteriormente foi possível perceber que o foco passou para os mercados financeiros.¹⁰ Porém, apesar de todos os benefícios que a globalização financeira trouxe, incluindo a possibilidade e as facilidades de investir no mercado externo e conquistar novos clientes e investidores, é preciso ressaltar que as realidades são diferentes em cada país. As políticas financeiras das instituições e empresas que atuam nesses mercados nem sempre seguem parâmetros éticos, preocupação social ou respeito aos investidores, podendo gerar enormes discrepâncias e prejuízos a todos aqueles envolvidos nas diversas etapas de exploração de suas atividades.

Nasce, no plano global, uma estrutura de prevalência ampla da governança corporativa catalisada pelas diretrizes da Organização para a Cooperação e Desenvolvimento Econômico – OCDE, inserin-

da Firma”: “In welfare economics, the firm is an imaginary or a typical reactor or initiator with accurate knowledge of his opportunities. Depending on the proposition in question, all combinations are again possible, but in any case, a new requirement is introduced: accurate knowledge of the environmental conditions on the part of all reactors and initiators.” MACHLUP, Fritz. Theories of the firm: marginalist, behavioral, managerial. *American Economic Review*, Pittsburgh, v. 57, n.1, p. 1-33, mar. 1967, p. 27. Ainda sobre o tema, é importante destacar que uma vertente doutrinária foi totalmente construída em torno da reconstrução da teoria em questão, que passou a ser baseada no conhecimento, considerado o recurso estrategicamente mais significativo de uma empresa. Seus proponentes argumentam que, como os recursos baseados em conhecimento são geralmente difíceis de imitar e socialmente complexos, as bases de conhecimento e capacidades heterogêneas entre as empresas são os principais determinantes da vantagem competitiva sustentada e do desempenho corporativo superior. Sobre o tema, conferir GRANT, Robert M. Toward a Knowledge-Based Theory of the Firm. *Strategic Management Journal*, Nova Jersey, v. 17, p. 109-122, jan./mar. 1996; KOGUT, Bruce; ZANDER, Udo. The network as knowledge: generative rules and the emergence of structure. *Strategic Management Journal*, Nova Jersey, v. 21, 2000, p. 405-425.

10 Denotando esta preocupação, Joseph Stiglitz aduz que: “O maior desafio não está apenas nas instituições propriamente ditas, mas nas mentalidades: para que se alcancem os benefícios potenciais da globalização, é necessário cuidar do meio ambiente, garantir que os pobres tenham voz nas decisões que os afetam e promover a democracia e o justo comércio.” STIGLITZ, Joseph E. *A globalização e seus malefícios*. São Paulo: Futura, 2002, p. 265.

do a eficácia horizontal dos direitos humanos no plano das relações econômicas¹¹ em consonância com as políticas de integridade almejadas e suas repercussões.

Sem dúvidas, os princípios orientadores oferecem instruções valiosas para que as corporações exerçam atividades empresariais de forma ética, mitigando os impactos negativos e elevando as expectativas de atendimento aos padrões de *compliance* em sintonia com o arcabouço normativo existente para a definição das políticas e procedimentos de conformidade, integrando o referido rol, dentre outros, os instrumentos internacionais e regionais.¹²

11 Sobre tal tema, Eduardo Saad-Diniz defende a estruturação de uma ‘justiça de transição corporativa’, cuja principal promessa “é justamente o fato de que ela representa a abertura ao diálogo e à participação das empresas, fundamentada em obrigação moral e propósito democrático, na transição e no enfrentamento à ascensão de dinâmicas autoritárias. [...] A um só tempo, a JTC dinamiza a avaliação crítica sobre a desestabilização dos procedimentos democráticos que advêm do setor privado e revê o papel das empresas na sociedade, de tal forma a inspirar iniciativas corporativas inovadoras orientadas à reconstrução social pós-conflito.” SAAD-DINIZ, Eduardo. Justiça de transição corporativa: a nova geração de estudos transicionais. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 167, ano 28, p. 71-128, mai. 2020, p. 117. Comentando a necessidade de compreensão da finalidade da responsabilidade social da empresa, com destaque para o meio ambiente – que é outro vetor importantíssimo dessa transformação de contornos mais amplos –, Renata Albuquerque Lima e Doralúcia Azevedo Rodrigues enfatizam que a “busca pela conscientização das empresas e dos consumidores encontra como obstáculos, no capitalismo, a extrema competitividade e a dificuldade em voltar recursos para a preservação ambiental, mas também é possível observar que a busca pela atuação de grupos empresariais que possuem boa reputação e são responsáveis perante o meio ambiente está entre as atuais preferências do mercado econômico.” LIMA, Renata Albuquerque; RODRIGUES, Doralúcia Azevedo. Os desafios da empresa no século XXI: a conciliação entre a responsabilidade social/ambiental e a atividade lucrativa. *Revista Semestral de Direito Empresarial*, Rio de Janeiro, n. 24, p. 169-195, jan./jun. 2019, p. 195.

12 Analisando as diferenças entre os modelos norte-americano e europeu de governança corporativa, bem como seus reflexos sobre o desenvolvimento da dogmática em torno da matéria, cf. GELTER, Martin. Comparative corporate governance: old and new. *ECGI Working Paper Series in Law*, Working Paper n. 321, jul. 2016. Disponível em: <https://ssrn.com/abstract=2756038>. Acesso em: 09 set. 2021. Ressaltando a importância da luta contra a corrupção e traçando um paralelo entre o Canadá e o Brasil, cf. BOUCHARD, Charlaïne; FÉRES, Marcelo Andrade; ONANA, Édouard. La lutte contre la corruption en droit international et dans les pratiques locales, entre normativisation, effectivité et incohérences: les cas du Québec et du Brésil. In: FORTINI, Cristiana; LARA, Fabiana Teodoro; FÉRES, Marcelo Andrade (Org.). *Estado*

Nos dizeres de Newton De Lucca:

Enfim, ao cabo de todas as reflexões desenvolvidas até aqui, parece-me razoável – e, mais do que razoável, prudente – imaginar-se que a ética empresarial só teria condições de prosperar, efetivamente, se fosse semeada num contexto social e numa época em que os valores mais profundos da dignidade do ser humano estivessem consagrados nas convenções sociais com características jurídicas de costume. Ora, no atual mundo globalizado da economia (...), será que somente o Estado, como fonte exclusiva do direito que é, pode resolver os conflitos de interesses existentes, seja pela disciplina expressa das normas escritas, seja pela interpretação e aplicação das chamadas cláusulas gerais?¹³

Para sistematizar o que se almeja com a governança, criou-se a sigla “GRC”, que tem ganhado peso em todos os estudos relacionados à governança corporativa, à gestão de riscos e ao *compliance*.¹⁴ O “G” representa a governança e se relaciona aos parâmetros de controle, supervisão e gestão de uma companhia, envolvendo análise, organização, metas, processos e objetivos. O “R” trata dos riscos existentes, inerentes ao negócio e outros que possam ocorrer por fatores internos ou externos, envolvendo um trabalho preventivo de mapeamento para que condutas indesejadas não sejam praticadas e desencadeiem eventual responsabilização. O “C” cuida do *compliance* propriamente dito, que está ligado a questões de diversas matérias (não

e empresa: encontros e desencontros em matéria de corrupção e programas de integridade. Belo Horizonte: D’Plácido, 2021, p. 55; 60-76; 113-120.

13 DE LUCCA, Newton. *Da ética geral à ética empresarial*. São Paulo: Quartier Latin, 2009, p. 414.

14 Cf. SOKOL, Daniel D. Cartels, corporate compliance, and what practitioners really think about enforcement. *Antitrust Law Journal*, Gainesville, v. 78, n. 201, p. 201-240, 2012.

apenas financeiras, jurídicas ou contábeis, mas até comportamentais e de posturas). Essa fórmula revela “análise jurídica e técnica que transcende o Direito, impondo um diálogo transversal e interdisciplinar.”¹⁵

No mundo corporativo preponderam, hoje, mercados ricos ou movidos a dados (*data-rich* ou *data-driven markets*¹⁶), o que despertou os olhares de empresas e de diversas organizações para a necessidade do fino trato das informações trocadas por meio da Internet, primando pela prevenção de danos quanto ao incessante fluxo de dados, pois, com o avanço da integração computacional e a facilitação do acesso dos cidadãos à web, torna-se cada vez maior o volume desses fluxos, que podem ser estruturados ou não. A despeito disso, a grande preocupação que surge não diz respeito à quantidade de dados, mas ao tratamento dispensado pelas grandes corporações às informações, pois marcos regulatórios especificamente direcionados à proteção da privacidade e dos dados pessoais passam a lhes impor deveres.

Fala-se, em linhas mais específicas, no atendimento aos ditames dos marcos regulatórios vigentes e especificamente ligados à proteção de dados pessoais, aos serviços, à integração de tecnologias, à segurança da informação e à TI em relação ao próprio negócio. Evidentemente, trata-se de uma disciplina inerente à governança corporativa e que visa ao atendimento das necessidades específicas da presença das Tecnologias de Informação e Comunicação – TICs na empresa, além do controle informacional no ambiente corporativo amplamente considerado.

No Brasil, a proteção aos grandes fluxos de informações é compreendida a partir de um conjunto de leis, composto pelo Marco

15 FALEIROS JÚNIOR, José Luiz de Moura. Notas introdutórias ao compliance digital. *In*: CAMARGO, Coriolano Almeida; CRESPO, Marcelo; CUNHA, Liana; SANTOS, Cleórbete (Coord.). *Direito digital*: novas teses jurídicas. 2. ed. Rio de Janeiro: Lumen Juris, 2019, p. 123.

16 MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. *Reinventing capitalism in the age of Big Data*. Nova York: Basic Books, 2018, p. 87-108.

Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) e pela Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) – apenas para exemplificar.

Segundo Juliano Madalena:

Portanto, para a correta aplicação do direito na internet, é de suma importância a análise da relação jurídica que dialoga com este fenômeno. [...] Por certo, o regime jurídico da internet obedece complexa tarefa interpretativa, exigindo um esforço multidisciplinar que possibilite a extração do conjunto dos fatos para a constituição de uma matéria. Contudo, considerando os aspectos jurídicos que a internet oferece à vida social é possível assentar a existência de uma disciplina particular do direito, que opera criando e balizando regras sociais de direito objetivo e subjetivo.¹⁷

Porém, a existência de regulamentos escritos não esgota o tema, eis que não são raros os exemplos difundidos na mídia sobre contrapontos jurídicos de direitos fundamentais que enfrentam carência de delimitação axiológica quando invocados para dar solução a relações travadas no mundo virtual,¹⁸ principalmente, na hipótese em que tais relações sejam capazes de acarretar danos. Isto não afasta do

17 MADALENA, Juliano. Regulação das fronteiras da Internet: um primeiro passo para uma teoria geral do direito digital. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital: direito privado e Internet*. 4. ed. Indaiatuba: Foco, 2021, p. 186.

18 Segundo van Dijk, essa é a terceira fraqueza da proteção jurídica conferida à privacidade: “The third weakness of legal privacy protection is that it still deals almost exclusively with informational privacy. It is a matter of data protection. However, ICT in general and media networks in particular increasingly enter the areas of relational and physical privacy. As a result, applications such as email, calling line identification, video surveillance with storage of recordings, and all kinds of monitoring of Internet use, are poorly protected.” VAN DIJK, Jan. *The network society*. 2. ed. Londres: Sage Publications, 2006, p. 118-119.

campo de cognição do Direito, contudo, a importância do controle regulatório, como destaca James Beniger: “Cada nova inovação tecnológica estende os processos que sustentam a vida social humana, aumentando, assim, a necessidade de controle e a melhoria da tecnologia de controle.”¹⁹

E, no contexto específico dos dados, os dilemas enfrentados são usualmente de grande complexidade. O aumento dos riscos de responsabilização pela má gestão de dados pessoais em decorrência do tratamento dispensado às informações coletadas de usuários gera problemas de governança na medida em que a inadequada curadoria de dados frequentemente remete a um contexto de previsibilidade de falhas, gerando tratamento irregular de dados pessoais (art. 44, II, LGPD).²⁰

Em suma, a delimitação de políticas adequadas permite identificar zonas de risco para que, antes mesmo da realização do tratamento de dados, se possa prevenir responsabilidades quanto à gestão de dados pessoais. É nesse aspecto que o próprio conceito de ‘tratamento irregular’ definido pela LGPD exsurge, pois o inciso II do artigo 44 da lei descreve exatamente a importância de que os ‘riscos e resultados’ sejam considerados na aferição do mencionado conceito.

Se o avanço da tecnologia representa fenômeno irrefreável e que, certamente, dará o tom da produção normativa no século XXI, além de irradiar efeitos sobre os diversos assuntos pertinentes à vida em sociedade, como a economia, a política e a inclusão social – definindo as bases da chamada sociedade da informação – também será a tecnologia o elemento de maior impacto para a Ciência do Direito,

19 BENIGER, James R. *The control revolution: technological and economic origins of the information society*. Cambridge: Harvard University Press, 1986, p. 434, tradução livre. No original: “Each new technological innovation extends the processes that sustain human social life, thereby increasing the need for control and for improved control technology.”

20 CROOTOFF, Rebecca. The Internet of Torts: expanding civil liability standards to address corporate remote interference. *Duke Law Journal*, Durham, v. 69, p. 583-667, 2019, p. 665.

que deverá se aprimorar para não permitir que a inovação ofusque a capacidade regulatória do Estado.²¹

É nesse cerne que a governança corporativa passa a incidir: com o fito de direcionar e monitorar a gestão de determinada empresa ou instituição, são definidos padrões de conduta adequados; por sua vez, o foco da governança de TI se torna mais categórico, passando a direcionar e monitorar as práticas de uso das TICs em uma organização. E, finalmente, com a constatação de que o elemento central do desenvolvimento tecnológico é, hoje, baseado no *Big Data*, surge a governança de dados:

Extraída do contexto maior da governança corporativa e tangenciando pontos da Governança de TI, a de dados foca em princípios de organização e controle sobre esses insumos essenciais para a produção de informação e conhecimento das empresas. O controle mais estrito e formal de dados não é um desafio surgido nos dias de hoje. Os dados, dentre os insumos corporativos, são aqueles que mais apresentam características de fluidez, perpassam diversos processos e sofrem mais transmutações, pois são trabalhados em diversos pontos do seu ciclo de vida, dando origem a outros, além de nem sempre possuírem uma fonte e um destino claramente formalizados.²²

Trata-se, basicamente, de grande aliada da governança corpo-

21 MARQUES NETO, Floriano de Azevedo. Pensando o controle da atividade de regulação estatal. In: GUERRA, Sérgio (Coord.). *Temas de direito regulatório*. Rio de Janeiro: Freitas Bastos, 2005, p. 202. Comenta: “A atividade regulatória é espécie do gênero atividade administrativa. Mas trata-se de uma espécie bastante peculiar. Como já pude afirmar em outra oportunidade, é na moderna atividade regulatória estatal que melhor se manifesta o novo paradigma de direito administrativo, de caráter menos autoritário e mais consensual, aberto à interlocução com a sociedade e permeado pela participação do administrado.”

22 BARBIERI, Carlos. *Governança de dados*. Rio de Janeiro: Alta Books, 2019, p. 35.

rativa, com papel de destaque na estruturação de diretrizes, responsabilidades, competências e habilidades assumidas pelas organizações e por seus membros com o intuito de controlar processos, garantir a segurança das informações, otimizar a utilização de recursos²³ e dar suporte para a tomada de decisões alinhadas com os interesses definidos na legislação de regência.

A preocupação com a governança corporativa a nível legislativo aportou no Brasil, de forma marcante, no final do Século XX, influenciada pelos seguintes eventos: em 1992, foi editada a Lei de Improbidade Administrativa brasileira (Lei nº 8.429/92); em 1995, foi publicada a “Basileia I”, que definiu regras para o mercado financeiro.²⁴ Já em 1997, foi editada a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, ratificada pelo Brasil e promulgada internamente pelo Decreto nº 3.678/2000; em 1998, foi publicada, no Brasil, a Lei nº 9.613, que definiu os crimes de lavagem e ocultação de bens e criou o COAF; ainda em 1998, foi publicada a Resolução nº 2.554, dispondo sobre a implementação de sistemas de controles internos nas corporações.²⁵

23 Importante destaque deve ser conferido às *boards* nas estruturas de governança corporativa: “The board of directors operates within a system of corporate governance. Governance systems can be roughly grouped according to whether the operation of the company by the board is determined by market forces (outsider control), or by mechanisms within the corporation and by its networks (insider control).” HOPT, Klaus; LEYENS, Patrick C. The structure of the Board of Directors: boards and governance strategies in the US, the UK and Germany. *ECGI Working Paper Series in Law*, Working Paper n. 567, mar. 2021. Disponível em: <https://ssrn.com/abstract=3804717>. Acesso em: 09 set. 2021.

24 FALEIROS JÚNIOR, José Luiz de Moura. *Administração Pública Digital*: proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. Indaiatuba: Foco, 2020, p.111-112.

25 O tema é de grande importância e também inspirou a adesão do Brasil a outros importantes atos multilaterais, como anotam Natália Chaves e Marcelo Féres: “Nas últimas décadas, a luta contra a corrupção assumiu proporções globais. O mundo levantou essa bandeira e muitas foram as convenções editadas sobre a matéria. O Brasil também se engajou nessa causa e tornou-se signatário de vários atos multilaterais, como, por exemplo, a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais In-

Além disso, em 2009, o Banco Central do Brasil publica a Circular nº 3.461, que consolidou todos os normativos relativos às atividades de prevenção à lavagem de dinheiro. Por sua vez, foi promulgada, no ano de 2012, a Lei nº 12.683, com importantes mudanças na lei de lavagem de capitais. Também é importante destacar o advento da Lei de Defesa da Concorrência (Lei nº 12.529/11), da Lei Anticorrupção brasileira (Lei nº 12.846/13) e de seu Decreto regulamentador (Decreto nº 8.420/15).

Devido ao incremento no uso da Internet como ferramenta de comunicação e de interação social, surgiram diversas questões desafiadoras para o Direito, particularmente o Civil e o do Consumidor, uma vez que se verificou a necessidade de regulamentar os direitos,²⁶ deveres e responsabilidades no uso da rede, com atenção às peculiaridades desse ambiente “virtual”.²⁷

ternacionais da Organização para a Cooperação e Desenvolvimento Econômico – OCDE, de 1997 (Decreto n. 3.678/2000); a Convenção Interamericana contra a Corrupção, de 1996 (Decreto n. 4.410/02); e a Convenção das Nações Unidas contra a Corrupção, de 2003 (Decreto n. 5.687/06).” CHAVES, Natália Cristina; FÉRES, Marcelo Andrade. O emprego de tecnologias e inovações no combate à corrupção. *In*: PARENTONI, Leonardo (Coord.); GONTIJO, Bruno Miranda, LIMA, Henrique Cunha Souza (Org.). *Direito, tecnologia e inovação*. Belo Horizonte: D'Plácido, 2020, v. 1, p. 592.

26 Colin Bennett, em importante estudo da década de 1990, sugeriu importante reflexão acerca das peculiaridades da regulação global da proteção de dados: “Data protection is not like environmental protection, in which states might agree on the desirable “level” of toxins in rivers and have a relatively clear and common understanding of what that “level” means. For data protection we can compare the “black letter of the law,” we can observe indicators of the scope of law (manual vs. automated data, public vs. private, etc.), and we can compare and contrast the functions and powers of the policy instruments. But it is fallacious to make inferences about the “level of protection” from the observation of these crude indicators. Any attempt to establish evaluative criteria for assessing performance is fraught with the central difficulty that the goals of data protection are not self-defining. What is needed is a more holistic perspective that sees data protection as a process that involves a wide network of actors (data users, data subjects, and regulators) all engaged in the co-production of data protection. The successful implementation of data protection requires a shift in organizational culture and citizen behavior.” BENNETT, Colin. Convergence revisited: toward a global policy for the protection of personal data? *In*: AGRE, Philip E.; ROTENBERG, Marc (Ed.). *Technology and privacy: the new landscape*. Cambridge: The MIT Press, 1997, p. 119-120.

O desenvolvimento tecnológico mudou sensivelmente o comércio e o mercado mundial, que atualmente se diversifica entre o meio físico e o meio digital, com exemplos variados de empresas que atuam no meio físico com extensão para o ambiente digital e até mesmo de outras que se direcionam exclusivamente para o meio digital.

Nesse contexto, novas diretrizes jurídicas passam a permear os modelos de negócio dessas companhias, que precisam estar atentas à realidade do mercado consumidor e a todas as diversas disciplinas jurídicas que lhes exigem um atuar em conformidade ao Direito.²⁸ É nesse sentido que surge o *compliance*, termo que revela a exigência da atuação conforme à lei e às diversas diretrizes e regulamentações aplicáveis²⁹ e que tem grande impacto quanto à prevenção de

27 Cf. TRUBEK, David. M.; TRUBEK, Louise. G. New governance and legal regulation: complementarity, rivalry or transformation. *University of Wisconsin Legal Studies Research Paper*, Madison, n. 1022, 2006.

28 FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p.706. Com efeito: “Também no *compliance* de dados pessoais o estabelecimento de *organização compatível com o risco da atividade* é elemento fundamental da robustez do programa, conforme estabelece o art. 50, §2º, inciso I, c. Cuida-se de assegurar que a estrutura corporativa será capaz de cumprir as determinações legais (manutenção do registro das operações, elaboração de relatório de impacto, etc.) mediante a adoção de procedimentos especificamente desenhados para as hipóteses de tratamento.”

29 Por toda a complexidade que permeia a regulação específica dos ecossistemas baseados em dados, Rolf Weber e Dominic Staiger propõem um modelo regulatório híbrido: “A hybrid approach to regulating data protection currently presents the best way forward, as it takes the need for clear rules as well as the technological capabilities of various industries into account by enabling them to create their own technological and organizational data protection frameworks that are based on the applicable industry characteristics. Future legislation should encompass five categories, including: - a right-to-know legislation that keeps users informed; - a prohibition legislation which prevents certain types of collection and distribution practices of information; - an IT security legislation that provides for the necessary security standards; - a utilization regulation that restricts the use of personal data having been collected; - a task-force legislation enabling technical community’s efforts to address privacy challenges created by technological shifts.” WEBER, Rolf H.; STAIGER, Dominic. *Transatlantic data protection in practice*. Berlim/Heidelberg: Springer-Verlag, 2017, p. 135.

ilícitos (inclusive no contexto da prevenção às práticas corruptivas no ambiente corporativo).³⁰

Em termos de governança corporativa, a avaliação do próprio negócio, sob os diversos pontos de vista do *compliance*, garante a solidez empresarial, parâmetro imprescindível ao florescimento do negócio. Porém, não se pode reduzir o escopo de atuação da governança a ponto de não contemplar a tecnologia da informação.

É complexo e extremamente aberto o debate doutrinário sobre a natureza da responsabilidade civil definida na LGPD. Parte da doutrina defende que o nexo de imputação remeteria ao risco da atividade em razão da realização do tratamento de dados, por expressa previsão do artigo 42;³¹ outra parcela se posiciona favoravelmente ao reconhecimento da culpa como fator de imputação.³² A despeito de

30 CHAVES, Natália Cristina; FÉRES, Marcelo Andrade. A inteligência artificial e a prevenção de ilícitos no âmbito do *compliance* anticorrupção. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência artificial e direito: ética, regulação e responsabilidade*. São Paulo: Thomson Reuters Brasil, 2019, p. 705. Anotam: “Por óbvio, como tudo na sociedade contemporânea, os mecanismos de *compliance* também envolvem o uso de ferramentas tecnológicas, incluindo sistemas dotados de inteligência artificial. A título exemplificativo, vale registrar que a maior parte das grandes corporações tem informatizado os seus procedimentos internos e desenvolvido *softwares* de gestão, com o objetivo de estabelecer padrões de conduta balizados pelo ordenamento jurídico interno e que não podem ser alterados manualmente pelos funcionários. Com isso, reduz-se a margem de erros e cria-se uma uniformidade no processo que facilita o controle. Sob essa ótica, qualquer ato fora do padrão será acusado pelo sistema, alertando os responsáveis a verificar o ocorrido. Ainda como parte desse controle interno, programas de computador voltados para o monitoramento de riscos também têm merecido especial atenção, na medida em que viabilizam a identificação de potenciais ameaças no exercício da atividade.”

31 Defendendo posição objetivista, conferir, por todos, MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 122; MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, nov. 2019, p. 27 *et seq.*; MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo: Revista dos Tribunais, v. 120, p. 468-486, nov./dez. 2018, p. 473.

32 Defendendo a natureza subjetiva do regime de responsabilidade civil em questão, tem-se, por todos, GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do

qualquer divergência, a governança de dados se revela aspecto importantíssimo, não apenas para as empresas que desenvolvem atividades com extensão ou exclusivamente em meio digital, mas para todas, uma vez que o trato com a tecnologia avança cada vez mais, passando a influenciar todos os modelos de negócio.

Exemplos a serem citados são a proteção de dados pessoais e a segurança da informação, que são duas faces de uma mesma moeda, embora esta esteja conectada aos postulados de confidencialidade, integridade e disponibilidade. Isso porque existem notícias de vazamentos de informações de inúmeros sites e portais criados para atender às mais diversas finalidades. Assim, nesta nova realidade virtual, o acesso a dados de usuários (dados pessoais) ganha relevância ímpar e passa a impor às companhias e organizações um zelo especial pela segurança da informação.

2. *Accountability* como primeiro vetor: governança e boas práticas na proteção de dados pessoais.

A Lei Geral de Proteção de Dados Pessoais é composta de importante rol de onze princípios. Um deles – a boa-fé objetiva³³ – cons-

tratamento de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 231-232; DANTAS BISNETO, Cícero. Dano moral pela violação à legislação de proteção de dados: um estudo de direito comparado entre a LGPD e o RGPD. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (Coord.). *Proteção de dados pessoais na sociedade da informação: entre dados e danos*. Indaiatuba: Foco, 2021, p. 228.

33 Eduardo Tomasevicius Filho destaca que: “A informação transmitida deve ser verdadeira, clara e relevante. Ademais, este dever só impõe a transmissão na medida necessária para reduzir custos de transação elevados. [...] Assim, há um ônus de se informar e um dever de informar que incidem simultaneamente. Para facilitar o cumprimento deste dever, existem ainda o dever de informar para ser informado e o dever de se informar para informar.” TOMASEVICIUS FILHO, Eduardo. *O princípio da boa-fé no direito civil*. São Paulo: Almedina, 2020. p. 486. Conferir, ainda sobre o tema, os apontamentos gerais apresentados em: MARTINS-COSTA, Judith. *A boa-fé no direito privado: critérios para a sua aplicação*. São Paulo: Saraiva Educação,

ta do *caput* do artigo 6º da lei; os outros dez estão listados no rol de incisos do mesmo dispositivo. Nesse momento, cumpre destacar a prevenção (inciso VIII) e a responsabilidade e prestação de contas (inciso X). Tais princípios estão intrinsecamente conectados aos propósitos da já citada cartilha de princípios da OCDE, que, agregada aos demais axiomas de regência da governança, despertou os valores importantíssimos para a estruturação de modelos de proteção “*ex ante*”: (i) *fairness*, compreendido como o senso de justiça e a equidade no tratamento dos acionistas; (ii) *disclosure* ou a transparência nas informações; (iii) *accountability*, a prestação de contas; (iv) *compliance*, o atuar em conformidade, cujo consagrado conceito foi sendo aprimorado pela doutrina especializada, tornando-se o paradigma almejado.

Para o momento, importa ressaltar que alguns desses princípios possuem importante função na compreensão que se pretende traçar quanto ao escopo protetivo da governança de dados na lei. Segundo Cíntia Rosa Pereira de Lima e Kelvin Peroli:

[...] (i) o nexo estrutural (*structural nexus*), entendido como o desenvolvimento de políticas e procedimentos na própria empresa capazes de promover a cultura de conformidade, em seu âmago; (ii) o fluxo de informações (*information flow*) da empresa necessita ser eficiente, no sentido de que o *compliance* deve ser implantado no fluxo de informações do alto comando até os empregados do chão de fábrica, para garantir que a comunicação entre todos, de todos níveis hierárquicos, seja rápida e eficaz; (iii) monitoramento e vigilância (*monitoring and surveillance*), sendo também função do *compliance* o monitoramento do com-

2018. p. 625; SILVA, Michael César. Convergências e assimetrias do princípio da boa-fé objetiva no direito contratual contemporâneo. *Revista Jurídica Luso-Brasileira*, Lisboa, v. 1, 2015, p. 1133-1186.

portamento dos empregados, a fim de garantir a sua adesão às políticas e procedimentos da empresa, o que gera, conseqüentemente, a vigilância, que deve ser minimizada e utilizada apenas para os fins corporativos; (iv) o *enforcement* das políticas, procedimentos e normas de direito, que devem ser direcionados tanto para as atividades que oferecem maior risco de não-conformidade, quanto para as que menos risco oferecem, o que pressupõe, em verdade, a análise e o gerenciamento de riscos efetivos pela empresa.³⁴

O legislador brasileiro, agindo em sintonia com modelos que vêm ganhando espaço noutras legislações,³⁵ previu a governança de dados como uma *faculdade* do agente, dela cuidando especificamente em seus artigos 50 e 51.³⁶ De fato, tudo parece sinalizar que a com-

34 LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. *Direito digital: compliance, regulação e governança*. São Paulo: Quartier Latin, 2019, p. 136.

35 É o caso do regulamento europeu: “The GDPR [Art. 32(2) GDPR; Art. 7(1) Directive 95/46/EC] forces data controllers to mitigate the risk of a potential privacy breach by establishing internal procedures to assess data protection risks of their products and services. Risk assessment provisions encourage data controllers to weigh technical data protection measures against risks faced by data processing activities. These measures must be proportionate to the envisaged risks.” TAMÒ-LARRIEUX, Aurelia. *Designing for privacy and its legal framework: data protection by design and default for the Internet of Things*. Basileia: Springer, 2018, p. 96.

36 “Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar

plexidade técnica dos processos relativos a dados amplia o espectro das atividades de processamento, que deixam de ser equiparáveis a outras atividades geradoras de riscos menores. Nesse contexto, a própria noção de *accountability* passa a congregiar sentidos variados.³⁷ É nesse ponto que se deve destacar a importância da base principiológica da LGPD para a estruturação de novos contornos à civilística tradicional.

Não há dúvidas de que o tratamento desenfreado e massivo dos dados pessoais torna o usuário parte vulnerável de qualquer relação jurídica, visto que, na esmagadora maioria das vezes, esse não terá sequer o conhecimento de que seus dados estão sendo coletados, muito menos de que estão sendo tratados e compartilhados com terceiros para os mais variados fins – e isto acaba se tornando ‘normal’.³⁸ Nesse compasso, violações a diversos direitos dos consumidores, redução da sua capacidade de escolha, discriminações e supres-

programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.”

37 VAN ALSENOY, Brendan. *Data protection law in the EU: roles, responsibilities and liability*. Cambridge: Intersentia, 2019, p. 318.

38 POUNDSTONE, William. *Head in the cloud: why knowing things still matters when facts are so easy to look up*. Nova York: Hachette, 2016, p. 253.

são da privacidade são práticas contumazes (embora espúrias) que se visou a combater com o advento da Lei Geral de Proteção de Dados.

3. A devida diligência como segundo vetor: um desdobramento virtuoso do princípio da prevenção.

A chamada devida diligência (*due diligence*, no inglês) nada mais é que uma auditoria realizada com o objetivo de prevenir responsabilidades (o que se alinha à principiologia mencionada).³⁹ No direito empresarial, trata-se de prática amplamente utilizada para análises de riscos de operações – integrando o contexto da governança corporativa – e compreendendo etapas que partem do pressuposto de que se deve verificar se o negócio está nas condições que o investidor acreditava estar quando da data de apresentação e proposta.

Esta prática é amplamente utilizada nos Estados Unidos da América, notadamente nas aquisições de empresas e na realização de investimentos, o que Luis Henrique Ventura classifica como nada mais, nada menos que uma auditoria empresarial.⁴⁰

Tudo parte de um pressuposto de cooperação entre investidor e vendedor, que, agindo de boa-fé, devem alinhar os procedimentos que irão contribuir para um estudo eficiente sobre as nuances do caso,⁴¹ normalmente compondo-se de cinco etapas principais, que

39 Cf. ROSA, Dirceu Pereira de Santa. A importância da *due diligence* de propriedade intelectual nas reorganizações societárias. *Revista da ABPI*, São Paulo, v. 60, set./out. 2002; LUPION, Ricardo. *Boa-fé objetiva nos contratos empresariais: contornos dogmáticos dos deveres de conduta*. Porto Alegre: Livraria do Advogado, 2011.

40 VENTURA, Luis Henrique. *Contratos Internacionais Empresariais*. Belo Horizonte: Del Rey, 2002, p. 59-60.

41 Cf. ASSI, Marcos. *Gestão de riscos com controles internos: ferramentas, certificações e métodos para garantir a eficiência dos negócios*. São Paulo: Saint Paul, 2012.

podem ser transpostas ao contexto específico da proteção de dados pessoais para reforço das medidas de *accountability*, em reforço ao que prevê o artigo 6º, inciso X, da LGPD, compreendido em conjunto com a prevenção descrita no inciso VIII do mesmo dispositivo e com os elementos do inciso II do artigo 44.

1) Declaração de intenção. Trata-se de estágio inicial que envolve a celebração de um acordo preliminar (conhecido como *engagement letter*),⁴² em que são determinadas as regras da devida diligência por documento que indica normas e temas estratégicos importantes, tanto para o potencial vendedor, quanto para o interessado (usualmente o consumidor, que também pode ser identificado como titular de dados). Também é o documento que contempla aspectos como confidencialidade, direito de preferência no negócio, entre outros. Sendo um acordo que formata uma negociação que se dará entre as partes, não existe como enumerar com precisão o que deve constar neste documento.

2) *Check listing*. Documento que é usualmente preparado para o mapeamento da *due diligence*, listando etapas e ciclos, bem como detalhando as informações que deverão ser disponibilizadas pela possível auditoria. É nesse cerne que passam a ter grande valor

42 Esse tipo de acordo pode contribuir eficazmente para o cumprimento do disposto na alínea “a” do inciso I do §2º do artigo 50 da LGPD, que exige do agente de tratamento de dados que “demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais”. Seu valor também pode ser identificado no contexto do inciso II e do §3º do mesmo dispositivo: “Merece destaque derradeiro, ainda neste campo, o disposto no §3º, que exige a atualização periódica das políticas de governança – o que ressalta a necessidade de auditorias cíclicas e revisões de métodos e procedimentos para a garantia da efetividade indicada no §2º, II, pois, como se disse, o programa somente servira de parâmetro para a avaliação de boa conduta empresarial e para a mitigação de responsabilidades se, reconhecidamente, for efetivo.” MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e compliance. In: LIMA, Cíntia Rosa Pereira de (Coord.). *Comentários à Lei Geral de Proteção de Dados*: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 363.

as normas admitidas pela Associação Brasileira de Normas Técnicas – ABNT:

No caso específico da privacidade e segurança da informação, a ABNT possui uma família específica de normas técnicas, a família 27000, e as principais normas para tratar esse assunto são a ABNT/NBR ISO/IEC 27001, 27002 e 27701. (...) As normas da família ISO/IEC 27000 são normas internacionais que possibilitam às organizações a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), através do estabelecimento de uma Política de Segurança, Controles e Gerenciamento de Riscos. O conjunto de normas ISO/IEC 27000 apresenta os requisitos necessários para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI) em qualquer organização, incluindo métodos de auditoria, métricas, controle e gerenciamento de riscos.⁴³

3) Fornecimento e/ou obtenção das informações. Definido o ponto de partida da averiguação que se pretenda fazer, inicia-se a fase mais árdua da devida diligência, que está relacionada à revisão do conjunto de informações levantadas, bem como à pesquisa e à coleta de dados complementares.

4) Consolidação. É a etapa em que, depois de consolidada a análise dos dados coletados, um extenso relatório é preparado, nos moldes solicitados pela contratante do serviço e seguindo os padrões adotados pelos advogados responsáveis.

43 FONSECA, Fernando; MELLO, Renata Avelar de. Frameworks para privacidade e proteção de dados pessoais. In: CRESPO, Marcelo Xavier de Freitas (Coord.). *Compliance no direito digital*. São Paulo: Thomson Reuters Brasil, 2020, p.113-115.

5) Entrega do relatório final. Corresponde ao relatório que poderá ser utilizado diretamente ou após análise minuciosa sobre a viabilidade da transação. A partir daí, caberá a ambas as partes continuar eventual revisão ou auditoria.

De modo geral, o procedimento de devida diligência revela exatamente a preocupação de uma atuação em conformidade às normas, com o fim de identificar riscos, mitigando-os em possíveis negociações. Nada mais é que uma formatação preventiva do *compliance*, aplicada, via de regra, às incorporações societárias e aos investimentos.

Para qualquer investidor, a possibilidade de demonstrar que agiu nos limites das cautelas minimamente esperadas é um trunfo no momento de afastar ou reduzir sua responsabilização por qualquer evento decorrente do negócio, principalmente, no plano jurídico. Primeiro, porque o valor do investimento pode ser prejudicado por problemas legais ocultos, como proteção insuficiente da propriedade intelectual, inexistência de boas práticas nas relações consumeristas, tributárias e trabalhistas etc.; segundo, porque termos jurídicos podem gerar impacto significativo sobre o capital real de retorno de investimentos de riscos.

Por essa razão, a *due diligence* jurídica abrange aspectos legais e riscos envolvidos nos negócios de uma empresa, incluindo os riscos relativos a possíveis responsabilidades (incluindo resolução de litígios e responsabilidades ambientais) contratos, assistências e outras áreas. Porém, uma vez que seu escopo é amplo e subdividido entre a análise financeira e a jurídica, percebe-se o que o estudo isolado desta última não deve estar dissociado dos aspectos econômicos, pois as normas jurídicas servem para instrumentalizar e viabilizar o mercado, de forma eficaz e justa.

Nessa linha de intelecção, Renato Ventura Ribeiro expõe que:

[...] o dever de diligência exige que o administrador deva estar munido das informações necessá-

rias para tanto, em especial aquelas relevantes e razoavelmente disponíveis. As informações necessárias para a tomada de decisões abrangem tanto a parte legal quanto a negocial, estando incluídas na última conhecimento da situação de mercado, política e produtos da empresa, dificuldades e propostas de soluções.⁴⁴

É importante lembrar que não são raras as legislações que impõem a responsabilização objetiva, particularmente no trato das relações jurídicas desniveladas, o que acaba por gerar uma preocupação ainda maior com *due diligence* para a prevenção de riscos, o que se coaduna com a noção de *accountability* destacada pela dicção do princípio contido no artigo 6º, inciso X, da LGPD. No contexto da governança de dados, este é um cenário sempre presente nas relações entre os agentes de tratamento que lidam com atividades de alto risco (especialmente em mercados robustecidos por aplicações baseadas em *Big Data*), haja vista o amplo controle exercido frente à hipossuficiência técnico-probatória de suas contrapartes, o que acaba acirrando o potencial de responsabilização por inobservância a deveres e rotinas de prevenção que decorrem da devida diligência.

E, evidentemente, esta responsabilização se aguça quando o ilícito diagnosticado envolve a má gestão de dados pessoais dos usuários nas relações de consumo,⁴⁵ o que margeia direitos fundamentais da pessoa, muitas vezes expostos a situações de nítido dano. Isto pode ocorrer, dentre outras hipóteses, pela veiculação de publicidade ilícita - notadamente, enganosa -, pela má utilização de *cookies*⁴⁶ ou pela má gestão de *links*.

44 RIBEIRO, Renato Ventura. *Dever de diligência dos administradores de sociedades*. São Paulo: Quartier Latin, 2006, p. 226-227.

45 Sobre as peculiaridades das relações de consumo levadas a efeito na Internet, conferir SILVA, Michael César; SANTOS, Wellington Fonseca dos. O direito do consumidor nas relações de consumo virtuais. *Revista de Informação Legislativa*, Brasília, ano 49, n. 194, abr./jun. 2012, p.261-281.

Destarte, não é de se olvidar dos riscos que circundam as empresas que fazem coleta de dados pessoais de seus usuários, ainda que sem a finalidade de explorar comercialmente os bancos de dados constituídos a partir dessas coletas, pois os riscos decorrentes do uso inadvertido e abstruso de dados pessoais, com graves implicações para a identificação da não observância aos parâmetros de governança estabelecidos em rotinas de devida diligência.

Conclusão.

Nesse breve ensaio, buscou-se traçar algumas pontuações sobre as origens da governança corporativa e seu aprimoramento até a consolidação da governança de dados, que é desdobramento natural da primeira. Na investigação realizada, pontuou-se que as origens do tema remontam ao Século XX e ao início do fenômeno da globalização, em que interações de todos os níveis e de todos os segmentos

46 Cookies são arquivos de texto gerados durante o acesso a um website que são gravados no disco rígido do computador para serem utilizados pelo navegador, sendo que alguns (cookies temporários) permanecem na memória RAM e são apagados assim que o programa navegador é encerrado, ao passo que outros (cookies permanentes) são gravados no disco rígido quando do término da navegação. Têm por objetivo básico fornecer maior conveniência na utilização da *Internet*, evitando que certos dados precisem ser fornecidos a cada vez que uma página é visitada, e armazenando informações relativas às preferências de um usuário. Para mais detalhes, consultar DENSA, Roberta; DANTAS, Cecília. Notas sobre publicidade digital: cookies e spams. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital: direito privado e Internet*. 4. ed. Indaiatuba: Foco, 2021, p. 694-700. Com efeito, a doutrina ainda sinaliza: “[...] um cookie, dependendo de como é feito, tem o poder de coletar informações do usuário como seu número de IP, o navegador e o sistema operacional que utiliza, o horário em que acessou o site, quais áreas do site que visitou mais vezes, de que outro site seu acesso se originou (caso tenha seguido um link), etc. Apenas a primeira informação das listadas acima já bastaria para marcar a invasão da privacidade do usuário. O número de IP (*Internet Protocol*) está para a *Internet* como a impressão digital está para a identificação de pessoas. O IP fornece o provedor, o navegador e o sistema operacional do usuário, por exemplo. Com o número do IP, pode-se (tendo o conhecimento técnico para tanto) facilmente saber a identidade real e a localização de qualquer um que tenha acessado a *Internet*”. QUEIROZ, Danilo Duarte de. Privacidade na *Internet*. *In*: REINALDO FILHO, Demócrito (Coord.). *Direito da Informática: temas polêmicos*, Bauru: Edipro, 2002, p. 88.

caracterizaram a fluidez da tecnologia e a relevância que esse tema tem para a implementação do *compliance* para o trato dos fluxos de dados.

Com o avanço da integração computacional e a facilitação do acesso dos cidadãos ao ambiente virtual, viu-se que o incremento do volume de informações captadas e trocadas contribuiu e continuará contribuindo para que a atual sociedade da informação avance a um novo paradigma de acirramento de riscos. Nesse contexto, destacou-se a relevância de que bases sólidas – que ultrapassem a própria norma e que envolvam rotinas coerentes com o grau de risco de cada atividade e com a viabilidade de revisões cíclicas e auditorias de dados para adequada curadoria – possam conduzir a uma reformulação do que a doutrina chama de devida diligência (ou *due diligence*, *no original, em inglês*).

O advento de marcos regulatórios é, portanto, o primeiro passo dessa reformulação paradigmática. Não obstante, o papel da devida diligência e da delimitação dos controles internos para o atendimento desses marcos a partir de serviços, da integração de tecnologias, da segurança da informação e do papel da TI em relação ao negócio, é de inegável valor para a consolidação do atendimento às necessidades específicas impostas pela presença da tecnologia e do controle informacional no ambiente corporativo, especialmente, para fins de mitigação da responsabilização pelo mapeamento de riscos e resultados (fatores expressamente contemplados no artigo 44, II, da LGPD para a construção do conceito de tratamento irregular). Os dois vetores apontados na construção da hipótese de pesquisa se mostraram pertinentes e adequados à concreta elucidação dos desafios que permeiam o tema, além de serem importantes elementos para a consolidação de uma cultura de governança e de boas práticas relacionadas a dados. Somente a partir disso é que se avançará virtuosamente rumo à concretização da principiologia de lastro preventivo insculpida na LGPD.

