XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

TÊMIS LIMBERGER

VALTER MOURA DO CARMO

AIRES JOSE ROVER

Copyright © 2018 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 - IMED – Rio Grande do Sul
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 I [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS

Coordenadores: Têmis Limberger; Valter Moura do Carmo; Aires Jose Rover. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia
ISBN: 978-85-5505-725-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34

CONPEDI

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

UNISINOS

Universidade do Vale do Rio dos Sinos
Porto Alegre – Rio Grande do Sul - Brasil
http://unisinos.br/novocampuspoa/

XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (Conpedi) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito e o Grupo de Trabalho Direito, Governança e Novas Tecnologias é exemplo de pesquisas desse tipo.

Como na última edição, houve uma diversidade grande de temas e tópicos. Numa tentativa de dar certa unidade temática, ainda assim podemos organizar os artigos em alguns grupos.

O primeiro e mais presente em termos numéricos de artigos foi o tema da Inteligência Artificial. Isso mostra o interesse que hoje está presente em toda comunidade jurídica, com o avanço de diversas técnicas e experimentos no judiciário e nos escritórios de advocacia. Um dos artigos literalmente afirmava que o direito não está imune a essa transformação e outro que é preciso estar atentos aos desafios regulatórios na advocacia. Também foi discutida a disponibilização de dados para que a inteligência artificial avance.

Outro grupo de artigos envolve o tema que sempre está presente de alguma forma, os dados pessoais e sua proteção. O direito à privacidade, a internet das coisas, a proteção dos dados pessoais e big data, o regulamento europeu de proteção de dados e dados personalíssimos na internet foram tópicos tratados.

Outro tema importante sempre presente neste gt foi o processo judicial eletrônico. Uma análise dos tribunais de justiça estaduais e o website do tribunal regional eleitoral do Paraná foram dois artigos que trataram o judiciário neste contexto de uso intensivo de tecnologia.

A internet foi outra temática bem discutida, como sempre. Os temas do discurso de ódio, liberdade de expressão, fake news e a pós-verdade não podiam deixar de estar presentes tendo em vista o seu grau de novidade. Já o acesso à internet, o (cyber)bullying, as redes sociais e a necessidade de coregulação na internet, já bastante discutidos, também foram tratados.

Fechando, os temas da responsabilidade civil, governança e anticorrupção foram bem representados. Temas afins como a política de comunicação e a política de segurança, o papel

das empresas sob a perspectiva ética, a política de governança do youtube e a herança e transmissão de bens virtuais podem ser aqui agrupados.

Enfim, os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Prof. Dr. Aires José Rover – UFSC

Profa. Dra. Têmis Limberger – UNISINOS

Prof. Dr. Valter Moura do Carmo – UNIMAR

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

A (IN)SEGURANÇA DOS ATIVOS DE INFORMAÇÃO: RESPONSABILIDADES PERANTE OS CIDADÃOS NA GESTÃO DAS SMART CITIES

SECURITY OF INFORMATION ACTIVITIES: RESPONSIBILITIES TO CITIZENS IN THE MANAGEMENT OF SMART CITIES

Alessandra Cristina Arantes Sutti [1]
Irineu Francisco Barreto Junior [2]

Resumo

Este artigo faz uma análise dos ativos informacionais de acordo com as normas de segurança da informação, apresentando a sua relevância na sociedade contemporânea, principalmente com relação à proteção desses ativos e os riscos em caso de inconformidade e violação dos dados pessoais nas smart cities. Por conseguinte, apresenta a accountability como uma das principais ferramentas para cumprimento da transparência pública e do dever estatal quanto à inviolabilidade da segurança dos cidadãos nas smart cities, aqui incluindo a segurança dos dados pessoais dos cidadãos enquanto consumidores dos serviços públicos, sem que haja conflito entre publicidade e privacidade dos cidadãos.

Palavras-chave: Smart cities, Sociedade da informação, Dados pessoais, Código de defesa do consumidor

Abstract/Resumen/Résumé

This paper presents an analysis of information assets, in accordance with the safety standards of information, showing the relevance of the information in contemporary society, especially with regard to the protection of these assets and the risks in case of disagreement and violation of personal data on smart cities. It presents the accountability as one of the main tools for compliance with public transparency and the state's duty regarding the inviolability of citizen security, here including security of personal data of citizens as consumers of public services, without which there is a conflict between advertising and privacy of citizens.

Keywords/Palabras-claves/Mots-clés: Smart cities, Information society, Personal data, Consumer protection law

---

[1] Advogada e Docente em Direito Empresarial da Escola de Negócios (FMU-SP). Mestranda em Direito da Sociedade da Informação e pós-graduada em Direito Ambiental e do Consumidor (FMU)

[2] Pós Doutorando em Sociologia (USP). Doutor em Ciências Sociais (PUC-SP). Docente do Programa de Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas FMU

Introdução

A informação é parte da vida do ser humano e a história, de certa forma, somente alcançou o ritmo observado no século XXI porque a informação foi compartilhada pelos meios tecnológicos, atingindo o patamar de moeda de troca ou mercadoria, mas certamente com valor imensurável na Sociedade da Informação. Nesse cenário, tornou-se relevante a discussão da proteção da informação e a possibilidade de vazamento ilícito e invasão da privacidade dos indivíduos, com afetação dos direitos fundamentais e da dignidade humana.

Apesar das inúmeras e importantes discussões travadas sobre o tema, este artigo versará sobre os ativos de informação, seguindo a linguagem e normas da Segurança da Informação, desmistificando o conceito real de informação para conceituar adequadamente os dados pessoais e o quão relevante é a proteção e inviolabilidade da privacidade de uma pessoa, que exerce seu papel de cidadão e consumidor, simultaneamente. Por outro lado, também serão apresentadas as ferramentas necessárias para que não haja conflito entre os princípios da transparência e da privacidade, mas, ao contrário, que elas se complementam desde que haja cumprimento das normas de Segurança da Informação por parte do Poder Público no momento da *accountability*.

Uma das grandes preocupações no Brasil com relação à proteção dos dados pessoais, aliás, era a suposta ausência de legislação específica e efetiva no caso de vazamento dessas informações, mas o presente artigo pretende demonstrar, de forma detalhada, como a legislação vigente já supria as lacunas para a inviolabilidade da segurança e proteção dos dados pessoais, vindo a recente Lei Geral de Proteção de Dados corroborar a aplicabilidade do Código de Defesa do Consumidor nessa questão.

A metodologia empreendida neste artigo reside no desafio de apresentar o fenômeno sob a ótica de uma relação jurídica consumerista, apresentando os requisitos essenciais para configurar a responsabilidade objetiva do fornecedor, enquanto pessoa jurídica de direito público (já que o foco são as *smart cities*), caracterizando os ativos de informação, incluindo a proteção, inviolabilidade, segurança e vazamento dos dados dos cidadãos-consumidores, caso o dever estatal de salvaguarda seja descumprido. Para tal é realizada a pesquisa doutrinária e documental jurídica, com ênfase nas teorias recentes e concernentes à temática abordada no artigo.

1. Os ativos de informação

A informação é um registro do que existe ou do que está prestes a existir e, inicialmente, não se deve abordar a quem ela pertence, onde ela se encontra e sequer sua finalidade, pois sua pretensão principal é dar ciência ou noticiar um fato existente (MACHADO, 2006, p. 25-26). A partir do momento que essa informação é lançada aos veículos de comunicação ou disseminada pelos meios tecnológicos, ela pode gerar o *status* de conhecimento, curiosidade, espionagem, devassa, manipulação, opinião e liberdade de expressão (MACHADO, 2006, p. 27-31).

Já em sentido estrito, a informação é considerada a exposição de uma determinada situação que verse sobre pessoas, coisas ou qualquer outra relação (MONTEIRO, 1989, p. 15-16), tendo como principal objetivo a persuasão (BERLO, 1999, p. 7-10), podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas (ABNT, 27002:2005, p. ix).

Com base no *status* que a informação assume por sua exposição, notadamente na Sociedade da Informação, as novas tecnologias e a internet representam ferramentas potencialmente importantes e simultaneamente perigosas para sua disseminação, pois a informação se transformou em um ativo social e mercadológico, ou seja, um bem imaterial e intangível, cujo valor pode ser negociado ou agadanhado, gerando tanto lucro quanto prejuízos de ordem econômica e moral.

> O valor da informação está na facilidade de encontrá-la para os processos de negócio. Ela tem um valor incalculável, mas, tê-las, apenas, não é o bastante. É preciso se saber o que fazer com elas. Partindo deste princípio básico, pode-se reconhecer a informação como inteligência (gestão do conhecimento), conhecimento (informação que sofrer análise), informação (dados que foram classificados e organizados) e dado (representação de fatos ocorridos ou medidas realizadas) (CARNEIRO, 2013, p. 17-18).

Isso significa que a informação se tornou um bem de troca, provavelmente a nova moeda da era digital (MARCELO; PEREIRA, 2005, p. 3) e, por consequência, a coexistência entre informação e tecnologia inclinou as pessoas e organizações à contínua vigilância tecnológica e incessante combate à engenharia social[1].

Essa é a razão pela qual as organizações públicas e privadas tratam a informação como patrimônio ativo, salvaguardado pela área da Segurança da Informação que, por meio de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, arquiteturas

[1] A engenharia social é a arte de obter ardilosamente informações a respeito de algo, alguém ou de uma instituição, seja lá qual for a maneira (por telefonemas, e-mails, *on the fly* ou pessoalmente, invasão de sistema operacional etc. (MARCELO; PEREIRA, 2005, p. 4).

digitais, softwares e hardwares (ABNT, 27002:2005, p. ix), busca resguardar os ativos de informação contra os ataques cibernéticos.

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 27002:2005, p. ix).

Aqui se depreende a relevância da proteção da informação: trata-se de um patrimônio valioso e, por isso, é reconhecida como ativo, ou seja, possui valor expressivo para a sustentabilidade e credibilidade dos negócios, bem como para a reputação e boa-fé dos indivíduos. A variedade de ameaças e vulnerabilidades na Sociedade da Informação exige segurança e vigilância dos ativos informacionais, vindo a Segurança da Informação buscar a proteção da informação contra vários tipos de ameaças, com o intuito de garantir a continuidade e minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio das organizações (ABNT, 27002:2005, p. ix).

Na verdade, a Segurança da Informação baseia-se na proteção dos dados, sejam organizacionais ou pessoais, da informação em si, da infraestrutura, dos sistemas operacionais e tecnológicos, além dos serviços que a suportam para oferecer maior credibilidade possível, tanto no ambiente convencional quanto no ambiente de tecnologia.

Portanto, os elementos que compõem os ativos de informação são: os ativos tangíveis (bens móveis e imóveis, capital físico e financeiro); os ativos intangíveis (qualidade, reputação, capital intelectual, marca, imagem); os ativos de serviços (energia elétrica, internet, iluminação etc.); os ativos de recursos humanos (usuários, funcionários, clientes, fornecedores); os ativos de informações propriamente ditas (físicas ou eletrônicas, que formam o banco de dados); os sistemas e programas (softwares) e a infraestrutura física (hardwares). Estes são assim qualificados:

> a) ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
> b) ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
> c) ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
> d) serviços: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;
> e) pessoas e suas qualificações, habilidades e experiências;

> f) intangíveis, tais como a reputação e a imagem da organização (ABNT, 27002:2005, p. 21).

Dessa forma, a Segurança da Informação deve estar alinhada aos intentos pessoais e organizacionais, garantindo que a informação, em sentido amplo, seja preservada e isenta de riscos de divulgação indevida (LIMA, 2018, p. 6) e de risco reputacional. Feito o inventário dos ativos de informação, é necessário estabelecer uma classificação da informação para que haja o compartilhamento da mesma; esta classificação é determinada por cada organização, partindo-se dos critérios legais (o que, por lei, pode ou não ser divulgado ou compartilhado; o que deve ser divulgado; e o que pode ou deve ser mantido sob sigilo) até os critérios que atendem as atividades internas e externas da organização (ABNT, 27002:2005, p. 21-24).

Uma vez classificados, os ativos de informação precisam ser rotulados como público, interno, confidencial ou restrito, sendo esse o nível de classificação que determinará a autenticidade, confidencialidade, usabilidade, integridade, criticidade, disponibilidade e sensibilidade da informação para fins de divulgação e trânsito (KONZEN, 2013, p. 17-18), ou como reservado, secreto e ultrassecreto, tratando-se de ativos de informação relativos aos órgãos públicos e entidades afins (LAI[2], 2011, p. 6).

Por conseguinte, a Segurança da Informação estabelece o gerenciamento da segurança em redes, zelando rigorosamente pelo fluxo de dados, implicações legais, monitoramento e proteção da informação, além de estabelecer controles adicionais para proteção de informações sensíveis que trafeguem em redes públicas (ABNT, 27002:2005, p. 49). Para este trabalho, portanto, os ativos de informação serão tratados com foco nas *smart cities*, notadamente quanto ao armazenamento, controle de informações on-line (dados pessoais dos cidadãos) pelos governos municipais.

2. A (in)segurança da informação nas *smart cities* e o vazamento de dados dos cidadãos

A Constituição Federal, em seu preâmbulo, anuncia a instituição de um Estado Democrático destinado a confirmar, dentre outros, a "segurança" como valor supremo de uma sociedade fraterna, pluralista e sem preconceitos (BRASIL, 2018, p. 13). Muito embora não

[2] Trata-se do art. 24 da Lei nº 12.527, de 18 de novembro de 2011, mais conhecida como Lei de Acesso à Informação (LAI), criada para fixar procedimentos à União, Estados, Distrito Federal, Municípios, entidades por estes controladas e entidades privadas, sem fins lucrativos, que recebam recursos públicos para concretizar ações de interesse público, com o objetivo de regular o acesso a informações garantidos na Constituição Federal.

faça parte do texto constitucional propriamente dito e não possua valor normativo, o preâmbulo traça uma linha mestra que condiciona seu valor integrativo e interpretativo com o conteúdo constitucional (HOLTHE, 2009, p. 40) e, por isso, se alinha à ideia de segurança nacional, doméstica, laboral, pública, pessoal e à própria segurança da informação.

Para melhor compreensão, segurança, do latim *secura*, significa 'um mal a evitar'; na definição comum, segurança significa ausência de risco. Mas quando definimos segurança no sentido sociológico, ela conflita com a liberdade individual, pois quanto mais livre é o indivíduo, mas difícil torna-se a proteção pelo Estado (IFILNOVA, 2018, p. 1) e, por isso, surgem as matérias indenizatórias e punitivas para composição de eventuais danos ou delitos que resultem desse conflito.

A segurança é aplicável a qualquer atividade humana: intelectual, técnica, econômica, política e até mesmo sentimental (IFILNOVA, 2018, p. 3), indicando que a Constituição Federal, ao garantir a inviolabilidade do direito à segurança[3], soergue seu *status* integrativo para salvaguarda da liberdade de comunicação, da intimidade, vida privada, honra e imagem das pessoas; do sigilo da correspondência e das comunicações telegráficas; dos dados e comunicações telefônicas; da liberdade de acesso e do direito à informação[4].

E a segurança no Estado Democrático de Direito assume seu *status* interpretativo diante dos fundamentos da cidadania e da dignidade da pessoa humana[5], pois, qualquer ato que colete, armazene, rastreie, invada, deturpe e/ou dissemine as informações dos cidadãos sem seu consentimento, mediante fraude ou ruptura da boa-fé e confiança, caracterizará a quebra da segurança digital.

> Na atualidade, a maioria das pessoas usa cartões magnéticos como uma espécie de chave para navegar no ciberespaço, seja para o pagamento de algum produto ou serviço no mercado, acessar suas contas correntes no caixa eletrônico, fazer uma transação bancária, entrar em danceterias ou na universidade, verificar as notas escolares, pagar o transporte público, armazenar créditos para o lanche na escola, seja para acessar serviços públicos, entre outras facilidades (GUERREIRO, 2006, p. 18).

Percebe-se, assim, que a diversidade de significados e autodescrições da sociedade já é suficiente para se constatar o papel fundamental que o fenômeno da informação desempenha na sociedade contemporânea e, por conseguinte, a privacidade (MENDES, 2014, p. 19).

---

[3] Referência ao art. 5°, *caput*, da Constituição Federal.
[4] Referência ao art. 5°, incisos IX, X, XII, XIV e XXXIII da Constituição Federal.
[5] Referência ao art. 1°, incisos II e III da Constituição Federal.

Fato é que, na era digital, a informação é um ativo que, em muitos casos, requer a proteção apropriada, de forma abrangente e atuante, exigindo gestão de riscos, *compliance*[6] e governança nas instituições, a fim de (não) gerar a (in) segurança. Por esse motivo, está em curso um processo transformacional profundo das práticas governamentais e corporativas diante da segurança da informação (D'ANDREA, 2012, p. 151), em razão dos avanços de crimes cibernéticos, engenharia social, *fake news*, *hacktivismo* e *ransomware*[7].

Algumas certificações vêm sendo referência no setor público, de forma a estabelecer boas práticas na contratação de serviços; todavia, sua prática não atingiu o grau de segurança, visto os inúmeros ataques em massa feitos por *hackers* e *hacktivistas* contra países, governos, políticos, expondo supostos casos de corrupção ou lesão à população (D'ANDREA, 2012, p. 153).

No Brasil, tais ataques atingiram severamente a imagem do país, órgãos públicos e empresas privadas, gerando desconfiança, passivo reputacional e o descrédito da população em utilizar os serviços públicos digitais (*e-gov*) e serviços bancários eletrônicos (D'ANDREA, 2012, p. 153), com o vazamento de dados pessoais dos usuários.

Vale ressaltar que a gestão de ativos nas *smart cities*[8] é considerada parte do sistema global de informações obtida ao prestarem serviços públicos, no momento em que captam os dados pessoais dos seus cidadãos, tornando-se guardiãs dos dados e detentores do dever de segurança e proteção digital destes. E são exatamente esses dados que se transformam em informações valorosas e, ao mesmo tempo, vulneráveis aos ataques cibernéticos, capazes de trespassar a criptografia, antivírus, *firewall*, senhas, biometria, autenticação de dois fatores, dentre outros.

> A todo o momento são divulgadas declarações sobre renda dos servidores públicos, localizações de GPS (*global positioning system*) obtidas mediante dados coletados a partir do telefone celular dos usuários, itinerários de voos, fotos, câmeras de segurança, informações postas em redes sociais e plataformas de correio eletrônico (*email*), dados sobre processos judiciais disponíveis inteiramente *online*, dentre outros (SAUAIA, 2018, p. 1).

---

[6] Expressão que significa agir de acordo com as regras.

[7] *Fake news* significam notícias falsas, com capacidade de viralização imediata; *hacktivismo* é uma ideologia que sustenta o desejo de liberdade de informação como uma extensão social da cidadania; *ramsonware* é um software nocivo que infecta o sistema-alvo e sequestra dados digitais, mediante extorsão digital para fins de restabelecer o *status quo* operacional.

[8] Segundo Danilo Doneda, a expressão *smart city* é utilizada para se referir a uma gama de situações, tornando-se uma *buzzword* (novidade, grande acontecimento). No planejamento urbano, por exemplo, *smart city* é evocada em relação a cidades edificadas a partir do zero, com alto grau de integração de seus processos e serviços pela utilização de tecnologias de informação e comunicação (TIC), mas é frequentemente usada em casos de inserção de sensores e serviços informatizados às estruturas já existentes em cidades.

Claro que cuidar da segurança dos dados pessoais está cada vez mais complexo, não apenas pelas ameaças e sofisticados ataques cibernéticos, mas principalmente pela mudança do perfil dos usuários, pelo crescimento desenfreado na adoção de dispositivos móveis (*app mobile*), além da diversidade de sistemas operacionais que exigem cada vez mais suporte técnico e da adesão ao trabalho remoto (D'ANDREA, 2012, p. 153).

E, em se tratando de órgãos públicos, que dependem de orçamento plurianual para investimento e atualização da carga tecnológica e sofre com contenção de despesas, notadamente em tempos de crise econômica, paira a sensação de descaso e insegurança com os dados pessoais e a privacidade dos cidadãos. As *smart cities* são como colônias de formigas, pois possuem uma espécie de inteligência emergente, ou seja, a habilidade de guardar e recuperar informações, reconhecer e responder a padrões de comportamento humano (SANTAELLA, 2016, p. 14).

Aplicando-se essa inteligência emergente à Tabela 2, pode-se afirmar que, nos últimos três anos, os órgãos públicos municipais ampliaram o uso da internet e de outras tecnologias para transmissão e oferta de serviços *online*, tanto que alguns destes não são mais ofertados no ambiente físico.

Isso é uma resposta às necessidades dos citadinos e caracteriza uma moldagem do comportamento governamental à prestação dos serviços públicos, em respeito à Lei de Acesso à Informação (LAI) e ao Código de Defesa do Consumidor, pois, tanto a informação quanto a privacidade são contextualizadas no dever de qualidade, boa-fé e confiança na prestação de serviços, mesmo que sejam de ordem pública. Contudo, a oferta de serviços públicos digitais não implica, necessariamente, na garantia governamental da segurança efetiva dos ativos de informação dos cidadãos, pois, vale lembrar, é preciso investimento e controle constante das informações digitais, senão a quebra da segurança de dados causará o vazamento dos dados dos cidadãos e sua recorrente invasão de privacidade.

O resultado é que nas cidades interioranas, muitas ainda não denominadas *smart cities* pela ausência infraestrutura tecnológica e zelo digital dos citadinos, prevalece a terceirização, especialmente em atividades de desenvolvimento de software (88%), de website (78%) e para serviços de hospedagem (79%), além do suporte técnico de seus sistemas internos (68%).

Quando falamos em certificações pelos órgãos públicos como alternativa de segurança dos ativos de informação, fica claro que a adoção ideal é pelo sistema interno, cujo método de

controle filtra ou previne quaisquer oportunidades para vazamento de informações sem demanda de espera para atendimento, pois mesmo sendo remoto, as terceirizadas não trabalham 24h para atender às chamadas de invasão digital.

Entretanto, para fins de terceirização, uma possível solução para a segurança dos ativos pelos terceirizados seria se os editais de licitação pública exigissem, no critério de "condições para participação", a certificação da empresa interessada no "Código de Prática para Gestão da Segurança da Informação", pertencente à ABNT 27002:2005, que prevê as seguintes condutas para limitar o risco de vazamento de dados, principalmente por meio dos *covert channels*[9]:

> a) a varredura do envio de mídia e comunicações para verificar a presença de informação oculta;
> b) o mascaramento e a modulação do comportamento dos sistemas e das comunicações para reduzir a possibilidade de terceiros deduzirem informações a partir do comportamento dos sistemas;
> c) a utilização de sistemas e software reconhecidos como de alta integridade, por exemplo utilizando produtos avaliados;
> d) o monitoramento regular das atividades do pessoal e do sistema, quando permitido pela legislação ou regulamentação vigente;
> e) o monitoramento do uso de recursos de sistemas de computação (ABNT, 27002:2005, p. 95).

Independentemente da dimensão tecnológica que dá vida às *smart cities*, quando o foco dos investimentos e melhorias estão direcionados somente à adoção e integração de novas tecnologias, deixando os cidadãos no papel de sujeitos ocultos, subtendidos ou indeterminados (SANTAELLA, 2016, p. 18), fere-se o Estado Democrático de Direito por submersão da cidadania e da dignidade da pessoa humana.

Ao submergir tais princípios e diante da inobservância de que as cidades são feitas para as pessoas (GEHL, 2013, p. 215), surge a passividade do dever estatal à segurança dos dados pessoais dos cidadãos e soergue a omissão estatal específica, com a consequente responsabilização pela insegurança digital. Não se pode olvidar, portanto, que:

> *"The 'Information Society', as we see it, should be a place where information technology is used to improve life satisfaction and support our individual and collective goals, not to erode or undermine them. Serving that purpose is what makes IT a true public profession"* (SPARROW, 2010, p. 3)[10].

[9] Os *covert channels* significam 'canal secreto'; são caminhos não previstos para conduzir o fluxo de informações, no entanto, podem existir em um sistema ou rede e, mediante sistemas seguros, podem ser removidos sem causar danos (ABNT, 27002:2005, p. 95).

[10] "A 'Sociedade da Informação', tal como a vemos, deveria ser um lugar onde a tecnologia da informação é usada para melhorar a satisfação com a vida e apoiar nossos objetivos individuais e coletivos, e não para erodir ou mina-los. Servir para esse propósito é o que faz da TI uma verdadeira profissão pública" (tradução livre dos autores).

Assim, ao prestar serviços públicos digitais de má qualidade, mesmo que esteja cumprindo com o direito à informação, este vem acompanhado fundamentalmente da preservação da dignidade humana e do exercício da cidadania, que só ocorrem mediante a segurança, guarda e privacidade dos dados pessoais dos cidadãos nas *smart cities*.

3. *Accountability* na gestão das *smart cities* e os dados pessoais dos cidadãos

A exigência de proteção dos dados pessoais dos cidadãos na gestão das *smart cities* aumenta consideravelmente à medida que prospera sua confiança nos serviços públicos e estes são inseridos, cada vez mais, em um banco de dados digital; no entanto, os cidadãos, que são consumidores de produtos e serviços públicos, exigem cada vez mais respeito à informação e sua privacidade.

Por outro lado, as empresas, públicas e privadas, acabam reconhecendo a proteção da privacidade como um ativo de segurança da informação e, por vêem a confiança dos cidadãos como valor agregado aos serviços públicos, acabam alinhando suas políticas de uso e privacidade digital com regulamentos e diretivas gerais de proteção de dados pessoais.

A União Europeia, por exemplo, consagrou a Diretiva 95/46/CE, de 24 de outubro de 1995, para tratamento adequado, proteção e livre circulação dos dados pessoais, considerando que o nível de proteção e direito das pessoas só seria equivalente se todos os Estados-membros assegurassem, em suas legislações nacionais, o direito transfronteiriço de circulação dos dados pessoais de seus cidadãos (UE, 1995, p. 32)[11].

Recentemente, tal diretiva foi revogada pelo Regulamento Geral sobre a Proteção de Dados (RGPD)[12] que, considerado um modelo a seguir por toda a comunidade europeia, aproveitou o ápice da economia digital global e conferiu o *status* de direito fundamental à segurança e à privacidade dos cidadãos com relação aos seus dados pessoais.

Já o Marco Civil da Internet veio estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tendo como alguns de seus princípios a proteção da privacidade e dos dados pessoais[13], cuja regulamentação e tratamento específico é dada pela Lei Geral de

[11] Referência ao item 8 da Diretiva 95/46/CE, de 24 de outubro de 1995.
[12] Referência ao Regulamento 2016/679/CE, de 27 de abril de 2016.
[13] Referência ao art. 3°, incisos II e III da Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet.

Proteção de Dados (LGPD), que dispõe sobre o tratamento dos dados pessoais, incluindo nos meios digitais, seja por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural[14].

Mas vale ressaltar que a Administração Pública deve prestar seus serviços regidos pelos princípios constitucionais da legalidade, impessoalidade, moralidade, eficiência e publicidade[15], além do princípio da segurança, que envolve o direito à sua inviolabilidade e a privacidade dos dados dos cidadãos, bem como as cidades, regidas por lei orgânica, devem seguir a informação e a transparência como deveres conexos à salvaguarda da segurança e da dignidade, estendendo-se ao ambiente digital.

O acesso à informação, aliás, está previsto na Constituição Federal e na Lei de Acesso à Informação (LAI), para fins de cumprimento dos princípios da transparência, informação e *disclosure*[16], além da Lei de Responsabilidade Fiscal[17] que prevê a *accountability*[18] para a governança pública, ou seja, a responsabilidade do gestor em prestar contas de sua gestão e divulgá-las como sinal de transparência de sua governabilidade.

Aliás, nas *smart cities*, a *accountability* é considerada a forma como a seara pública lida com o tratamento e transparência com relação às políticas públicas e tomadas de decisões, ou seja, como o gestor responde às expectativas dos cidadãos, notadamente com relação à proteção dos seus dados pessoais (FERNANDES, 2018, p. 3).

Assim, tanto a *disclosure* quanto a *accountability* são vitais para uma *smart city*, pois geram, ao gestor público, a obrigação de prestar contas e divulgá-las à sociedade, com relação à utilização dos recursos e dados pessoais colhidos que lhe são confiados para serem administrados em favor da coletividade, de forma fiel, justa, objetiva e transparente (ARAÚJO, 2004, p. 16).

É fato que as *smart cities* precisam de um governo sólido, transparente e referência em *e-gov*, para criar um banco de dados seguro, promover sinergia entre políticas públicas, infraestrutura informacional, conteúdo e softwares (KNIGHT, 2006, p. 18), afinal:

---

[14] Referência ao art. 1° da Lei nº 13.709, de 14 de agosto de 2018.
[15] Referência ao art. 37 da Constituição Federal.
[16] Trata-se do processo de divulgação das informações sobre a gestão pública, aos usuários externos.
[17] Referência à Lei Complementar n. 101, de 4 de maio de 2000.
[18] Trata-se da prestação de contas (informação, publicidade, transparência e divulgação) de todos os atos prestados pelo governo.

> As cidades digitais definem uma forma de complementar a organização das cidades reais, reunindo uma vasta gama de redes digitais e softwares, os quais facilitam os múltiplos aspectos sociais e econômicos das vidas nas cidades: comércio, segurança, saúde, educação, trabalho, lazer, transporte e outros (PANHAN, 2016, p. 25)

Isso porque as novas tecnologias abrem possibilidades de interação entre os atores sociais e governamentais, de forma a traduzir vínculos cada vez mais colaborativos e participativos, evidenciando uma tutela proativa e transparente, que contribui para o cumprimento do dever público de informação, transparência e *accountability*, pois:

> A rede se tornou o espaço da liberdade e do pertencimento social que facilita a compreensão da netrópole - cidade virtual ligada por pontos eletrônicos que formam comunidades fechadas e abertas, inter-relacionando-se a partir de múltiplos interesses, desejos e necessidades pessoais e coletivas (GUERREIRO, 2006, p. 18).

Esse é o motivo pelo qual a disponibilização da informação para o cidadão, que é o 'cliente preferencial' da ação estatal, e da maneira como este a processa (digital ou fisicamente), deve ser feita com total transparência pela Administração Pública (TORRES, 2004, p. 42), sendo a *accountability* uma responsabilidade quitável mediante prestação de contas (ARAÚJO, 2004, p. 16).

Assim, o descumprimento do Poder Público, notadamente quanto ao tratamento de dados pessoais, pode acarretar-lhe responsabilidades de várias vertentes, tanto para o ente público quanto para seu gestor, que se submeterão às autoridades nacionais para medidas cabíveis no caso de violação da segurança e proteção de dados pessoais[19].

4. Os ativos de informação na visão do Código de Defesa do Consumidor: um ensaio

Levando-se em consideração o conceito de ativos de informação explanados anteriormente[20], podemos resumi-los como sendo os dados pessoais e privados de alguém e que, por norma constitucional, são invioláveis[21]. Todavia, na Sociedade da Informação, a própria informação foi levada à categoria de mercadoria: possui valor econômico e valor de uso (HARVEY, 2013, p. 18), uma vez que:

> O advento do *Informacionalismo* é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no

[19] Referência ao art. 31 da Lei nº 13.709, de 14 de agosto de 2018.
[20] Vide item 2, pp. 3-4 ou ABNT 27002:2005, p. 21.
[21] Referência ao art. 5°, *caput* e inciso X, da Constituição Federal

> qual há uma gradativa valoração da informação como mercadoria e fator de geração de valor econômico (BARRETO JUNIOR, 2015, p. 6).

Isso significa que, ao tratar da economia da informação e do avanço ininterrupto das tecnologias, por si só, temos ampliados os riscos e a insegurança com relação à privacidade dos dados pessoais dos cidadãos-consumidores (MENDES, 2014, p. 55), necessitando de chancela legal para que a inviolabilidade e proteção aos dados pessoais seja efetiva. E, ao contrário do que grande parte da doutrina defende, o Brasil possui normas abertas capazes de amparar tal inviolabilidade e responsabilizar em caso de vazamento dos dados pessoais. Um dos precursores do conceito de privacidade no Brasil, aliás, foi o Código de Defesa do Consumidor[22], que estabeleceu integral proteção da pessoa nas relações de consumo, incluindo seus interesses econômicos, sua integridade e sua personalidade.

Por tratar-se de uma lei de ordem pública e de função social, intervindo na realidade social e na autonomia da vontade (MARQUES *et al*., 2016, p. 80), o caráter principiológico do Código de Defesa do Consumidor se mostra suficiente para solucionar os conflitos relacionados à violação dos dados pessoais (MENDES, 2014, p. 54). Além disso, a Constituição Federal afirma que o Estado promoverá a defesa do consumidor, na forma da lei[23] e, por ser a informação uma mercadoria, a ordem econômica só será exercida desde que respeite a vida digna e o princípio da defesa do consumidor[24].

Portanto, ao tornar a informação ou os ativos de informação[25] uma mercadoria, paira a aplicabilidade do Código de Defesa do Consumidor à proteção e segurança dos dados pessoais da pessoa, enquanto produto e serviço, notadamente na gestão das *smart cities*.

4.1. Proteção dos dados pessoais: direito básico do consumidor

O Código de Defesa do Consumidor, por tratar-se de uma microssistema permeável, faz interface com outras fontes legais (MARQUES *et al*., 2016, p. 411) e, com o advento da Lei Geral de Proteção de Dados (LGPD), que aporta a defesa do consumidor como fundamento[26], a proteção dos dados pessoais pode ser instituída à categoria de direitos básicos do consumidor, em conformidade com o art. 7° do códex consumerista.

---

[22] Referência à Lei nº 8.078, de 11 de setembro de 1990.
[23] Referência ao art. 5°, inciso XXXII, da Constituição Federal.
[24] Referência ao art. 170, *caput* e seu inciso V, da Constituição Federal.
[25] Vide item 2, pp. 3-4 ou ABNT 27002:2005, p. 21.
[26] Referência ao art. 2°, inciso VI da Lei nº 13.709, de 14 de agosto de 2018.

4.2. Proteção dos dados pessoais: direito ao acesso à informação e sua veracidade

O reconhecimento da proteção dos dados pessoais como direito básico do consumidor envolve uma dupla dimensão de tutela: em primeiro lugar, a tutela contra os riscos que ameaçam a personalidade do consumidor com relação à coleta, armazenamento, processamento, utilização e circulação de seus dados pessoais e, em segundo lugar, a garantia que o consumidor possui em controlar o fluxo de seus dados na Sociedade da Informação (MENDES, 2014, p. 56).

A primeira tutela diz respeito ao direito que o consumidor tem em acessar as informações ao seu respeito e que estas sejam verídicas, notadamente àquelas coletadas para prestação de serviços públicos, como é o caso do RG, CPF, antecedentes criminais, cadastros em órgãos públicos, previsto constitucionalmente[27] e plausível de *habeas data*[28].

A segunda tutela refere-se ao controle dos dados pessoais pelo próprio consumidor, também denominado autodeterminação informativa, com a salvaguarda de sua boa-fé objetiva e liberdade material (MENDES, 2014, p. 56), apesar do fluxo de dados na aquisição de produtos e serviços, e que não exclui a responsabilidade do fornecedor em salvaguardar seus dados pessoais.

4.3. Proteção dos dados pessoais: legitimidade

O tratamento dos dados pessoais, seja por órgão público ou privado, deve ser autorizado pelo consumidor (dimensão subjetiva), uma vez que, se afetam sua personalidade, somente este pode decidir a respeito do fluxo de seus dados (MENDES, 2014, p. 57), salvo se houver previsão legal ou casos excepcionais que dispensem sua autorização.

Além disso, a proteção dos dados pessoais deve respeitar a boa-fé objetiva, as expectativas do consumidor, os impactos e riscos (dimensão objetiva) na coleta, armazenamento, processamento, utilização e circulação desses dados, notadamente se houver informação sobre todas as condições no tratamento e proteção destes (MENDES, 2014, pp. 57-59).

[27] Referência ao art. 5°, inciso XXXIII, da Constituição Federal.
[28] Referência ao art. 5°, inciso LXXII, da Constituição Federal.

A legitimidade do consumidor para reclamar pela proteção e tratamento dos seus dados pessoais, portanto, parte do pressuposto de um negócio jurídico, pois, como dito anteriormente, a informação é uma mercadoria e, como tal, deve ser tratada como produto e serviço em conformidade com o Código de Defesa do Consumidor.

4.4. Proteção dos dados pessoais: produto e serviço

Sendo a informação uma mercadoria (BARRETO JUNIOR, 2015, p. 6), cumpre-nos analisar a economia da informação pessoal (dados pessoais, tecnologia e o mercado) sob a ótica do Código de Defesa do Consumidor. A informação, aqui considerada como os dados pessoais e seu tratamento pelo fornecedor, é um ativo intangível, portanto, bem material (se sua base for contratual, documental, na forma física) ou imaterial (se for base de dados, arquivos na nuvem ou armazenados no sistema), caracterizando um produto[29].

A informação, enquanto direito de obtenção e proteção do consumidor e dever de prestação e tratamento pelo fornecedor, também é um serviço[30] e, principalmente nas *smart cities*, caracteriza um serviço público tanto com relação ao tratamento dos ativos informacionais quanto ao sigilo, privacidade e repasse das informações de forma verídica, transparente e precisa.

4.5. Violação da proteção dos dados pessoais: responsabilidades do fornecedor

A Sociedade da Informação trouxe ao fornecedor o papel de guardião de acesso aos dados pessoais dos consumidores, assim considerando na economia do compartilhamento, viabilizada pelo consumo de produtos e serviços pela internet, celulares e computadores (MARQUES *et al*., 2016, p. 199).

Nesse caso, havendo violação e vazamento dos dados pessoais, a responsabilização do fornecedor ocorrerá pelo Código de Defesa do Consumidor, levando-se em consideração a legitimidade do consumidor (quem teve seu direito básico de proteção aos dados pessoais

[29] Referência ao art. 3°, §1° do Código de Defesa do Consumidor.
[30] Referência ao art. 3°, §2° do Código de Defesa do Consumidor.

violados) e do fornecedor (quem tinha o dever da inviolabilidade dos dados pessoais, o guardião da informação que quebrou seu dever de proteção).

Considerações Finais

A análise proposta neste artigo restou evidente a inter-relação entre informação, segurança, privacidade e transparência, bem como a responsabilidade estatal para salvaguardar os dados pessoais dos cidadãos, notadamente na Sociedade da Informação, onde há intenso volume de compartilhamento dos ativos de informação. Ainda, restou notório que as tecnologias de informação e comunicação (TIC's) podem fortalecer a democracia, ampliar o exercício da cidadania, promover o controle social, inibir a corrupção e contribuir para a segurança da informação de forma mais eficaz, principalmente se adotadas nas *smart cities* de forma a conceber um portal *e-gov* que respeite a Lei de Acesso à Informação, mas é preciso implantar plataformas de segurança que impeçam invasões, violações e insegurança no acesso dessas informações.

Também foram apresentados, de forma detalhada, os ativos de informação em sua linguagem mais técnica, trazendo à realidade jurídica a contextualização dos dados pessoais dos cidadãos, bem como a *accountability* como elemento basilar para a proteção e inviolabilidade da segurança desses ativos.

Por outro lado, o artigo fez um ensaio sobre a legislação vigente sobre os ativos de informação e as responsabilidades provenientes de sua coleta, armazenamento, uso e disseminação destes, principalmente com a inserção do Código de Defesa do Consumidor e a nova Lei Geral de Proteção de Dados.

Sob a ótica das *smart cities*, portanto, ficou demonstrado que o Brasil está adequado e juridicamente revestido com relação à privacidade e eventual vazamento dos dados pessoais, principalmente no que concerne à informação como serviço público que, vinculada ao Código de Defesa do Consumidor; todavia, ainda há um longo caminho para as smart cities na adoção da Segurança da Informação a fim de garantir a segurança dos ativos de informação.

Referências Bibliográficas

ARAÚJO, Inaldo da Paixão Santos. *Introdução à auditoria operacional*. 2ª ed. Rio de Janeiro: Editora FGV, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. *ABNT NBR ISO/IEC 27002:2005*: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. São Paulo/Rio de Janeiro: ABNT, 2005.

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells, p. 100-127. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira (orgs.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015.

BERLO, David K. *O processo da comunicação.* 2ª ed. São Paulo: Martins Fontes, 1999.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília/DF: Supremo Tribunal Federal/Secretaria de Documentação, 2018.

CARNEIRO, Leonardo Geral dos Santos. *O uso da informação como diferencial estratégico e competitivo para as organizações*. Belo Horizonte/MG: UFMG, 2013.

D'ANDREA, Edgar R. Pacheco. Segurança da informação: a importância estratégica. In: DUBOIS, Richard; LINS, João. *Inovação na gestão pública*. São Paulo: Saint Paul Editora, 2012.

GEHL, Jan. *Cidades para pessoas*. 2ª ed. São Paulo: Perspectiva, 2013.

GUERREIRO, Evandro Prestes. *Cidade digital*: infoinclusão social e tecnologia em rede. São Paulo: Editora Senac São Paulo, 2006.

HARVEY, David. *Para entender o capital*, livro I. São Paulo: Boitempo Editorial, 2013.

HOLTHE, Leo Van. *Direito Constitucional*. 5ª ed. Salvador/BA: JusPODIVM, 2009.

KNIGHT, Peter. *Rumo ao e-Brasil*. Rio de Janeiro: Garamond, 2006.

KONZEN, Marcos Paulo. *Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança*. 121 f. Dissertação (Mestrado em Engenharia de Produção). Universidade Federal de Santa Maria - UFSM/RS: Santa Maria, 2013.

LIMA, Adriano. *Gestão da segurança e infraestrutura de tecnologia da informação*. São Paulo: Editora Senac São Paulo, 2018.

MACHADO, Paulo Affonso Leme. *Direito à informação e meio ambiente*. São Paulo: Malheiros Editores Ltda., 2006.

MARCELO, Antonio; PEREIRA, Marcos. *Engenharia social*: hackeando pessoas. Rio de Janeiro: Brasport, 2005.

MARQUES, Claudia Lima; BENJAMIN, Antônio Herman V.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 5ª ed. São Paulo: Revista dos Tribunais, 2016.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

_____. O direito básico do consumidor à proteção de dados pessoais. *Revista de Direito do Consumidor (RDC)*, v. 23, n. 95, p. 53-75. São Paulo: Revista dos Tribunais, set./out. 2014.

MONTEIRO, Jorge Ferreira Sinde. *Responsabilidade por conselhos, recomendações ou informações*. Coimbra/Portugal: Almedina, 1989.

PANHAN, André Marcelo. *Construindo cidades inteligentes*. Curitiba: Appris, 2016.

SANTAELLA, Lucia (org.). *Cidades inteligentes*: por que, para quem? São Paulo: Estação das Letras e Cores, 2016.

SAUAIA, Hugo Moreira Lima. *A proteção dos dados pessoais no Brasil*. Rio de Janeiro: Lumen Juris, 2018.

TORRES, Marcelo Douglas de Figueiredo. *Estado, democracia e administração pública no Brasil*. Rio de Janeiro: EDitora FGV, 2004.

***Websites* Consultados**

BRASIL. *Constituição Federal*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 30/06/2018.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 21/08/2018.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*: Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21/08/2018.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*: Lei de Acesso à Informação (LAI). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 26/7/2018.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*: Código de Defesa do Consumidor (CDC). Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078compilado.htm>. Acesso em: 26/7/2018.

BRASIL. *Lei Complementar nº 101, de 4 de maio de 2000:* Lei de Responsabilidade Fiscal. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp101.htm>. Acesso em: 30/06/2018.

DONEDA, Danilo. *Um panorama de proteção de dados para as cidades inteligentes*. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-panorama-de-protecao-de-dados-para-as-cidades-inteligentes-04072018>. Acesso em 06/07/2018.

FERNANDES, Katy. *O princípio da responsabilidade pró-ativa "Accountability"*. Disponível em: <https://pt.linkedin.com/pulse/o-principio-de-responsabilidade-pr%C3%B3-ativa-katy-fernandes>. Acesso em: 02/07/2018.

LOPES, Karen M. Gross; MACADAR, Marie Anne; LUCIANO, Edimara Mezzomo. Valor público: o cidadão no centro da gestão pública, p. 75-84. In: MARTINHÃO, Maximiliano Salvadori (coord.). *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro*: TIC governo eletrônico 2017. São Paulo: CGI.br, 2018. Disponível em: <https://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>. Acesso em: 30/06/2018.

MARTINHÃO, Maximiliano Salvadori (coord.). *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro*: TIC governo eletrônico 2017. São Paulo: CGI.br, 2018. Disponível em: <https://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf>. Acesso em: 30/06/2018.

SPARROW, Elizabeth. *The information dividend*: why it makes you 'happier'. London: The British Computer Society (BCS)/The Chartered Institute for IT, september/2010. Disponível em: <http://policy.bcs.org/sites/policy.bcs.org/files/info-dividend-full-report.pdf0___.pdf>. Acesso em: 03/06/2018.

THE NOVA INSTITUTE OF PHILOSOPHY - IFILNOVA. Dicionário de filosofia moral e política. Lisboa/Portugal: Faculty of Social and Human Sciences (FCSH)/Universidade Nova de Lisboa, 2018. Disponível em: <http://www.ifilnova.pt/file/uploads/20b80ffab42e5adbe998e8d35b6450a0.pdf>. Acesso em: 26/07/2018.

UNIÃO EUROPEIA. *Diretiva 95/46/CE, de 24 de outubro de 1995*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 30/06/2018.

UNIÃO EUROPEIA. *Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE, de 27 de abril de 2016*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 30/06/2018.