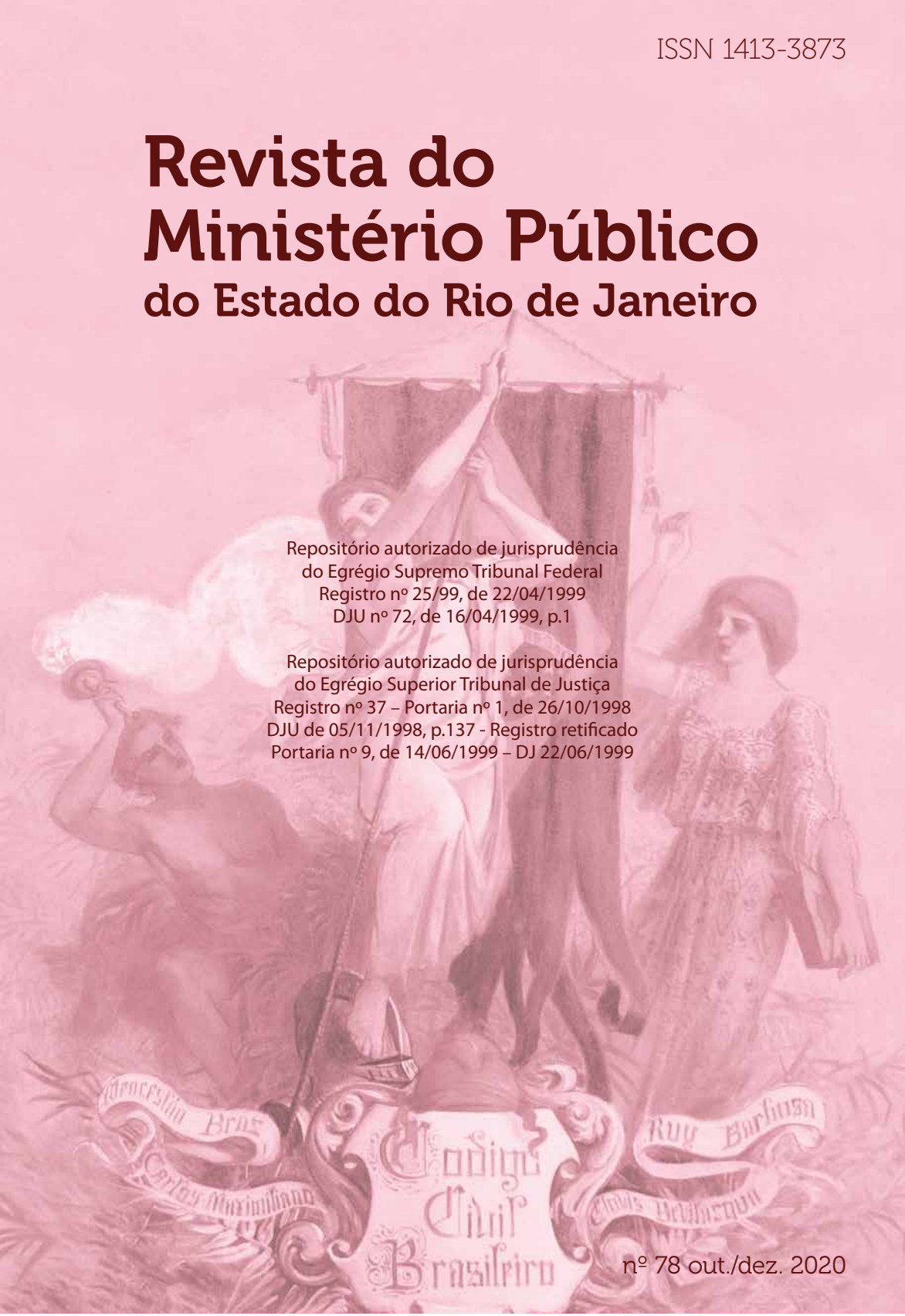
ISSN 1413-3873

Revista do Ministério Público
do Estado do Rio de Janeiro



Repositório autorizado de jurisprudência
do Egrégio Supremo Tribunal Federal
Registro nº 25/99, de 22/04/1999
DJU nº 72, de 16/04/1999, p.1

Repositório autorizado de jurisprudência
do Egrégio Superior Tribunal de Justiça
Registro nº 37 – Portaria nº 1, de 26/10/1998
DJU de 05/11/1998, p.137 - Registro retificado
Portaria nº 9, de 14/06/1999 – DJ 22/06/1999

nº 78 out./dez. 2020

Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais

Guilherme Magalhães Martins*
José Luiz de Moura Faleiros Júnior**

Sumário

1. Introdução

O avanço incessante da inovação fez florescer, há décadas, vasto rol de interessantes desafios que concernem à ciência jurídica devido à dessincronia da atividade legiferante estatal com o potencial transformador da tecnologia.

A chamada "sociedade da informação", vislumbrada desde os idos de 1960, se consolidou em ritmo acelerado nos derradeiros anos do século XX, a ponto de gerar mudanças estruturais na dinâmica das relações interpessoais em todo o planeta. Um lépido cenário de facilidades adveio das promessas de hiperconectividade e comunicação instantânea, rompendo fronteiras territoriais e diferenças culturais para pavimentar o caminho rumo a um novo universo, no qual o substrato mais precioso deixou de ser escasso: a informação, capturada em volumes colossais, nunca antes foi tão desejada e, em verdade, tão relevante para conjecturar o funcionamento de estruturas políticas, econômicas e sociais.

Seu valor intrínseco e individualmente considerado não se alterou. Em conjuntos avultados, todavia, com ricas conexões e pujança interpretativa aplicada a partir de complexas operações algorítmicas, a informação adquiriu *status* inédito. Em razão dessa drástica mudança, há muito já se buscava solução legislativa adequada, capaz de conferir tutela e salvaguardar direitos, mas, ao mesmo tempo, sobrelevar

* Doutor e Mestre em Direito Civil pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro. Membro honorário do Instituto dos Advogados Brasileiros, junto à Comissão de Direito do Consumidor. Professor permanente do Doutorado em Direito, Instituições e Negócios da Universidade Federal Fluminense (UFF). Professor adjunto de Direito Civil da Faculdade Nacional de Direito – Universidade Federal do Rio de Janeiro (UFRJ). Diretor do Instituto Brasileiro de Política e Direito do Consumidor – BRASILCON.

** Mestre em Direito pela Faculdade de Direito da Universidade Federal de Uberlândia (UFU). Especialista em Direito Processual Civil, Direito Civil e Empresarial, Direito Digital e *Compliance* pela Faculdade de Direito Prof. Damásio de Jesus (FDDJ). Professor de cursos preparatórios para a prática advocatícia. Pesquisador do Grupo de Estudos em Direito Digital da Universidade Federal de Uberlândia (UFU). Advogado.

o potencial de controle do Estado nesse novo contexto. Ainda que tardiamente, dezenas de nações passaram a editar marcos regulatórios especificamente voltados à proteção de dados pessoais, e o Brasil não fez diferente.

Na esteira da iniciativa europeia – formalmente nomeada de Regulamento Geral de Proteção de Dados (RGPD) – editada em 27 de abril de 2016 e implementada em 25 de maio de 2018, promulgou-se, no Brasil, a Lei nº 13.709, de 14 de agosto de 2018, já alterada antes mesmo do início de sua vigência pela Medida Provisória nº 869, de 27 de dezembro 2018, posteriormente convertida na Lei nº 13.853, de 08 de julho de 2019, que, entre várias modificações, consolidou a nomenclatura epigrafada no texto atual da norma: "Lei Geral de Proteção de Dados Pessoais (LGPD)".

2. A privacidade transformada em *commodity*

Nunca antes foi tão premente a necessidade de se consolidar a proteção de dados pessoais, uma vez que "o potencial do *Big Data* ultrapassa meras aplicações práticas, pois também torna possível a interpretação de comportamentos humanos"[1].

No atual estado da arte, a tecnologia permite a operabilidade das comunicações entre indivíduos (*person-to-person*, P2P), entre indivíduos e máquinas (*human-to-machine*, H2M) ou entre máquinas (*machine-to-machine*, M2M), em clara sinalização do avanço rumo à "*web* inteligente"[2], marcada pela presença da "Internet das Coisas" (*Internet of Things*, ou *IoT*)[3], que também se situa na fronteira da chamada *web 4.0* ou "Internet de Todas as Coisas" (*Internet of Everything*, ou *IoE*) – é a era dos *zettabytes*![4]

Nesse novo contexto, já se sinaliza, entre outras contingências, que: (i) os sistemas existentes (já complexos) se tornarão mais interconectados e imersos; (ii) as interações dos componentes intra e intersistêmicas aumentarão; (iii) os serviços existentes serão modificados enquanto surgem as oportunidades para novos serviços; (iv) a percepção humana do meio ambiente e da realidade mudará; (v) a escala e o escopo dos problemas de segurança serão bastante ampliados.[5]

Todas essas mudanças se originam da transformação da informação em verdadeira *commodity*, em razão de ser-lhe conferindo valor inédito e contemplativo de uma nova gama de riscos a serem atendidos pela legislação de controle – com efeitos irradiados pelas normas constitucionais –, tendo em vista que, "na dimensão tecnológica, (...), a identidade pessoal parece se dilatar"[6]. Isto conduz à reformulação de vetustas propostas de proteção à privacidade, que passa a ostentar contornos mais

[1] KLOUS, Sander; WIELAARD, Nart. *We are Big Data*: the future of the information society. Amsterdã: Atlantis Press, 2016, p. 12, tradução livre.
[2] FREDETTE, John *et al*. The promise and peril of hyperconnectivity for organizations and societies. *In:* DUTTA, Soumitra; BILBAO-OSORIO, Beñat (Ed.). *The global information technology report 2012*: living in a hyperconnected world. Genebra: Insead; World Economic Forum, 2012, p. 113.
[3] GREENGARD, Samuel. *The internet of things*. Cambridge: The MIT Press, 2015, p. 189.
[4] FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013, p. 5.
[5] LOSKOT, Pavel. Computational security for the IoT and beyond. *In:* HU, Fei (Ed.). *Security and privacy in Internet of Things (IoTs)*: models, algorithms, and implementations. Boca Raton: CRC Press, 2016, p. 357.
[6] RODOTÀ, Stefano. *Il diritto di avere diritti*. Roma/Bari: Laterza, 2012, p. 347, tradução livre.

largos, a indicar a necessidade de uma proteção mais específica, voltada aos dados pessoais[7], e que precisa "valer-se de uma estratégia integrada na qual são utilizados diversos instrumentos de tutela, que representam manifestações específicas em diversas áreas de um mesmo direito"[8].

Em anos recentes, o aprimoramento das diretrizes da Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE) propiciou um importante amadurecimento do tema, denotando nuances fundamentais para a consolidação de legislações voltadas à proteção de dados pessoais em todo o globo.[9] Entretanto, há inúmeras dúvidas que ainda demandam respostas, embora seja certo que a "virada empírica" da técnica para a tecnologia[10] modifica substancialmente a forma com que cada Estado passa a se valer da mera produção legislativa para acompanhar tendências que geram reflexos globais.

O artigo 2° da LGPD brasileira estabelece os fundamentos que a legislação busca alcançar; entre eles, destacam-se a autodeterminação informacional e o livre desenvolvimento da personalidade. O RGPD europeu cita 72 vezes a palavra "consentimento"[11], ao passo que o artigo 7º da lei brasileira lhe confere a natureza de requisito essencial para o tratamento dos dados pessoais. Isso significa que, não sendo o consentimento livre, informado e inequívoco (artigo 5º, XII), a medida se torna ilegal.

Em um contexto no qual os mercados são movimentados por influxos constantes de dados (gerando os chamados *data-rich markets*)[12], a informação se transforma em moeda e a privacidade, no contraponto, em verdadeira *commodity*. O controle desses fluxos passa a demandar atuação preventiva, transpondo modos clássicos de enfrentamento de contingências a partir do atuar repressivo, e inaugura importante viés para a consolidação de novos modelos de operacionalização do poder de polícia estatal. Fala-se em *compliance* ou governança para denotar verdadeira reinserção ética nos procedimentos de segurança da informação adotados para as operações que revolvem à coleta e ao tratamento de dados pessoais.

---

[7] DAVIES, Simon G. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. *In:* AGRE, Philip E.; ROTENBERG, Marc (Ed.) *Technology and privacy*: the new landscape. Cambridge: The MIT Press, 1997, p. 156.

[8] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 409.

[9] BIONI, Bruno R.; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019, p. 800-801.

[10] VERBEEK, Peter-Paul. The technological lifeworld. *In:* ACHTERHUIS, Hans (Ed.). *American philosophy of technology*: the empirical turn. Tradução de Robert P. Crease. Indianapolis: Indiana University Press, 2001, p. 145-146.

[11] EUROPA. *Regulamento Geral de Proteção de Dados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 07 ago. 2019.

[12] MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. *Reinventing capitalism in the age of Big Data*. Nova Iorque: Basic Books, 2018, p. 7.

3. Segurança da informação e governança

Da mesma maneira que a necessidade de criação de novos parâmetros de controle se alinha à revisitação de clássicos institutos jurídicos como a responsabilidade civil e o *jus imperii* estatal, a governança e a boa gestão devem caminhar em comunhão para que esta revigorada metodologia de controle tenha efeitos pragmáticos eficazes. A segurança da informação é o mote pelo qual se desenvolve esta nova temática; desse modo, o chamado *compliance* refuncionaliza a eficácia da própria legislação, não podendo se reduzir a uma mera noção satelitária, uma vez que, ao revés, deve se alçar a um novo patamar.

O artigo 46 da LGPD é categórico ao trabalhar com a exigência de que sejam implementadas medidas voltadas à efetivação de controles de segurança da informação capazes de mitigar os riscos do tratamento de dados. Já o artigo 48 impõe a observância aos deveres de transparência (art. 6º, VI), segurança (art. 6º, VII) e prevenção (art. 6º, VIII), demandando dos agentes de tratamento de dados que atuem em conformidade, em respeito a tais premissas, procedendo de forma colaborativa e diligente na persecução de responsabilidades por eventuais incidentes com dados pessoais – cuja fiscalização passa a ser realizada por agências dotadas de aparelhamento adequado para a garantia de maior efetividade investigatória[13] (no Brasil, isto será feito pela Agência Nacional de Proteção de Dados).

Para citar um exemplo, a transparência surge, nesse contexto, como um dever correlato ou desdobrado do cerne de discussão dessa nova função preventiva. Impõe-se a revelação da ocorrência do evento danoso (que não se confunde com a própria revelação indevida do dado)[14], se transfigurando em atributo atrelado à ética empresarial que deve reinar em todas as etapas de desenvolvimento e implementação dos processos de coleta, tratamento e armazenagem de dados pessoais.

Nota-se, na LGPD, verdadeira tendência à modificação da tradicional judicialização de questões que podem (e devem) ser prevenidas, gerando flexibilidade para os modelos tradicionais da atuação estatal.[15] Caminho diverso se percorreu por ocasião da promulgação do Marco Civil da Internet (Lei nº 12.965/2014), particularmente quanto à redação de seu artigo 19 e à exigência de comando judicial para a remoção de conteúdos ofensivos.[16]

Nota-se, com isso, que a LGPD se compõe de institutos profícuos; a governança classicamente abordada por André-Jean Arnaud[17] ressurge com importância destacada

[13] HUSTINX, Peter. The role of data protection authorities. *In:* GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; TERWANGNE, Cécile de; NOUWT, Sjaak (Ed.). *Reinventing data protection?* Cham/Basileia: Springer, 2009, p. 136.
[14] NORBERG, Patricia A.; HORNE, Daniel R.; HORNE, David A. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, v. 41, nº 1, p. 100-126, 2007, p. 102.
[15] PIERRE, Jon. Governance and institutional flexibility. *In:* LEVI-FAUR, David (Ed.). *The Oxford handbook of governance*. Oxford: Oxford University Press, 2012, *passim*.
[16] MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2ª ed. São Paulo: Revista dos Tribunais, 2014, p. 328-330.
[17] ARNAUD, André-Jean. *La gouvernance*: un outil de participation. Paris: LGDJ, 2014, p. 273-275.

no que diz respeito à coordenação dos agentes de tratamento, de grupos sociais e instituições da iniciativa privada, na ação pública-política voltada à delimitação de objetivos próprios, discutidos e definidos coletivamente, como a elaboração de programas de ação e políticas públicas concertadas e capazes de alcançar tais objetivos, se articula por lógicas divergentes de ação no processo de construção de um consenso organizacional interativo e voltado à solução célere e adequada de contingências.[18]

A motivação e a responsividade que se espera de um arcabouço hígido e eficaz[19] de políticas de integridade devem convergir para prevenir a criação de programas inócuos e cuja existência se manifesta unicamente no papel.[20] Isso revela uma dimensão inexorável da segurança da informação que precisa ser observada para que seja levada a efeito a proteção de dados pessoais.[21] Significa dizer que, para além da tutela da responsabilidade civil pelos danos decorrentes da violação aos deveres de cautela e proteção da segurança dos dados, o legislador cuidou de estabelecer um critério geral de prevenção que deve ser efetivo.

O artigo 50, §1º, da LGPD apresenta extensa lista de requisitos para a aferição da concretude prática de um programa de integridade que, se existente, certamente deverá ser considerado para a delimitação da extensão de eventuais danos e para a apuração de responsabilidades, com possibilidade de mitigação.

A doutrina europeia enumera algumas medidas que, exemplificativamente, podem vir a compor um programa de integridade voltado à proteção de dados pessoais: minimização do processamento de dados pessoais; anonimização; permissibilidade ao monitoramento do tratamento pelo titular; implemento ou incremento de medidas de segurança da informação; a adoção de treinamentos regulares de equipes etc.[22]

Ao se transcender a própria legislação para oportunizar o *compliance*, vê-se surgir vasto rol de novas nuances que somente quem está diretamente atrelado ao tratamento de dados poderá antever e evitar. Nesse compasso, lamenta-se a opção do legislador por trabalhar com essa nova função como mera faculdade.

Na exata medida em que o titular dos dados submetidos a coleta e tratamento deve ser visto como figura hipervulnerável na relação assimétrica de consumo, travada na Internet, surgem determinadas normas especiais para tutelar a peculiaridade de cada grupo passível de sofrer os impactos do tratamento de dados.[23] Dessa forma,

---

[18] ANDERSEN, Kim Viborg. Reengineering public sector organizations using information technology. *In:* HEEKS, Richard. *Reinventing government in the information age*: international practice in IT-enabled public sector reform. Londres: Routledge, 1999, p. 320-324.

[19] MINTZBERG, Henry. *Criando organizações eficazes*: estruturas em cinco configurações. Tradução de Cyro Bernardes. 2ª ed. São Paulo: Atlas, 2003, p. 24 *et seq*.

[20] CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de *compliance*. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 55.

[21] SILVERMAN, Michael G. *Compliance management for public, private, or nonprofit organizations*. Nova Iorque: McGraw Hill, 2008, p. 206.

[22] VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR)*: a practical guide. Basileia: Springer, 2017, 38-40.

[23] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro. Forense, 2019, p 165.

ainda que não se possa considerar que a autodeterminação informacional revele uma absoluta desconexão do controle de dados, ressalta-se a importância da "integridade contextual, alcançada através do equilíbrio harmonioso de regras sociais, ou normas, com valores, fins e propósitos locais e gerais. Isso nunca é uma harmonia estática, no entanto, porque, com o tempo, as condições mudam e os contextos e normas evoluem junto com eles."[24]

4. Considerações finais

Em linhas propedêuticas, buscou-se destacar a importância da Lei Geral de Proteção de Dados Pessoais brasileira para a revisitação de conceitos jurídicos clássicos no novo contexto informacional. A rapidez com que a inovação avança torna o labor estatal mais difícil, haja vista o lapso temporal sempre mais elástico entre o surgimento de uma nova contingência e a apresentação de uma solução adequada para a sua tutela, ainda que outros aparatos normativos preexistentes confiram suficiente salvaguarda jurídica.

É de se ressaltar a boa intenção do legislador brasileiro quanto ao estabelecimento de um marco regulatório que complementa o conjunto normativo para reforçar o contexto de proteção a direitos fundamentais que, por outro lado, não pode nisto se esgotar. Se a privacidade é, nesta nova sociedade da informação, reinterpretada em razão de seu principal corolário, o direito fundamental à proteção de dados pessoais, deve-se primar pelo atingimento do escopo essencial da autodeterminação e das funções do consentimento para a exata compreensão da extensão da proteção conferida aos dados pessoais, que passa pela segurança da informação e pela governança.

O chamado '*compliance*', então, adquire novos contornos, imiscuindo-se aos filtros da reparação civil em cenários específicos que – embora facultativos – mudam toda a dinâmica de aferição de riscos e responsabilidades, sendo importante mecanismo para a atuação de todos os agentes envolvidos em operações de coleta e tratamento de dados, inclusive o Estado, neste novo contexto.

Referências

ANDERSEN, Kim Viborg. Reengineering public sector organizations using information technology. *In:* HEEKS, Richard. *Reinventing government in the information age*: international practice in IT-enabled public sector reform. Londres: Routledge, 1999.

ARNAUD, André-Jean. *La gouvernance*: un outil de participation. Paris: LGDJ, 2014.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro. Forense, 2019.

[24] NISSENBAUM, Helen. *Privacy in context*: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010, p. 231, tradução livre.

_____; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de *compliance*. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

DAVIES, Simon G. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. *In:* AGRE, Philip E.; ROTENBERG, Marc (Ed.). *Technology and privacy*: the new landscape. Cambridge: The MIT Press, 1997.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

EUROPA. *Regulamento Geral de Proteção de Dados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 07 ago. 2019.

FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013.

FREDETTE, John *et al*. The promise and peril of hyperconnectivity for organizations and societies. *In:* DUTTA, Soumitra; BILBAO-OSORIO, Beñat (Ed.). *The global information technology report 2012*: living in a hyperconnected world. Genebra: Insead; World Economic Forum, 2012.

GREENGARD, Samuel. *The internet of things*. Cambridge: The MIT Press, 2015.

HUSTINX, Peter. The role of data protection authorities. *In:* GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; TERWANGNE, Cécile de; NOUWT, Sjaak (Ed.). *Reinventing data protection?* Cham/Basileia: Springer, 2009.

KLOUS, Sander; WIELAARD, Nart. *We are Big Data*: the future of the information society. Amsterdã: Atlantis Press, 2016.

LOSKOT, Pavel. Computational security for the IoT and beyond. *In:* HU, Fei (Ed.). *Security and privacy in Internet of Things (IoTs)*: models, algorithms, and implementations. Boca Raton: CRC Press, 2016.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2ª ed. São Paulo: Revista dos Tribunais, 2014.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. *Reinventing capitalism in the age of Big Data*. Nova Iorque: Basic Books, 2018.

MINTZBERG, Henry. *Criando organizações eficazes*: estruturas em cinco configurações. Tradução de Cyro Bernardes. 2ª ed. São Paulo: Atlas, 2003.

NISSENBAUM, Helen. *Privacy in context*: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NORBERG, Patricia A.; HORNE, Daniel R.; HORNE, David A. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, v. 41, nº 1, p. 100-126, 2007.

PIERRE, Jon. Governance and institutional flexibility. *In:* LEVI-FAUR, David (Ed.). *The Oxford handbook of governance*. Oxford: Oxford University Press, 2012.

RODOTÀ, Stefano. *Il diritto di avere diritti*. Roma/Bari: Laterza, 2012.

SILVERMAN, Michael G. *Compliance management for public, private, or nonprofit organizations*. Nova Iorque: McGraw Hill, 2008.

VERBEEK, Peter-Paul. The technological lifeworld. *In:* ACHTERHUIS, Hans (Ed.). *American philosophy of technology*: the empirical turn. Tradução de Robert P. Crease. Indianapolis: Indiana University Press, 2001.

VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR)*: a practical guide. Basileia: Springer, 2017.