I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

Copyright © 2020 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sudeste - Prof. Dr. César Augusto de Castro Fiuza - UFMG/PUCMG – Minas Gerais
Vice-presidente Nordeste - Prof. Dr. Lucas Gonçalves da Silva - UFS – Sergipe
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Secretário Executivo - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - Unimar/Uninove – São Paulo

Representante Discente – FEPODI
Yuri Nathan da Costa Lannes - Mackenzie – São Paulo

Conselho Fiscal:
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. Aires José Rover - UFSC – Santa Catarina
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP – São Paulo
Prof. Dr. Marcus Firmino Santiago da Silva - UDF – Distrito Federal (suplente)
Prof. Dr. Ilton Garcia da Costa - UENP – São Paulo (suplente)

Secretarias:
Relações Institucionais
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – Santa Catarina
Prof. Dr. Valter Moura do Carmo - UNIMAR – Ceará
Prof. Dr. José Barroso Filho - UPIS/ENAJUM– Distrito Federal
Relações Internacionais para o Continente Americano
Prof. Dr. Fernando Antônio de Carvalho Dantas - UFG – Goías
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Maria Aurea Baroni Cecato - Unipê/UFPB – Paraíba

Eventos:
Prof. Dr. Jerônimo Siqueira Tybusch (UFSM – Rio Grande do Sul)
Prof. Dr. José Filomeno de Moraes Filho (Unifor – Ceará)
Prof. Dr. Antônio Carlos Diniz Murta (Fumec – Minas Gerais)

Comunicação:
Prof. Dr. Matheus Felipe de Castro (UNOESC – Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho (UPF/Univali – Rio Grande do Sul Prof.
Dr. Caio Augusto Souza Lara (ESDHC – Minas Gerais

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP – Pernambuco

---

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: : Danielle Jacon Ayres Pinto; Aires Jose Rover; Fabiano Hartmann Peixoto – Florianópolis: CONPEDI, 2020.

Inclui bibliografia
ISBN: 978-65-5648-086-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O I ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 23 e 30 de junho de 2020, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação. Foi o maior sucesso nesses tempos de pandemia. Mais do que nunca se viu a tecnologia servindo como instrumento de ação no campo do conhecimento e da aprendizagem, o que este GT sempre defendeu e esteve atento discutindo os limites e vantagens dessa utilização. Os artigos apresentados, como não podia deixar de ser, mostraram que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas, em sua sequência de apresentação no sumário e apresentação no GT. No primeiro bloco temático temos:

• marco civil da internet no brasil

• proteção de dados pessoais do trabalhador

• governança de dados aplicada a big data analytics

• consentimento do titular dos dados

• princípios da lei geral de proteção de dados

• blockchain e LGPD

No segundo bloco:

• inteligência artificial, bots e sexismo

• inteligência artificial para melhoria do judiciário

• danos causados por veículos autônomos

• implicações éticas

• direitos da personalidade

• reconhecimento facial

No terceiro bloco:

• Peter Häberlee a democracia digital

• constitucionalismo digital

• inclusão digital e inclusão social

• democracia participativa

No quarto e último bloco:

• deepweb e a (in)segurança dos cidadãos

• criptoativos e soberania tradicional

• fakenews e direito à saúde

• intimações judiciais na internet

• aplicativo uber

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para a leitura na integra dos artigos.

Aires José Rover –UFSC

Fabiano Hartmann Peixoto - Universidade de Brasília

Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota técnica: O artigo intitulado “Marco civil da internet no Brasil: conquistas e desafios” foi indicado pelo PPGD/UNIVEM, nos termos do item 5.1 do edital do Evento.

Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias II apresentados no I Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 8.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

GOVERNANÇA DE DADOS APLICADA A BIG DATA ANALYTICS: A NECESSIDADE DE GESTÃO DOS DADOS EM BIG DATA PARA ALÉM DA LGPD

DATA GOVERNANCE APPLIED TO BIG DATA ANALYTICS: THE NEED FOR DATA MANAGEMENT IN BIG DATA BEYOND THE BRAZILIAN DATA PRIVACY LAW.

Artur Potiguara Carvalho [1]
Fabiano Hartmann Peixoto [2]
Fernanda Potiguara Carvalho [3]

Resumo

Vivemos o paradoxo dos dados, onde, ao mesmo tempo em que queremos a maior transparência das instituições que nos permeiam, tomamos consciência dos riscos gerados com a exposição em massa de informações. Surge a transparência indesejada, oriunda de mecanismos cada vez mais potentes de processamento de dados aliados a ambientes de Big Data. Ambos, mesmo com as limitações trazidas a LGPD, ainda seguem com lacunas preocupantes de regulamentação. A governança surge então como uma alternativa, para o aprimoramento na gestão de dados em Big Data, ao mesmo tempo que proporciona maior transparência dos mecanismos de tratamento de dados.

Palavras-chave: Big data, Governança de dados, Lgpd, Regulação, Big data analytics

Abstract/Resumen/Résumé

We live in the data paradox, where, at the same time that we want greater transparency from the institutions around us, we become aware of the risks generated by the mass exposure of information. Unwanted transparency emerges, arising from increasingly powerful data processing mechanisms combined with Big Data environments. Both, even with the limitations brought by privacy protection law, still with worrying regulatory gaps. Governance then emerges as an alternative for improving data management in Big Data, while providing greater transparency of data processing mechanisms.

Keywords/Palabras-claves/Mots-clés: Big data, Data governance, Data privacy law, Regulation, Big data analytics

---

[1] Mestrando em Engenharia Elétrica pela Universidade de Brasília, Analista de TI do Banco de Brasília S.A.

[2] Doutor em Direito, Professor da Faculdade de Direito e do PPGD-UnB. Líder do Grupo de Pesquisa DR.IA. Coordenador do Projeto Victor e Projeto Mandamus.

[3] Mestranda em Direito pela Universidade de Brasília. Pós-Graduada em Direito Processual Constitucional pela Escola Superior da Magistratura do Estado de Goiás. Analista Judiciária.

1.Introdução

Em um contexto de Estado Democrático de Direito, a transparência e a disponibilização dos dados públicos devem ser fomentadas. Uma restrição a obtenção dessas informações na rede de forma simplificada pode acarretar em privilégio indevido de empresas que disponham de instrumentos de acesso, causando a desigualdade e afetando a livre concorrência. Ou mesmo gerar a inconveniente comercialização de dados que deveriam ser de acesso público.

Por outro lado, se questiona a possibilidade de se exigir uma prestação de contas sobre o uso e a finalidade da obtenção desses dados, através da exigência da governança dos dados, no seu tratamento em contexto de *Big Data Analytics*.

Dessa forma, elegeu-se como problema de pesquisa deste artigo o seguinte questionamento: *"A governança de dados é uma aliada necessária na mitigação da transparência indesejável oriunda de Big Data Analytics?"*

O problema de pesquisa foi dividido em três eixos, que serão respondidos ao longo do artigo, quais sejam:

1) *Há a formação de uma transparência indesejável no tratamento de dados em ambientes de Big Data?*
2) *A LGPD é suficiente para regulamentar o tratamento de dados?*
3) *A transparência indesejável oriunda dos processamentos de Big Data Analytics pode ser mitigada com a governança dos dados?*

A hipótese de pesquisa, por sua vez, é a assertiva de que a governança em contexto de *Big Data* é necessária. O objetivo do artigo é demonstrar os argumentos que nos levaram a essa conclusão.

O dado deve servir à sociedade, e, principalmente quando ele é usado para gerar um banco de dados, o seu uso deve ser fiscalizado. A governança, é, portanto, apontada como uma das formas de se gerir a formação de bancos de dados, e de se exigir a prestação de contas quanto ao seu uso.

A hipótese é de que se trata de uma ferramenta necessária, porque, mesmo com as limitações trazidas pela LGPD principalmente quanto aos dados pessoais, muitas questões ainda ficaram sem respostas. A regulamentação do tratamento dos dados, de forma geral, segue sem balizas claras, dando margem a situações de risco sobre informações de estado e segurança, estratégicas, comerciais, e inclusive pessoais.

A pesquisa propõe como base teórica, o campo dos Estudos Sociais em Ciência e Tecnologia, principalmente os estudos sobre a sociedade de risco.

A metodologia se baseará no levantamento e análise bibliográfica e documental interdisciplinar nas áreas de Direito e Ciência da Informação, além da análise de casos relacionados ao tema de pesquisa. O método de abordagem será o hipotético-dedutivo, e terá como vertente teórico-metodológica predominante a jurídico-dogmática.

2.O Princípio da Transparência, a formação de *Big Data* e a transparência indesejável

Numa era em que dados são disponibilizados na internet, mesmo quem nunca teve contato com ela pode ser afetado. Os efeitos da disposição de dados em redes conectadas extravasam o ambiente virtual, atingindo a vida de milhares de pessoas, ainda que elas nunca tenham acessado a internet.

Em poucas décadas, seria inimaginável a democratização e a velocidade de trocas de informação que se observa hoje. Houve uma progressiva diminuição de custos, principalmente no viés técnico (CONSTANTIOU; KALLINIKOS, 2015, p.3), o que proporcionou o surgimento de enormes bancos de dados em poucos anos, o chamado *Big Data*.

Apesar das divergências, *Big Data* pode ser conceituado como a utilização de novos métodos de domínio da informação para produção de bens ou serviços (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 14).

Em parte, esse cenário de inúmeros dados dispostos na rede foi viabilizado pelas políticas de transparência. De fato, na esteira de tornar transparente a coisa pública, a lei Complementar 131/09, por exemplo, também conhecida como “lei da transparência”, tornou acessível informações sobre a execução orçamentária e financeira do governo, lançando à rede uma grande quantidade de dados que estariam restritos aos órgãos públicos.

Além da exposição dos dados, o compartilhamento deles, tanto dentro do setor público quanto entre o setor público e o privado tiveram uma expansão, a partir do fortalecimento da transparência. Isso fomenta o fluxo de grandes bancos de dados, ou seja, facilita a formação de *Big Data.*

Dentro de órgãos públicos uma medida para aprimoramento desses bancos de dados foi o Decreto Federal nº 8.789/2016, atualmente revogado pelo Decreto nº 10.046, de 2019, o qual previa o compartilhamento de dados entre a administração direta e indireta, ainda que as informações partilhadas não digam respeito diretamente à atividade exercida pela pessoa jurídica que as recebe. O Decreto previa o compartilhamento independentemente de convênios, para facilitar a formação desse grande banco de dados públicos

Um caso de compartilhamento, anterior ao mencionado decreto, deu ensejo à investigação pelo MPDFT (Ministério Público do Distrito Federal e Territórios). Trata-se do suposto pagamento de quantias vultosas pela administração à empresa pública Serpro (Serviço Federal de Processamento de Dados) a fim de adquirir dados, inclusive pessoais, de forma organizada (CRUZ, 2018).

Por sua vez, o compartilhamento de dados entre os setores público e privado ganhou destaque no Acordo de Cooperação Técnica 7/2013 do TSE, que envolveu a tentativa de acordo para compartilhamento de dados entre o Tribunal Superior Eleitoral e o Serasa EXPERIAN, o qual foi interrompido por decisão judicial. (HAIDAR, 2013)

Lessig aborda a questão da aquisição de um caráter econômico dos dados, e da sua utilização como mecanismo de controle: "Sua natureza é o seu código, e seu código está mudando de uma posição que desabilitava o controle para uma outra, que permitirá um tipo extraordinário de controle. É o comércio que está fazendo com que isso ocorra; o governo irá ajudar. Antes que isso aconteça, deveríamos decidir se é desse jeito que queremos que as coisas sejam" (LESSIG, 1999, pg. 61).

Nesse sentido, a transparência se torna uma ferramenta ambígua para o uso dos dados na rede.

De um lado, ela é desejada, na medida em que proporciona a democracia. Pela rede, a transparência e a acessibilidade permitem a implementação da mais forte ferramenta de combate a corrupção e desvios legais: a auditoria popular. Permitem ainda diversas outras ferramentas cidadãs, como o acesso ao andamento de um processo; às publicações oficiais, às informações sobre novas política pública; a certidões e informações sobre os próprios dados pessoais, dentre tantas outras possibilidades.

Desse modo, é possível se observar uma mudança substancial no alcance dos dados públicos. Antes, essas informações atingiam um número restrito de pessoas que acompanhava o diário oficial, por exemplo, ou os murais das repartições públicas; ou mesmo que se dispunha a ir presencialmente aos órgãos públicos solicitar informações e certidões. Hoje, através da rede, atingem um número irrestrito de pessoas, dentro e fora do Brasil. A tendência é claramente, o aprofundamento dessa transparência, como já vem ocorrendo com as serventias extrajudiciais[1], e com os diversos esforços para a informatização de sistemas burocráticos, como processos administrativos e judiciais, licitações públicas etc.

[1] A exemplo dos serviços prestados pelo site "Cartório 24 horas" lançado pela Associação dos Notários e Registradores do Brasil (ANOREG Brasil), que permite, por exemplo, a emissão de segunda via simplificada de certidões. Disponível em: https://www.cartorio24horas.com.br/institucional#infraestrutura

Por outro lado, ao mesmo tempo em que surge essa transparência que fomenta a democracia, há o surgimento de uma transparência não desejável. Isso porque, primeiro, não só dados públicos têm ganhado o espaço no fluxo de dados digitais, mas também dados pessoais.

De inúmeras formas, os cidadãos, ao se inserirem na rede, publicizam seus dados privados, as vezes de forma espontânea. Numa verdadeira sedução do consumo, os clientes repassam seus próprios dados, de forma consciente, em cadastros para uso gratuito de ferramentas, aplicativos, redes sociais, por exemplo.

Outras vezes, os cidadãos deixam seus rastros, imperceptivelmente captados e repassados de máquina a máquina no que se denomina internet das coisas. O termo, criado por Kevin Ashton, é conceituado como a rede, supervisionada ou não, de objetos conectados, programados para agirem por conta própria. (MANCINI, 2018)

Um segundo fator que leva ao surgimento da transparência indesejável é que a informação pública disponibilizada passa a servir a outros propósitos para além de informar e conscientizar a população. Isso acontece porque os dados ganham novos significados à medida que agregados, classificados, valorados, separados dentro das plataformas de *Big Data*. Através do que se denomina *Big Data Analytics*, uma metodologia de análise de dados, é possível instrumentalizar os dados, pessoais ou não, para fins determinados, por exemplo, para a busca de padrões de comportamento de consumidores ou para descoberta de tendência de mercados.

Esses fatores acabam por suscitar discussões acerca dos riscos que envolvem tanto a publicização dos dados, quanto os objetivos desejados em seu tratamento. É o que se abordará a seguir.

3.*Big Data Analytics* e a transparência indesejável

A disponibilização da grande quantidade de dados nas redes possibilita o surgimento de uma transparência indesejável, devido, tanto à publicização de dados pessoais nas redes, gerando violações de privacidade; quanto à utilização dos dados para os objetivos mais variados.

Os dados coletados na rede ficam disponíveis para consultas de forma retroativa, o que faz com que o usuário não tenha dimensão dos impactos que podem ser gerados a partir da sua disponibilização.

Assim, o manejo dos dados pode ser uma eficiente fonte de aquisição, consolidação e exercício de poderes econômicos e políticos. Isso porque até mesmo informações públicas, que isoladamente não teriam potencialidade lesiva, quando combinadas entre si ou com dados

privados, podem dar ensejo a formas de violações que atingem valores democráticos elementares.

Para ilustrar como a combinação de dados pode apontar aspectos muito sensíveis da vida privada dos seus titulares, toma-se por exemplo o estudo denominado MetaPhone promovido pela Universidade de Stanford, através do centro de estudos sobre internet e sociedade da Universidade (MAYER & MUTCHER, 2014). A pesquisa se deu pela análise de metadados coletados por um aplicativo fornecido para os participantes da pesquisa. "Metadados" significa basicamente "dados" sobre "dados". São dados utilizados para identificar outros dados, a fim de se organizar ou gerir essas informações a fim de se descrever pacotes de dados, sem que eles sejam violados. (DIAMANTINI et. Al., 2019, p.305).[2]

O aplicativo coletava apenas informações sobre duração de chamadas, horário de realização e telefone discado. Não eram identificados os participantes da pesquisa, mas apenas os dados coletados por seu aplicativo. Os pesquisadores procederam ao estudo cruzando as informações com a lista pública de telefones para identificar a quem pertenciam os números discados. Através dessa simples análise, foi possível se averiguar que um dos participantes sofria de esclerose múltipla, outro sofria de arritmia; uma das participantes havia realizado um aborto em uma clínica durante a pesquisa e um participante cultivava plantas alucinógenas.

A pesquisa aponta, portanto, que os dados públicos, quando analisados por meio de combinações entre si, ou com dados pessoais, podem resultar em invasões sérias da vida privada do titular.

No entanto, diferente do que pode parecer à primeira vista, há uma grande falha na visão de que o uso de *Big Data Analytics* interfere apenas na proteção da privacidade.

A potencialidade lesiva do uso discriminatório de dados afeta também a isonomia entre os cidadãos, a moralidade das relações comerciais, a livre concorrência de mercado, e até mesmo situações de estratégia de governo e de segurança pública, entre outras.

Exemplos sobre essas possibilidades não faltam. Por exemplo, no que tange às relações comerciais, têm-se o Caso 39749, em que a Comissão Europeia condenou o site de pesquisa Google quanto à acusação de que o site emitia pesquisas direcionadas para influenciar os consumidores em seu comparador de preços.

Desta forma pode-se destacar quatro motivos pelos quais o uso e tratamento ilimitado de dados podem significar riscos, para além da privacidade:

---

[2] Uma das formas de classificação de metadados é o Dubin Core, que recebeu o padrão ISO 15836:2009. Disponível em: http://dublincore.org/metadata-basics/

Em primeiro lugar, porque os dados são fatores econômicos diferenciais, a medida em que proporcionam o oferecimento de produtos e serviços personalizados de acordo com a demanda do cliente. Assim, o monopólio sobre dados pode significar também o monopólio de mercados, já que, segundo Mayer-Schönberger e Cukier, os dados ganharam o valor econômico que tinha a propriedade intelectual, sendo um importante ativo financeiro; um combustível que move a economia da informação. (MAYER-SCHÖNBERGER; CUKIER, 2013).

Em segundo lugar, porque o uso dos dados pode se refletir em aprofundamento de desigualdades sociais, marginalizações e práticas discriminatórias, na medida em que classifiquem usuários a partir de dados considerados sensíveis (como os referentes à raça, cor, sexo, preferência religiosa ou política etc.). Desta forma, a má utilização de dados pode interferir em questões de justiça social.

Em terceiro, porque, através do tratamento de dados em sede de *Big Data Analytics*, os dados governamentais podem revelar bem mais do que "gostariam de dizer", expondo estratégias de Estado, ou mesmo, informações que seriam sigilosas, mas que são dedutíveis através da sobreposição de dados.

E, em quarto lugar destaca-se que nem sempre, os resultados obtidos no tratamento de dados se traduzem em análises verídicas da realidade. Tanto os objetivos que se deseja auferir com o tratamento de dados em *Big Data*, quanto os próprios resultados obtidos, podem gerar informações indesejáveis, indesejadas, e nem sempre verossímeis, posto que abarcam as próprias limitações dos seus programadores e de seus contextos sociais.

Há um mito tecnicista de que as decisões dos engenheiros de software efetivadas nos programas de *Big Data Analytics* são neutras, destacadas da carga social que cerca o profissional. Esse mito, muito criticado pelo advogado americano Lawrence Lessig, tem permitido que os programadores estabeleçam o código como uma lei intangível (LESSIG, 1999), que, obscura, se distancia das leis aplicadas hodiernamente no "mundo real". Segundo o autor, a nova lei é o código, e os novos legisladores os seus programadores. Como afirma o autor, "*Código é lei*, (...) *codifica valores, mesmo assim, espantosamente, muitas pessoas insistem em dizer que código é apenas uma questão de engenharia*". (LESSIG, 1999, pg. 59)

Lessig demonstra uma especial preocupação sobre a transparência desses códigos que, apesar de afetarem diretamente a vida de milhares de cidadãos, permanecem alheios a um processo público transparente de legitimação, e fora das possibilidades de alcance dos mecanismos de revisão constitucional (LESSIG, 1999, pg. 207).

As informações sobre os riscos apresentados, e limitações intrínsecas às próprias ferramentas de tratamento vêm ganhando notoriedade, principalmente após as notícias

mundiais sobre vazamento de dados, e seu uso na influência de comportamentos, notadamente após os processos eleitorais em vários países.

Em decorrência disso, os atores políticos buscam formas de regulamentar o uso de dados e as ferramentas de tratamento.

4. Regulação, Uso e Tratamento de Dados

O debate acerca do poder de influência dos códigos sobre o consumo, opinião pública, soberania e segurança ganhou destaque internacional com as revelações de Edward Snowden, e com o escândalo da Cambridge Analytica, que levantaram importantes questionamentos quanto ao papel da rede no resultado das urnas na eleição presidencial dos Estados Unidos.

Por isso a captação de dados tornou-se extremamente valiosa, afinal, em última análise, combinada a técnicas de *Big Data Analytics*, se reflete em forma moderna de poder e controle. (MENEZES NETO, 2016, p. 121).

Nesse sentido, como fator de poder, o aprimoramento de banco de dados se transforma em instrumento tanto para empresas privadas quanto para os governos. A acumulação perene e desenfreada de dados se tornou cada vez mais vantajosa.

Isso porque permite, conforme mencionado, o uso futuro desses dados em demandas que podem até não ser previsíveis hoje, fazendo com que informações consideradas não "importantes", ganhem significado quando aliadas entre si e a outros fatores. Nesse contexto, inaugura-se uma espécie de "corrida pelos dados", que, ainda desregulamentada, viola direitos e comercializa dados e expõem os cidadãos.

Pela importância que assumem esses dados no contexto de uma *data-driven society* e pela transnacionalidade do assunto, têm crescido as preocupações internacionais quanto a proteção desses dados. Nesse sentido, a Diretiva n. 95/46/CE do Parlamento Europeu, revogada posteriormente pelo Regulamento Geral sobre a Proteção de Dados (RGPD), Regulamento (UE) 2016/679.

No Brasil, além dos mencionados regulamentos de compartilhamento, a lei federal no 12.414/2011 (de consulta a informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito) e o marco civil da internet, lei 12.965/14, tiveram grande importância por promover a abertura ao debate sobre as implicações jurídicas no novo meio digital. Quanto à proteção de dados especificamente, ainda restaram graves lacunas mesmo após essas leis, o que buscou ser sanado a partir da criação da lei específica de Proteção de Dados Pessoais.

A Lei 13.709, aprovada em 14 de agosto de 2018, conhecida por Lei Geral de Proteção de Dados Pessoais-LGPD, contou com participação popular no anteprojeto de lei, promovida pela Secretaria de Assuntos legislativos do Ministério da Justiça, e também com audiências públicas durante sua tramitação.

A previsão é de que a Lei passe a viger em sua integralidade a partir de agosto de 2020. No entanto, ainda no período de *vacatio legis*, a LGPD já sofreu alterações trazidas pela Lei 13.853/2019.

Quanto ao *Big Data*, a lei não menciona expressamente essas bases de dados, mas prevê diretrizes que podem nortear a utilização dessas ferramentas.

Não há uma proibição do armazenamento de grandes massas de dados. Ao contrário, a lei normatiza mecanismos de captação de dados ao superar os entraves que a exigência de livre consentimento do titular poderia trazer.

De fato, o princípio da autodeterminação informativa, que se remete ao consentimento expresso e inequívoco do usuário na transmissão de seus dados, foi relativamente mitigado na lei. Isso porque, em muitos casos, não há a exigência da concordância do titular, por vezes por não ser nem mesmo viável. É o que ocorre, por exemplo, quando se trata de internet das coisas, onde, ainda que não se esteja conectado à internet, dados são repassados máquina à máquina, seja para manutenção futura, para *back up*, para orientar o funcionamento do aparelho etc. São dados repassados que não passam pela esfera do conhecimento do usuário, muito menos pela sua concordância, sendo que se essa autorização fosse necessária a cada transmissão de dado poderia inclusive inviabilizar o funcionamento da tecnologia, na prática.

Nesse sentido, a lei traz uma série de alternativas para a aquisição de dados (art. 7º), No entanto, no que diz respeito a dados públicos o projeto de lei foi mais flexível, prevendo, por exemplo, a dispensa de consentimento para a aquisição de dados pessoais tornados públicos pelo titular (art. 7º §4º) e balizando o seu uso a partir da "finalidade, boa-fé e interesse público que justificaram a sua disponibilização" (art. 7º §3º).

Foi expressamente prevista a comunicação ou uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado, também independentemente de consentimento do titular ou de informação ao órgão competente (art. 27, inciso III).

Desta forma, pode-se afirmar que a LGPD reconhece a importância dos dados na *data-driven society*, seguindo a linha de transparência de dados públicos e estipulando parâmetros mínimos de proteção a dados pessoais.

Todavia, ao mesmo tempo que a lei viabiliza esse armazenamento, também prevê limites ao uso de dados pessoais, como o princípio da necessidade, que limita o tratamento

desses dados ao “mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”. (art. 6º)

Nesse sentido, a lei lança as diretrizes de que, mesmo em grandes massas de dados, como ocorre em *Big Data*, os dados pessoais não poderão mais ser armazenados de forma irrefletida, sem que haja uma relação entre o dado e as finalidades a que ele se destina.

Isso porque até mesmo o armazenamento de dados é considerado uma forma de tratamento pela lei, conforme se deduz do art. 5º, X, que conceitua tratamento como “ toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.” A restrição, portanto, alcança dados pessoais.

A LGPD conceitua em seu art. 5º o que seriam dados pessoais, como sendo a “informação relacionada a pessoa natural identificada ou identificável;” (art. 5º, I). Além disso, a lei prevê uma proteção ainda maior para dados pessoais sensíveis, que são dados pessoais “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, II).

Há no entanto, a possibilidade de armazenamento mais flexível de dados pessoais caso eles sejam anonimizados, já que a própria lei prevê que uma vez anonimizados, esses dados perdem a característica de dados pessoais (art. 12), deixando assim de ter que obedecer estritamente o princípio da necessidade. Dados anonimizados são aqueles relativos “a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (art. 5º, III).

Dessa forma, o que se percebe é que a Lei, apesar de prever restrições ao uso de dados pessoais, acabou por deixar lacunas no que se refere ao *accountability* na gestão dos dados que não são considerados pessoais, dentre eles os dados públicos e os dados anonimizados.

Até mesmo quanto aos dados pessoais, algumas questões sensíveis foram deixadas em aberto. Pode-se exemplificar a partir da Lei 13.853/2019, que modificou a LGPD, e gerou acaloradas discussões sobre aspectos como a necessidade de revisão por pessoa natural dos processos decisórios oriundos de algoritmos, dentre os quais está o *Big Data Analytics*. O assunto é tratado no art. 20 da LGPD, e acabou prevalecendo que, mesmo que o tratamento se utilize de dados pessoais, a revisão humana é dispensável, bastando que se garanta o direito genérico de revisão, ainda que essa revisão seja realizada pela mesma ferramenta de tratamento.

Portanto, percebe-se ainda frágil a estrutura de acompanhamento e gestão dos dados e de seu tratamento, especialmente no contexto de *Big Data.*

Uma outra questão importante gira em torno da problemática da fiscalização do *Big Data Analytics*, de modo que se assegure a proteção dos dados sem que haja a quebra de algoritmo, ou seja, sem que o software contratado, objeto de propriedade industrial, seja violado ou exposto.

Para ilustrar essa situação, há um julgado do STJ sobre a legalidade do chamado credit scoring, que nada mais é do que um algoritmo, no modelo do *Big Data Analytics*, que visa o cálculo do risco da concessão de financiamento para particulares (STJ, 2014).

A corte julgou que o uso do algoritmo não viola a igualdade, desde que sejam disponibilizados aos clientes, uma vez solicitado, os dados que serviram de parâmetro para o cálculo de viabilidade. O assunto foi sumulado pelo STJ[3].

Por outro lado, a mesma corte entendeu que seria inviável a quebra da criptografia do algoritmo utilizado para o cálculo da viabilidade de empréstimo, justamente por estar protegido pela propriedade intelectual.[4]

A questão gera polêmica, dividindo opiniões entre teóricos que defendem a mitigação do conceito de propriedade intelectual no que diz respeito aos algoritmos, enquanto outros defendem meios alternativos de fiscalização, como decidida pela Corte superior, quando se exigiu a disponibilização dos dados usados para o cálculo de viabilidade, sem que se publicizasse a forma do cálculo.

Infelizmente, a LGPD também não confere uma resposta definitiva a esses casos, como o visto, possibilitando, no máximo a revisão da decisão realizada pelo algoritmo, não necessariamente supervisionado por um humano, deixando pouca margem para o *accountability* dessas situações.

Nesse sentido, a governança se insere juntamente com a legislação como uma das ferramentas úteis para a melhor gestão e transparência desses mecanismos.

5. A Governança e a Gestão dos Dados

---

3 Súmula 550-STJ: A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

4 "O consumidor terá direito de saber a sua pontuação e as informações pessoais utilizadas. No entanto, nem o consumidor nem ninguém terá direito de saber a metodologia de cálculo, ou seja, qual foi a fórmula matemática e os dados estatísticos utilizados no "credit scoring". Isso porque essa fórmula é fruto de estudos e investimentos, constituindo segredo da atividade empresarial (art. 5º, IV, da Lei n.12.414/2011)". (CAVALCANTE, 2018)

Na sociedade do conhecimento (*Data-Driven Society*) vislumbrada por Peter Drucker e Peter Senge (DRUCKER, 2000, p. 9-26) (SENGE, 2006), com a ameaça cada vez mais intensa aos dados - ativos importantíssimos - ampliam-se também os controles e processos formais para o seu tratamento e uso, através do fortalecimento dos processos de governança corporativa, de TI e de dados, como sentinelas da qualidade e segurança (FERNANDES; ABREU, 2014) (BARBIERI, 2011).

Nesse sentido, aliado ao *compliance* com a legislação pertinente, está a governança, principalmente porque, como vimos, a legislação acaba por traçar diretrizes vagas à gestão e ao *accountability* do tratamento dos dados, especialmente quando se trata de dados não pessoais.

Governança de dados é definido pelo art. 2º, XV, do Decreto nº 10.046/2019 como sendo o "exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos".

A governança então surge como um mecanismo que atende, tanto os interesses de proteção e contenção de riscos no uso de dados, quanto as demandas dos controladores e operadores de dados.

É comum que se pense em governança como um dispositivo "enrijecedor" que dificulta a correta exploração dos dados, quando na verdade, um dos objetivos da boa governança de dados é permitir a melhora da tomada de decisão e reduzir os atritos operacionais (FERNANDES; ABREU, 2014).

É por entender a importância da correta governança de dados como facilitadora de processos de análises de dados em *Big Data*, que várias instituições tem revisto seus processos e papéis quanto a governança de dados e *Big Data*.

A preocupação com o atendimento a demandas de transparência do tratamento e de controle a legislação pertinente pode até reduzir, a curto prazo, a capacidade e a produtividade dos processos que agregam valor ao produto ou serviço alvo da organização, uma vez que parte dos esforços são dedicados à implantação de controles e prevenção a riscos (FERNANDES; ABREU, 2014). Além disso, Uma vez que embasadas em políticas internas, as áreas de controle interno das organizações tendem a ser menos permissivas em usos de dados principalmente nos contextos de análises exploratórias, cenário tal que o resultado a ser alcançado não é necessariamente claro, conhecido e explícito antes da análise (BARBIERI, 2011).

Configura-se assim um aparente conflito entre dois interesses distintos e concorrentes. Por um lado, um modelo de governança de dados e *compliance* a LGPD, que institui controles, processos e "travas" ao livre acesso ao dado.

Por outro lado, o *Analytics* (principalmente no *Big Data*, onde deseja-se a maior quantidade e variedade de informação) extraindo-se valor exatamente do livre acesso e combinação de dados.

Entretanto, não trata, como pode parecer à primeira vista, de modelos conflitantes, mas sim de modelos interdependentes e de cooperação mútua.

Isso porque, a longo prazo, há a melhoria na gestão, e inclusive o melhor aproveitamento dos dados nos tratamentos em *Big Data Analytics*. Desta forma, incluem-se nos resultados a longo prazo na adoção destas boas práticas, o alcance de objetivos comuns a projetos de bussiness intelligence (BI), como a redução de custos operacionais, a mitigação de riscos envolvendo a legislação e a alavancagem do negócio com identificação de nichos de mercado pouco/não explorados, para citar alguns exemplos.

Alguns modelos de governança de dados já foram propostos no sentido de conferir meios para melhor gestão dos dados, e dos processos que envolvem o seu tratamento. Empresas com representatividade no ramo, tais como IBM, *Gartner* (IBM, 2014, CRAIG, 2017), pesquisadores da área (COCHRANE, 2009) e também por institutos de pesquisa e desenvolvimento (CMMI, DAMA, DGI, TDWI) (TDWI, 2018, DAMA, 2012, THOMAS, 2009, SEI, 2010) são alguns exemplos dessas iniciativas.

Dessa forma, ainda que esses frameworks não tenham sido criados para se estabelecer especificamente o *compliance* às legislações sobre proteção de dados pessoais, elas norteiam a gestão daqueles dados que não são tão fortemente resguardados por essas leis, inclusive no quesito de segurança de dados.

A governança, portanto, pode ser vista como uma interessante ferramenta para se evitar a ocorrência daquilo que os especialistas chamam de *data swamps*, "pântanos de dados", ou seja, do tratamento desordenado de dados, que geram altos custos e dificultam sobremaneira sua gestão.

Nesse sentido, destacam-se algumas das principais ferramentas de gestão que podem facilitar o tratamento ordenado de dados, mitigando os riscos da transparência indesejável, uma vez que conferem maior accontability para as práticas de gestão e para o tratamento dos dados:

1) DAMA-DMBOK - Um dos guias mais conhecidos para estabelecimento do gerenciamento estratégico de dados é o proposto pela *Data Management Association* (DAMA) denominado *Data Management Body of Knowledge* (DAMA-DMBOK). Assim como outras

estruturas *"body of knowledge"* tais como PMBOK ou CMBOK, o DMBOK é um "corpo de conhecimento" sobre gerenciamento de dados e tem por objetivo delimitar uma visão geral e abrangente sobre o assunto, definindo um padrão para função de gerenciamento de dados além da terminologia e melhores práticas de governança de dados, sem contudo detalhar técnicas e métodos específicos (FERNANDES; ABREU, 2014). O DMBOK é composto por dez funções de dados relacionadas à função de GD (BRACKETT; EARLEY, 2018).

2) COBIT – Trata-se de um framework desenvolvido pela Information Systems Audit and Control Association – ISACA e é baseado na norma internacional correspondente à norma brasileira NBR ISO/IEC 38500:2009 que, por sua vez, fornece princípios para os dirigentes e a alta direção nas atividades de avaliação, gerenciamento e monitoração de tecnologias da informação (TI). Especificamente sobre questões relacionadas às informações e dados, o framework COBIT na sua versão 5 endereça duas práticas de gerenciamento sendo elas APO 01.06 e APO 03.02 (FERNANDES; ABREU, 2014). Em adição às práticas de gerenciamento, a ISACA possui 2 um guia de referência acerca de governança e gerenciamento de informação: o COBIT 5: Enabling Information (AUDIT; ASSOCIATION; ISACA, 2012).

3) DGI Framework – Um framework criado pelo Data Governance Institute (DGI) constituído por 10 componentes e criado para empreender iniciativas em governança de dados.

4) CMMI – Trata-se do resultado da integração de vários modelos de capacidade CMMs (Capability Maturity Models) desenvolvidos pelo Software Engineering Institute (SEI) da Carnegie Mellon University (CMU) como encomenda do Departamento de Defesa norteamericano (DoD). Se propõe a ser um modelo único, integrado, flexível e componentizado de melhoria contínua de processos, envolvendo várias disciplinas (FERNANDES; ABREU, 2014).

5) MR-MPSBR - Criado pela Associação para Promoção da Excelência do Software Brasileiro (SOFTEX) em 2003, com o objetivo de tornar-se um modelo alternativo ao internacional (CMMI). O modelo foi criado para auxiliar pequenas e médias empresas brasileiras que não dispunham de orçamento suficiente para obter os níveis de maturidade do modelo estrangeiro. O MPSBR se baseia nas normas ISO/IEC 12207:2008, ISO/IEC 15504, ISO/IEC 20000, CMMI-DEV e CMMI-SVC (FERNANDES; ABREU, 2014).

6) IBM - A IBM também possui um framework estruturado sobre quatro componentes principais: Resultados – pautados em ações focadas em riscos de dados e em valoração dos ativos de informação; Viabilizadores – entre os quais a conscientização de governança de dados, estrutura organizacional dedicada, data stewardshipment e responsabilidade mútua entre TI e negócio; Disciplinas Centrais - Gerência de Qualidade de Dados, Gerência de Ciclo da

Informação e Segurança e Privacidade de Informação; e Disciplinas de Apoio – Arquitetura de Dados, Gestão de Metadados e Controle & Auditoria (CRAIG, 2017).

7) Outros modelos – Existem ainda outros modelos que viabilizam a gestão desses dados, tais como: Gartner (CRAIG, 2017), TDWI (TDWI, 2008), 5W2H (BARBIERI, 2011) e 5 Steps to Data Governance (COCHRANE, 2009).

Portanto, o que se percebe é uma variedade de estruturas que podem ser escolhidas de acordo com o modelo de negócio desenvolvido, voltado para os objetivos que se deseja alcançar com determinado *Big Data.*

O uso dessas ferramentas de gestão ajuda a mapear as decisões estratégicas do negócio, fazendo com que exista a documentação da utilização desses dados. Ou seja, a governança funciona como uma espécie de controle interno, assegurando que exista alguma transparência nos mecanismos decisórios dos desenvolvedores e controladores de dados.

Por este motivo, a governança desponta como uma dupla aliada, pois, como mencionado, além de alavancar o próprio negócio, evitando *data swamps,* torna auditáveis documentalmente as decisões tomadas em *Big Data.*

6. Conclusão

É claro que, num paradigma informacional como o que vivemos, é inevitável que os dados continuem circulando em larga escala pelas redes, e é desejável que as instituições que nos permeiam promovam, cada vez mais, a transparência dos seus dados e de suas gestões, ressalvados os cuidados atinentes aos dados pessoais.

A LGPD parece despontar como uma legislação emergencial, no que diz respeito à necessidade de se estabelecer parâmetros mínimos de proteção aos dados pessoais, até então capturados e utilizados em *Big Data,* sem nenhuma restrição.

No entanto, a LGPD não trás direcionamento aos dados não pessoais, que, se mal utilizados, podem interferir inclusive na questão de privacidade além de em outras tantas questões, como na segurança pública, estratégia de governo, concorrência, etc.

Nesse sentido, defende-se a governança de dados na perspectiva da abordagem de análise de riscos como uma aliada necessária na mitigação da transparência indesejável. Principalmente porque a transparência indesejável é oriunda de processos de *Big Data Analytics* (e portanto, do tratamento do dado como um passivo da organização) feitos de forma desorganizada e não documentada, já que ainda desregulamentados.

À escolha da instituição, a adoção de um framework de governança adequado auxilia na transparência dos processos decisórios no tratamento de dados, e na melhor organização e gestão dos dados.

Trata-se, portanto, de um mecanismo que promete vantagens para ambos os lados, o da sociedade e o do gestor, uma vez que permite à organização que realiza o tratamento a devida análise dos riscos associados ao tratamento do dado e por isso mesmo deve ser incentivado.

7. Referências Bibliográficas:

AUDIT, I. S.; ASSOCIATION, C.; ISACA. **Cobit 5**: Implementation ISACA, 2012.

BARBIERI, C. **BI2–Business intelligence**: Modelagem & Qualidade. Elsevier Editora, 2011.

BALLARD, C.; COMPERT, C.; JESIONOWSKI, T.; MILMAN, I.; PLANTS, B.; ROSEN, B.; SMITH, H. et al. **Information governance principles and practices for a big data landscape**: IBM Redbooks, 2014. Disponível em:<https://www.redbooks.ibm.com/redbooks/pdfs/sg248165.pdf>. Acesso em: 04/02/2020

*BBC NEWS. **Snowden:** leaks that exposed US spy programme.* Disponível em: http://www.bbc.com/news/world-us-canada-23123964. Acesso em

BRACKETT, M.; EARLEY, P. S. **The dama guide to the data management body of knowledge**
(dama-dmbok guide). Technics Publications, 2009

BRASIL. **Lei 12.527.** Lei geral de acesso a informação (LAI). Brasília, DF: Presidência da República, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 28/03/2020.

BRASIL. **Lei 12.965.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28/03/2020.

BRASIL. **Lei 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28/03/2020.

CASTELLS, M. **A sociedade em rede**: a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CAVALCANTE, Márcio André Lopes. **Propositura de ação de exibição de documentos relativos ao Crediscore**. Manaus: Buscador Dizer o Direito, 2018. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/cdf1e288ca02272e717c9d5e4cb180bd> Acesso em: 15/08/2018

CELLA, José Renato Graziero; COPETTI, Rafael. **Compartilhamento de dados pessoais e a administração pública brasileira.** Rev. de Direito, Governança e Novas Tecnologias. e-ISSN: 2526-0049.Maranhão. v. 3 .n. 2 .p. 39 - 58 . 2017.

CONFESSORE, Nicholas. **Cambridge Analytica and Facebook:** The Scandal and the Fallout So Far. New York Times. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Acesso em: 01/02/2020

CONSTANTIOU, Ioanna D.; KALLINIKOS, Jannis. **New games, new rules**: big data and the changing context of strategy. Journal of Information Technology, v. 30, n. 1, p. 44-57, 2015.

CRAIG, T. Eim**. 1.0:** Setting up enterprise information management and governance. Gartner, Disponível em: <http://https://www.gartner.com/doc/3831267>. Acesso em: 04/02/2020.

CRUZ, Bruna Souza. **Por que o governo compra dados dos próprios cidadãos?** Tecnologia Uol. 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/06/18/entenda-por-que-o-governo-compra-dados-publicos-dos-proprios-cidadaos.htm> Acesso em 03/12/2019.

COCHRANE, Mike. **Five Steps to Data Governance.** Information Magazine. 2009. Disponível em <https://www.information-management.com/news/5-steps-to-data-governance> Acesso em: 01/05/2019.

DAMA DMBOK, Edição em português impressa em 2012. **Capítulo Brasileiro da DAMA International**, 2012.

DIAMANTINI, Claudia et al. Find the Right Peers: Building and Querying Multi-IoT Networks Based on Contexts. In: **International Conference on Flexible Query Answering Systems**. Springer, Cham, 2019. p. 302-313

DRUCKER, P. F. **O advento da nova organização**. Harvard Business Review (Org). Gestão do conhecimento, v. 9, 2000, p. 9–26.

EUROPEAN COMMISSION. **Caso 39749**. 2018. Disponível em: <http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740> Acesso em 01/12/2019.

FERNANDES, A. A.; ABREU, V. F. D. **Implantando a Governança de TI**: Da estratégia à Gestão de Processos e Serviços. Brasport, 2014.

HADAIR, Rodrigo. **TSE mantém nulo convênio e dá prazo para Serasa**. Conjur, 2013. Disponível em: <https://www.conjur.com.br/2013-ago-13/tse-mantem-nulo-convenio-serasa-prazo-defesa-empresa> Acesso em: 05/08/2018.

IBM International Technical Support Organization. **Information Governance Principles and Pratices for a Big Data Landscape**. 2014. Disponível em <www.redbooks.ibm.com/redbooks/pdfs/sg248165.pdf> Acesso em: 20/05/2019.

ISACA. **COBIT® 5 Enabling Information.** Rolling Meadows, 2013.

LATOUR, Bruno**. Jamais fomos modernos**: ensaio de antropologia simétrica. 2ª edição. Rio de Janeiro. Editora 32. 2009.

LESSIG, Lawrence. **Code and other laws of cyberspace**. New York: Basic Books, 1999.

LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

MANCINI, Mônica. **Internet das Coisas**: História, Conceitos, Aplicações e Desafios. PMI São Paulo. 2018. Disponível em <https://pmisp.org.br/documents/acervo-arquivos/241-internet-das-coisas-historia-conceitos-aplicacoes-e-desafios/file>. Acesso em: 12/08/2019 .

MAYER, J; MUTCHER, P. **MetaPhone**: The Sensitivity of Telephone Metadata. Web Policy. 2014. Disponível em: <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>. Acesso em: 01/07/2019.

MAYER-SCHÖNBERGER, V., CUKIER, K. ***Big Data: A Revolution That Will Transform How We Live, Work, and Think***. New York: Houghton Mifflin Harcourt, 2013.

MENEZES NETO, Elias Jacob. **Surveillance, democracia e direitos humanos**: os limites do Estado na era do *big data*- Tese de Doutorado Universidade do Vale do Rio dos Sinos - Unisinos. 2016.

STJ. **REsp 1.419.697-RS**, 2ª Seção. Relator: Min. Paulo de Tarso Sanseverino, julgado em 12/11/2014 (recurso repetitivo) (Informativo 551).

SEI. **CMU/SEI – CMMI® for Development,** Version 1.3, Novembro, 2010.

SENGE, P. M. **The fifth discipline**: The art and practice of the learning organization. Broadway Business, 2006.

TDWI – The Data Warehousing Institute**. TDWI Advanced Analytics Maturity Model Guide**. 2018. Disponível em: <https://tdwi.org/pages/assessment/adv-all-tdwi-advanced-analytics-maturity-model.aspx> Acesso em: 05/05/2019.

THOMAS, Gwen. **The DGI Data Governance Framework**. The Data Governance Institute, 2009.