FÁBIO CORREA XAVIER
LUCAS PAGLIA
COORDENAÇÃO

BOAS PRÁTICAS PARA OS MUNICÍPIOS BRASILEIROS

CONSELHEIRO DIMAS RAMALHO
APRESENTAÇÃO
MINISTRO AUGUSTO NARDES
PREFÁCIO

ADEMIR BENTO SIMÃO
ANA CARLA BLIACHERIENE
ANDRA ROBERT DE CARVALHO CAMPOS
ANDRESSA CARVALHO DA SILVA
ANDREY GUEDES OLIVEIRA
BEATRIZ SCAVAZZA
BRUNO HENRIQUE CORDEIRO DE SOUZA
CAMILA NASCIMENTO
DÁVIS ALVES
EDUARDO TUMA
ELIZABETE CAMPOS
FÁBIO CORREA XAVIER
FÁTIMA L. S. NUNES
FERNANDO ANTONIO TASSO
JULIA LONARDONI RAMOS
LUCAS PAGLIA
LUCIANO VIEIRA DE ARAÚJO
LUIS MÁRCIO BARBOSA
MARIA BERNARDETE FERREIRA
MARIA GABRIEL GRINGS
MATUSALÉM DOS SANTOS CARVALHO
MELISSA GIACOMETTI DE GODOY
NILSON BRITO
PATRÍCIA PECK PINHEIRO
RAFAEL FELGUEIRAS ROLO
RENATO MÜLLER DA SILVA OPICE BLUM
RICARDO CAMPOS
RHIMA AHMAD CHARANEK SANTANA
RODRIGO HIROSHI RUIZ SUZUKI
SABRINA LUCILA DE ARAUJO
VANESSA D'ALESSIO GIARONE SUZUKI
VERENA IANNINO SOARES ROLO
WALLACE DA SILVA PEREIRA

IGCP
INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLIC
MENTE ABERTA
RGB
DA GOVERNANÇA À ESPERANÇA

BOAS PRÁTICAS PARA OS MUNICÍPIOS BRASILEIROS

FÁBIO CORREA XAVIER
LUCAS PAGLIA
COORDENAÇÃO

BOAS PRÁTICAS PARA OS MUNICÍPIOS BRASILEIROS

CONSELHEIRO DIMAS RAMALHO
APRESENTAÇÃO
MINISTRO AUGUSTO NARDES
PREFÁCIO

ADEMIR BENTO SIMÃO
ANA CARLA BLIACHERIENE
ANDRA ROBERT DE CARVALHO CAMPOS
ANDRESSA CARVALHO DA SILVA
ANDREY GUEDES OLIVEIRA
BEATRIZ SCAVAZZA
BRUNO HENRIQUE CORDEIRO DE SOUZA
CAMILA NASCIMENTO
DAVIS ALVES
EDUARDO TUMA
ELIZABETE CAMPOS
FÁBIO CORREA XAVIER
FÁTIMA L. S. NUNES
FERNANDO ANTONIO TASSO
JULIA LONARDONI RAMOS
LUCAS PAGLIA
LUCIANO VIEIRA DE ARAÚJO
LUIS MÁRCIO BARBOSA
MARIA BERNARDETE FERREIRA
MARIA GABRIELA GRINGS
MATUSALÉM DOS SANTOS CARVALHO
MELISSA GIACOMETTI DE GODOY
NILSON BRITO
PATRÍCIA PECK PINHEIRO
RAFAEL FELGUEIRAS ROLO
RENATO MÜLLER DA SILVA OPICE BLUM
RICARDO CAMPOS
RHIMA AHMAD CHARANEK SANTANA
RODRIGO HIROSHI RUIZ SUZUKI
SABRINA LUCILA DE ARAUJO
VANESSA D'ALESSIO GIARONE SUZUKI
VERENA IANNINO SOARES ROLO
WALLACE DA SILVA PEREIRA

IGCP
INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO
MENTE ABERTA
RGB
DA GOVERNANÇA À ESPERANÇA

Coordenação Editorial
Pedro Camilo de Figueirêdo Neto

Conselho Editorial

DOUTORES:
Fábio S. Santos
Ionã Carqueijo Scarante
João Evangelista do Nascimento Neto
José Gileá
José Rômulo de Magalhães Filho
Luciano Sérgio Ventim Bomfim
Maria João Guia (Portugal)
Nadialice Francischini de Souza
Régia Mabel Freitas
Ricardo Maurício Freire Soares
Sheila Marta Carregosa Rocha
Urbano Félix Pugliese do Bomfim

MESTRES:
Angelo Boreggio
Bruno Barbosa Heim
Daniela Magalhães Costa de Jesus
Isan Almeida Lima
Jerusa de Arruda
Katia Maria Mendes da Silva
Magno Conceição das Merces
Marcelo Politano de Freitas
Pedro Camilo de Figueirêdo Neto
Raphael Lima R. Leal
Sueli Bonfim Lago

Programação Visual de Capa
Fernando Campos

Diagramação
Alfredo Barreto

Revisão
Adriano Ferreira & Joana Cunha

A reprodução total ou parcial desta obra, por qualquer modo, somente será permitida com autorização da editora.
(Lei nº 9.610 de 19.02.1998)

CIP – Brasil. Catalogação na fonte

Xavier, Fábio Correa; Paglia, Lucas -
LGPD: boas práticas para os municípios brasileiros / coordenação Fábio Correa Xavier e Lucas Paglia – Salvador, BA: Editora Mente Aberta, 29 de setembro de 2022.

238 p.
ISBN: 978-85-66960-57-0

1. LGPD. 2. Boas práticas. 3 Municípios. I. Xavier, Fábio Correa. II. Paglia, Lucas. III. Título.

CDD 340

Impresso no Brasil

Rede Governança Brasil - RGB

DIRETORIA EXECUTIVA
Presidente – Petrus Elesbão Lima da Silva
Vice-presidente - Flávio Feitosa Costa
Diretor administrativo-Financeiro - Henrique Farinon
Diretor jurídico - Leonardo Andreotti Paulo de Oliveira
Diretora de relações institucionais - Elise Eleonore de Brites

CONSELHO DE ADMINISTRAÇÃO
Presidente – Prof. Luiz Antonio Peixoto Valle
Vice–presidente – Francisco Alexandre Colares Melo Carlos
Conselheiro – Nelson Teich
Conselheira – Vera Raquel Lopes Linhares da Silva
Conselheiro – Paulo Renato Menzel
Conselheiro – João Felipe Cunha Pereira
Conselheira – Carla Simone Viana Lage

CONSELHO DE ÉTICA
Presidente – Roberta Muniz Codignoto
Conselheiro Titular – Bruno Galvão Ferola
Conselheira Titular – Marcella Blok
Conselheira Suplente – Clarissa Freitas Rodrigues de Lima Carvalho

CONSELHO FISCAL
Presidente – Renata Andrade Santos
Conselheiro Titular – Elys Tevânia
Conselheiro Suplente – Walter Marinho

COMITÊ RESPONSÁVEL PELO PROJETO
Comitê de Governança em Lei Geral de Proteção de Dados – LGPD

COORDENAÇÃO DO COMITÊ DE GOVERNANÇA EM LEI GERAL DE PROTEÇÃO DE DADOS - LGPD
Fábio Correa Xavier
Lucas Paglia

COORDENAÇÃO DA PUBLICAÇÃO
Cristiane Nardes Farinon

GERENTE DE OPERAÇÕES
Cíntia Caroline da Silva e Silva Reis

Instituto Latino-Americano de Governança e Compliance Público – IGCP

PRESIDENTE
Ricardo Todeschini Zilio

CONSELHO FISCAL
Presidente do Conselho Fiscal – João Benício Aguiar
Conselheira – Izabela Zanotelli Collares
Conselheiro – Luiz Gustavo Wiechoreki

DIRETORIA EXECUTIVA
Diretora administrativa, de ensino e projetos - Dinaura Tedesco
Diretor financeiro - Henrique Farinon
Diretora de governança - Cristiane Nardes

GERÊNCIA DE PROJETOS
Celina Rocha Franco

COORDENAÇÃO DE PROJETOS
Sérgio Ricardo Costa Reis
João Vitor Machado Barbosa

CONSULTORA JURÍDICA
Ana Carolina Massa Gomes

DEDICATÓRIAS

À minha amada companheira de todas as horas, Andressa Carvalho, pelo apoio e amor incansável e ilimitado. Te amo!

Aos meus amados pais, Ana e Raimundo (*in memoriam*), pilares da minha formação como pessoa.

Aos meus amados filhos, Gabriel e Isabella. Que eu tenha a sabedoria de meus pais para servir de exemplo para vocês.

Fábio Correa Xavier

À Bruna, minha dose diária de iluminação para ser uma pessoa melhor.

Aos meus queridos pais e alicerces: Alfio e Ligia. À minha amada irmã e exemplo de perseverança, Luciana.

Às raízes de minha vida, meus avós maternos e paternos, que até hoje seguem sendo inspiração para a construção da minha família.

Lucas Paglia

SOBRE OS COORDENADORES

FÁBIO CORREA XAVIER

Diretor do Departamento de Tecnologia da Informação (CIO) do Tribunal de Contas do Estado de São Paulo. Professor e coordenador de graduação na Faculdade Descomplica. Colunista do MIT Technology Review. Secretário executivo do Comitê Gestor de Tecnologia, Governança e Segurança da Informação dos Instituto Rui Barbosa (IRB(. Coordenador do Comitê de LGPD e do Comitê de Tecnologia e Inovação da Rede Governança Brasil (RGB). Membro do Conselho de Administração do Instituto do Câncer Dr. Arnaldo. Profissional certificado Exin Privacy and Data Protection. Mestre em Ciência da Computação pela USP. MBA em Gestão de Negócios pelo IBMEC-RJ. Especialização Network Engineering pela JICA-Japão. Pós-graduado em Lei Geral de Proteção de Dados. Pós-graduado em Direito Público. Pós-graduado em Gestão Pública e Responsabilidade Fiscal. Pós-graduado em Projetos de Redes. Possui mais de 30 anos de experiência na área de tecnologia e segurança da informação, com atuação em empresas de grande porte, do setor público e privado. Atuação por mais de quinze anos em atividades de ensino, como professor, coordenador de graduação, pós-graduação e coordenação geral. Avaliador de curso do Basis do MEC/INEP e professor integrante das comissões assessoras do Enade/2008 e Enade/2011, na área de redes de computadores. Alguns prêmios e reconhecimentos recebidos: Prêmio de Inovação Judiciário Exponencial (Executivo de Tecnologia, edição 2022); Prêmio Empresa +Digital 2020, categoria Governo; Ranking 100 Empresas + Inovadoras no Uso de TI 2020, 2021 e 2022 (TCESP); Prêmio Security Leaders Case do Ano 2020, sendo um dos finalistas em 2019. Finalista do prêmio CIO Destaque no CIO Jud Nacional de 2019. CIO homenageado na cerimônia 4Network Awards 2019. Ganhador do Prêmio Security Leaders 2013, na área de Governo, sendo finalista em outras duas oportunidades: 2014 e 2018. Autor dod livrod: *Roteadores Cisco: guia básico de configuração e operação* (Novatec, 2010), *Tecnologias, Inovação e outros assuntos em análise* (Amazon, 2021) e *LGPD no setor público: boas práticas para a Jornada de Adequação* (Clube de Autores/Amazon, 2022). É coautor: do ebook *Cartilha de*

Governança em Proteção de Dados para Municípios (RGB/Mente Aberta, 2021); do capítulo "Ações para adequação à LGPD pela Administração Pública" no e-book *Comentários à Lei Geral de Proteção de Dados Pessoais* (Migalhas, 2021); do capítulo "Passos mínimos necessários para adequação à LGPD pelas cortes de contas brasileiras" no livro *Os Tribunais de Contas, a pandemia e o futuro do controle* (Fórum, 2021). Publicou diversos artigos nos portais Jota, Migalhas e MIT Technology Review Brasil.

LUCAS PAGLIA

Sócio-fundador da LP Consultoria em Privacidade. Sócio-fundador da P&B Compliance. Pós-graduado em Compliance pela Fundação Getúlio Vargas (FGV), certificado pelo Insper em Proteção de Dados & Privacidade, certificado como especialista e como PMO (líder de projeto) para Governança em Privacidade pelo Data Privacy Brasil e formado pelo Colégio Brasileiro de Executivo de Saúde (CBEX) de especialização em Healthcare Compliance. Especialista em cibersegurança pela Universidade de Harvard. Especialista convidado do GT-1 ANPD/CNPD para elaboração da Política Nacional de Proteção de Dados. Coordenador do Comitê de LGPD da Rede Governança Brasil (RGB). Membro do Comitê de Privacidade e DPO da Federação Paulista de Futebol (FPF). Membro do Fórum Permanente das Microempresas e Empresas de Pequeno Porte (Sebrae). Conselheiro fiscal da Associação Latino-Americana de Governança. DPO da Willis Towers Watson Brasil e demais empresas. Professor da Puccamp, Universidade Caxias do Sul, Unindústria Corporativa Sesi Senai e professor convidado do Colégio Brasileiro de Executivos de Saúde - CBEX.

SOBRE OS AUTORES

ADEMIR BENTO SIMÃO

Consultor na Fundação Carlos Alberto Vanzolini (FCAV), graduado em Administração de Empresas, pós-graduado em Comércio Eletrônico pela ESPM, com especialização em Projetos e Processos e atualização em LGPD pela FCAV.

BEATRIZ SCAVAZZA

Coordenadora Executiva de Projetos Estratégicos da área de Gestão de Tecnologias em Educação da Fundação Carlos Alberto Vanzolini há 22 anos. Doutora em Psicologia da Educação, respondeu pela implantação e gestão das áreas de Extensão Universitária da Pontifícia Universidade Católica de São Paulo (PUC-SP) no período de 1990 a 1996, instituição em que ocupou a posição de professora titular, e também da Universidade de Mogi das Cruzes (1997-1999).

ANA CARLA BLIACHERIENE

Advogada. Professora de Direito da EACH-USP (Gestão de Políticas Públicas). Livre-docente em Direito Financeiro (USP). Mestre e doutora em Direito (PUC-SP). Diretora presidente da Escola Superior de Gestão e Contas do Tribunal de Contas do Município de São Paulo. Coordenadora do Comitê "Inovação, Transição Digital de Governos e Avaliação de Políticas Públicas" do Instituto Rui Barbosa. Conselheira do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), Conselho Consultivo da ANPD. Coordenadora do Grupo de Pesquisas SmartCitiesBr (USP) e da Especialização em Políticas Públicas para Cidades Inteligentes (USP/TCE-CE). Vice-coordenadora da Especialização Auditoria e Inovação para o Setor Público (USP/IRB). Atua nas áreas de inovação, Lei Geral de Proteção de Dados (LGPD), novas tecnologias aplicadas à gestão pública e Smart Cities (cidades inteligentes), finanças públicas e orçamento, gestão, políticas públicas, controle, eficiência e transparência do Estado e da administração pública.

ANDRA ROBERT DE CARVALHO CAMPOS

Subsecretária de Serviços ao Cidadão, Tecnologia e Inovação na Secretaria de Governo do Estado de São Paulo. Experiência em gestão administrativa, da qualidade, processos e projetos de gestão de contratos corporativos e gestão documental; revisão de procedimentos, metas, indicadores da qualidade e melhoria contínua a partir do escopo da ISO 9001:2000; implantação e reestruturação de áreas orgânicas, quanto ao seu planejamento e estratégias; implantação e gestão de projetos segundo a metodologia PMI, implantação ERP acompanhando os prazos e cronograma e desenvolvimento de site institucional – Portal. Vivência na implementação e implantação de sistemas de gerenciamento empresarial – análises de desempenho e alocação de recursos humanos, condução de equipes, causas e implementações de melhorias; elaboração de diagnóstico físico e funcional visando reestruturação de diretorias.

ANDRESSA CARVALHO DA SILVA

Assessora técnica no Tribunal de Contas do Estado de São Paulo. Advogada, especialista em Direito Público pela Escola de Magistratura Estadual do Rio Grande do Sul (Esmafe/RS) e especialista em Processo Civil pela UniDomBosco. Realiza, atualmente, pós-graduação em Direito Tributário e em Direito Penal e Processual Penal. Possui, ademais, graduação em Licenciatura em Letras pelo Instituto de Biociências, Letras e Ciências Exatas (2005), e é mestre e doutora em Estudos Linguísticos pelo Instituto de Biociências, Letras e Ciências Exatas.

ANDREY GUEDES OLIVEIRA

Especialista em Segurança da Informação, Governança de TI e Privacidade de Dados, com mais de 20 anos de experiência em tecnologia no mercado nacional e internacional. Docente de MBAs, pós-graduação e graduação nas áreas de Segurança e Tecnologia da Informação e Administração de Empresas.

BRUNO HENRIQUE CORDEIRO DE SOUZA

Advogado no Opice Blum, Bruno e Vainzof Advogados. Pós-graduado em Direito Civil pela Escola Paulista de Direito (EPD).

CAMILA NASCIMENTO

Advogada formada pelo Centro de Estudos Superiores Aprendiz, Barbacena, Minas Gerais. Pós-graduada em Direito Constitucional Aplicado, Faculdade Damásio de Jesus. Pós-graduada em Direito Empresarial (Faculdade Legale). Pós-graduanda em Processo Civil Empresarial e Lei Geral de Proteção de Dados Pessoais (Faculdade Legale). Especialista em Direito Civil e Comunicação (Associação Brasileira de Direito Civil em parceria com a Faculdade de Direito da Universidade de Coimbra, Portugal). Especialista em Direito Digital, Novas Tecnologias e Novos Temas de Proteção de Dados (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP). Certificada Data Protection Officer (Itcerts, Canadá). Certificada ISFS e PDPP (Exin).

DAVIS ALVES

Doutor em Administração de TI (Ph.D) na Florida Christian University (EUA), convalidado no Brasil. Mestre em Administração com foco em TI Verde (2015). Extensão em Gestão de TI pela FGV/SP (2011). Pós-graduado em Gerenciamento de Projetos (2009). Graduado em Redes de Computadores e Internet (2008). Residiu para estudos nos Estados Unidos e Nova Zelândia. Possui as certificações ITIL® Expert, 4 MP, COBIT®, ISO-20000®, ISO-27002®, EXIN® Agile Scrum Master, Lean IT, Green IT, ICS MCSA® Windows Server 2003, Cloud Computing, EXIN® Data Protection Officer (DPO) e CISO – Certified Information Security Officer – ISO-27001 Professional, Cyber Security. Psicanalista. Ethical Hacker (Human Hacking através da Fisiognomonia). DAC® Wireless. DCP® Switching. DSS® IP Surveillance. É consultor de Gestão de Sustentabilidade de TI, com produtos e consultorias em Green IT para órgãos públicos municipais do Brasil, além de consultor em privacidade de dados (LGPD). Em 2019 assumiu como presidente da ANPPD®. Figura como DPO pioneiro no Brasil na área de Segurança da Informação & Ethical Hacker, tendo formado mais de 4,5 mil DPOs no país. Em 2020 recebeu o título de Membro de Honra da Digital Law Academy passando a integrar o seleto grupo do Conselho Superior, que reúne os mais respeitados juristas federais, desembargadores e grandes nomes do Direito Digital no Brasil. Membro do Conselho Nacional de Proteção de Dados (CNPD), nomeado como suplente pelo presidente da República do Brasil. Atuou como sócio-gerente na Millennium Hardware® responsável pela coordenação técnica de projetos de infraestrutura de TI, além de lecionar Gestão de Serviços, Segurança da Informação e Redes de Computadores na Universidade Paulista (Unip) como professor

titular. Professor concursado da Universidade Municipal de São Caetano do Sul (USCS). Professor da Universidade Federal de São Carlos – (UFSCar) e DARYUS/Faculdade Impacta. Academicamente é membro do Congresso Científico Internacional POMS, nos Estados Unidos, onde participa como presidente da sessão de Sustentabilidade. Já no Brasil faz parte do Núcleo Desenvolvedor Estruturante (NDE) da Universidade Paulista do curso superior de Tecnologia em Redes de Computadores, responsável pela adequação do curso junto ao MEC, onde obteve a nota máxima (5). Também responde como instrutor credenciado pelo Exin/PeopleCert com foco em ITIL®, GDPR, ISO-27001®, Green IT, além de pesquisador e palestrante em diversos eventos científicos internacionais relacionados com TI Verde & GDPR na Espanha, Holanda e Estados Unidos – tendo seus estudos publicados nesses países.

EDUARDO TUMA

Conselheiro do Tribunal de Contas do Município de São Paulo. Advogado, ex-presidente da Câmara Municipal de São Paulo e ex-vereador pela Cidade de São Paulo (2013/2016 e 2017/2020). Licenciado de Abril a Maio de 2018 para ocupar o cargo de secretário-chefe da Casa Civil da Prefeitura de São Paulo. Atualmente é professor doutor do Centro Universitário das Faculdades Metropolitanas Unidas (FMU/SP) e da Universidade Nove de Julho (Uninove). Pós-doutor em Direito pela Universidade Paris I, Panthéon-Sorbonne, e doutorando em Filosofia pela PUC/SP. Doutor em Filosofia do Direito e mestre em Direito do Estado pela PUC/SP. Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU/SP) e em Teologia pelo IBES/SP. Possui extensão universitária pela Universidade de Harvard (Government-Modern Presidential Politics) e especialização em Direito Tributário pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU/SP).

ELIZABETE CAMPOS

Consultora na Fundação Carlos Alberto Vanzolini (FCAV), graduada em Letras pela Universidade São Judas Tadeu, com formação técnica em qualidade e produtividade (USP/Cecae) e ferramentas de gestão pela FCO.

FÁTIMA L. S. NUNES

Professora titular da Universidade de São Paulo. Bacharel em Ciência da Computação pela Universidade Estadual Paulista Júlio de Mesquita. Mestre em Engenharia Elétrica pela Universidade de São Paulo. Doutora em Ciências (Física Computacional) pela Universidade de São Paulo. Livre-docente pela Universidade de São Paulo, na área de Processamento Gráfico. Suas pesquisas são predominantemente na área de computação, com ênfase em realidade virtual, processamento de imagens, recuperação de dados multimídia por conteúdo. Possui ampla experiência na gestão pública, em especial na área acadêmica. Durante cinco anos foi diretora de tecnologia da informação da Superintendência de Tecnologia de Informação da USP. Atualmente coordena o Escritório de Gestão de Indicadores de Desempenho Acadêmico (Egida-USP).

FERNANDO ANTONIO TASSO

Juiz de direito em São Paulo. Graduado em Direito pela PUC-SP. Especialista em Gestão e Governança de Tecnologia da Informação pela FIAP. Juiz formador de magistrados habilitado pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam). Coordenador de Tecnologia da Informação e Direito Digital da Escola Paulista da Magistratura (EPM), onde também é coordenador do Núcleo de Estudos em Direito Digital.

JULIA LONARDONI RAMOS

Advogada, cursando LLM em Direito Digital na Universidade Presbiteriana Mackenzie. Formada em Direito pela Pontifícia Universidade Católica do Paraná. É Certified Information Privacy Professional/Europe (CIPP/E) e Certified Information Privacy Manager (CIPM) pela International Association of Privacy Professionals (IAPP). Data Protection Officer (DPO) pela Exi.

LUCIANO VIEIRA DE ARAÚJO

Livre-docente da área de dados da EACH (USP). Professor do curso de Sistemas de Informação (EACH-USP). Doutor em Bioinformática e mestre em Ciência da Computação pela USP. Realiza pesquisas na área

de ciência de dados (*learning from data*, *big data*, *data science* e No Sql) aplicada a inovação tecnológica aplicada à gestão pública, transformação digital governamental e cidades inteligentes. Coordenador do grupo de Pesquisas USP SmartCitiesBr. Coordenador tecnológico do projeto do Museu do Ipiranga Virtual. Vice-coordenador da Especialização em Políticas Públicas para Cidades Inteligentes (USP/TCE-CE). Chefe de gabinete da Escola Superior de Gestão e Contas do Tribunal de Contas do Município de São Paulo, onde desenvolve projeto de transformação digital da educação. Membro do Comitê "Inovação, Transição Digital de Governos e Políticas Públicas" do Instituto Rui Barbosa. Revisor de revistas científicas nacionais e internacionais e de projetos de pesquisa para a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp). Recebeu prêmios nacionais e internacionais na área de ciência e inovação.

LUIS MÁRCIO BARBOSA

Coordenador executivo da área de Gestão de Tecnologias em Educação da Fundação Carlos Alberto Vanzolini. Psicólogo pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Tem atuado no apoio à gestão de portfólio de projetos educacionais em larga escala com o apoio de tecnologias de comunicação e informação.

MARIA BERNARDETE FERREIRA

Assessora em Direito Administrativo na Fundação Carlos Alberto Vanzolini (FCAV). Graduada em Jornalismo pela Escola de Comunicações e Artes (USP) e Direito pela Faculdade São Marcos, São Paulo.

MARIA GABRIEL GRINGS

Mestre e doutora em Direito Processual pela Faculdade de Direito da Universidade de São Paulo (USP). Bacharel em Direito pela Universidade Federal do Paraná (UFPR). Pesquisadora do Instituto Legal Grounds. Advogada.

MATUSALÉM DOS SANTOS CARVALHO

Consultor Sênior na Fundação Carlos Alberto Vanzolini (FCAV). Graduado em Tecnologia da Informação e Administração, pós-graduado

em Engenharia de Produção, Qualidade e Logística pelo Instituto de Pesquisa Tecnológica de São Paulo (IPT) e em Gestão Empresarial pela FGV/SP. Certificado CBPP pela ABPMP Internacional. Atualizações em Compliance pela FGV e ONU, bem como em LGPD pela FCAV.

MELISSA GIACOMETTI DE GODOY

Geógrafa formada pela Universidade de São Paulo em 2002. Doutora pelo Programa de Pós-Graduação em Geografia Humana da USP desde 2009. Estudou a política municipal de habitação em São Paulo após 1988 e o Programa de Arrendamento Residencial. Foi bolsista Capes. Trabalha no Governo do Estado de São Paulo (GESP) desde 2011 até 2018. Desde 2015 é gestora de projetos e assessora na Coordenadoria de Serviços ao Cidadão da Secretaria de Governo. No Gesp, também foi assessora e diretora de Planejamento Metropolitano e Territorial, na então Secretaria de Planejamento e Desenvolvimento Regional do Estado de São Paulo (2012-2014), e assessora na então Secretaria de Gestão Pública (2011). Foi gestora de ensino e pesquisa na Fundação João Pinheiro, instituição do Governo de Minas Gerais (2010-2011). Foi pesquisadora do GPPlab (Laboratório de Gestão de Políticas Públicas) da Fundação Getulio Vargas de São Paulo (2015). Foi pesquisadora do Laboratório de Geografia, Política e Planejamento Territorial e Ambiental (Laboplan) da Universidade de São Paulo (2002-2009). Durante doutorado, foi a*ffiliate research student* (pesquisadora-visitante) no University College London (UCL) da Universidade de Londres (2007-2008), com bolsa do CNPq. Foi pesquisadora do Centro de Estudos em Administração Pública e Governo/Programa Gestão Pública e Cidadania da Fundação Getúlio Vargas de São Paulo (2004-2007).

NILSON BRITO

Especialista em Projetos, Privacidade e Proteção de Dados. Formado pela Universidade Fumec, pós-graduado, MBA pelo IETEC, em Belo Horizonte. Possui atualmente o título de DPO pelo EXIN®. Tem expertise em gestão de projetos, segurança da informação, redes, telecom, consultoria. Atualmente é parceiro e consultor na empresa SMDATA em projetos LGPD, além de participar em grandes empresas dos segmentos de Telecom, Tecnologia da Informação, Inovação Tecnológica, entre outras. Escritor de artigos na Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD®), com artigos publicados em literaturas dedicadas à LGPD e mencionados em cursos relacionados à LGPD.

PATRÍCIA PECK GARRIDO PINHEIRO

CEO e sócia-fundadora do Peck Advogados. Advogada especialista em Direito Digital, Propriedade Intelectual, Proteção de Dados e Cibersegurança. Graduada e doutorada pela Universidade de São Paulo. PhD em Direito Internacional. Conselheira titular nomeada para o Conselho Nacional de Proteção de Dados (CNPD) da Autoridade de Proteção de Dados Pessoais Brasileira (ANPD). Professora de Direito Digital da ESPM. Professora convidada da Universidade de Coimbra, em Portugal, e da Universidade Central do Chile. Professora convidada de Cibersegurança da Escola de Inteligência do Exército Brasileiro. Foi presidente da Comissão Especial de Privacidade e Proteção de Dados da OAB-SP. Membro do conselho consultivo da iniciativa Smart IP Latin America do Max Planck Munique para o Brasil. Advogada Mais Admirada em Propriedade Intelectual de 2007 a 2022. Recebeu o prêmio Best Lawyers 2020/2021, Leaders League 2021/2020/2019, Compliance Digital pelo LEC em 2018, Security Leaders em 2012 e 2015, a Nata dos Profissionais de Segurança da Informação em 2006 e 2008, o prêmio Excelência Acadêmica – Melhor Docente – da Faculdade FIT Impacta em 2009 e 2010. Condecorada com cinco medalhas militares: Medalha da Ordem do Mérito Ministério Público Militar em 2019, Ordem do Mérito da Justiça Militar em 2017, Medalha Ordem do Mérito Militar pelo Exército em 2012, Medalha Tamandaré pela Marinha em 2011, Medalha do Pacificador pelo Exército em 2009. Árbitra do Conselho Arbitral do Estado de São Paulo – Caesp. Autora/coautora de 33 livros de Direito Digital. Presidente do Instituto iStart de Ética Digital. Programadora desde os 13 anos. Certificada em Privacy e Data Protection Exin.

RAFAEL FELGUEIRAS ROLO

Doutor em Teoria do Estado e Direito Constitucional pela Pontifícia Universidade Católica no Rio de Janeiro (PUC/RJ, 2016-2020), com período sanduíche na University of London (Birkbeck, 2018-2018). Mestre em Direito Processual pela Universidade do Estado do Rio de Janeiro (Uerj, 2013-2015). Graduação em Direito pela Universidade Federal do Pará (UFPA, 2004-2009). Procurador do Estado do Pará (desde 2010). Professor (desde 2019). DPO da PGE/PA (desde 2021).

RENATO MÜLLER DA SILVA OPICE BLUM

Advogado e Economista. Mestre pela Florida Christian *University*; Chairman Fundador no Opice Blum, Bruno e Vainzof Advogados; Patrono Regente do Curso de Pós-graduação em Direito Digital e Proteção de Dados da Escola Brasileira de Direito – EBRADI; Professor coordenador dos cursos de Direito Digital e Proteção de Dados da FAAP. Coordenador do MBA em Digital Legal 360°: Proteção de Dados, Gestão e Inovação da LCA; Professor em cursos no INSPER.

RICARDO CAMPOS

Docente assistente (*wissenschaftlicher Mitarbeiter*) na Faculdade de Direito da Goethe Universität Frankfurt am Main, Alemanha. Ministra, junto com Gunther Teubner, Thomas Vesting e Rudolf Wiethölter, o tradicional seminário semanal de teoria do Direito da Faculdade de Direito de Frankfurt. Trabalhou como tutor de Filosofia do Direito junto ao prof. Klaus Günther (Frankfurt/Main) e foi assistente júnior (*studentische Hilfskraft*) na cátedra de Sociologia da Universidade de Passau, Alemanha. Mestre em Teoria do Direito (LL.M – Master of Laws) pela Goethe Universität, Frankfurt am Main (2010). Cursou graduação em Direito (2008) na Universidade Federal de Juiz de Fora, na Goethe Universität Frankfurt am Main (Alemanha), e na Universität Passau (Alemanha). Docente do programa de mestrado em Teoria do Direito LL.M Legal Theory da cooperação entre a academia europeia de teoria do direito e da Goethe Universität Frankfurt am Main. Possui experiência acadêmica nas áreas de direito público, direito regulatório, regulação de mídia, proteção de dados, privacidade e teoria do direito.

RHIMA AHMAD CHARANEK SANTANA

Consultora na Fundação Carlos Alberto Vanzolini (FCAV). Graduada em Administração de Empresas e pós-graduada em Gestão Empresarial pela FGV. Atualizações em Compliance pela FGV, em Privacidade e Proteção de Dados pela Data Privacy Brasil e em LGPD pela FCAV.

RODRIGO HIROSHI RUIZ SUZUKI

Chief Information Security Officer na Logicalis Latin America, responsável pela segurança da informação, continuidade de negócios e proteção de dados. É mestre em Ciências da Computação e possui as certificações CISA, CISM, CRISC, CDPSE, ISO 27001 Lead Auditor e ISO 22301 Lead Auditor. Tem mais de 25 anos de experiência em TIC, sendo os últimos 20 dedicados à segurança da informação.

SABRINA LUCILA DE ARAUJO

Consultora na Fundação Carlos Alberto Vanzolini (FCAV). Psicóloga e mestre em Psicologia Experimental pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Pós-graduada em Análise do Comportamento pela USP. MBA em Gestão de Projetos pela FGV. Realizou curso de atualização em LGPD pela FCAV.

VANESSA D'ALESSIO GIARONE SUZUKI

Coordenadora de Segurança da Informação na Clavis Segurança da Informação, responsável pela coordenação e governança de riscos de clientes. É pós-graduada em Gestão de Riscos e Continuidade de Negócios e possui a certificação ISO 27001 Lead Auditor. Tem mais de 15 anos de experiência em TIC, sendo os últimos 10 dedicados à segurança da informação.

VERENA IANNINO SOARES ROLO

Graduação em Direito pela Universidade da Amazônia (2006). Advogada (desde 2008).

WALLACE DA SILVA PEREIRA

Analista de Sistema formado em Contábeis e Direito pela Univali em Santa Catarina. Pós-graduado em Desenvolvimento de Software também pela Univali e pós-graduando em Direito Digital pela IDP. Professor do curso de graduação e pós-graduação em Administração, Direito e Análise e Desenvolvimento de Sistemas da Faculdade Cesusc. Certificado Exin Segurança da Informação ISO/IEC 27001. Servidor público há 28 anos no Tribunal de Contas do Estado de Santa Catarina, atualmente ocupa o cargo de diretor de tecnologia da informação da instituição.

PREFÁCIO

Estimados leitores,

Os grandes avanços da tecnologia nas últimas décadas e o aumento exponencial na utilização das informações trouxeram diversas conjunções não previstas e inimagináveis pelas legislações vigentes até então. Isso tornou crucial a composição da primeira legislação geral de proteção de dados no Brasil, que visa a proteger as informações das pessoas naturais e regulamentar as atividades que se utilizam dos nossos dados. Nesse sentido, após anos de muitos estudos, debates, audiências públicas e votações, foi criada, sancionada e promulgada a Lei n. 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

A presente obra elucida os contornos sobre a utilização das informações e os impactos trazidos pela LGPD ao poder público, trazendo um arcabouço de orientações com base nas diretrizes elaboradas pela Autoridade Nacional de Proteção de Dados (ANPD) e nas boas práticas de governança voltadas aos entes públicos, além de estabelecer conceitos doutrinários desenvolvidos pelos maiores especialistas de privacidade e proteção de dados do país.

Como relator da LGPD no Tribunal de Contas da União (TCU), e com muitos anos promovendo e disseminando o tema da governança no Brasil, sinto-me muito honrado por ser imbuído da liderança deste projeto primoroso, que visa a amparar os agentes públicos nos novos desafios trazidos pela utilização, cada vez maior, de novas tecnologias, além de ajudar a fortalecer a garantia e os direitos fundamentais da privacidade e da proteção de dados de toda a nação.

Desde a promulgação do Decreto n. 9.203 de 2017, que dispõe sobre a política de governança da administração pública, obtivemos avanços expressivos em relação à governança pública, tanto no âmbito federal quanto nos estados e municípios. O conceito de governança é fluido e sempre receberá as novas legislações. Nesse sentido, visto que a LGPD demanda dos agentes públicos o controle das atividades que utilizam dados pessoais, o monitoramento dos processos e a implementação das melhores estratégias para gestão dessas informações, torna-se essencial a adoção de boas práticas de governança. A própria LGPD destinou uma seção especial para as boas práticas e governança, permitindo e indicando aos agentes de tratamento

que implementem um programa de governança em privacidade, trazendo requisitos mínimos para ele.

O momento de promulgação e entrada em vigor da LGPD foi extremamente tempestivo, tendo em vista a abundância de informações que cada indivíduo concebe a todo instante sobretudo com as novas tecnologias presentes no mercado e, em relação ao poder público, o avultado volume de dados tratados, sendo primordial uma transformação cultural na utilização das informações. Para que essa transformação cultural seja viável e eficaz, é essencial ponderar, em todas as atividades e relações, os direitos de privacidade e proteção de dados, desde a concepção até a eliminação das informações. Além disso, é necessário criar mecanismos de governança que sopesem as conjunturas da organização e abarquem os procedimentos para coleta de dados pessoais, segurança das informações, controles de acesso, mitigação dos riscos, resposta aos titulares de dados, atendimento às demandas da ANPD, bem como ações educativas a todos os colaboradores e à sociedade em geral.

Em virtude disso, o livro fomenta questões sobre a importância da governança em proteção de dados pelo poder público e os aspectos práticos sobre controles e estratégias para monitoramento e continuidade da gestão dos dados pessoais e do programa de adequação dos órgãos públicos.

Gostaria de agradecer e cumprimentar, afetuosamente, todos os especialistas participantes deste livro, que se debruçaram sobre o tema e trouxeram, de forma extremamente enriquecedora, toda a experiência adquirida em longos anos de trabalho com privacidade e proteção de dados e que, diuturnamente, debatem sobre os caminhos os quais a LGPD irá percorrer e os cenários para os próximos anos.

Em especial, gostaria de agradecer aos coordenadores desta obra, Lucas Paglia e Fábio Correa Xavier, que também coordenam o Comitê de LGPD da Rede Governança Brasil (RGB), e, em nome deles, todos os demais membros desse comitê que participaram de forma intensa e dedicada da construção e organização deste material. O trabalho de forma voluntária desses membros contribui ainda mais com o crescimento da governança de dados pessoais no Brasil e no setor público.

Portanto, desejo que estas páginas possam não só fazer com que os leitores compreendam melhor os conceitos da LGPD aplicados ao setor público, mas também que despertem seu interesse pelo universo da proteção de dados. Assim, estimo profundamente que este livro possa contribuir para a transformação da sociedade brasileira, tornando-a mais segura e garantindo os direitos de seus cidadãos.

Fraterno abraço!

Augusto Nardes
Ministro do Tribunal de Contas da União

APRESENTAÇÃO

Neste livro, Fábio Correa Xavier e Lucas Paglia reuniram agentes públicos e privados para tratarem das boas práticas para a implementação da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) pelos municípios brasileiros.

A LGPD, de observância obrigatória por todos, tem sido aplicada gradualmente, consideradas as peculiaridades dos diversos setores e tipos de dados a serem administrados. Os desafios são grandes e a mobilização dos agentes fundamental para a implementação da lei.

Três características tornam esta coletânea essencial e de consulta obrigatória sobre o tema.

Em primeiro lugar, a qualidade dos autores aqui reunidos, que se destacam como profissionais e acadêmicos e trazem reflexões a respeito de suas vivências e estudos.

Em segundo plano, o livro se destaca pelo relato de experiências de entes públicos na implementação da LGPD, o que permite a difusão de ideias e programas governamentais que fomentam a aplicação da Lei n. 13.709/2018, algo fundamental no cenário de difusão dos meios eletrônicos de comunicação.

Por fim, os temas abordados demonstram a abrangência e complexidade envolvidas na gestão de dados pessoais pela administração pública, considerados os deveres a ela impostos, inclusive o de publicidade, e a diversidade de órgãos e entidades que a compõem.

A lei está em vigor e o desafio de seu cumprimento pelos órgãos e entidades administrativas está posto. A presente obra contribui para a implementação da norma e o alcance de suas finalidades.

Dimas Ramalho
Presidente do Tribunal de Contas do Estado de São Paulo

SUMÁRIO

1 Recomendações e boas práticas para a jornada de adequação à LGPD pelos municípios, 27
Fábio Correa Xavier

2 Governança em privacidade de dados: a LGPD e seu artigo 50, 49
Lucas Paglia

3 Lei Geral De Proteção de Dados e seus impactos no ciclo de políticas públicas no município, 68
Ana Carla Bliacheriene
Luciano Vieira de Araújo
Fátima L. S. Nunes

4 Jornada do Estado de São Paulo para adequação à LGPD, 77
Andra Robert de Carvalho Campos
Ademir Bento Simão, Beatriz Scavazza
Elizabete Campos, Luis Márcio Barbosa
Maria Bernardete Ferreira
Matusalém dos Santos Carvalho
Melissa Giacometti De Godoy
Rhima Ahmad Charanek Santana
Sabrina Lucila de Araujo

5 O direito fundamental à proteção de dados no ordenamento e a transparência administrativa: há convivência harmônica?, 94
Andressa Carvalho da Silva

6 Segurança da informação: proteção contra vazamento de dados, 111
Andrey Guedes Oliveira

7 A importância da gestão de projetos e gestão de serviços para o DPO, 127
Davis Alves
Nilson Brito

8 Políticas públicas municipais de fomento à proteção de dados pessoais pelo setor privado, 134
Eduardo Tuma
Fernando Antonio Tasso

9 Monetização de dados por entes públicos, 150
Patrícia Peck Garrido Pinheiro
Camila Nascimento
Julia Lonardoni Ramos

10 Mecanismos e medidas práticas para obtenção de resultado no tratamento de dados, 161
Renato Müller da Silva Opice Blum
Bruno Henrique Cordeiro de Souza

11 Transferência internacional de dados pessoais e compliance digital, 172
Maria Gabriela Grings
Ricardo Campos

12 Apontamentos acerca da constitucionalidade do art. 52, X, XI, XII e § 3.º da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados): considerações à luz do princípio republicano e da continuidade do serviço público, 186
Verena Iannino Soares Rolo
Rafael Felgueiras Rolo

13 *Cybersecurity* e LGPD, 201
Rodrigo Hiroshi Ruiz Suzuki
Vanessa D'Alessio Giarone Suzuki

14 A LGPD como norteadora da criação de cidades inteligentes, 219
Wallace da Silva Pereira

Como citar os capítulos deste livro conforme a ABNT, 237

1
RECOMENDAÇÕES E BOAS PRÁTICAS PARA A JORNADA DE ADEQUAÇÃO À LGPD PELOS MUNICÍPIOS

Fábio Correa Xavier

Resumo

Neste artigo, busco apresentar as recomendações e boas práticas, especialmente em segurança da informação, para a adequação à LGPD pelos municípios. O artigo é baseado em dois guias orientativos da Autoridade Nacional de Proteção de Dados.

Palavras-chave: segurança da informação; guia orientativo; LGPD.

1 Introdução

A Lei Geral de Proteção de Dados – Lei n. 13.709/2018, doravante LGPD – aplica-se tanto ao setor privado quanto ao setor público. Segundo Silva (2020, p. 9), a LGPD "[...] altera em muito a maneira como as empresas – e não só elas, mas também os órgãos e entidades públicas – devem gerenciar os dados". Silva (2020, p. 32) argumenta, ainda, que "[...] já havia leis que abrangiam os temas privacidade e proteção de dados; no entanto, a LGPD veio para consolidar um microssistema de tratamento desses dados: quem, como, quando, onde, porque, com que fim podem ser usados esses dados".

Não obstante, a Administração Pública vem há muito tempo coletando dados pessoais de maneira indiscriminada e sem se preocupar com princípios elencados no art. 6.º da LGPD – especialmente finalidade, adequação, necessidade ou mesmo segurança –, e nem com o caput do art. 23, que define que o tratamento de dados pessoais pelas pessoas jurídicas de direito público "[...] deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (BRASIL, 2018). Via de regra, optava-se por maximizar a coleta de dados, mesmo sem ter a certeza em relação à sua necessidade para atender sua finalidade pública, para executar suas competências e atribuições legais, como previsto no caput do art. 23 da LGPD. E a consequência é destacada por Barbosa e Oliveira

(2020), que são bem incisivos ao afirmar que uma "enorme quantidade de dados pessoais e dados sensíveis estão sob o domínio do Poder Público, como informações financeiras e fiscais (Imposto de Renda), de educação (histórico escolar), de saúde (prontuário médico), de consumo (Nota Fiscal Paulista), entre inúmeras outras". E como os dados são as novas *commodities* do século XXI, dada sua importância comercial e estratégica, é importante que o setor público faça a adequação para ficar em conformidade com a novel legislação, sem prejuízo da consecução de suas atividades finalísticas. E essa adequação vale para toda e qualquer entidade pública, inclusive para os municípios de pequeno (e até médio) porte, que possuem invariavelmente dificuldades com disponibilidade de recursos – orçamentários, de infraestrutura e pessoal –, o que torna a jornada de adequação mais hercúlea.

2 TRATAMENTO DE DADOS PESSOAIS PELOS MUNICÍPIOS

A LGPD possui um capítulo específico que discrimina as regras para o tratamento de dados pelo poder público (capítulo IV, artigos 23 a 30). Além disso, é importante destacar que o porte da empresa – e entendo que, de forma similar, o porte dos municípios – não altera o direito fundamental que o titular de dados tem à proteção de seus dados pessoais, nem desobriga a observação da boa-fé e dos princípios do art. 6.º. Essa afirmação vai ao encontro do que afirmou Pinheiro (2021, p. 59): "um dos objetivos da LGPD é assegurar a proteção e o livre desenvolvimento da personalidade da pessoa natural", e que isso está relacionado à garantia de titularidade de seus dados e "inviolabilidade da vida privada".

Em função disso, e a título exemplificativo, mesmo não possuindo funcionários especializados em segurança da informação, os agentes de tratamento de pequeno porte não podem deixar de tomar as medidas administrativas e técnicas de segurança da informação, conforme previsto nos artigos 46, 47, 48 e 49 da LGPD.

Reforçando seu papel orientativo, a ANPD tem trabalhado na elaboração de guias orientativos para a sociedade, titulares e agentes de tratamento, elucidando questões que são fruto de debate em relação à LGPD. Neste texto, abordarei dois guias orientativos que podem (e devem) ser utilizados como referência pelos municípios em sua jornada de adequação à LGPD.

O primeiro, lançado em janeiro de 2022, é o guia orientativo *Tratamento de dados pessoais pelo poder público*, que busca esclarecer diversas dúvidas dos gestores públicos na implementação da lei, especialmente pela necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na LGPD.

O segundo, lançado em outubro de 2021 e intitulado *Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte* (BRASIL,

2021b) – incluindo um *checklist*[1] para facilitar a visualização das sugestões que serão adotadas – sugere padrões técnicos mínimos de segurança que as micro e pequenas empresas, além de startups, podem utilizar para proteger os dados pessoais sob sua guarda. Contudo, o guia informa que "As medidas sugeridas devem ser entendidas como boas práticas e **devem ser complementadas** com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização" (BRASIL, 2021b, grifos nossos). O guia não tem efeito normativo vinculante e trata-se apenas de um guia de boas práticas, que poderá ser atualizado e aperfeiçoado sempre que necessário. Embora não seja direcionado aos municípios, entendo que tais orientações possam ser seguidas por esses entes públicos, como forma de se construir um ambiente institucional mais seguro e, consequentemente, materializar os princípios da boa-fé, segurança e prevenção.

3 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

O guia orientativo *Tratamento de dados pessoais pelo poder público* (LANDERDAHL *et al.*, 2021) aborda quatro aspectos principais: (i) as bases legais mais comuns para respaldar o tratamento de dados pelo poder público; (ii) os princípios mais aderentes às peculiaridades do setor público; (iii) orientações acerca do compartilhamento de dados pessoais pelo Poder Público; (iv) cuidados na divulgação de dados pessoais.

3.1 BASES LEGAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma legislação transversal que trata de proteção de dados pessoais. A LGPD define que os dados pessoais só podem ser tratados em consonância com pelo menos uma das hipóteses legais previstas no art. 7.º. As hipóteses – ou bases – legais, portanto, são presunções autorizativas para que um agente de tratamento, público ou privado possa realizar operações com dados pessoais, como a coleta, classificação, utilização, acesso, transmissão, processamento, armazenamento, eliminação e transferência, dentre outras.

Em função das peculiaridades do setor público e com base nos questionamentos recebidos, a ANPD focou o capítulo III do seu guia orientativo em quatro das dez bases legais previstas no art. 7.º: consentimento (inciso I), cumprimento de obrigação legal e regulatória (inciso II), execução de políticas públicas (inciso IV) e legítimo interesse (inciso IX).

1 Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf.

3.1.1 Consentimento

Previsto no art. 7.º, I, da LGPD, como uma hipótese de tratamento de dados pessoais, o consentimento é definido no art. 5.º, XII como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Em outras palavras, o titular dos dados pessoais deve dar seu consentimento para o controlador tratar seus dados pessoais de forma clara, livre, sem coação, inequívoca, com base na transparência da informação da finalidade do tratamento – uma vez que o art. 8.º, § 4.º, torna nulo o consentimento para autorizações de tratamento genéricas – e por escrito ou outro meio que demonstre indubitavelmente a vontade real do titular. Antes da LGPD, o consentimento também era tratado na Lei n. 12.965/2014, o Marco Civil da Internet (MCI). No MCI, em seu art. 7.º, que trata dos direitos do usuário de internet, o inciso VII define que o compartilhamento de dados pessoais, incluindo registros de conexão e acesso a aplicações, só pode ser feito mediante consentimento "livre, expresso e informado". O titular deve ter pleno conhecimento do que está sendo consentido, de forma transparente, objetiva, sem tecnicismo jurídico e/ou técnico, adequada e ostensiva. O termo de consentimento deve informar a finalidade específica para o tratamento, a forma e a duração, a identificação do controlador e informações de contato, se os dados serão compartilhados (finalidade e identificação dos outros controladores e operadores), responsabilidades dos agentes de tratamento e direitos do titular, conforme o art. 18, especialmente quanto ao seu direito de revogar o consentimento a qualquer momento, sem necessidade de justificativa.

O art. 8.º determina, ainda, que caso o consentimento seja dado por escrito, o texto deverá ser uma cláusula destacada das demais (art. 8.º, § 1.º), dando ênfase e clareza, para que o titular não tenha dúvidas de que está dando seu consentimento espontâneo. O MCI, em seu art. 7.º, IX, vai na mesma toada, indicando que o consentimento deverá ocorrer de forma "destacada das demais cláusulas contratuais". Isso é importante, pois cabe ao controlador o ônus da prova de que o consentimento foi obtido de acordo com as regras da LGPD (art. 8.º, § 2.º).

Com base nessas características que devem ser observadas quando do uso do consentimento, o guia da ANPD considera que essa não é a base legal "mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais" (LANDERDAHL *et al.*, 2021, p. 7). Nesses casos, há um "desbalanceamento de forças", em que as prerrogativas do poder público acabam sendo impostas ao titular dos dados, impedindo-o de manifestar sua livre vontade, sem prejuízo ao exercício de direitos fundamentais ou aplicação de restrições para usufruir dos serviços públicos.

Contudo, o consentimento pode ser utilizado como base legal desde que o tratamento de dados pessoais não seja obrigatório, por obrigações ou atribuições legais da instituição. Dessa forma, o titular dos dados pessoais poderá manifestar livremente sua vontade real, dando ou não o consentimento.

3.1.2 Cumprimento de obrigação legal e regulatória

A LGPD permite que o tratamento de dados pelo Poder Público seja realizado para o cumprimento de obrigação legal ou regulatória, conforme art. 7.º, II, e art. 11, II, "a". O conceito de obrigação legal é reforçado no art. 23, ao destacar que o tratamento de dados pessoais no setor público deverá ser realizado "com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (BRASIL, 2018), observando, ainda, o interesse público e o atendimento da finalidade pública do controlador.

O guia aborda essa base legal segundo dois contextos normativos: normas de conduta e normas de organização.

Segundo Barroso (2009, p. 227), as normas de conduta seriam aquelas "destinadas a reger, diretamente, as relações sociais e o comportamento das pessoas. Normas de conduta [...] preveem um fato e a ele atribuem um efeito jurídico". Ou seja, as normas preveem um fato e uma implicação jurídica para esse fato. Por exemplo, se houver um fato gerador, haverá um tributo.

Já as normas de organização são aquelas criadas para estruturação de órgãos e entidades, estabelecendo suas competências e atribuições. Tais normas, "[...] em lugar de disciplinarem condutas, as normas de organização, também chamadas de normas de estrutura, instituem órgãos, atribuem competências, definem procedimentos" (BARROSO, 2019, p. 227).

Assim, o cumprimento de obrigações legais e regulatórias pode ser uma necessidade gerada por normas de conduta ou de organização. No primeiro caso, o agente de tratamento do setor público deve obrigatoriamente cumprir uma determinação legal expressa, sob pena de sofrer uma consequência prevista no ordenamento jurídico. Na segunda hipótese, o tratamento se dará para atendimento à finalidade da existência daquele órgão ou instituição pública, para cumprimento de suas atribuições legais, razão de sua existência.

3.1.3 Execução de políticas públicas

Outra base legal prevista na LGPD para o tratamento de dados pela administração pública é para a "execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres", conforme art. 7.º, III, e art. 11, II, "b" (BRASIL, 2018).

O guia busca definir as expressões administração pública e políticas públicas, de forma a esclarecer a aplicação dessa base legal.

Administração Pública abrangeria, segundo a ANPD, "tanto órgãos e entidades do Poder Executivo quanto dos Poderes Legislativo e Judiciário, inclusive das Cortes de Contas e do Ministério Público, **desde que estejam atuando no exercício de funções administrativas** (LANDERDAHL *et al.*, 2021, p. 12). Portanto, todos os órgãos e entidades dos três poderes e das três esferas federativas podem usar essa base legal para a consecução de políticas públicas. Mas o que seriam políticas públicas?

Como a expressão políticas públicas não foi definida no art. 5.º da LGPD, o guia recomenda que sejam consideradas as definições usuais da expressão. Assim, segundo Peters (1986), política pública é a soma das atividades dos governos, que agem diretamente ou através de delegação, e que influenciam a vida dos cidadãos. Dye (1984, p. 3) sintetiza a definição de política pública como "o que o governo escolhe fazer ou não fazer". O guia ressalta que, para a aplicação dessa base legal, a política pública deve ser instituída por um ato formal – lei, regulamento, contratos, convênios e instrumentos congêneres. Além disso, quanto ao aspecto material, a política deve determinar, de forma específica, um programa ou ação governamental, com objetivos definidos e priorizados, e com reserva de meios necessários para sua execução, além da definição do prazo para se chegar aos resultados pretendidos.

Uma última recomendação acerca dessa base legal é que os agentes de tratamento da administração pública devem observar o previsto no art. 23, sendo que o tratamento "[...] deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (BRASIL, 2018).

3.1.4 Legítimo interesse

Uma das dez hipóteses previstas é o legítimo interesse (art. 7.º, IX) do controlador ou de terceiros, podendo ser utilizada para o tratamento de dados pessoais não sensíveis, desde que não viole os direitos e as liberdades fundamentais do titular, nem a sua privacidade (art. 2.º, I) e autodeterminação informativa (art. 2.º, II), liberdade para o desenvolvimento da própria personalidade do titular – especialmente os direitos à privacidade e intimidade (artigo 5.º da CF).

Ao contrário das outras bases legais previstas no art. 7.º, o legislador escolheu por incluir um artigo específico (art. 10), que dita alguns parâmetros para a aplicação do legítimo interesse: o controlador deve ter finalidades legítimas e situações concretas que terão que ser analisadas sempre e individualmente, para confirmar a sua aplicação. O art. 10 elenca situações concretas, a título exemplificativo: no inciso I, "o apoio e promoção de atividades do controlador", coadunando com os fundamentos previstos no art. 2.º, V – "desenvolvimento econômico e tecnológico e a inovação"

– e VI – "a livre iniciativa, a livre concorrência e a defesa do consumidor", inclusive a busca do lucro, conforme previsto no art. 170 da CF/88. Nesse sentido, o legítimo interesse pode ser visto como uma alternativa de uso de dados responsável com potencial de desenvolvimento econômico e a inovação, garantindo o direito à privacidade dos titulares. Ainda no art. 10, inciso II, temos outro exemplo de situação concreta: "a proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais". Além disso, o art. 37 destaca que o controlador e o operador devem manter registro das operações de tratamento de dados que realiza, "especialmente quando baseado no legítimo interesse". Ressalta-se, novamente, que o legítimo interesse não se estende ao operador, sendo uma base legal exclusiva do controlador.

Destaca-se que, no caput do art. 10, há ênfase para o uso dessa base legal com finalidade legítima. Podemos entender por finalidade legítima o uso revestido de boa-fé, especialmente no atendimento à legítima expectativa do titular dos dados. Nesse sentido, destaco que a boa-fé seria o "princípio dos princípios", interpretação ratificada pela sua posição no caput do artigo 6.º, revelando sua centralidade frente aos demais princípios listados nos incisos subsequentes. O uso dessa base legal deve, ainda, não contrariar a lei, estar em consonância com as regras de conduta da sociedade e deve prever que, quando baseado no legítimo interesse do controlador, o tratamento se restrinja exclusivamente aos dados pessoais necessários para a finalidade pretendida. Seria, portanto, uma categoria capaz de contemplar qualquer interesse protegido pela ordem jurídica que deve ser sopesado – ou balanceado – com os direitos do titular dos dados, tornando-se uma base legal mais ampla. Se, na técnica de sopesamento ou balanceamento, os interesses do titular superarem o interesse do controlador, o uso dessa base legal para o tratamento de dados não será possível.

O uso do legítimo interesse como base legal deve ainda observar os princípios da necessidade e da transparência, sendo o controlador responsável por adotar medidas para garantir esses princípios. O uso do legítimo interesse como uma base legal para o tratamento de dados pessoais acaba por gerar um ônus argumentativo maior quanto ao princípio da finalidade, uma vez que, provavelmente para evitar seu uso indiscriminado, o legislador optou por frisar que sua aplicação só é possível em uma situação concreta. Contudo, apresenta-se como uma base legal mais flexível, dinâmica e exatamente por isso requer o uso constante da técnica de balanceamento entre os interesses do titular, de terceiros e do controlador, além de considerar as já citadas liberdades individuais. Para isso, seu uso deve ser precedido de uma detalhada análise de riscos, documentada, para atendimento ao previsto no § 3.º do art. 10.

Por fim, o guia destaca que "[...] a aplicação do legítimo interesse é limitada no âmbito do setor público. Em particular, a sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público" (LANDERDAHL *et al.*, 2021, p. 9).

3.2 PRINCÍPIOS MAIS ADERENTES ÀS PECULIARIDADES DO SETOR PÚBLICO

Pestana (2014, p. 155) destaca que princípios jurídicos:

> [...] representam uma categoria expressional, construída pelo homem, segundo os valores considerados importantes e relevantes em uma sociedade acerca de determinados sujeitos, objetos e das relações que estabelecem entre si, assim reconhecidos pela ordem jurídica, os quais reúnem, em seu entorno, os enunciados e normas jurídicas voltadas para prescrever condutas e disciplinar as relações intersubjetivas.

O mesmo autor autor afirma ainda que:

> [...] conhecer princípios equivale a conhecer a essência da matéria sob atenção, facilitando, sobremaneira, a dissecação do objeto sob estudo. Desconhecer os princípios, ao reverso, é caminhar tateantemente por entre disposições e preceptivos, sem visão de largueza e amplitude, prejudicando, com tons de definitividade, a possibilidade que se encerra de investigar-se e aprofundadamente conhecer-se o objeto (PESTANA, 2014, p.156).

Dessa forma, conhecer os princípios definidos pela LGPD em relação ao tratamento de dados pessoais é fundamental para que a lei seja bem aplicada pelos agentes de tratamento. O guia *Tratamento de dados pessoais pelo Poder Público* apresenta orientações "não exaustivas, com foco nas peculiaridades do setor público" acerca de cinco dos onze princípios elencados no art. 6.º da LGPD – incluo aqui o princípio da boa-fé, citado no caput do referido artigo. As orientações do guia abordam os seguintes princípios:

i) **finalidade** (art. 6.º, I): o tratamento de dados pessoais pelo Poder Público deve sempre buscar atender a uma finalidade pública legítima (lícita, compatível com o ordenamento jurídico e amparada em uma base legal), específica (com delimitação do escopo de tratamento), explicitada de forma clara e precisa, e em linguagem simples e de fácil compreensão e acesso pelo titular dos dados;

ii) **adequação** (art. 6.º, II): princípio que impõe a compatibilidade entre o tratamento dos dados pessoais e as finalidades que são informadas ao titular, ou seja, o tratamento deve ser adequado à finalidade informada;

iii) **necessidade** (art. 6.º, III): princípio que consagra a minimização do tratamento dos dados, ou seja, o tratamento deve se limitar ao mínimo necessário para atendimento à finalidade declarada, usando somente os dados necessários para tal (proporcionais e não excessivos). É necessário verificar se os dados coletados são efetivamente necessários para as finalidades declaradas;

iv) **transparência** (art. 6.º, VI): disponibilização de informações claras, precisas e de fácil acesso pelo titular sobre como se dá o tratamento de seus dados pessoais e sobre os respectivos agentes de tratamento. O princípio da transparência busca garantir a fluidez de informações para o titular que tem seus dados tratados, impondo uma postura ativa dos agentes de tratamento na disponibilização de informações exigidas pela lei, independentemente de uma requisição do titular;

v) **livre acesso** (art. 6.º, IV): princípio ligado intimamente ao da transparência, o livre acesso objetiva garantir ao titular consulta facilitada e gratuita sobre a forma e duração do tratamento e sobre a integralidade de seus dados pessoais, ou seja, assegura aos titulares acesso e conhecimento sobre que dados pessoais estão sendo tratados. Esse princípio garante também a cientificação do titular sobre a forma por meio da qual ele poderá acessar os dados tratados. Ademais, de forma complementar ao princípio da transparência, exige que os agentes de tratamento disponibilizem canais efetivos para que o titular possa exercer os seus direitos, previstos no art. 18 da LGPD (XAVIER, 2021a).

Importante destacar que tratamentos posteriores só podem ser feitos se estiverem alinhados à finalidade original. Caso contrário, o titular dos dados pessoais deve ser informado sobre a nova finalidade, inclusive em caso de compartilhamento dos dados pessoais. Como o guia destaca, "o tratamento posterior para novas finalidades somente poderá ser realizado se 'observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei' (art. 7º, § 7º)" (LANDERDAHL *et al.*, 2021, p. 14).

Quanto aos princípios da transparência e livre aceso, ressalta-se que a identidade e informações de contato do encarregado pelo tratamento de dados pessoais (XAVIER, 2021b) devem ser amplamente divulgadas, inclusive no site da instituição, como previsto no art. 41 § 1.º. Já o art. 9.º do referida normativa define as informações que devem ser disponibilizadas aos titulares: (i) finalidade específica do tratamento; (ii) forma e duração do tratamento, observados os segredos comercial e industrial; (iii) identificação do controlador; (iv) informações de contato do controlador; (v) informações

acerca do uso compartilhado de dados pelo controlador e a finalidade; (vi) responsabilidades dos agentes que realizarão o tratamento; e (vii) direitos do titular, com menção explícita aos direitos contidos no art. 18 da lei.

Embora o guia não tenha abordado, acredito que o princípio da qualidade de dados deve ser observado com muito zelo pelo poder público. Esse princípio consubstancia-se na garantia, assegurada aos titulares dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Nessa toada, a qualidade dos dados é fundamental para que o poder público possa planejar e executar políticas públicas, pois "[...] sem dados confiáveis, os governos ficam sem informações adequadas para conduzir políticas públicas efetivas e acabam gerando desperdício de escassos recursos e, como consequência, desamparo e abandono para a população mais vulnerável" (XAVIER; VAZ, 2021).

4 ORIENTAÇÕES ACERCA DO COMPARTILHAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

O guia define que compartilhamento de dados é a "[...] operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública". O art. 5.º, em seu inciso XVI, da LGPD, define o uso compartilhado de dados.[2]

Fato é que o compartilhamento de dados é importante para o atingimento dos objetivos institucionais de muitos órgãos e entidades do poder público. A própria LGPD consagra essa necessidade, uma vez que define, no art. 25, que os dados devem ser mantidos em formato "interoperável e estruturado para o uso compartilhado", como afirma o próprio guia.

Assim, a LGPD, em seu art. 7.º, inciso III, autoriza o tratamento e compartilhamento de dados pessoais pela administração pública, quando os dados são "necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei" (BRASIL, 2018). Assim, desde que com o fito de executar políticas públicas – conceito que já abordamos anteriormente –,o poder público poderá proceder com o compartilhamento de dados necessários, observado o capítulo IV da Lei Geral de Proteção de Dados.

---

2 "XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados" (BRASIL, 2018).

Para que o compartilhamento seja feito em consonância com os regramentos da LGPD, o guia destaca alguns pontos que devem ser observados pelos entes públicos:

i) **formalização e registro**, por meio de processo administrativo, com todos os documentos, incluindo análise técnica e jurídica, com a exposição de motivos para o compartilhamento, demonstrando a aderência à LGPD. O ajuste deverá ser feito por meio de ato formal entre os agentes de tratamento que farão o compartilhamento de dados. Caso o compartilhamento seja uma ação recorrente, recomenda-se a adoção de um ato normativo interno – portarias e instruções normativas – que dariam o devido formalismo, padronização e celeridade a essas operações, definindo competências, procedimentos, prazos e requisitos essenciais a serem observados nos processos de compartilhamento de dados;

ii) **objetivo e finalidade**, definindo claramente nos atos de formalização, quem é a outra entidade que irá receber os dados, para qual finalidade específica, indicando a iniciativa, ação ou programa que será executado ou a atribuição legal do ente público que será cumprida com o compartilhamento, bem como a definição de quais dados serão objeto de compartilhamento, limitando-os ao "estritamente necessário para as finalidades do tratamento", atendendo ao princípio da necessidade;

iii) **base legal**, com todos os cuidados já descritos no item 3.1 deste texto;

iv) **duração do tratamento**, uma vez que o tratamento de dados pessoais deve ter um prazo definido, ao final do qual os dados pessoais devem ser eliminados, salvo para os casos previstos no art. 16 da LGPD. Assim, o "instrumento que autoriza ou formaliza o compartilhamento deve estabelecer, de forma expressa, o período de duração do uso compartilhado dos dados, além de esclarecer, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento" (BRASIL, 2022);

v) **transparência e direitos dos titulares**, para atendimento ao princípio da transparência (art. 6.º, VI) – informações sobre o compartilhamento de forma clara, precisa e de fácil acesso, inclusive para que o titular possa exercer seus direitos previstos no art. 18 – e ao previsto no art. 23, inciso I,[3] disponibilizando as informações no site da instituição;

3 "I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos" (BRASIL, 2018).

vi) **prevenção e segurança**, medidas técnicas e administrativas para proteção dos dados pessoais, conforme art. 6.º, VII, e 46 da LGPD. Esse tema será tratado detalhadamente na próxima seção deste texto;

vii) **compartilhamento entre entes públicos e setor privado**, observando o previsto no art. 26, § 1.º,[4] e no art. 27 da LGPD;

viii) **Relatório de impacto à proteção de dados pessoais**, documento definido no art. 5.º, inciso XVII,[5] que deve ser elaborado de acordo com o art. 38,[6] como forma de subsidiar a decisão da autoridade competente para autorização ou não do compartilhamento, contendo pelo menos a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados;

ix) **funções e responsabilidades dos agentes de tratamento** envolvidos no uso compartilhado de dados pessoais, detalhando no instrumento do item (i) as instruções e as condições que devem ser observadas pelo operador ao realizar o tratamento dos dados pessoais, conforme art. 39 da LGPD.[7]

5 CUIDADOS NA DIVULGAÇÃO DE DADOS PESSOAIS

Muito se discute sobre o eventual conflito entre a LGPD e a Lei de Acesso à Informação (Lei n. 12.527, de 17 de novembro de 2011 – LAI). Contudo,

4 "§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação); II - (VETADO); III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei; IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019) V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)" (BRASIL, 2018).

5 "XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018).

6 "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL, 2018).

7 "Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria" (BRASIL, 2018).

ambas as legislações são interrelacionadas e até mesmo complementares. O que é imperioso notar é que o objetivo geral dos dois instrumentos é distinto. Segundo Barros (2020):

> [...] enquanto a LAI volta-se à disciplina das questões atinentes aos dados públicos — que, portanto, não são de propriedade, não integram a esfera de direitos de nenhum indivíduo isolada ou pessoalmente considerado –, a LGPD trata justamente dos dados pessoais, inseridos na esfera de intimidade e proteção do cidadão.

Silva (2020, p. 25) também segue nessa linha, afirmando que "[...] cada uma possui um enfoque diferenciado, dado já pela própria nomenclatura: uma prescreve a proteção e outra, o acesso". A autora continua o raciocínio, afirmando que "[...] a LAI também pode ser considerada uma lei que contribuiu para a proteção dos dados pessoais, pois reforçou o equilíbrio entre 'acesso, qualidade de informação, proteção à privacidade e sigilo'" (SILVA, 2020, p. 25). A tabela comparativa abaixo, elaborada por Silva (2021), mostra claramente a conexão entre "os preceitos legais em negrito e, em itálico, correlação entre os direitos e garantias pelo preceituado no dispositivo referenciado":

Tabela 1 – Comparação entre a LAI e LGPD.

LAI	LGPD
Art. 31, § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de **previsão legal ou consentimento** expresso da pessoa a que elas se referirem.	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de **consentimento** pelo titular; II – para o cumprimento de **obrigação legal** ou regulatória pelo controlador;
§3º O consentimento referido no inciso II do §1º não será exigido quando as informações forem necessárias: I – **à prevenção e diagnóstico médico**, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VIII – **para a tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
§3º O consentimento referido no inciso II do §1º não será exigido quando as informações forem necessárias: II – **à realização de estatísticas e pesquisas científicas** de evidente interesse público ou geral, previstos em lei, **sendo** vedada a identificação da pessoa a que as informações se referirem;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: IV – **para a realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

LAI	LGPD
§3º O consentimento referido no inciso II do §1º não será exigido quando as informações forem necessárias: III – **ao cumprimento de ordem judicial**;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VI – para o **exercício regular de direitos em processo judicial**, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
§3º O consentimento referido no inciso II do §1º não será exigido quando as informações forem necessárias: *IV – à defesa de direitos humanos*;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VII – *para a proteção da vida ou da incolumidade física do titular ou de terceiro*;
§3º O consentimento referido no inciso II do §1º não será exigido quando as informações forem necessárias: V – à proteção do interesse público e geral preponderante.	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III – pela administração pública, para o tratamento e uso compartilhado de *dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*, observadas as disposições do Capítulo IV desta Lei;

Fonte: Silva (2021).

Superada essa discussão, ao realizar o tratamento de dados pessoais, o poder público deve fazê-lo em conformidade com as disposições da LGPD. A divulgação de dados pessoais também é uma operação de tratamento e, portanto, protegida pela LGPD. Assim, o ente público deve atentar para os mecanismos que garantam a proteção dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares, observando os princípios e a base legal aplicável ao tratamento. Deve-se, também, realizar uma ampla análise, com uma minuciosa avaliação de riscos e impactos da divulgação para os titulares.

O guia da ANPD traz algumas orientações relevantes quando da divulgação de dados pessoais pelo poder público:

i) **ter maior cautela com dados pessoais sensíveis**, definidos no art. 5.º, II, uma vez que possuem proteção jurídica especial e que podem ser usados de forma indevida, caso sejam divulgados em desconformidade com a LGPD;

ii) **verificar o ajuste aos princípios da finalidade, adequação e necessidade**, ou seja, se os dados pessoais coletados e divulgados

são efetivamente aqueles estritamente necessários e adequados para o atingimento da finalidade da divulgação;

iii) **adotar medidas de mitigação de riscos**, por meio de um relatório de impacto à proteção de dados (RIPD), de forma a diminuir o potencial lesivo aos direitos dos titulares;

iv) **tomar medidas técnicas e administrativas eficazes** para comprovar a aderência aos princípios da segurança, prevenção e da responsabilização e prestação de contas, como previsto nos arts. 46 a 49 e 50, § 1.º. Utilizar técnicas de anonimização ou pseudonimização[8] são bons exemplos que podem (e devem) ser manejados;

v) **considerar que a transparência** sobre o tratamento de dados pessoais é uma forma de garantir que o titular possa exercer seus direitos, como solicitação de correção ou atualização, bloqueio e eliminação de dados desnecessários, excessivos ou em desconformidade com a finalidade, como previsto no art. 18.

6 SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

O segundo guia que abordarei neste texto é o que trata de boas práticas de segurança da informação. O *Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte* (BRASIL, 2021b) é dividido em medidas administrativas, medidas técnicas e recomendações para dispositivos móveis e serviços na nuvem.

6.1 MEDIDAS ADMINISTRATIVAS EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

As medidas administrativas são aquelas que tratam de política e procedimentos relacionados à segurança da informação. As medidas citadas no guia são:

i) **política de segurança da informação**, mesmo que seja simplificada, perfaz um conjunto de diretrizes e regras para viabilizar o planejamento, implementação e o controle de ações de segurança da informação dentro da instituição;

ii) **conscientização e treinamento**, uma vez que as pessoas muitas vezes são negligenciadas, mas são parte vital para o sucesso de qualquer ação em relação à segurança da informação e proteção de dados;

8 Saiba mais sobre essas técnicas lendo o artigo "O uso dos processos de anonimização e pseudonimização no contexto da LGPD" (XAVIER, 2021c).

iii) **gerenciamento de contratos**, com a inclusão de termos de confidencialidade para funcionários e em contratos com fornecedores e clientes nos quais deve haver a inclusão de cláusulas que determinem as responsabilidades e funções em relação à LGPD.

Adicionalmente, diferentemente dos agentes de tratamento de pequeno porte, os municípios de pequeno porte **devem indicar um encarregado pelo tratamento de dados pessoais**, como definido no art. 23, inciso III, da LGPD. O encarregado é o responsável pelas comunicações entre o controlador, o titular de dados e a ANPD, sendo um canal interativo entre esses atores. Além disso, o encarregado é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. O ideal é que o indicado tenha conhecimento multidisciplinar – legislação, privacidade e proteção de dados, tecnologia da informação, segurança da informação, metodologias de análise de risco e governança, administração e atendimento às demandas internas e externas. Além disso, ele deve ter autonomia, independência e recursos – financeiros, estrutura e pessoal – para exercer suas atribuições. Deve-se, também, evitar possíveis conflitos de interesse e acúmulo de funções dentro da instituição. No meu artigo "O encarregado de dados no setor público" (XAVIER, 2021b), discorri mais sobre o tema.

A necessidade de indicação do encarregado é ratificada pelo *Guia orientativo para definições de agentes de tratamento de dados pessoais e do encarregado* (BRASIL, 2021a) que afirma que órgãos e entidades públicas devem indicar um encarregado de dados, baseando-se no já citado art. 23, inciso III. Ademais, conforme §1.º do artigo 41 da LGPD, a identidade e as informações de contato do encarregado devem ser publicadas no sítio eletrônico do controlador, para que ele possa ser facilmente encontrado, tanto pela ANPD quanto pelos titulares dos dados e demais interessados, atendendo ao princípio da transparência. Isso é importante, pois os "direitos dos titulares (art. 18) são, em regra, exercidos em face do controlador, a quem compete, entre outras providências, fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento" (BRASIL, 2021a).

6.2 MEDIDAS TÉCNICAS EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

As medidas técnicas seriam aquelas mais relacionadas às tecnologias e controles que podem ser implementados em relação à segurança da informação.

O guia cita as seguintes medidas técnicas:

i) **controle de acesso**, baseado na necessidade de acesso aos dados pessoais, implementando política de senhas complexas e desabilitando senhas padrões de fabricantes. Também recomenda que não se faça o compartilhamento de senhas entre funcionários e que se adote o princípio do menor privilégio, ou seja, atribuir o nível de acesso necessário para a realização das atividades de cada funcionário. Por fim, recomenda a utilização de autenticação multifator. Ressalto que o processo de autenticação é uma das medidas que abordei em outros dois artigos no MIT Technology Review: "Regra de Pareto para a segurança digital: 3 ações que mitigam 80% dos ataques" (XAVIER, 2021e) e "Quais são os padrões técnicos mínimos exigidos pela LGPD?" (XAVIER, 2021d);

ii) **segurança dos dados pessoais armazenados**, com ressalva para a observação ao princípio da necessidade (art. 6.º, III), com a minimização da coleta dos dados, atentando-se para a configuração segura das estações de trabalho – o *hardening* que citei no artigo "Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques" (XAVIER, 2021e) – e não utilização de dispositivos de armazenamento externo, como HD ou *pendrives*. Essa medida também se relaciona com as cópias de segurança (backup) e uso de criptografia nos dados armazenados;

iii) **segurança das comunicações**, com a utilização de protocolos de comunicação seguros – como TLS/HTTPS – e aplicativos com criptografia fim a fim, inclusive com o uso de e-mails criptografados, se forem utilizados para envio de dados pessoais. Há ainda a necessidade de se utilizar tecnologias de proteção de tráfego, como sistema de *firewall*, antivírus, *antispyware* e anti-spam. Por fim, remover qualquer dado pessoal que esteja em redes públicas, como o site da empresa, caso não exista a necessidade de tal publicidade; (iv) manutenção de programa de gerenciamento de vulnerabilidades, para monitorar e aplicar correções de sistemas e aplicativos lançadas pelos servidores. É importante manter os sistemas atualizados, para se minimizar o risco de ser vítima de um ataque que explore vulnerabilidades conhecidas. Essa também é uma das 3 ações que eu citei no meu artigo "Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques" (XAVIER, 2021e). Além disso, deve-se também manter antivírus e *antimalwares* sempre atualizados e com varreduras periódicas em todos os dispositivos da empresa;

iv) **manutenção de programa de gerenciamento de vulnerabilidades**, para monitorar e aplicar correções de sistemas e aplicativos lançadas pelos servidores. É importante manter os sistemas atualizados, para se minimizar o risco de ser vítima de um ataque que explore vulnerabilidades conhecidas. Além disso, deve-se também manter antivírus e *antimalwares* sempre atualizados e com varreduras periódicas em todos os dispositivos da empresa.

7 RECOMENDAÇÕES PARA DISPOSITIVOS MÓVEIS E SERVIÇOS NA NUVEM

Para dispositivos móveis, como notebooks, *tablets* e *smartphones*, o guia sugere que estejam sujeitos aos mesmos procedimentos de controle de acesso implantados para os demais equipamentos da empresa, incluindo autenticação multifator. O guia recomenda, ainda, que a empresa separe os dispositivos móveis de uso privado daqueles de uso institucional. Ou seja, a recomendação é que não se utilize dispositivos móveis particulares para fins institucionais, uma vez que estão mais sujeitos a vulnerabilidades, trazendo mais risco para o agente de tratamento. Uma última recomendação é a implementação de funcionalidade que permita apagar todos os dados no dispositivo, de forma remota, para ser usada em caso de perda ou roubo do equipamento.

Quanto a serviços na nuvem, é importante ter um contrato de acordo de nível de serviço (Service Level Agreement – SLA) adequado, que contemple a segurança dos dados armazenados e uso de autenticação multifator, para acesso aos serviços e dados pessoais que estão na nuvem.

7.1 BOAS PRÁTICAS DO MERCADO

Segurança da informação é uma área muito dinâmica. Muito embora as recomendações feitas no guia possam servir como um caminho inicial para os municípios de pequeno porte, há outras práticas e recomendações que podem (e devem) ser buscadas, para que se tenha um ecossistema de privacidade e proteção de dados cada vez mais efetivo. Por exemplo, há boas práticas já consolidadas no mercado, como as normas da família 27.000 da ABNT/ISO/IEC. Recomendo também a observância das principais violações que ensejaram a aplicação de multas pelas autoridades de proteção de dados da Europa, a partir das quais podemos identificar onze boas práticas, como já abordei no artigo "Quais são os padrões técnicos mínimos exigidos pela LGPD?" (XAVIER, 2021d), e que cito a seguir:

i) **monitoramento de contas de usuário privilegiadas** – contas privilegiadas são aquelas que têm permissão para alterar sistemas de segurança e, consequentemente, conseguem acessar todos os dados sensíveis. Se esse tipo de conta for comprometido por um ataque ou mesmo se for utilizada de forma indevida, a privacidade dos dados sensíveis será comprometida. Assim, é importante a implantação de soluções técnicas para monitorar o uso de contas privilegiadas, para evitar o seu uso indevido;

ii) **monitoramento do acesso e uso de bancos de dados com dados pessoais** – todo acesso aos bancos de dados que possuem dados pessoais também deve ser monitorado e registrado, para que seja possível

rastrear eventuais usos indevidos. Um ponto de atenção é com as contas de administradores do banco de dados, que como as contas privilegiadas, podem ter acesso aos dados pessoais;

iii) **implementação de *hardening* de servidores, para evitar acesso a contas de administradores ou super usuários** – mais uma vez, a preocupação com as contas privilegiadas é tratada neste caso. *Hardening* de servidores é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas em servidores com o objetivo principal de torná-lo preparado para enfrentar tentativas de ataque, especialmente ataques para exploração de contas privilegiadas;

iv) **encriptação de dados pessoais e dados pessoais sensíveis** – a criptografia é uma técnica que cifra os dados, tornando-os ininteligíveis para os que não têm acesso às regras e chaves utilizadas. É uma técnica importante que trabalha para garantir a confidencialidade dos dados, um dos pilares da segurança da informação;

v) **uso de autenticação multifator** – que trabalha em um dos pontos mais sensíveis e explorados pelos invasores, o roubo de credenciais, por meio de técnicas de *phisphing*, por exemplo. O uso de autenticação multifator verifica a identidade do usuário por meio de duas ou mais credenciais de acesso. Pode-se utilizar, por exemplo, algum critério que o usuário saiba (a senha), outro critério que ele possua (dados biométricos) ou algo que ele possua (um *token*);

vi) **controle de acesso rígido para aplicações, com base na necessidade e remoção de acesso quando não for mais necessário** – privilegiando o princípio da necessidade, definido no art. 6.º da LGPD, com a exclusão do dado ao final do seu ciclo de vida;

vii) **teste de invasão frequente** – a equipe técnica deve implantar soluções técnicas de proteção e, além disso, fazer testes de invasão frequentes de forma a validar se os controles implementados são eficazes. Aqui é importante utilizar o ciclo PDCA – **planejar (Plan)** as soluções técnicas, **executar (Do)**, implantar a solução planejada, **verificar (Check)** sua implantação (onde entra o teste de invasão) e **atuar (Act)**, fazendo as correções e ajustes necessários, reiniciando o ciclo;

viii) **não armazenamento de senhas em texto claro, em arquivos não criptografados** – o que parece ser uma atitude óbvia, mas que infelizmente ainda é negligenciada, dado o volume de multas aplicadas pelas autoridades europeias. O armazenamento de senhas em arquivos com texto claro é um grande risco para a segurança da informação e sua existência deve ser mapeada e eliminada;

ix) **registro de tentativas de login sem sucesso** – esse tipo de situação pode indicar um ataque de força bruta que, em caso de sucesso, pode colocar em risco todo o aparato de segurança implantado. Em conjunto com essa prática, deve-se implantar políticas de senhas fortes, com uso de senhas

longas e diversos tipos de caracteres. O sucesso do ataque de força bruta se baseia na utilização de senhas simples;

x) **revisão manual de códigos para verificação se há dados pessoais indevidos** – é importante verificar os códigos de sistemas para verificar se não há dados pessoais "chumbados", especialmente senhas de sistemas e credenciais de usuários. Esse tipo de informação não pode existir nas linhas de códigos de sistemas de informação;

xi) **processamento de dados de cartões de acordo com o padrão PCI DSS**, um padrão mundialmente reconhecido para tratamento de dados de pagamento com uso de cartão. As iniciais PCI DSS vêm do inglês *Payment Card Industry Data Security Standard.*

8 CONSIDERAÇÕES FINAIS

A adequação à LGPD não é uma tarefa simples: é, de fato, uma jornada. A ANPD, ciente de suas atribuições pedagógicas e de divulgação de boas práticas, tem trabalhado na elaboração de guias orientativos para esclarecer questões recorrentes sobre a interpretação da LGPD, de forma não vinculativa.

Nesse sentido, os dois guias tratados neste texto – *Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte* e *Guia tratamento de dados pessoais pelo poder público* – podem servir como uma bússola para o processo de conformidade com a lei para os órgãos e entidades públicas, especialmente para os municípios brasileiros.

O mais importante é que todos busquem um comportamento digital cada vez mais seguro e alinhado à LGPD, de forma que os direitos dos titulares de dados pessoais (XAVIER, 2021a) sejam sempre respeitados.

REFERÊNCIAS

BARBOSA, Daniela B.; OLIVEIRA, Victor F. LGPD: a necessidade de proteção dos dados do setor público. **O Estadão**, São Paulo, 12 set. 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-a-necessidade-de-protecao-dos-dados-do-setor-publico/. Acesso em: 25 dez. 2020.

BARROS, Laura Mendes Amando de. LAI x LGPD: embate em um mesmo campo ou espectros de incidência diferentes? **Consultor Jurídico**, 25 nov. 2020. Disponível em: https://www.conjur.com.br/2020-nov-25/laura-barros-lai-lgpd. Acesso em: 20 fev. 2021.

BARROSO, L. R. **Curso de direito constitucional contemporâneo**. São Paulo: Saraiva, 2009.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições de Agentes de Tratamento de Dados Pessoais e do** Encarregado. Brasília, maio 2021a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 14 jun. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília, out. 2021b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 5 out. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de dados pessoais pelo poder público**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 10 maio 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 20 fev. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 dez. 2020.

DYE, Thomas D. **Understanding Public Policy**. Englewood Cliffs: Prentice-Hall, 1984.

LANDERDAHL, Cristiane; MAIOLINO, Isabela; BARBOSA, Jeferson Dias; CARVALHO, Lucas Borges de. **Tratamento de dados pessoais pelo poder público**. Brasília: ANP, jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 16 fev. 2022.

PESTANA, Marcio. **Direito Administrativo Brasileiro**. 4. ed. São Paulo: Atlas, 2014.

PETERS, B. G. **American Public Policy**. Chatham: Chatham House, 1986.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva, 2021.

SILVA, Andressa Carvalho da. **Lei Geral de Proteção de Dados e a responsabilidade estatal**: implicações no âmbito dos tribunais de contas. 2020. Monografia (Especialização) – Curso de Direito Público, Universidade de Caxias do Sul, Porto Alegre, 2020.

SILVA, Andressa Carvalho da. LGPD e o microssistema de proteção de dados. *In*: MIGALHAS, Editora (ed.). **Comentários à Lei Geral de Proteção de**

Dados Pessoais – LGPD: Lei nº 13.709/2018. Ribeirão Preto: Migalhas, 2021. Disponível em: https://www.livrariamigalhas.com.br/e-books/comentarios-a-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 25 dez. 2020.

XAVIER, Fabio Correa. O encarregado de dados no setor público. **Migalhas**, 29 jan. 2021b. Disponível em: https://www.migalhas.com.br/depeso/339636/o-encarregado-de-dados-no-setor-publico. Acesso em: 30 ago. 2021.

XAVIER, Fabio Correa. LGPD: conheça seus direitos como titular de dados pessoais. Conheça seus direitos como titular de dados pessoais. **MIT Technology Review**, 31 ago. 2021a. Disponível em: https://mittechreview.com.br/lgpd-conheca-seus-direitos-como-titular-de-dados-pessoais/. Acesso em: 31 ago. 2021.

XAVIER, Fabio Correa. O uso dos processos de anonimização e pseudonimização no contexto da LGPD. **Migalhas**, 1.º abr. 2021c. Disponível em: https://www.migalhas.com.br/depeso/342896/o-uso-dos-processos-de-anonimizacao-e-pseudonimizacao-da-lgpd. Acesso em: 2 mar. 2022.

XAVIER, Fabio Correa. Quais são os padrões técnicos mínimos exigidos pela LGPD? **MIT Technology Review**, 25 mar. 2021d. Disponível em: https://mittechreview.com.br/quais-sao-os-padroes-tecnicos-minimos-exigidos-pela-lgpd/. Acesso em: 31 ago. 2021.

XAVIER, Fabio Correa. Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques. **MIT Technology Review**, 4 jun. 2021e. Disponível em: https://mittechreview.com.br/regra-de-pareto-para-a-seguranca-digital-3-acoes-que-mitigam-80-dos-ataques/. Acesso em: 31 ago. 2021.

XAVIER, Fabio Correa; VAZ, Wesley. A importância da qualidade de dados para a eficiência e efetividade das políticas públicas. **MIT Technology Review**, 20 maio 2021. Disponível em: https://mittechreview.com.br/a-importancia-da-qualidade-de-dados-para-a-eficiencia-e-efetividade-das-politicas-publicas/. Acesso em: 22 fev. 2022.

2
GOVERNANÇA EM PRIVACIDADE DE DADOS: A LGPD E SEU ARTIGO 50

Lucas Paglia

1 INTRODUÇÃO

A Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) tem, por objetivo principal, proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. A lei versa sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica (pública ou privada), sendo que os documentos físicos, assim como os digitais, estão contemplados nesta proteção (BRASIL, 2018).

Nesse sentido, a LGPD define um importante passo para a construção da cultura de privacidade e proteção de dados pessoais dos órgãos da administração pública, sejam municipais, estaduais ou federais, e empresas privadas e de economia mista – obrigando todas a cumprir o disposto em lei. Destaca-se, entre suas características, a horizontalidade, pois permeia todos os departamentos das empresas, órgãos e departamentos na administração pública, os mais diversos setores privados nos quais o tratamento de dados pessoais pode envolver diferentes titulares, desde os próprios colaboradores/servidores até consumidores, clientes, fornecedores e usuários dos serviços públicos (RONDÔNIA, 2022).

Sendo assim, um programa de governança em privacidade deve atender a alguns requisitos, mas, em especial, aos elencados no artigo 50 da própria LGPD. Denominada "Das boas práticas e da governança", a seção tem apenas dois artigos, entre outros incisos elencados algumas das recomendações que devem ser seguidas pelas empresas durante a sua implementação da LGPD, contudo com claros apontamentos de continuidade do projeto em momentos posteriores à adequação em si – "Dia 2 da LGPD" ou "Início da fase de governança e monitoramento do Projeto".

O artigo 50 da LGPD traz as principais diretrizes que o legislador observou no início da criação da cultura de privacidade e proteção de dados no Brasil:

a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) estabelecer diretrizes e regras que possam ser aplicáveis a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) ser um instrumento que inspira relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) estar integrado a sua estrutura geral de governança e estabelecer e aplicar mecanismos de supervisão internos e externos;

g) contar com planos de resposta a incidentes e remediação;

h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

2 O QUE É GOVERNANÇA?

Se considerarmos que governar tem o sentido de administrar (gerir, comandar, chefiar e orientar), controlar, influenciar e até mesmo conduzir, a governança acontecerá através da implantação e integração entre *liderança*, *estratégia* e *controle* (mecanismos da governança), postos em prática para *avaliar*, *direcionar* e *monitorar* as iniciativas locais do(a) prefeito(a) e sua equipe, potencializando a estruturação de uma rede interna e externa que deve adotar e se comprometer com uma cultura de gestão baseada em resultados, transparência, participação e eficiência. Em outras palavras, a governança auxilia o(a) prefeito(a) a organizar a gestão.

Figura 1 – O ciclo da governança

Fonte: Rede Governança Brasil (2021).

No meio corporativo, a definição apresentada no site do Instituto Brasileiro de Governança Corporativa (IBGC) sobre governança corporativa é: "o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas" (GOVERNANÇA..., [202-?]).

Em resumo, pode-se dizer que a governança, em ambiente público ou privado, refere-se ao conjunto de práticas que uma empresa ou órgão público adota para consolidar as suas estruturas e sua gestão, indicando a direção a ser seguida, demonstrando confiabilidade e fidelização.

Sendo assim, uma das definições da governança, seja ela pública, seja privada, é compreender todos os processos de governar, seja pelo estado ou até mesmo por um governo eleito ou conselhos de administração, até mesmo por uma rede de um sistema social através de leis, normas, políticas, regimentos internos, poder ou até linhagem de sucessão, por exemplo. Todos podem ser considerados sociedades organizadas – sociedades que possuem regras de governança.

O ato da governança é composto por decisões de hierarquia, controle, mas, principalmente, ciclos de liderança, estratégia e controles. A figura 1, extraída da *Cartilha de Governança Pública Municipal* da Rede Governança Brasil, demonstra efetivamente o ciclo PDCA (planejar, fazer, checar e agir – em tradução literal para o português). Tal ciclo é capaz de relatar toda a constante e necessária evolução que todas as sociedades, administrações, redes ou empresas privadas devem ter para continuar o processo de governança – a melhoria constante.

Nesse sentido, *monitorar*, *avaliar* e *direcionar* são os três resultados obtidos a partir da imagem acima. Estes resultados comprovam a eficácia do sistema de governar.

Sendo assim, dentre as mais variadas organizações que podem governar, o mais formal é um governo, na administração pública. Já na administração privada, seria um conselho ou até mesmo a existência de um organograma desenvolvido e adaptado à realidade de cada organização. Assim, esse órgão, cuja única responsabilidade é tomar decisões vinculantes (como um estado), pode estabelecer leis ou criar regras de controle – como procedimentos e políticas. Não obstante, outros tipos de governo incluem uma organização, um grupo sociopolítico (chefe, tribo, gangue, família, denominação religiosa etc.) ou outro grupo informal de pessoas.

Figura 2 – Relação entre governança e gestão.

Fonte: Rede Governança Brasil (2021).

A governança, portanto, é a maneira de determinar ações, que podem regras e/ou normas, controles estruturados e regulados. Obviamente, o grau de formalização das ações da organização que necessita que o faz por lei, ou da organização privada que escolhe o "caminho da governança", é motivado pelo nível de controle que os líderes (*liderança*) devem ou precisam ter.

Além disso, a governança pode assumir diversas formas, que deverão ser impulsionadas pelas motivações diferentes e que podem obter resultados diferentes (*estratégia*). Os resultados decorrem dessas escolhas e medidas tomadas pelos governantes e líderes – públicos ou privados. A estratégia escolhida é essencialmente vinculada ao *tone at the top* – "o exemplo vem de cima". A estratégia deve naturalmente ser desenhada dentro dos padrões aceitos e cabíveis dentro de cada organização.

Foi nesse contexto que a governança instituiu-se como um dos maiores pilares de sustentabilidade e manutenção das organizações que a utilizam como meio de obter autoridade, domínio ou até mesmo governo (*controle*). A forma natural de se controlar uma organização pública ou privada é controlar as ações realizadas, escolher a liderança que determina a estratégia e resultados a serem obtidos. Assim, a necessidade de controle é facilmente explicada como um dos fatores preponderantes para o sucesso da implantação da governança como um processo nas empresas e na administração pública.

Nessa linha de raciocínio, a governança geralmente refere-se a um nível específico de governança associado a um tipo de organização (incluindo governança pública, governança global, governança sem fins lucrativos, governança corporativa e governança de projetos), um "campo" particular de governança associado a um tipo de atividade ou resultado

(incluindo governança ambiental, governança da internet e governança de tecnologia da informação) ou um "modelo" particular de governança, muitas vezes derivado de uma teoria empírica ou normativa (incluindo governança regulatória, governança participativa, governança multinível, metagovernança e governança colaborativa).

A governança também pode definir agendas normativas ou práticas. Conceitos normativos de governança justa ou boa governança são comuns entre as organizações políticas, do setor público, voluntárias e do setor privado.

3 AS ETAPAS DA ADEQUAÇÃO À LGPD

A fim de obter os primeiros passos para a criação de um Projeto de Governança de Dados Pessoais ou a Governança em Privacidade, é fundamental percorrer os artigos anteriores da Lei Geral de Proteção de Dados. Estes descrevem o trajeto a ser desempenhado pelas organizações (sejam públicas ou privadas) para entender o fluxo de dados pessoais existentes.

Figura 3 – Mecanismos de governança.

Fonte: Lima (2018).

Como fase inicial do projeto de adequação à Lei Geral de Proteção de Dados temos o diagnóstico preliminar ou mapeamento de dados, a execução e o monitoramento, conforme se verá adiante.

3.1 FASE DE DIAGNÓSTICO OU MAPEAMENTO DE DADOS

A etapa de diagnóstico e mapeamento destina-se a analisar e identificar o fluxo inicial dos dados pessoais e dados pessoais sensíveis que transitam dentro das organizações. Ou seja, mapear os três estágios principais que

o dado percorre dentro "de casa": i) entrada/origem; ii) armazenamento/retenção; iii) compartilhamento/expurgo.

Assim, no início do projeto de adequação à LGPD deve ser identificado, por meio de entrevistas e/ou formulários preenchidos, o fluxo de vida útil do dado pessoal no objetivo de responder aos itens anteriores. Nesse momento, é essencial compreender também a quais leis, regulações e regras estão sujeitas cada organização, pois foi determinado pelo legislador identificar finalidades claras e justificativas coerentes para a utilização de cada um dos dados pessoais coletados/tratados.

O artigo 37 da Lei Geral de Proteção de Dados determina que "o controlador e o operador devem manter registro de operações de tratamento de dados pessoais que realizarem" (BRASIL, 2018). Além disso, visa a subsidiar a elaboração do relatório de impacto de proteção de dados pessoais (RIPD) e outras ações necessárias, como a identificação de lacunas frente às exigências da LGPD ou de outras normas. O objetivo é realizar o levantamento das ações que o órgão desenvolve com dados pessoais, delimitando-se o escopo das operações de tratamento de dados pessoais, abrangendo, no mínimo: a identificação dos agentes de tratamento; as fases do ciclo de vida do tratamento; a descrição do fluxo do tratamento; a hipótese legal de tratamento; a finalidade e previsão legal do tratamento; quais dados são tratados; a categoria dos titulares; as informações sobre compartilhamento; a classificação das medidas de segurança; as informações sobre transferência internacional; as informações sobre contratos, termos ou congêneres que estejam correlatos com o tratamento.

Ao final, as organizações deverão ter obtido os registros das operações de tratamento de dados pessoais considerando cada processo existente na organização. Importante destacar que, a partir do princípio da governança, bem como da necessidade de atualização frequente dos registros, é importante sempre manter tais registros atualizados e, por isso, deve-se estabelecer um ciclo de periodicidade para revisão.

Dentro da etapa de mapeamento, deve ser considerado o gerenciamento de direitos individuais dos titulares de dados pessoais, a gestão de eventual consentimento e o rastreamento de preferências e a redução de responsabilidade por violação.

3.2 FASE DE EXECUÇÃO

Como próxima etapa do processo de adequação à LGPD das organizações, devemos passar a implementar as mudanças necessárias e diagnosticadas no momento inicial do projeto. Ou seja, considerando os dados obtidos no mapeamento dos processos e fluxo de dados pessoais, são identificados os *gaps* a serem implementados. A construção das medidas de adequação é iniciada no mapeamento, mas a partir dos *gaps* mapeados a fase de execução

passa a ser obrigatória. Salvo contrário, o mapeamento resta infrutífero.

Essa etapa é desenvolvida em alguns passos, sendo que alguns dos/as principais passos/ações serão descritos/as abaixo de forma a amparar o caminho a ser percorrido pelas organizações que visam a definir os parâmetros, regras e boas práticas.

Nesse sentido, a fase de execução é uma parte muito focada em documentação e definição de parâmetros. Por exemplo: a lei determina que todo tratamento de dados pessoais deva ser feito de forma transparente e com finalidades claras, precisas e informadas aos titulares de dados pessoais. De forma irrestrita, as organizações devem cumprir esses princípios, mas de que forma? A solução encontrada a fim de cumprir os requisitos propostos foi a de criar um documento chamado Política de Privacidade, em que os processos são descritos de forma clara e de fácil acesso aos titulares de dados pessoais com o escopo de ser transparente e conter todas as finalidades para as quais os dados são utilizados.

Por conseguinte, a fase de execução é, de fato, a fase em que se executa e se criam as documentações com o objetivo de cumprir a lei e trazer claridade aos tratamentos de dados pessoais ao titular do dado e até mesmo às autoridades responsáveis por seus controles.

Alguns outros documentos que serão identificados como mandatórios durante a fase de mapeamento são:

1) políticas e práticas para proteção da privacidade;
2) cultura de segurança e proteção de dados e *privacy by design*;
3) relatório de impacto à proteção de dados pessoais (RIPD);
4) adequação de cláusulas contratuais;
5) identificação de riscos por atividade de tratamento de dados pessoais;
6) identificação de dados pessoais sensíveis;
7) outros.

Logo, à fase de execução resta o objetivo de trazer documentação concreta ao processo de adequação à LGPD, trazido pela Lei n. 13.709/2018. A necessidade de realizar procedimentos de melhorias se dá pela nova regulamentação criada, mas melhora substancialmente a governança e sucessão de processos nas organizações. Os processos que a cultura de privacidade e, por certo, a cultura da governança desejam criar a fim de desenvolver procedimentos de melhorias a curto, médio e longo prazo (este como foco principal), são mais bem compreendidos quando concretos, quando existentes.

A ideia de manutenção das execuções propostas pelo mapeamento será compreendida na etapa posterior ao projeto, todavia a concretização dos procedimentos e processos que anteriormente não estavam desenhados e

implementados só é possível quando a fase de execução é completamente finalizada.

3.3 ETAPA DE MONITORAMENTO

A última etapa do projeto de adequação à LGPD é a de monitoramento, que inclui: os indicadores de performance, a gestão de incidentes, a análise de resultados e o reporte de resultados. No entanto, essa fase só deverá ser iniciada se concluídas as fases anteriores, principalmente a fase de execução.

O início do monitoramento é a primeira fase de implantação da governança das organizações, pois é a partir dele que os primeiros indicadores são coletados e analisados. Sendo assim, somente após a primeira "rodada" de resultados é que o ciclo de melhorias pode ser iniciado.

Assim, independente de prazo a ser concluído o projeto, a análise de resultados só tem efetividade após o primeiro ciclo de monitoramento ser finalizado, uma vez que a revisão de metas só traz novos controles se demonstrado que as conclusões iniciais não trouxeram os resultados esperados.

Vale destacar que, conforme a doutrina indica, entre os indicadores de performance cabe apontar: os índices de serviços com dados pessoais inventariados, os índices de serviços com termos de uso elaborado, o índice de conscientização em segurança, entre outros (NETO, 2020).

Nesse sentido, a terceira etapa do projeto determina que metas e indicadores de performance e desempenho das execuções realizadas na fase anterior tenham sido criados, tendo em vista a recomendação de comparação entre resultados desejados e resultados coletados no primeiro ciclo de indicadores.

Como já elucidado, a análise e o reporte dos resultados obtidos precisa ser constante para verificar a eficácia ou a necessidade de melhorias e adaptações no processo.

Cumpre mencionar que, após realizadas as três etapas determinadas em lei e integrantes do projeto de adequação à LGPD, uma das premissas maiores da perspectiva do legislador na criação da lei em si foi a inclusão da *legítima expectativa* dos titulares de dados pessoais.

É certamente um dos ditames centrais da lei, para não dizer o principal; é o teor "princípio lógico" que a LGPD carrega nos seus artigos. Explica-se: na construção da lei, o legislador preocupou-se em não definir quais são todos os limites de tratamento de dados, mas sim influenciar no conceito geral e amplo da *legítima expectativa* que o titular de dados pessoais tem da utilização de seus dados durante o ciclo de vida útil, já explicado.

Assim, durante o tratamento dos dados pessoais deve se preservar a característica inicial sobre qual o dado foi coletado e quão transparente suas finalidades foram repassadas ao titular. O titular deve, portanto, entender o

uso de todos os seus dados já no momento da coleta inicial e compreender a forma do tratamento prevista pelo controlador e operador dos dados.

Nesse sentido, o dado pessoal, quando coletado para preenchimento de um cadastro, por exemplo, deve ser, além de informado ao titular, mantido por toda a sua trajetória

Por exemplo: se o dado pessoal foi coletado com a finalidade de realizar cadastro de consumidor em uma farmácia, destacando-se o cumprimento dos princípios da finalidade e transparência, e o aceite ou outra base legal foi cumprida e identificada no mapeamento dos processos, esse mesmo dado pessoal não deveria ser utilizado para cadastro em um outro comércio com produto não anteriormente citato, mesmo que do mesmo grupo econômico.

Reitera-se que o uso do dado pessoal dentro da farmácia para outra finalidade, mas contida dentro da legítima expectativa daquele uso (por exemplo, o aviso de uma promoção para um consumidor que frequentemente se utiliza de um remédio que é vendido nesta farmácia) é abarcado pela base legal da legítima expectativa e poderia ser utilizado, mesmo que ausente nas primeiras coletas de processos e finalidades do uso deste dado pessoal.

Denota-se, portanto, que a irregularidade a ser evitada, contida na ideia principal do legislador na criação da LGPD, não é o uso do dado pessoal sem finalidade anteriormente prevista, mas sim o uso para finalidades que não remetem à legítima expectativa que o titular de dados pessoais tinha ao fornecer aquele dado pessoal – no exemplo, para um cadastro em uma farmácia.

4 GOVERNANÇA COMO PROCESSO: O PASSO SEGUINTE AO MONITORAMENTO

Em seu sentido mais abstrato, a governança é um conceito teórico que se refere a ações e processos. Assim, a governança como um processo deve ser observada e delineada no sentido de preservação das estruturas independente das pessoas que ocupam os cargos e postos. A preservação se dá pela manutenção fidedigna da estratégia adotada pelas organizações e empresas, e que não deve ser alterada ou substituída salvo em acordo da liderança de novos controles a serem implementados.

Ainda, também em seu sentido abstrato, a definição de processo se dá por "conjunto de atividades inter-relacionadas ou interativas que usam ou transformam entradas para entregar um resultado". Pode-se inferir a partir disso que a estrutura organizacional da governança decorre das estratégias, políticas de governança, estruturas para tomadas de decisões e responsabilização através das quais funcionam arranjos de governança das organizações. Não obstante, requer-se definir a importância da responsabilidade de cada departamento, órgão, pessoa, entidade e terceiros para o cumprimento das responsabilidades ali determinadas – *accountability*.

Ou seja, a governança quando implantada deve também observar a sua manutenção dentro das estruturas. A governança tem por alcance o longo prazo, e não somente o curto e médio prazos. As metas são calculadas nos três momentos, mas com foco no longo prazo – criando o processo correto a obter o resultado desejado.

Logo, a estruturação da governança como um processo tem por objetivo:

i) refletir a identidade missão ou propósito da organização em relação à sociedade e suas partes interessadas;

ii) aumentar a eficácia organizacional, sustentabilidade, responsabilidade e equidade;

iii) cumprir o propósito da organização;

iv) evitar grandes incidentes.

Contudo, a organização que desenhar suas atividades com base na governança não pode acreditar que somente isso é o necessário. A revisão dos controles implementados junto aos resultados obtidos sempre deve ser analisada a partir de metas (números programados e desejáveis) e, quando necessário, realizar ajustes aos pontos "fora da curva". O ciclo PDCA, conforme demonstrado acima, é a forma recomendada de trazer perspectivas hialinas e objetivas aos alvos desenhados anteriormente.

Em breve retrocesso, a governança deve reflexionar quais os resultados a organização quer atingir, aumentando a eficácia no sentido de organizar as estruturas e, principalmente, os processos internos e externos. Naturalmente, ao revisar os pontos anteriormente previstos, os processos se atualizam, devendo buscar a melhoria constante, mesmo na ausência das pessoas ou terceiros que participaram das criações dos processos.

Nesse diapasão, nota-se, portanto, que as pessoas são os meios pelos quais os processos decorrem, entretanto não podem ser maiores do que os processos em si. A busca do equilíbrio entre resultado, eficácia e governança também é observada no artigo da LGPD e, consequentemente, na implementação do programa de governança de dados pessoais recomendada.

Sendo assim, no caso da proteção de dados, deve-se observar o titular no centro da discussão. A partir dos modelos elucidados, denota-se uma importante determinação de quem é o foco dos processos a se obter a chamada de governança. No projeto de adequação à LGPD, o titular de dados pessoais, seja um hóspede de um hotel, seja mesmo um paciente de um hospital, deve ser respeitado como objeto a ser colocado no foco da governança.

Figura 4 – Atores da LGPD.

Fonte: Oliveira *et al.* (2020).

5 A GOVERNANÇA EM PRIVACIDADE DE DADOS PESSOAIS

Os agentes de tratamento de dados pessoais – controladores e operadores –, no âmbito de suas competências, com relação ao tratamento de dados, podem elaborar, individualmente ou por intermédio de associações, regras de boas práticas e de governança que determinem as condições de organização, os padrões técnicos, as normas de segurança, entre outros, nos termos do artigo 50, caput, da LGPD.

Ao estabelecer as referidas regras, os controladores e os operadores devem levar em consideração, no que se refere ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade, bem como a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. Conforme mencionado anteriormente, as fases do projeto de adequação são essenciais para identificar esses pontos.

Outrossim, as regras de boas práticas e de governança devem ser atualizadas e publicadas de maneira periódica.

Vale destacar o papel central da Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão responsável por determinar as principais alterações legislativas e de interpretação da letra fria da lei. Além disso, é responsável por zelar pela proteção dos dados pessoais; por elaborar as diretrizes para a política nacional de proteção de dados pessoais e da privacidade; por fiscalizar e aplicar sanções nos casos de tratamento de dados que descumprirem a legislação, por meio de processo administrativo, que assegure o contraditório, a ampla defesa e o recurso, entre outros.

A ANPD ainda tem como objetivo receber e analisar as denúncias enviadas pelos titulares de dados pessoais e pode, de ofício, determinar

explicações acerca do tratamento de dados realizados pelos controladores e operadores de dados pessoais.

Assim, o programa de governança em privacidade de dados pessoais pode ser entendido como o conjunto de regras de boas práticas e de governança que determinem as condições de organização, o regime de funcionamento, os procedimentos, as reclamações dos titulares, as normas de segurança, os padrões técnicos, as obrigações para os envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de diminuição de riscos e outros aspectos referentes ao tratamento de dados pessoais.

No artigo 50, § 2.º, da LGPD, são indicadas as características mínimas de um programa de governança em privacidade de dados pessoais, quais sejam:

• o comprometimento do controlador com a adoção de processos e políticas internas que assegurem o cumprimento, de maneira abrangente, de normas e boas práticas relacionadas à proteção de dados pessoais;

• a aplicação a todo conjunto de dados pessoais que estejam sob seu controle, independentemente da forma como foi realizada a coleta;

• a adaptação à estrutura, à escala e ao volume de suas operações, assim como à sensibilidade dos dados tratados;

• o estabelecimento de políticas e salvaguardas de acordo com o processo de avaliação sistemática de impactos e riscos à privacidade;

• o estabelecimento da relação de confiança com o titular, por intermédio de atuação transparente e que assegure mecanismos de participação do titular;

• a integração da estrutura geral de governança, o estabelecimento e a aplicação de mecanismos de supervisão internos e externos;

• com planos de resposta a incidentes e remediação;

• a atualização constante com base nas informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Uma vez estruturado, o programa de governança em privacidade de dados pessoais deve ser implementado de acordo com as instruções estabelecidas nos documentos de privacidade depreendidos das etapas do projeto de adequação à LGPD. Esse é o momento que comprova o papel principal da correta elaboração das etapas do projeto.

Um bom projeto incorre em um bom programa de governança em privacidade, sendo certo que o papel da governança nesse momento é determinar a efetividade dele. É, ainda, a governança que identifica se os controles e metas previstos anteriormente terão os resultados obtidos.

Nesse momento, é importante que a equipe de proteção de dados pessoais, liderada pelo encarregado de dados, conduza todos os esforços para garantir que as políticas e os procedimentos estabelecidos sejam

corretamente aplicados pelo resto da equipe funcional. O gerenciamento do ciclo de vida dos dados deve possuir todos os processos, padrões e funções bem definidos e registrados.

Logo, a criação da denominação da expressão governança em privacidade decorre da necessidade da criação do próximo estágio da adequação à LGPD.

Observando de modo prático, após concluído o "dia 1 da LGPD", que consiste em identificar os dados pessoais, mapear os fluxos internos das organizações, realizar as mudanças identificadas e mitigar os riscos apresentados, conforme trazido anteriormente, faz-se necessário retomar o projeto da criação da estrutura da governança, dessa vez em privacidade e proteção dos dados pessoais.

Assim, cada política, norma e ação criada pelas organizações deve ser documentada para demonstrar a efetividade de seu programa de governança quando houver questionamento e, em especial, a pedido da ANPD. A adoção de políticas de boas práticas e governança não apenas auxilia o cumprimento das obrigações estabelecidas pela LGPD, como também demonstra os esforços nesse sentido, e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por tratamento inadequado de dados pessoais.

Conforme já mencionamos, a governança irá possibilitar um aumento em sua capacidade de gestão, aumento do controle e integridade das informações, servindo como base de sustentação dos seus processos internos.

Dessa forma, é possível verificar que os requisitos para um programa de governança presentes na LGPD seguem as diretrizes adotadas por grandes empresas e órgãos públicos.

A implementação de medidas de segurança e de procedimentos de retenção e eliminação de dados pessoais, limitações de acesso e compartilhamento, realização de tratamento de dados internacionais, gerenciamento de terceiros e notificações sobre vazamento de dados é determinante para o bom andamento e efetiva mitigação dos riscos levantados pelo mapeamento de dados.

Passando por outras etapas do programa de governança em privacidade, deve-se observar, além da revisão do próprio programa em si, algumas das lacunas apontadas pelo mapeamento de dados pessoais realizados anteriormente. Entre as ações que consistem, não só na própria adequação, mas também como partes fundamentais da etapa da governança.

Em um dos momentos do fluxo de dados, é identificado quem são os demais agentes de tratamento de dados, que na maioria das vezes são operadores desses dados em nome dos controladores. Um dos riscos mais intangíveis em caso de incidentes de segurança da informação são esses terceiros pela ausência de maiores informações.

É possível, portanto, que esdes terceiros apresentem falhas nas suas adequações, o que, pelo princípio da responsabilidade objetiva que a lei criou

em cima desses terceiros, seja também responsabilidade do controlador. Uma das formas encontradas para dirimir esse impacto e consequentemente mitigar os riscos desses operadores foi a elaboração de cláusulas contratuais de responsabilização e prestação de contas.

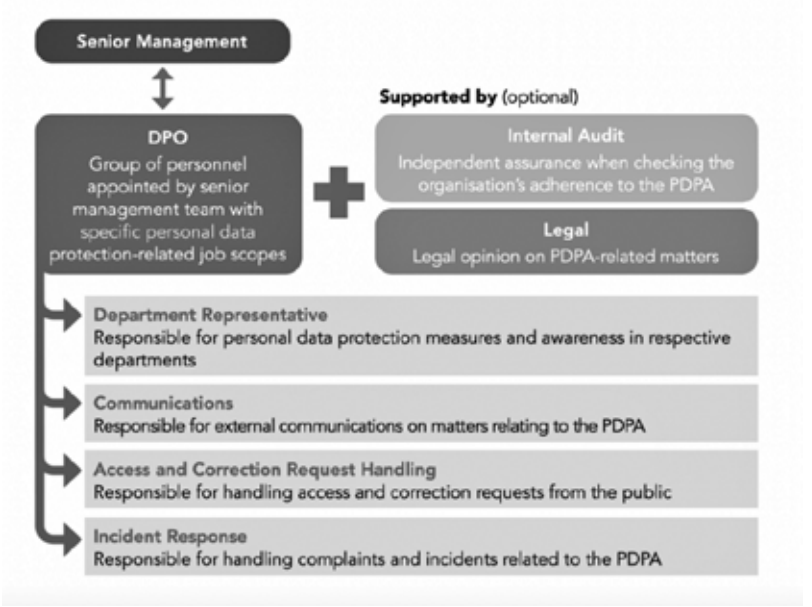
Essas cláusulas são responsáveis por obrigar a adequação dos terceiros/operadores de dados que agem em nome do controlador, trazendo mais governança em privacidade para os titulares que confiaram seus dados a tais controladores.

Uma vez que os terceiros são parte integrante do sistema de tratamento dos dados pessoais, uma forma de continuação do tratamento em si, esses se veem obrigados a participar do programa de governança dos controladores e, portanto, a existência de cláusulas contratuais.

Outro ponto de suma importância, e já destacado anteriormente, é a nomeação de um encarregado de dados pessoais – o *data protection officer* (DPO). Ele é a figura responsável pela manutenção da adequação à LGPD e posteriormente ao programa de privacidade de dados

Conforme denota-se na figura abaixo, extraída *Guide to Developing a Data Protection Management Programme* (PERSONAL..., 2021), da autoridade de proteção de dados de Cingapura, o encarregado de dados é o agente condutor do programa em si.

Figura 5 – Grupo de pessoal nomeado (com apoio dos departamentos de auditoria e jurídico).



Fonte: Personal... (2021).

Destaca-se, entre as principais atividades supramencionadas, o conceito de *privacy by design*, a ideia de que medidas técnicas e administrativas de privacidade e proteção de dados devem ser implementadas desde a concepção do desenvolvimento de um sistema.

O conceito de *privacy by design* ressalta ao menos três valores: (i) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (ii) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente; (iii) o respeito aos titulares de dados, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos.

Como título exemplificativo, o Ministério da Economia, em documento publicado (OLIVEIRA *et al.* 2020), traz alguns exemplos de medidas técnicas e organizacionais *privacy by design* que incluem:

a) uso de criptografia para proteção de bases de dados e meios de comunicação;
b) minimização e pseudonimização de bases de dados;
c) controle de acesso baseado em funções;
d) mecanismo de respostas a requisições e reclamações dos titulares de dados;
e) plano de respostas a incidentes e remediação de segurança e privacidade;
f) segurança física;
g) políticas de privacidade para aquisição de produtos/serviços;
h) políticas de gerenciamento da segurança da informação;
i) política de retenção e eliminação de dados pessoais.

Dos exemplos apontados acima, existem duas práticas que se tornam entre as mais importantes sobre o *privacy by design*, pois incluem o titular de dados no centro da discussão, assim como já apontado anteriormente, que são: os mecanismos de respostas aos pedidos, dúvidas e eventuais reclamações dos titulares de dados e a gestão de suspeitas de incidentes de segurança e privacidade (e até mesmo a condução de resposta a estes incidentes). Esses mecanismos têm como objetivo respeitar os direitos dos titulares de dados previstos na LGPD e preparar-se para cenários indesejados de vazamento de dados, identificando que áreas deverão ser envolvidas para conter o dano, informar as partes interessadas relevantes (como ANPD e titulares de dados) e lidar com responsabilizações judiciais.

A governança de dados e a governança em privacidade, que são estruturas diferentes, mas convergentes, passam pelo idealismo que a lei trouxe. O incidente de segurança da informação, por exemplo, pode ocorrer, mas a correta condução e gestão das medidas corretivas para reduzir os impactos

e riscos aos titulares, assim como a comunicação assertiva e tempestiva dos fatos, é parte fundamental.

Ou seja, a governança, nesse momento, é totalmente correlacionada a atingir esses objetivos, pois, mesmo que a adequação tenha identificado tais lacunas nas organizações, mesmo que os documentos e procedimentos tenham sido criados e desenvolvidos, a correta condução dos incidentes e resposta aos titulares de dados – e revisão de possíveis ajustes necessários – só terá resultado concreto através da governança.

Nesse ponto, é importante destacar que, muitas vezes, e de forma equivocada, fala-se em "governança de dados" como sinônimo de estrutura jurídico-regulatória relacionada ao tema de proteção de dados. No entanto, de acordo com o Data Maturity Body of Knowledge (DAMA INTERNATIONAL, 2017), a governança de dados "o exercício de autoridade e controle (planejamento, monitoramento e execução) sobre o gerenciamento de ativos de dados", e "fornece orientação e supervisão para o gerenciamento de dados, estabelecendo um sistema de direitos de decisão sobre dados que atenda às necessidades da empresa". Vale ressa Vale ressaltar que os "dados" referidos englobam tanto os considerados "pessoais" quanto os "não pessoais", como dados estratégicos da empresa e dados de pessoas jurídicas.

Assim, a governança em privacidade, por sua vez, é destinada e desenhada para os dados considerados "pessoais" pela LGPD – aqueles que identificam ou tornam identificável uma pessoa natural – e tem como base um direito humano fundamental, a privacidade. A conformidade normativa tem um papel fundamental, mas as atividades de um programa de governança em privacidade não se resumem ao simples cumprimento do mínimo disposto no art. 50, mas vão além dele.

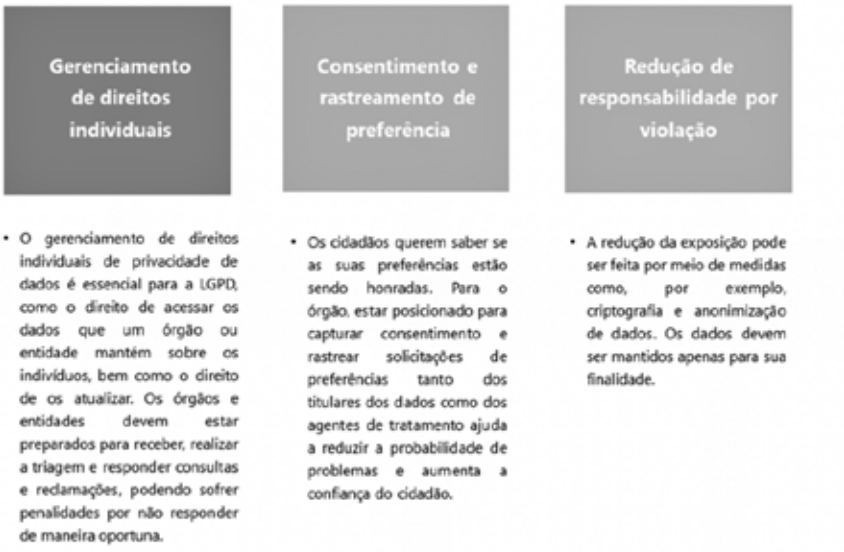
Nesse sentido, a intenção do legislador não é apenas atender aos ditames legais e concretizá-los em documentação que as organizações, privadas ou públicas, estão adequadas à lei, mas também explorar, em especial, os princípios e fundamentos da lei, com destaque para a legítima expectativa do titular de dados pessoais, e, ainda, transparecer como estratégia da liderança através de seus controles. Ou seja, transformar a privacidade e sua governança em ativo das organizações.

Nesse processo, quando as empresas demonstram ir além do cumprimento legal em matéria de proteção de dados e privacidade, sendo proativas no reforço à transparência, boa-fé, segurança dos dados e não discriminação no uso dos dados pessoais, por exemplo, ao mesmo tempo em que promovem a inovação, a autodeterminação informativa, o livre desenvolvimento da personalidade e o respeito à privacidade, esse conjunto todo acaba por valorizá-la ainda mais aos olhos dos titulares.

Logo, a governança em privacidade é um planejamento que se transforma em ativo. Além disso, promove o compliance e auxilia de forma concreta e efetiva a atuar na prevenção a sanções administrativas e judiciais.

Não obstante, gera principalmente impactos positivos na operação da empresa e a valoriza. Como a governança de dados tem como um de seus pilares o compliance em matéria de privacidade e proteção de dados pessoais, acaba apresentando uma intersecção com a governança em privacidade. Ambas estão debaixo do guarda-chuva da governança corporativa, um sistema que dirige a organização por meio de boas práticas que contribuem para sua gestão e longevidade, bem como para o bem comum.

Figura 6 – Considerações etapa de construção e execução.



Fonte: Oliveira *et al.* (2021).

6 CONSIDERAÇÕES FINAIS

Considerando a vigência da lei e a sua relevância para as organizações, tanto públicas quanto privadas, é de suma importância compreender a legítima expectativa do legislador para aplicar a legítima expectativa do titular de dados como centro do debate.

Pelo que foi exposto anteriormente, o caminho mais adequado para percorrer a LGPD em sua essência é a criação de um programa de governança em privacidade de dados pessoais, que, certamente, foi bem instruído nas fases anteriores da adequação à LGPD, descritas em etapas. Para relembrar, a adequação à LGPD é o "Dia 1", e a existência do programa de privacidade de dados pessoais passa a ser o "Dia 2" do aculturamento das organizações.

De modo prático, a governança como conceito clássico de organização e estruturação de sistemas e processos deve ser também objeto de estudo e destaque nos moldes da legislação brasileira de dados. Não obstante, o próprio roteiro criado pela lei ressalta a importância da governança no artigo 50 e subsequentes.

Por outro lado, as organizações públicas e privadas que pararem no "Dia 1" do projeto deverão encontrar dificuldades de conscientização e aculturamento ao longo do tempo.

Nesse sentido, a forma recomendada de implantar os processos de governança passa pelos treinamentos dos colaborares e real entendimento do objetivo do programa.

Logo, para que a transformação exigida pela LGPD surta efeitos, a organização deve passar para o "Dia 2", no sentido de obter indicadores de resultados para compreender se os objetivos traçados anteriormente estão de fato precisos e efetivos. A melhor forma de realizar o monitoramento exigido em lei, e parte integrante da criação da governança em privacidade, é por meio de números e coletas de informações ao monitorar, avaliar e direcionar possíveis ajustes e alterações.

A criação, portanto, de um programa de governança em privacidade de dados. Torna-se um ativo organizacional, composto por estruturas de governança, compliance e metodologias de revisões de processos, a fim de obter resultados mais efetivos, condutas mais apropriadas, aculturamento dos novos desafios digitais e, principalmente, acolher a intenção da Lei Geral de Proteção de Dados: o titular de dados pessoais respeitado como centro do debate.

REFERÊNCIAS

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (encarregado)**. São Paulo: Revista dos Tribunais, 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jul. 2022.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a órgãos e entidades da administração pública**. 2. ed. Brasília: TCU; Secretaria de Planejamento, Governança e Gestão, 2014. Disponível em: https://portal.tcu.gov.br/data/files/FA/B6/EA/85/1CD4671023455957E18818A8/Referencial_basico_governanca_2_edicao.PDF. Acesso em: 16 jul. 2022.

CABELLA, D. M. S.; FERREIRA, R. M.; KAUER, G. S.; KAUER, S. K. Afinal de contas: o que é a "Governança em Privacidade" da LGPD? **Migalhas**, 3 jul. 2020. Disponível em: https://www.migalhas.com.br/depeso/330230/afinal-de-contas--o-que-e-a--governanca-em-privacidade--da-lgpd. Acesso em: 16 jul. 2022

DAMA INTERNATIONAL. **Dama-Dmbok**: Data Management Body of Knowledge. 2. ed. [*s.l.*]: Technics Publications, 2017.

GOVERNANÇA corporativa. **IBGC**, [202-?]. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 16 jul. 2022.

LIMA, Diana Vaz de. Como promover a boa governança na gestão municipal. Brasília, DF: CNM, 2018. Disponível em: 10.13140/RG.2.2.36455.06566. Acesso em: 14 out. 2020.

NETO, Thaís. Boas práticas de governança na proteção de dados: o programa de governança em privacidade. **Instituto de Direito Real**, 19 out. 2020. Disponível em: https://direitoreal.com.br/artigos/boas-praticas-de-governanca-na-protecao-de-dados-o-programa-de-governanca-em-privacidade. Acesso em: 9 ago. 2022.

OLIVEIRA, Denis Marcelo *et al.* **Guia de Elaboração de Programa de Governança em Privacidade** – Lei Geral de Proteção de Dados Pessoais. Brasília: Ministério da Economia, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso em: 9 ago. 2022

PERSONAL DATA PROTECTION COMMISSION SINGAPORE. **Guide to Developing a Data Protection Management Programme**. [*s.l.*]: SG Digital, 2021. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Management-Programme-14-Sep-2021.ashx?la=en. Acesso em: 16 jul. 2022.

RONDÔNIA. Proteção de dados – LGPD. Introdução. **Portal do Governo do Estado de Rondônia**, 2022. Disponível em: https://rondonia.ro.gov.br/setic/institucional/lgpd/introducao/. Acesso em: 5 set. 2022.

3
LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NO CICLO DE POLÍTICAS PÚBLICAS NO MUNICÍPIO

Ana Carla Bliacheriene
Luciano Vieira de Araújo
Fátima L. S. Nunes

1 INTRODUÇÃO

A inserção da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) no sistema normativo brasileiro apresentou uma série de obrigações legais e desafios para os agentes públicos, uma vez que as ações estatais também implicam o tratamento de dados pessoais (sensíveis ou não) dos cidadãos, como o fito de garantir a prestação dos serviços públicos. No que concerne ao setor público, o foco da regulamentação legal é que a necessidade da prestação de serviços não descure do dever de proteção dos dados e da intimidade dos seus respectivos titulares.

As relações entre as organizações estatais e os cidadãos também foram cuidadas na LGPD, que impôs deveres de ação e de abstenção a serem obedecidos pelas organizações públicas.

Nos termos da política editorial desta obra, propõe-se um texto ensaístico no qual abordem-se alguns dos desafios do tratamento dos dados pelas organizações públicas, em especial as municipalidades, à luz do conjunto normativo da LGPD.

Como referencial, foram estudadas a Lei Geral de Proteção de Dados, documentos instrutivos (manuais, cartilhas e outros) dos órgãos federais de processamento de dados, textos de escolha livre, a partir de uma revisão narrativa de parte da literatura de proteção de dados, a partir da base do Google Acadêmico. A leitura acessada apoiou o levantamento dos aspectos que têm dirigido os estudos preliminares da novel legislação, quanto à suas implicações no setor público.

O fio condutor do ensaio foi compreender como a regulamentação da proteção de dados impacta o planejamento e a implementação de políticas públicas no município.

2 POLÍTICAS PÚBLICAS COMO PROBLEMAS PÚBLICOS

Pensar política pública e seus ciclos implica pensar etapas administrativas e operacionais para sua efetivação.

Acolheu-se, como base deste ensaio, o conceito de política pública e modelo de ciclo de política pública proposto por Secchi (2014). Assim, "política pública" foi entendida a partir do "problema público" como sendo a diretriz, o caminho, a estrada que se escolhe para resolvê-lo, pela União, estados, distrito federal ou pelos municípios. Essas diretrizes tanto podem ser estratégicas quanto operacionais. É nas diretrizes de caráter operacional em que a LGPD passa a ter um grande impacto nas ações da administração pública.

Os "problemas públicos" indicam uma discrepância entre uma situação fática diagnosticada e a situação ideal, prevista na legislação que determina a ação estatal.

A administração pública irá resolver esses "problemas públicos" diretamente (administração pública direta), por meio de suas secretarias e órgãos – todos vinculados hierarquicamente ao chefe do Poder Executivo – ou indiretamente (administração pública indireta), por meio de suas autarquias, fundações, sociedades de economia mista ou empresas públicas (Decreto n. 200/1967, art. 4.°).

A legislação foi ampliando os espaços de entregas de bens e serviços públicos, pela via de novos modelos de gestão, permitindo que agentes privados e da sociedade civil se tornassem parceiros da administração pública e responsáveis por entregas relevantes à sociedade: concessões; parcerias público privadas (PPP), organizações sociais (OS), organizações da sociedade civil de interesse público (OSCIP), dentre outros.

Além desses modelos, há ainda a possibilidade de contratação de empresas privadas, pela administração pública, pela via da Lei de Licitação (Lei n. 14.133/2021), para aquisição de bens, obras e serviços públicos, além da realização de algumas de suas atividades operacionais.

Em todas essas situações, seja diretamente, seja indiretamente ou por meio de terceiros particulares, a administração pública maneja dados públicos, dentre os quais dados pessoais dos cidadãos, que precisam estar resguardados e protegidos, conforme a nova legislação.

3 CICLO DE POLÍTICAS PÚBLICAS E SUAS INTERCONEXÕES COM A PROTEÇÃO DE DADOS

Ainda na literatura de Secchi (2014), as política públicas têm um ciclo ou fases que podem se dividir em até sete grandes etapas: identificação do problema; construção da agenda; formulação de alternativas; processo decisório; implementação; avaliação e extinção.

Cada vez mais agentes públicos têm buscado elementos mais seguros para a tomada da decisão política (agenda) e de gestão (formulação de alternativas e implementação, avaliação) no exercício de suas funções públicas.

Daí a importância de um diagnóstico realizado de forma adequada. Nesse sentido, o uso de bases de dados públicas e privadas têm sido frequentes para a tomada de decisão pública.

Nesse sentido, já se observa na literatura alguns autores que adotam a expressão "política pública baseada em evidência", que começou a ser popularizada a partir do documento oficial do governo britânico de 1999, *Modernizing Government* (GREAT BRITAIN, 1999).

A base desses textos está na ideia de que as decisões administrativas devem partir de problemas reais, cunhados a partir de um diagnóstico cientificamente validado, e não a partir de vieses ideológicos.

Nesse sentido, os avanços tecnológicos que permitem a captação de uma miríade de dados, seu armazenamento em grandes bancos e o aumento da capacidade de processamento pelos atuais hardwares e de interpretação e interconexão por variados softwares ampliaram as vias de atuação dos agentes estatais, que passaram a ser também vítimas frequentes de ataques cibernéticos.

Conhecido como o petróleo do século XXI, os dados passaram a chamar atenção de organizações criminosas que se reinventam em práticas delituosas no ambiente digital.

Se, de um lado, as novas tecnologias abriram espaços para o surgimento de um governo "*data-driven*", possibilitando a transição digital do governo (Lei n. 14.129/2021), de outro a necessária regulação da proteção de dados (Lei n. 13.709/2018) gera desafios na cultura organizacional das entidades públicas que precisam inovar em processos, ao mesmo tempo em que protegem os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural referente aos cidadãos.

Não é muito difícil, a partir do conceito das etapas do ciclo de políticas públicas, compreender que os dados – em especial os dados dos cidadãos – permeiam, de forma intensa, cada decisão do gestor público para a entrega de bens e serviços públicos.

4 IDENTIFICAÇÃO DO PROBLEMA E CONSTRUÇÃO DA AGENDA

A identificação do problema e a construção da agenda prevê a definição de quais são os problemas ou temas entendidos como relevantes, sintetizando em uma frase sua essência.

Uma vez escolhido o problema a ser atacado, ele precisa entrar numa etapa de decisão política de acolhê-lo como prioritário. Deve entrar no radar de relevância e prioridade do gestor: entrar na "agenda".

Há três condições essenciais para que um problema entre na agenda política: atenção ou relevância; possibilidade de ser resolvido (resolubilidade); competência para sua resolução.

O uso de base de dados tem sido uma grande fonte para a delimitação do diagnóstico e, consequentemente, dos problemas públicos que serão atacados posteriormente pelas políticas públicas.

Igualmente, o acesso e a análise de bancos de dados podem ser fundamentais para aferir a relevância, a resolubilidade e a competência da estrutura da administração pública em conferir uma solução adequada, por meio de uma análise de risco.

5 A FORMULAÇÃO DE ALTERNATIVAS E PROCESSO DECISÓRIO

Nessa etapa, buscam-se soluções passando pelo estabelecimento de objetivos e estratégias para atacar o problema público. Ou seja, deve-se escolher, dentre várias possibilidades, aquelas mais convenientes para a sua resolução.

A formulação de alternativas pode ser feita a partir de três técnicas: observação de tendências (projeções); uso de teorias e analogias (predições); juízos de valor (conjecturas).

Já os modelos para a formulação de alternativas podem ser: racionalidade absoluta e racionalidade limitada, que são fortemente influenciados pela existência e qualidade de dados para o diagnóstico prévio do problema e de suas dimensões.

Assim, a projeções, predições e o modelo da racionalidade absoluta são fortemente dependentes do uso de bases de dados.

6 IMPLEMENTAÇÃO

A fase de implementação é aquela em que normas, processos e rotinas se convertem em ações efetivas da administração pública.

Nessa etapa é comum serem criadas bases de dados para análise posterior e retroalimentação das bases existentes. Mas também é aqui que a relação da administração pública com o cidadão se aproxima de forma radical, seja como demandante do serviço público específico, seja como potencial usuário no universo da cidadania.

7 AVALIAÇÃO E EXTINÇÃO

Aqui, a observação de obstáculos e as falhas na condução anterior da política pública ou da tomada de decisão podem, em tempo, detectar problemas mal formulados, objetivos mal traçados, metas exageradas, promovendo uma readequação do projeto para sua nova versão ou criando

aprendizados organizacionais para tentativas futuras de abordagem desse mesmo problema, caso a decisão seja pela extinção da política pública.

O processo de avaliação da política pública é o "processo de julgamentos deliberados sobre a validade de propostas para a ação pública" (SECCHI, 2014. p. 53). A avaliação pode ocorrer antes (*ex ante*), durante (*in itinere)* ou depois (*ex post*) da implementação da política pública.

São elementos para uma avaliação qualificada das políticas públicas a existência de: critérios (economicidade, eficiência, eficácia, efetividade, equidade); indicadores (medir *input*, *output* e resultado – *outcome*); padrões (repetições relevantes para o ciclo da política pública).

Cada vez mais, o uso de dados tem sido demandado para que as avaliações consigam ser úteis e possam interferir na qualificação do ciclo das políticas públicas.

Uma vez passadas essas etapas, uma política pública pode ser mantida (com ou sem ajustes) ou extinta. As causas da extinção de uma política pública são: o problema público foi resolvido; os programas ou leis foram avaliados de forma negativa e tidos como ineficazes; o problema perdeu progressivamente a importância deixando de ser relevante para a ação pública.

8 PRINCIPAIS ASPECTOS DA LGPD NO SETOR PÚBLICO

A LGPD aplica-se a qualquer órgão ou entidade pública da administração pública direta ou indireta (art. 3.°). Há, no entanto, algumas exceções previstas no art. 4.º da lei que delimitam quando não se aplica seus dispositivos para tratamento de dados que tenham como finalidade exclusiva: jornalística e artística; acadêmica; segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (BRASIL, 2018).

Além desses, também no art. 4.º há referência expressa ao tratamento de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes brasileiros de tratamento ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado à LGPD.

Como regra, entende-se que o setor público deve estar apto à proteção dos dados, obedecendo aos regramentos da LGPD, excetuando-se as situações expressamente previstas no art. 4.º da lei.

No entanto, o fato de não se aplicar a LGPD em uma situação concreta não exime o Estado do seu dever de proteção à privacidade e à intimidade dos cidadãos, amplamente normatizada na Constituição Federal – o Marco Civil da Internet, regime jurídico administrativo que prevê, inclusive, a

responsabilidade objetiva do Estado quanto aos danos causados pelos seus prepostos ao cidadão.

Como visto, a administração pública trata permanentemente os dados dos cidadão, como base para atuação pública. A nova legislação não veio impedir que assim se faça, mas tão somente veio estabelecer alguns requisitos obrigatórios (art. 7.° LGPD) para que esse tratamento seja garantidor dos direitos fundamentais à intimidade, privacidade e proteção dos dados do cidadão (art. 5.º, CF/88).

Quando os dados a serem tratados não forem dados sensívei,s essa operação deve ser precedida da manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada (consentimento) e que possa ser revogado pelo titular dos dados, a qualquer momento.

Nesse sentido é importante que a política de tratamento e proteção de dados esteja claramente disponível ao cidadão nos sites institucionais, nos portais de transparência e portais de prestação de serviços digitais do governo.

Autorizações genéricas, sem especificação clara da finalidade do tratamento de dados são nulas de pleno direito.

Além do tratamento precedido de autorização expressa, há outras situações em que a legislação permite o tratamento, tais quais:

> Art. 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;[9]
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;[10]

9 Aqui podem ser enquadradas as atividades das universidades e instituições de pesquisa públicas.

10 Nessa classificação entrariam os contratos administrativos celebrados com base na Lei de Licitação ou outras correlatas que regulamentos os contratos realizados entre a administração pública e agentes privados.

> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);[11]
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; [...] (BRASIL, 2018).

A questão torna-se mais delicada quando o objeto do tratamento é dado sensível. Nesse caso o consentimento simples não é suficiente para o tratamento do dado. Trata-se de um consentimento qualificado, específico e destacado, para finalidades determinadas e expressamente esclarecidas.

A exemplo dos dados não sensíveis do art. 7.º da LGPD, o art. 11 estabeleceu hipóteses para o tratamento dos dados sensíveis, sem a necessidade de autorização prévia do seu titular.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...]
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;[12]
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização[13] dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

11 Estariam aqui entendidos os processos sindicantes e processantes de servidores que correm junto a administração pública ou ainda processos administrativos que correm perante o fisco ou agente de fiscalização edilícia.

12 Aqui estão excluídas as políticas públicas relativas a contratos e convênios.

13 A anonimização surge como um elemento extra e condicionante do uso dos dados para a proteção do seu titular.

> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais[14] (BRASIL, 2018).

Observe-se que, nessas hipóteses, a despeito da inexigibilidade de autorização prévia do titular de dados para seu tratamento pela administração pública, a administração não está dispensada de tornar clara e transparente a política de tratamento desses mesmos dados.

É importante destacar que a regra é que o titular dos dados possa a qualquer tempo requerer que: dados sejam apagados; um consentimento prévio seja revogado; seus dados sejam transferidos para outro fornecedor de serviços etc. Apenas em situações excepcionais e previstas em lei, esses direitos são mitigados.

O princípio da finalidade deve ser um farol a iluminar todas as ações do agente público no tratamento dos dados pessoais dos titulares.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; [...]
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) (BRASIL, 2018).

Diante de tantos impactos na rotina do ciclo das políticas públicas, é de absoluta relevância que os agentes públicos atentem para o tema do gerenciamento de riscos e falhas nos sistemas de proteção de dados, garantindo respostas que mitiguem os efeitos dos danos e que cessem a continuidade das eventuais falhas de sistema.

O sistema de gerenciamento de riscos deve contemplar: um modelo de governança de TI adequado; adoção de boas práticas de acordo com os

14 Nessa hipótese podemos colocar situações em que seja necessária a coleta de dados biométricos para acessar serviços públicos ou exercer direitos de cidadania.

melhores padrões do mercado; planos de contingência e auditorias regulares; capacitação do encarregado de proteção de dados e dos servidores da organização para uma cultura de proteção de dados; mapear o fluxo de dados e de seus sistemas (tráfego, armazenagem, compartilhamento); promover as mudanças necessárias.

9 CONCLUSÃO

O tema da aplicação e do impacto da LGPD no setor público está muito longe de ser encerrado, nem foi esgotado os desafios que os gestores públicos já encontram no exercício de suas atividades.

O presente ensaio buscou relacionar alguns desses desafios com a teoria do ciclo das políticas públicas (SECCHI, 2014), apontando que a administração pública vive dos dados e é uma forte importante de sua produção, com possibilidade ilimitada de causar danos ao cidadão, caso não atenda aos parâmetros protetivos mínimos da LGPD.

Nesse sentido, a regulamentação da proteção dos dados, inspirada no modelo europeu e materializada no Brasil pela Lei Geral de Proteção de Dados, tem gerado muitos impactos na administração pública, impulsionando alteração na gestão da máquina administrativa, como também nos sistemas da informação destinados à prestação de serviços públicos, que crescem vertiginosamente com a regulamentação do governo digital.

REFRÊNCIAS

BRASIL. **Decreto-lei n. 200, de 25 de fevereiro de 1967**. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm. Acesso em: 4 ago. 2022.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 12 abr. 2022.

GREAT BRITAIN. **Modernising Government**. London: Stationery Office, 1999.

SECCHI, Leonardo. **Políticas Públicas:** conceitos, esquemas de análise, casos práticos. 2. ed. São Paulo: Cengage Learning, 2014.

XAVIER, Fabio Correa. LGPD no Setor Público: bases legais para o tratamento de dados pessoais. **Migalhas**, 7 mar. 2022. Disponível em: https://www.migalhas.com.br/depeso/360877/lgpd-no-setor-publico-bases-legais-para-o-tratamento-de-dados. Acesso em: 12 abr 2022.

4
JORNADA DO ESTADO DE SÃO PAULO PARA ADEQUAÇÃO À LGPD

Andra Robert de Carvalho Campos
Ademir Bento Simão, Beatriz Scavazza
Elizabete Campos, Luis Márcio Barbosa
Maria Bernardete Ferreira
Matusalém dos Santos Carvalho
Melissa Giacometti De Godoy
Rhima Ahmad Charanek Santana
Sabrina Lucila de Araujo

Resumo

O presente artigo tem como objetivo apresentar o caminho e metodologia de adequação à Lei Geral de Proteção de Dados utilizado pelo Governo do Estado de São Paulo.

Palavras-chave: LGPD; medidas práticas; setor público; Governo do Estado; adequação.

1 INTRODUÇÃO

O caminho do Estado de São Paulo rumo à adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) está intrinsecamente ligado à estratégia, já em curso, de aprofundamento da transformação digital. Isso significa, entre outros aspectos, a promoção de um governo digital que utiliza as tecnologias da informação e comunicação (TICs) para implementar, de forma ampla e transversal, a governança e a proteção de informações e dados pessoais, resultando em ações inter-relacionadas e indissociáveis do processo de adaptação à lei.

A Emenda Constitucional n. 115, de 10 de fevereiro de 2022, evidencia a importância e a atualidade da proteção de dados pessoais, alçada à condição de direito fundamental de brasileiros e estrangeiros residentes no país, juntamente com temas como vida, liberdade, igualdade, segurança e propriedade.

Também é parte essencial deste objetivo a promoção de uma mudança cultural dos gestores e colaboradores de todos os níveis da administração pública. Para garantir maior proteção, eficácia e segurança no tratamento

dos dados e das informações do cidadão pelo Estado, é fundamental a adoção das boas práticas recomendadas em relação aos fluxos técnico-operacionais e à elaboração e execução dos serviços públicos.

O que se pretende com este texto é apresentar os passos dados por São Paulo para a instituição das normas relativas à Política de Governança de Dados e Informações (PGDI) e à Política de Proteção de Dados Pessoais (PPDP), publicadas em dezembro de 2021, e que corresponderam a:

– requisitos para a adequação à LGPD – as condições prévias necessárias;
– metodologia aplicada para a estruturação das ações previstas e implementadas;
– ações complementares em andamento;
– principais conceitos adotados.

É nesse contexto que o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP), da Secretaria de Governo, apoiado pela Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação (SSCTI), e em consonância com o Conselho Estadual de Tecnologia da Informação e Comunicação (Coetic), vem promovendo a jornada do Estado de São Paulo para adequação à LGPD. Trata-se de um percurso desafiador, especialmente se considerados o porte e a complexidade da administração pública paulista. Mas certamente também serão muitas as oportunidades para o aprimoramento dos serviços ofertados aos cidadãos.

2 REQUISITOS PARA A JORNADA DE ADEQUAÇÃO À LGPD NO ÂMBITO DO PODER PÚBLICO

Como já se sabe, a LGPD é de grande impacto para a administração pública, impondo profundas alterações culturais e, especialmente, grandes adaptações nas formas de gestão usualmente adotadas.

Sua observância não é obrigatória somente em razão da vigência e das sanções expressamente dispostas, mas também pelas implicações comportamentais que se impõem ao conjunto dos setores público e privado, afetados, em igual medida, pelas regras de proteção aos dados pessoais, acompanhando boas práticas internacionais.

O direito à privacidade, amparado pela LGPD, depende da proteção dos dados e das informações relativas a uma pessoa natural identificada ou identificável que transitem nas esferas do poder público durante o exercício de competências, atribuições legais e atividades, em meios de suporte físico e digital.

Tal prerrogativa alcança, portanto, um sem-número de titulares (colaboradores, contratados, fornecedores e usuários de serviços públicos etc.), com a administração pública respondendo pelo tratamento dos dados

pessoais em operações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (LGPD, artigo 5.º, X) (BRASIL, 2018).

São obrigações que resultam num contexto de alta complexidade, multifacetado e de abrangência nacional. Por isso, é urgente a adequação das administrações públicas de qualquer esfera da federação, mediante um processo que certamente implicará ampla revisão de operações, conceitos e estratégias.

Nessa jornada, é essencial iniciar por um cuidadoso planejamento, para que a LGPD seja internalizada com eficácia no Estado e nos municípios. Dentre as boas práticas relacionadas a esse compromisso, está a observação de alguns requisitos, entendidos como imprescindíveis a um processo de adequação minimamente satisfatório.

O primeiro é o da oferta de marcos regulatórios locais para a lapidação da temática da LGPD e os principais atores desse processo. Os arcabouços jurídicos de referência poderão, certamente, servir de farol para identificar as necessidades normativas a serem estruturadas, visando à definição das formas, metas, competências e dos organismos que irão desenvolver as atividades decorrentes.

No Estado de São Paulo, essa etapa encontrou eco em diversos atos. São eles:

• Decreto n. 64.601, de 22 de novembro de 2019, que recriou a Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação e reorganizou o Conselho Estadual de Tecnologia da Informação e Comunicação (Coetic);

• Decreto n. 64.790, de 13 de fevereiro de 2020, que instituiu o Comitê de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP) como o principal articulador e regulamentador do assunto;

• Resolução da Secretaria de Governo n. 86, de 2 de setembro de 2020, que estabeleceu as competências para a elaboração da Política de Governança de Dados e Informações no âmbito da Administração Pública estadual;

• Decreto n. 65.347, de 9 de dezembro de 2020, que dispôs sobre a aplicação da LGPD no estado, tratando expressamente das atribuições do CGGDIESP e do encarregado de dados, bem como das competências para a elaboração da política estadual de proteção de dados pessoais;

• Decreto n. 66.016, de 15 de setembro de 2021, que reestruturou a Secretaria de Governo e a Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação, fundamentais para o início do processo de adequação e implementação das medidas.

A identificação dos atores não se esgotou nas áreas mencionadas, e envolveu também outras instâncias administrativas, como a Procuradoria-Geral do Estado e a Companhia de Processamento de Dados do Estado de São Paulo (Prodesp), como membros do CGGDIESP, a Ouvidoria-Geral do Estado, na qualidade do encarregado pelo tratamento de dados pessoais da administração direta, e a Coordenadoria de Tecnologia da Informação e Comunicação (Coortic), como área de apoio técnico aos órgãos colegiados Coetic e CGGDIESP.

O segundo requisito está no entendimento da relevância da plena articulação entre os órgãos e as entidades envolvidos, com canais de integração ágeis e eficientes para um tratamento uniforme de toda a administração (direta e indireta) no processo.

O princípio da descentralização administrativa, os compromissos com a transparência estampados na Lei de Acesso à Informação e a harmonização das ações e medidas adotadas devem estar corretamente dimensionados para os efeitos da LGPD.

A eficiente interlocução dos agentes de tratamento da administração pública na condição de controladores, operadores ou encarregados de dados, estes últimos enquanto o canal de comunicação com a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados, é condição essencial para o sucesso e a absorção das medidas de adequação.

Por fim, o terceiro requisito é a aplicação de um diagnóstico atualizado para a identificação dos graus de conformidade à LGPD dos órgãos e das entidades da administração pública.

É preciso, antes, conhecer, para então ajustar, adequar e regrar. O diagnóstico deve ser estruturado para que resulte em indicadores confiáveis e que possibilitem a aferição dos diferentes estágios de conhecimento, conceituação, expectativas, providências e adaptações (já realizadas ou a serem realizadas) para o embasamento de ações regulatórias, operacionais, de capacitação ou de monitoramento capazes de promover a adequação à LGPD em toda a administração pública.

3 METODOLOGIA APLICADA NO ESTADO DE SÃO PAULO

No âmbito da administração pública paulista, coube ao Comitê de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP), da Secretaria de Governo, articular e coordenar as atividades relacionadas aos processos de verificação da adequação e implementação das ações de conformidade à LGPD.

Com base nas premissas apontadas, o planejamento e a implementação do processo tiveram as seguintes atividades:

• **realização de diagnóstico** – estruturação e aplicação dos instrumentos elaborados com o objetivo de aferir o grau de adequação dos órgãos e das entidades à legislação federal;-

• **pesquisa sobre arcabouço legal** – levantamento e estudo das normas e dos regramentos estaduais para o estabelecimento de uma visão integrada e sólida das bases normativas incidentes (direta ou indiretamente) no processo de adequação;

• **elaboração das referências normativas principais** – desenvolvimento de análises que apontaram para a eficácia da produção de textos estruturantes contendo as diretrizes para a política de governança de dados e informações (PGDI) e a política de proteção de dados pessoais (PPDP). Esses documentos foram complementados com os desdobramentos e as providências direcionadas para a conformidade do estado às boas práticas de governança de dados e informações, e, especialmente, à segurança e proteção dos dados pessoais sensíveis e de crianças e adolescentes;

• **identificação das múltiplas participações** – definição clara de papéis e responsabilidades dos órgãos e das entidades em todo o processo e da função vital do CGGDIESP na orquestração de ações estratégicas e centralizadas, desenhando, de forma articulada, os respectivos fluxos regulamentadores e operacionais;

• **capacitação** – diante da multiplicidade de fatores a serem observados e que exigem um bom nível de conhecimento para o enfrentamento das questões, tornou-se fundamental implementar ações direcionadas à disseminação de informações aos colaboradores da administração;

• **segurança no tratamento dos dados** – os padrões das normas de segurança da informação, de proteção de dados pessoais e de gestão de dados e informações, presentes na família de normas internacionais ISO/IEC 27000, foram utilizados como base da formulação das questões elaboradas para o diagnóstico aplicado, e para a definição das providências elencadas nos desdobramentos da PGDI e da PPDP.

As ações sinérgicas possibilitaram uma troca produtiva de informações entre os organismos envolvidos. Essa condição contribuiu para a articulação entre a administração direta e indireta, na busca por uma ação conjunta e integrada visando à conquista de resultados concretos, com monitoramento contínuo de todo o processo.

3.1 DIAGNÓSTICO EM LGPD – COMO FOI A IMPLEMENTAÇÃO

O diagnóstico foi proposto como uma ação autoavaliativa (por meio de questionários) e integrada a iniciativas de comunicação e capacitação, de modo a sensibilizar os gestores dos órgãos e das entidades sobre o tema e qualificar os participantes de forma on-line, assíncrona e interativa.

Essa capacitação foi indispensável para possibilitar um macromapeamento dos processos de tratamento de dados pessoais, uma vez que para realizar a autoavaliação é preciso ter conhecimento mínimo sobre os conceitos da nova legislação, que dispõe sobre como devem ser tratadas tais informações, com atenção ao respeito e aos direitos do titular dos dados pessoais. Para tanto, durante todo o processo do diagnóstico, foram disponibilizadas equipes destinadas a solucionar as dúvidas dos participantes.

Os respondentes foram escolhidos pelos dirigentes dos órgãos e das entidades, considerando-se o conhecimento sobre a lei e os aspectos práticos que impactam questões relacionadas à atividade-fim, a processos, à tecnologia da informação e a temas jurídicos.

Foram, assim, definidos perfis mais abrangentes dos colaboradores que participaram das ações de sensibilização e capacitação anteriores ao diagnóstico. Essa avaliação foi composta por 13 temáticas relativas à LGPD: coleta, eliminação, incidentes/riscos, instrumentos contratuais, direitos dos titulares, processamento, sistemas, governança, compartilhamento, armazenamento, segurança, base legal e princípios.

A utilização da norma técnica (Família ISO 27000) contribuiu para a elaboração das questões e das alternativas, tornando-as mais prescritivas e concretas. As perguntas propostas consideraram referências para o processo de adequação, e, nesse sentido, foram padronizadas alternativas e modeladas gradações dos itens de resposta, a fim de melhor direcionar o processo.

O objetivo foi identificar os níveis de adequação à LGPD em cada órgão e entidade participante, visando a auxiliar no desenvolvimento de planos de ação e de conformidade para racionalizar recursos de orientação e viabilizar a formação das equipes envolvidas em próximas capacitações, orientações técnicas e nas ações de comunicação e divulgação.

Os principais indicadores analisados no diagnóstico foram:

- o grau de vulnerabilidade dos temas em relação à LGPD;
- o grau de adequação geral, considerando-se o nível de vulnerabilidade de cada órgão e entidade;
- o patamar de conhecimento em relação às temáticas da legislação;
- os riscos potenciais aos quais o estado está sujeito a partir dos aspectos abordados no levantamento;
- as consequências possíveis para cada risco potencial mapeado no diagnóstico;
- o grau de severidade dos riscos, considerando-se a chance de ocorrência, a partir das respostas, e o impacto e as consequências;
- a priorização das recomendações para cada órgão e entidade que respondeu ao questionário.

O diagnóstico nos órgãos e nas entidades da administração pública estadual alcançou, aproximadamente, 90% de retorno em relação aos questionários. As respostas foram analisadas em três dimensões:

• grupo de órgãos definido pela coordenação dos trabalhos (compondo amostra para uma visão mais rápida dos resultados);
• totalidade dos questionários preenchidos (consolidando uma visão geral do Estado de São Paulo)
• foco em cada órgão e entidade (que recebe os resultados do diagnóstico, sistematizados e consolidados, a partir da análise de suas respostas).

Aspecto importante dos trabalhos de diagnóstico sobre a LGPD diz respeito à elaboração de devolutiva dos resultados para cada órgão ou entidade participante, em formato de capacitação, tal como aplicado desde a fase inicial de preenchimento das informações do questionário, marcando a formação em serviço que se adotou no processo de adequação à LGPD no estado.

3.2 DOCUMENTOS NORMATIVOS DAS POLÍTICAS PGDI E PPDP DO ESTADO DE SÃO PAULO

De forma paralela, porém articulada ao diagnóstico, foi instituído um grupo de trabalho com atribuições que incluíram a elaboração dos documentos normativos com as diretrizes para a governança de dados e informações, o tratamento de dados pessoais, a política de privacidade e a segurança dos dados e informações sob a responsabilidade do estado. Isso, contudo, em nada prejudica a aplicação subsidiária e complementar de normas e regras específicas, adaptadas às particularidades de cada órgão ou entidade da administração pública direta e indireta.

Assim, foram estruturadas a política de governança de dados e informações (PGDI) e a política de proteção de dados pessoais (PPDP) do Estado de São Paulo. Elas foram instituídas pelas Deliberações Normativas n. 1 e nº 2 do CGGDIESP, de 30 de dezembro de 2021, e publicadas no dia subsequente.

Os trabalhos desenvolvidos foram baseados, por exemplo, em exame e estudos de documentos disponíveis nas áreas técnicas e normativas do Estado, no *benchmarking* em relação a outros entes da federação e em experiências internacionais. Também fizeram parte os debates com os principais atores dos processos relativos à LGPD, especialmente os órgãos colegiados do CGGDIESP e Coetic.

O principal resultado das análises foi a decisão de circunscrever os documentos normativos aos seus aspectos mais abrangentes e perenes, adotando-se os princípios e as diretrizes gerais presentes na lei federal. As

questões de natureza técnica ou operacional e os aspectos regulamentadores adicionais foram consolidados como providências e documentos complementares, transferindo, assim, a rotina de ajustes, adequações e alterações para as medidas adicionais.

Acrescente-se, ainda, que toda a análise desenvolvida pelo Estado de São Paulo foi realizada com amparo na legislação vigente e em *frameworks*[15] estabelecidos. Eventuais alterações legislativas ou de entendimento jurisprudencial que venham a ocorrer, em razão até mesmo da recente implementação da lei, ensejarão a atualização e a adequação dos documentos da PGDI e da PPDP.

Na política de governança de dados e informações (PGDI) estão contidos os princípios, os objetivos e as diretrizes gerais para a governança de dados e informações, com destaque para a gestão de documentos, segurança dos dados e informações em todo o ciclo de vida, controle de acessos, sigilo, armazenamento e eliminação.

Igualmente relevantes são os dispositivos relativos ao gerenciamento de riscos, à gestão de incidentes de segurança, à integração e interoperabilidade dos dados, ao controle de acessos físicos e digitais, à resposta a incidentes de segurança e ao monitoramento.

Na política de proteção de dados pessoais (PPDP), além de objetivos e princípios, podem ser localizados os temas, finalidades e bases legais, agentes de tratamento, direitos dos titulares, coleta, uso, compartilhamento, armazenamento e eliminação de dados pessoais, e incidentes de segurança com dados pessoais, bem como consta o modelo da política de privacidade e tratamento de dados pessoais

Ainda que um dos aspectos fundamentais do processo de adequação esteja na identificação das diretrizes relacionadas à governança de dados e informações, principalmente quanto à proteção de dados pessoais e dados pessoais sensíveis, os desdobramentos são necessários para concretizar os direcionadores dos referidos normativos.

Com o objetivo de destacar a importância desse elo, a estruturação dos anexos da PGDI e PPDP (na forma de medidas adicionais regulatórias, técnico-operacionais e comportamentais) e a definição dos responsáveis

15 Especial destaque para o Sistema de Gestão de Privacidade da Informação, previsto na ISO/IEC 27701 (utilização dos controles e diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação – SGPI –, como extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, para a gestão da privacidade dentro do contexto do Estado de São Paulo) e em capítulos do DAMA-DMBOK (DAMA-DMBOK. *Guide to the Data Management Body of Knowledge*, DAMADMBOK v2, 2017.). Além dos seguintes suportes normativos: Constituição da República Federativa do Brasil de 1988, art. 37; Lei Federal n.º 13.709/18; Lei Federal n.º 12.527/11; Decreto Estadual n.º 58.052/12; Decreto Estadual n.º 64.601/19; Decreto Estadual n.º 64.790/20; Resolução SG-86/20; Decreto Estadual n.º 65.347/20; ISO/IEC 29100:2020; ISO/IEC 29151:2020.

integraram os documentos normativos, contendo a identificação das ações a serem desenvolvidas de forma centralizada, na busca pelo alcance de uma uniformidade na atuação do estado em questões estratégicas.

Entretanto, cabe registrar que tais medidas orientam também as ações descentralizadas cabíveis aos órgãos e entidades, no âmbito de suas respectivas atuações.

A partir dos resultados do diagnóstico em LGPD e da definição de premissas e critérios preestabelecidos, torna-se possível escalonar a priorização dos desdobramentos, o que possibilita, por sua vez, uma visão organizada e articulada dos temas e providências.

Para a definição das ações prioritárias devem ser consideradas as providências necessárias aos órgãos e às entidades para o início do processo de adequação com base nas ações estruturantes, de forma a prover maior compreensão sobre aspectos comuns ou relacionados aos normativos norteadores.

A partir do diagnóstico, também foram considerados os temas de alta vulnerabilidade para parcela significativa dos grupos de participantes da administração pública estadual.

A organização por temas favoreceu a articulação entre as providências indicadas nos dois normativos, por meio de ações conjuntas que envolveram, por exemplo, capacitação e comunicação, favorecendo sua viabilização e o maior entendimento sobre os temas.

Como premissa final da priorização, foi identificada a necessidade de articulação entre os diversos atores para as providências de acordo com as fases estabelecidas.

É fundamental que a implementação das medidas de adequação aconteça por fases e esteja organizada por estratégias de articulação dos temas e pré-requisitos para viabilizar a adequação à LGPD.

Ressalte-se que, para envolver e engajar os agentes, devem ser elaboradas devolutivas ao nível estratégico da administração, apresentando os resultados do diagnóstico com as devidas ênfases por grupos de órgãos e entidades.

Com a avaliação dos resultados, o detalhamento das fases de implementação e a formação de equipes de adequação, as ações podem ser mais bem compreendidas pelos responsáveis pela execução. Ao mesmo tempo, busca-se garantir uma base de conhecimento para que orientações, informações ou documentos venham a ser realmente aproveitados nos contextos específicos da administração pública.

Não menos relevante é a constatação de que a estruturação das providências requeridas pela PGDI e pela PPDP implica a apresentação de resultados agregados, como a padronização das ações de adequação à LGPD e a adoção de uma gestão proativa, integrada, sistemática e efetiva na implementação.

4 AÇÕES COMPLEMENTARES – MONITORAMENTO E SISTEMAS

O monitoramento da implementação das medidas para adequação à LGPD é aspecto fundamental e deve ser considerado desde o início do processo. Por essa razão, a base de levantamento para o diagnóstico foi desenvolvida com o objetivo de possibilitar futuras sondagens para avalições da evolução geral da conformidade dos órgãos e das entidades em relação à LGPD – nas ações a serem desenvolvidas de forma centralizada, nas iniciativas com implementação por órgãos e entidades e nas medidas que se desdobram de orientações e padrões centrais.

A aferição poderá ser feita a partir da análise da evolução dos planos de conformidade elaborados e atualizados por órgãos e entidades, envolvendo também os indicadores de incidentes.

O ciclo de monitoramento completo deve envolver, portanto, indicadores relacionados ao diagnóstico, aos planos de conformidade, às capacitações e aos treinamentos realizados e à efetiva implementação das providências e dos documentos complementares indicados nos instrumentos normativos da PGDI e da PPDP.

As ações de adequação à LGPD impõem a necessidade de revisão das operações nos órgãos e nas entidades, bem como a adoção de novas estratégias nas infraestruturas físicas e tecnológicas, para fins de incorporação dos requisitos da lei.

Esse é um contexto que aponta para a obrigação de serem incorporadas novas tecnologias, metodologias de gestão e de execução na área da tecnologia da informação (TI), bem como a adequação e a integração dos sistemas legados, transacionais ou não, em uso em toda a administração estadual.

Conforme dispõe o artigo 1.º da LGPD, sua aplicação não abrange somente os dados eletrônicos estruturados, mas também os dados pessoais ou sensíveis que são coletados e armazenados em meios físicos, ou seja, não estruturados. Isso demonstra a importância da participação ativa das áreas das atividades-fim em conjunto com as equipes de TICs.

Dessa maneira, o mapeamento dos sistemas de apoio tem relevância estratégica para as ações de adequação à LGPD, tanto para aquelas que serão desenvolvidas de forma centralizada quanto para as descentralizadas.

Os sistemas de apoio tecnológico que exigem revisão e atualização podem ser classificados em:

a) *sistemas de infraestrutura tecnológica*, que são relacionados com a segurança da informação ou segurança cibernética e que visam à identificação preventiva ou à contenção de incidentes em todas as suas particularidades;

b) *sistemas de informação computadorizados* resultantes da integração entre tecnologia, pessoas e organização, visando à automação da gestão gerencial

e ao apoio às atividades operacionais de atendimento ou relacionamento com os cidadãos, e sistemas especialistas ou de gestão integrada, com foco na atividade-fim de cada órgão ou entidade.

Os sistemas de tecnologia devem ser adequados para garantir que os dados e as informações estejam estruturados, de forma a possibilitar o uso compartilhado na execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo cidadão.

Essa diretriz está na PGDI. Ela aparece no item que trata de integração e interoperabilidade, cujas atividades devem ser planejadas, desenvolvidas, testadas e implementadas, de maneira que os diversos sistemas utilizados estejam integrados e as bases de dados utilizadas passem por melhoria contínua, com o objetivo de torná-los acessíveis por mecanismos de busca, leitura, consulta e recuperação de dados.

Por fim, os sistemas devem ser revisados e atualizados com a finalidade de implementação do controle da coleta de dados pessoais e da adoção dos procedimentos de revisão das entradas de informação do dado pessoal, considerando-se os serviços públicos prestados, os limites para a coleta de dados estritamente necessários e as finalidades para o tratamento.

5 PRINCIPAIS CONCEITOS ADOTADOS

Os conteúdos da política de governança de dados e informações (PGDI) e da política de proteção de dados pessoais (PPDP) adotam os conceitos e terminologias presentes na LGPD. As políticas contemplam o que deve ser assimilado pela administração pública paulista no que diz respeito à abordagem da governança e do tratamento de dados e informações, com indicativos para a operacionalização nos anexos que tratam das providências e documentos complementares aos normativos.

Os principais conceitos presentes nos normativos tiveram por referência as três dimensões que embasam a PGDI e a PPDP e constituem seus temas essenciais. São elas: a governança de dados, a segurança da informação e a proteção de dados pessoais. Conforme a figura abaixo, cada tema está contido no outro, sendo que a privacidade está presente na proteção de dados pessoais.

Figura 1 – As três dimensões da PGDI e da PPDP

Fonte: São Paulo (2022).

Como se pretendeu demonstrar, a governança de dados e informações abarca os demais temas. Segundo o *Data Management Body of Knowledge* (DAMA, 2017), ela consiste em exercer autoridade e controle (planejamento, monitoramento e execução) sobre o gerenciamento de ativos de dados, com o objetivo de garantir que sejam geridos de forma adequada, de acordo com as diretrizes estabelecidas e as melhores práticas, em prol da tomada de decisão responsável e qualificada (artigo 7.º da PGDI). O DMBOK e os padrões dispostos no arcabouço das normas ISO/IEC 27000 foram referências conceituais importantes para as diretrizes instituídas na PGDI.

5.1 POLÍTICA DE GOVERNANÇA DE DADOS E INFORMAÇÕES (PGDI)

O conjunto temático da PGDI pode ser sintetizado conforme a figura 2.

Dentre os princípios dispostos no artigo 6.º da LGPD, reproduzidos na PGDI de São Paulo, destacam-se aqueles que tratam da finalidade e da necessidade, por serem pilares para a adequação da administração pública estadual, visto que fundamentam a coleta e o tratamento dos dados pessoais para a prática das políticas públicas embasadas em leis, decretos e demais regulamentações.

> **VI – finalidade:** garantia de tratamento da informação para propósitos legítimos, específicos, explícitos e informados ao titular; [...]
>
> **VIII – necessidade:** limitação do tratamento ao mínimo necessário para o alcance da respectiva finalidade, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento (SÃO PAULO, 2021a).

Figura 2 – Temas da política de governança de dados e informações.

Fonte: São Paulo (2022).

São diretrizes que se complementam, na medida em que os dados a serem coletados deverão sempre observar a limitação do tratamento ao mínimo necessário para o alcance da respectiva finalidade.

Esse entendimento é essencial, pois implica importante mudança de cultura da administração e da sociedade. O costume é o de solicitação de dados pessoais em excesso. Basta observar, por exemplo, o hábito de requerer comprovante de residência em qualquer cadastro, muitas vezes sem reflexão sobre sua real necessidade. Aqui, destaca-se o papel fundamental da capacitação para o conjunto dos colaboradores, de forma a promover a conscientização sobre os direitos dos titulares de dados pessoais protegidos pela LGPD.

Em artigo publicado pelo jornal espanhol El País, Miguel Criado (2015) reportou estudo de um grupo de pesquisadores do Media Lab, do Instituto Tecnológico de Massachusetts (MIT). Nesse trabalho, demonstrou-se que quatro compras com o cartão bastam para identificar praticamente qualquer pessoa.

Os padrões de uso dos cartões possibilitaram descobrir a identidade de 90% dos consumidores de uma amostra de 1,1 milhão de pessoas anônimas, graças aos metadados e aos modelos de *big data*. A amostra veio de um grande banco de país integrante da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). O algoritmo matemático possibilitou identificar uma pessoa por meio, apenas, de seus hábitos de compra.

O estudo retrata a importância dos princípios mencionados, do entendimento e da aplicação dos aspectos relativos à governança e à segurança de dados e informações que se encontrem sob a responsabilidade do Estado.

5.2 POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (PPDP)

O conjunto temático da PPDP pode ser assim sintetizado:

Figura 3 – Temas da Política de Proteção de Dados Pessoais.

Fonte: São Paulo (2022).

Dentre os temas da PPDP, em finalidades e bases legais, destaca-se a política de privacidade e tratamento de dados pessoais para fins de atendimento ao artigo 23 da LGPD e ao seu inciso I, que determinam ao poder público efetuar o tratamento de dados pessoais para o exercício de sua atividade e a execução de suas competências e atribuições legais, desde que sejam fornecidas informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas.

Deve estar claro para o titular de dados, no mínimo:

- como e por quê são tratados os dados pessoais;
- quais os mecanismos para a segurança de dados pessoais;
- quais os mecanismos para o armazenamento de dados pessoais;
- compartilhamento de dados pessoais, se houver;
- quais os direitos dos titulares de dados pessoais;
- como são usados os *cookies*;
- quais os canais de atendimento e o contato do encarregado de dados pessoais;

• quais os principais conceitos e agentes.

Coerentemente, o mesmo dispositivo da LGPD obriga a divulgação da política de privacidade, razão pela qual ela deve estar disponível no site de cada órgão e entidade integrante da administração pública estadual, para que o titular dos dados pessoais tenha fácil acesso ao tratamento de dados específico ali realizado.

6 CONSIDERAÇÕES FINAIS

Desde o início de sua vigência, a LGPD passou a regular todas as atividades de tratamento de dados pessoais no território nacional, tanto pela iniciativa privada quanto pelo setor público.

Dessa maneira, a adequação à LGPD na administração pública, em todas as suas esferas, é necessária para a conformidade com os dispositivos legais. Essa adequação, como analisa Pinheiro (2021, p. 29), não é livre de desafios:

> [...] a implementação da conformidade à LGPD trará um impacto grande nas instituições, podendo contribuir para o aumento do "custo Brasil", especialmente nos setores de *Startups*, pequenas empresas e no setor público, com especial atenção aos que tratam muitos dados pessoais sensíveis, como os de saúde.
>
> Mas é importante ter em mente que não basta ter a lei de proteção de dados pessoais, é preciso educar, capacitar. Por isso a importância do papel orientativo da Autoridade (ANPD) [...] para encontrar medidas viáveis de implementação da nova regulamentação, que gerem menor impacto possível nos setores produtivos e que sejam adaptados e aderentes aos usos e costumes.

As ações de capacitação direcionadas aos agentes públicos, de forma geral, ganham relevância e são fundamentais para o pleno entendimento da importância dos aspectos que envolvem o tratamento de dados e informações para o exercício das respectivas competências legais.

O relatório *The OECD Digital Government Policy Framework* (em tradução livre, A abordagem da Organização para a Cooperação e Desenvolvimento Econômico – OCDE para a Política de Governo Digital), de 2020, traz a reflexão de que os governos desenham serviços públicos como uma resposta às necessidades das pessoas.

Assim, a atualização dos processos e operações beneficia-se de uma visão voltada a conectar as diferentes partes da administração, de modo a aprimorar não apenas a eficiência, mas também a efetividade e a experiência do cidadão usuário do serviço público.

O governo digital, na visão da OCDE, faz uso das tecnologias da informação e comunicação (TICs) para aderir aos princípios que regem uma boa gestão e alcançar as metas das políticas públicas.

Para se chegar ao governo digital desenvolvido, no entanto, é necessário amadurecer significativamente os conceitos e as práticas da governança de dados e informações (que inclui a segurança da informação), bem como da proteção de dados pessoais (que abrange a privacidade).

Nesse sentido, a estratégia maior de aprofundamento da transformação digital em curso em São Paulo beneficia-se do caminho de adequação à LGPD. E a recíproca é verdadeira, considerando-se a mencionada ligação intrínseca entre os temas.

Dessa forma, foram elencados aqui os principais aspectos na jornada para a adequação do Estado de São Paulo à LGPD. Trata-se, efetivamente, de um rol de recomendações e sugestões que se pretendem úteis para os gestores públicos em seus caminhos para adequação à norma maior.

Cabe, por fim, considerar que os paradigmas para a observância da rede de proteção disponibilizada pela LGPD aos titulares de dados pessoais serão cada vez mais cruciais para o compartilhamento de dados entre os entes federados, em especial no que diz respeito às políticas públicas que possam ser efetivadas de forma conjunta, e que se destinam a oferecer melhorias e maior praticidade aos beneficiários e usuários finais.

REFERÊNCIAS

BRASIL. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: Autoridade Nacional de Proteção de Dados, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 15 jan. 2022.

BRASIL. Guia Orientativo. **Tratamento de Dados Pessoais pelo Poder Público**. Brasília: Autoridade Nacional de Proteção de Dados, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 15 jan. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 fev. 2022.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei n.º 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras

providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 10 fev. 2022.

CRIADO, Miguel Ángel. Quatro compras com o cartão bastam para identificar qualquer pessoa. Artigo. **El País**, 30 jan. 2015. Disponível em: https://brasil.elpais.com/brasil/2015/01/29/ciencia/1422520042_066660.html. Acesso em: 10 fev. 2022.

DAMA International. **DAMA-DMBOK:** Data Management Body of Knowledge. 2. ed. [*s.l.*]: Technics Publications, 2017.

OECD. **The OECD Digital Government Policy Framework: Six dimensions of a Digital Government**. OECD Public Governance Policy Papers No. 02, 2020. Disponível em: https://www.oecd-ilibrary.org/docserver/f64fed2a-en.pdf?expires=1645465718&id=id&accname=guest&checksum=04FE92047FC3DB26712FEDF87BAFF478. Acesso em: 10 fev. 2022.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva Educação, 2021.

SÃO PAULO. **Deliberação Normativa CGGDIESP-1, de 31 de dezembro de 2021**. Institui a Política de Governança de Dados e Informações (PGDI). Disponível em: http://www.imprensaoficial.com.br/DO/BuscaDO2001Documento_11_4.aspx?link=%2f2021%2fexecutivo+secao+i%2fdezembro%2f31%2fpag_0014_83278eb63c244f5f461896b59cd13d92.pdf&pagina=14&data=31/12/2021&caderno=Executivo%20I&paginaordenacao=100014. Acesso em: 30 maio 2022.

SÃO PAULO. **Deliberação Normativa CGGDIESP-2, de 31 de dezembro de 2021b**. Institui a Política de Proteção de Dados Pessoais (PPDP). Disponível em: http://www.imprensaoficial.com.br/DO/BuscaDO2001Documento_11_4.aspx?link=%2f2021%2fexecutivo+secao+i%2fdezembro%2f31%2fpag_0018_84eab5fb412392376e50ec5d1e7faa48.pdf&pagina=18&data=31/12/2021&caderno=Executivo%20I&paginaordenacao=100018. Acesso em: 30 maio 2022.

SÃO PAULO. **Política de Governança de Dados e Informações e Ações em desenvolvimento a respeito da LGPD**. São Paulo: Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação, 2022. Disponível em: https://portal.fazenda.sp.gov.br/servicos/aps/Documents/Apresenta%C3%A7%C3%A3o%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados_LGPD.pdf. Acesso em: 30 maio 2022.

5
O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO ORDENAMENTO E A TRANSPARÊNCIA ADMINISTRATIVA: HÁ CONVIVÊNCIA HARMÔNICA?

Andressa Carvalho da Silva

1 INTRODUÇÃO

Alçado formal e recentemente à categoria de direitos fundamentais na Constituição Federal (CF/88) pela Emenda n. 115/2022,[16] a proteção de dados parece ser, à primeira vista, incompatível com a divulgação de dados que garante a publicidade e a transparência dos atos e contratos administrativos. Seria possível a publicação relativa à qualificação pessoal dos envolvidos, de modo a garantir o acesso à informação? Sendo a Lei Geral de Proteção de Dados (LGPD) aplicável à administração pública, como ficaria a publicidade dos atos, (re)conhecida pela doutrina e pela jurisprudência como condicional à eficácia dos atos administrativos? É dizer: como proteger o dado da pessoa humana inserido em um ato administrativo ou mesmo em um contrato administrativo?

O advogado Ronaldo Lemos (2022) afirmou, em artigo intitulado "Lei de proteção de dados está sendo usada contra transparência" quem "Atualmente, a LGPD tornou-se a ferramenta preferida dos gestores que querem ocultar suas atividades, promover retrocessos e suprimir o acesso a dados que são públicos, necessários para a realização de políticas públicas, ou de fundamento constitucional". A fala se relaciona aos questionamentos expostos, cujas respostas parecem estar encontrando seus alicerces paulatinamente.

Sem qualquer pretensão de esgotar o tema, este capítulo buscará tratar da aplicação da LGPD no setor público em relação à publicidade e

16 "Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX: 'Art. 5º [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.'" Estabeleceu também, a emenda, a competência da União para organizar e fiscalizar a proteção de tratamentos pessoais, *nos termos da lei* e competência privativa da União para legislar sobre a matéria.

à transparência. Assim, serão apresentadas breves considerações sobre os fundamentos normativos que levam à inafastável proteção dos dados, sobre a relação entre a LGPD e a Lei de Acesso à Informação (LAI) e, finalmente, sobre publicação de dados de qualificação – como condição de eficácia dos atos administrativos – e sua confluência com a proteção de dados pessoais.

2 O TRATAMENTO DE DADOS PESSOAIS NO BRASIL – O "TRAJETO" PARA A LGPD

Inicialmente, mister se faz repisar que a LGPD não trata somente de dados em suporte informatizado. Seu objetivo é proteger dados em qualquer tipo de suporte (uma folha de papel, um bloco de notas, formulários – digitais ou não –, dentre outros). No entanto, a associação digital a tal proteção é decorrente do grande armazenamento que os meios de informática possibilitaram: hoje, um maldoco de dados consegue cooptar e "manusear" dados de modo que seria humanamente impossível. Há a mudança do suporte – a qual foi a principal motivação da lei.

Ao levar-se o viés especificamente para a administração pública, vê-se que A LPGD estabelece, em seu artigo 7.º, hipóteses nas quais o uso de dados será permitido, dentre as quais se encontram o consentimento do titular e a obrigação legal ou regulatória pelo controlador. Há também a previsão de inciso específico para a administração pública,[17] no qual se estabelece explicitamente a finalidade a ser por esta observada. Outrossim, a LGPD reservou capítulo específico para o tratamento feito pela administração pública – capítulo IV, no qual estão inseridas duas seções: sobre as regras e sobre as responsabilidade (BRASIL, 2018).

Sabe-se que A LGPD foi editada visando a atender as emergentes demandas de proteção de dados pessoais em face das novas tecnologias. No entanto, a preocupação com proteção de dados e privacidade não se originou com a LGPD: vários dispositivos constitucionais e infraconstitucionais já regulavam essa proteção. Por tal motivo, os ditames normativos agora postos devem ser analisados sob a ótica daquilo que já prescrevia o sistema legal pátrio, *sistematicamente*. Como dizem Oliveira e Lopes (2019), é preciso ter em mente que o sistema de proteção de dados esteve sempre em formação, de modo que as questões submetidas ao judiciário não podem ser vistas somente do ponto de vista do novo regramento, como se esse fosse uma "panaceia para todos os males virtuais": é preciso considerar todos os dispositivos que tratam a questão. Ou seja, defende-se que haja um "microssistema"

17 "Artigo 7º [...] I – mediante o fornecimento de **consentimento pelo titular**; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei" (BRASIL, 2018, grifos nossos).

de proteção de dados, gerado a partir da leitura em conjunto das normas relativas ao tema. Algumas delas, inclusive, são referências expressas dentro desse sistema – o artigo 23 da LGPD, por exemplo, que está no capítulo dedicado à administração pública, faz alusão a quem seriam as pessoas públicas ali tratadas: as constantes do artigo 1.º da LAI.[18]

Nesse diapasão, ligada umbilicalmente à proteção de dados, a privacidade é reconhecida como direito universal, tratado inclusive no artigo 12 da Declaração Universal dos Direitos Humanos. Nessa linha dogmática, a CF/88 previu, no artigo 5.º,[19] o rol de direitos fundamentais, nos quais é possível notar preocupação latente do constituinte de alçar à categoria de garantia fundamental diversos aspectos relacionados à intimidade, à vida privada, à proteção da imagem e, agora, explicitamente, dos dados. Além de conferir essa proteção em título específico, propiciou o remédio que assegurasse a observância de tais direitos, a saber, o *habeas data*, que confere ao titular dos dados o direito a ter o pleno conhecimento de seu registro em entidades de caráter público ou governamental, ou a retificá-los, consoante próprio artigo 5.º, inciso LXXII, da CF/88. Como dizem Salvio, Rogenfisch e Ladeira (2019, p. 25):

> [...] o legislador constituinte não apenas garantiu os direitos fundamentais como propiciou instrumentos e ferramentas a serem invocados em caso de tentativa ou de supressão de tais direitos como, por exemplo, o habeas data, para fins de retificação de registro ou para que seja prestada informação acerca dos registros contidos sobre determinada pessoa nos bancos de dados (ênfase nossa). Dessa forma, encontram-se resguardados os direitos da personalidade – tanto por meio de ação preventiva como pela repressão a ato já praticado –, assim como o direito de acesso e à retificação de informação, direitos conferidos ao titular dos dados tanto na GDPR quanto na LGPD.

18 "Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios" (BRASIL, 2011).

19 "IV - **é livre a manifestação do pensamento**, sendo vedado o anonimato; V - é assegurado o direito de resposta, proporcional ao agravo, além **da indenização por dano material, moral ou à imagem**; [...] X - são **invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,** assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII - **é inviolável o sigilo** da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988, grifos nossos).

Sendo o *habeas data* remédio assegurado a qualquer pessoa (física ou jurídica), de procedimento gratuito (art. 5.º, LXXVII), disciplinado pela Lei n. 9.507/1997, seu manejo requer a recusa de informações pela autoridade administrativa. Ou seja, seu vetor é o acesso à informação do titular, a seus dados, a um direito inafastável decorrente de sua de personalidade.

Impende-se breve parênteses para ressaltar que, à parte a conexão dos dados pessoais com a tutela da intimidade e da privacidade, já se reconhecia, antes mesmo da supracitada emenda, a autonomia do *direito fundamental à proteção de dados pessoais*, visto que seu objeto seria distinto, conforme mostra Mendes (2020), analisando decisão proferida pelo STF ao referendar medida cautelar nas ADIs n. 6387, 6388, 6389, 6393, 6390, suspendendo a aplicação da Medida Provisória n. 954/2018 – que libera o compartilhamento de dados pessoais por empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE):

> Destacam-se aqui três aspectos centrais da decisão para compreender o seu significado e efeitos no ordenamento brasileiro: primeiro, a superação da falácia de que existiriam dados pessoais neutros desprovidos de proteção, consolidando o dado pessoal como merecedor de tutela constitucional. Como decorrência, tem-se o reconhecimento de um direito autônomo à proteção de dados pessoais e o seu duplo efeito sobre os deveres do Estado (um dever negativo de não interferir indevidamente no direito fundamental e um dever positivo de adotar medidas positivas para a proteção desse direito).

Outro diploma no qual se observa essa "proteção" é o Código Civil (Lei n.º 10.406/2002) , que igualmente prevê a tutela de referidos direitos de personalidade, dentre os quais está a proteção de dados (BRASIL, 2002). Para Tartuce (2020, p. 210), a LPGD regulou o tema, preocupando-se "com os dados e informações comercializáveis das pessoas naturais, inclusive nos meios digitais" e objetivando "proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade" .

Cite-se, por exemplo, a tutela civil dada ao nome, que, segundo o art. 17 do CC/2002, não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda que não haja intenção difamatória. Essa proteção também é conferida para os casos de uso comercial, sem autorização. Ressalta-se que o nome é também protegido pela Lei de Registros Públicos – Lei n. 6.015/1973. Oliveira e Lopes (2019) apontam que, no Brasil, as primeiras leis de proteção de dados foram de caráter público, sendo a Lei de Arquivos Públicos também expoente dessa vertente – Lei n.º 8.159/1991.

Outra lei que está muito ligada à proteção de dados é o Marco Civil da Internet (MCI) – Lei n.º 12.965/2014 –, que também trouxe menção expressa à proteção à privacidade e à proteção de dados pessoais, *na forma*

da lei, como princípios que disciplinam o uso da internet no Brasil.[20] A lei inclusive traz uma seção para tratar "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas" – arts. 10 a 12. O artigo 7.º do MCI, por sua vez, também elenca diversos direitos, conexos a tais princípios, como, por exemplo, a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação", no inciso I (BRASIL, 2014). Nota-se que tais direitos, mais que dialogarem com a LGPD, dialogam diretamente com a CF/88.[21]

Prescreve também o MCI o sigilo das comunicações armazenadas e, assim como a LGPD, prevê o consentimento para o tratamento de dados pessoais, que vem como uma mão alternativa, uma outra via, ao lado de hipóteses legalmente previstas. Todas as hipóteses de tratamento de dados pessoais, então, ou seriam amparadas pelo consentimento expresso ou por lei. Nessa toada, também o Código de Defesa do Consumidor (CDC) dispôs sobre o direito de acesso por parte do consumidor aos seus dados pessoais que estejam arquivados. Não se faz menção expressa a consentimento, mas os parágrafos do art. 43 prescrevem que a abertura de cadastro, ficha, registro e dados pessoais e de consumo seja comunicada por escrito ao consumidor de forma objetiva, clara, verdadeira e em linguagem de fácil compreensão (BRASIL, 2014).

Ou seja, como dizem Oliveira e Lopes (2019, p. 60), é preciso ter em mente que o sistema de proteção de dados esteve sempre em formação, de modo que as questões submetidas ao Judiciário não podem ser vistas somente do ponto de vista do novo regramento, como se esse fosse uma "panaceia para todos os males virtuais": é preciso considerar todos os dispositivos que tratam a questão.

Avançando, então, em seus contornos, pode-se dizer que o direito fundamental à proteção de dados enseja tanto um direito subjetivo de defesa do indivíduo (dimensão subjetiva), como um dever de proteção estatal (dimensão objetiva). Na dimensão subjetiva, a atribuição de um direito subjetivo ao cidadão acaba por delimitar uma esfera de liberdade individual de não sofrer intervenção indevida do poder estatal ou privado. A dimensão objetiva representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir da qual surgem deveres de proteção do Estado para a garantia desse direito nas relações privadas. Isso significa

20 "Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei" (BRASIL, 2014).

21 Art. 5.º, X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

que os atos do Estado passam a ser controlados tanto por sua ação, como também por sua omissão (MENDES, 2020).

Também nessa perspectiva, Peck (2018, p. 32) afirma que essa nova legislação visa a fortalecer a proteção da privacidade do titular de dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

3 A TRANSPARÊNCIA E O ACESSO À INFORMAÇÃO: INTERSECÇÃO COM A LAI

Observa-se que a LGPD parece ser corolário de um sistema de proteção de um direito fundamental que já estava implicitamente posto – e, após a EC n. 133/2020, expressamente previsto. Assim, as informações sobre as pessoas naturais devem ser resguardadas. A seu turno, a Lei de Acesso à Informação busca a "observância da publicidade como preceito geral e sigilo como exceção" (art. 3, inc. I), considera informação como "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato" (inciso I do art. 4º) e tem o tratamento de informação como "conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação" (inciso V do mesmo artigo) (BRASIL, 2011).

Diante de tal cenário e sendo a informação pessoal "aquela relacionada à pessoa natural identificada ou identificável", forma-se, em uma leitura apressada, uma aparente antinomia entre a LGPD e a LAI, na qual a publicidade é a regra. Claro é que cada uma possui um enfoque diferenciado, explicitado já pela própria nomenclatura: uma prescreve a proteção e a outra, o acesso. No entanto, é preciso ter em mente que a LAI também pode ser considerada uma lei que contribuiu para a proteção dos dados pessoais, pois reforçou o equilíbrio entre "acesso, qualidade de informação, proteção à privacidade e sigilo" e a "diversificação de categorias – secreta, ultrassecreta e reservada –, além do detalhamento dos critérios para a classificação das informações" (PECK, p. 64).

Não se pode olvidar que a referida lei regula o acesso às informações na esfera pública. No entanto, também a ela estão sujeitas pessoas físicas ou entidades privadas que, por vínculo com o poder público, realizam tratamento de dados. Assim, devem adotar providências necessárias para

que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes de sua aplicação[22].

Ademais, prevê a LAI que o tratamento de informações pessoais deve respeitar a "intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (art. 31) (BRASIL, 2011). Adota-se restrição por um período de 100 anos, sendo autorizada a divulgação ou o acesso por meio de *previsão legal* ou *consentimento* das pessoas às quais se referirem.[23] Ou seja, nota-se que há diálogo entre o que previu a LAI e os regramentos da LGPD: necessidade de consentimento ou de previsão legal para o manuseio dos dados.

Também é possível notar, por meio de leitura comparativa, que as exceções à necessidade de consentimento na LAI em muito se aproximam das previsões de tratamento na LGPD. Para melhor elucidar tal diálogo, destaca-se, na tabela abaixo, termos que mostram a conexão entre os preceitos legais em negrito e, em itálico, correlação entre os direitos e garantias pelo preceituado no dispositivo referenciado:

Tabela 1 – Leitura comparativa entre a LAI e LGPD.

LAI	LGPD
Art. 31, § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de **previsão legal ou consentimento** expresso da pessoa a que elas se referirem.	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de **consentimento** pelo titular; II - para o cumprimento de **obrigação le**gal ou regulatória pelo controlador;

22 "Art. 26 [...] Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei" (BRASIL, 2011).

23 "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem" (BRASIL, 2011).

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - **à prevenção e diagnóstico médico**, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VIII - **para a tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: III - ao cumprimento de ordem judicial;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VI - para o **exercício regular de direitos em processo judicia**l, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: IV - à defesa de direitos humanos;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: V - à proteção do interesse público e geral preponderante.	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Fonte: elaboração própria.

A comparação acima permite observar que, de fato, a previsão quanto à proteção de dados já era existente no Brasil, a qual seria resguardada por meio da devida tutela judicial.[24] No entanto, a LAI mostra-se, segundo

24 Interessante pontuar que, segundo estudo realizado pela ONG Artigo 19, 77% das ações discutindo acesso à informação são a favor da publicidade (TEIXEIRA, 2017).

Matos e Ruzik (2019), insuficiente para a delimitação de quais dados pessoais precisariam de consentimento para tratamento. Essa lacuna teria sido suprida pela LGPD, que dita que dados pessoais seriam aqueles que permitem a identificação relacionada à pessoa natural identificada ou identificável – não é necessário a definitiva identificação da pessoa, portanto. Mas ambas as leis empregam "o conceito indeterminado de interesse público a justificar o acesso de terceiros a dados pessoais – inclusive, em certas hipóteses, de dados sensíveis" (MATOS; RUZIK, 2019, p. 209). Para os autores, o conceito de interesse público seria, a rigor, a proteção de direitos fundamentais:

> Por interesse público em matéria de dados pessoais, portanto, deve-se compreender aquilo que atende ao direito fundamental assegurado no inciso XXXIII do artigo 5º, conjugado com o artigo 37 da Constituição, ou seja, aquilo que é necessário para o controle social da transparência pública" (MATOS; RUZIK, 2019, p. 217).

Mas a LGPD, como já foi dito anteriormente, veio regrar não somente o uso e o tratamento de dados pela administração pública, mas *também* por ela. Desse modo, as alterações ou especificações estabelecidas pelo novo regramento precisam ser observadas. A administração pública, vale lembrar, sempre age *secundum legem*. Necessário, então, verificar também qual seria esse valor ou papel de dados pessoais para a administração pública. Certo é que, diante do novel cenário social, imperiosa a delimitação do que se entende por dados pessoais, quais são os seus usos permitidos, os princípios que regem a matéria, enfim, sua regulamentação. Apesar da existência de leis que abrangiam os temas tratados na LGPD, a lei veio para consolidar um microssistema de tratamento desses dados: quem, como, quando, onde, porque, com que fim podem ser usados. Como diz Vainzof (2019), dados pessoais são hoje verdadeiras *commodities*, dado seu grande valor comercial e estratégico, a depender da quantidade, qualidade e capacidade de tratamento.

4 A PUBLICIDADE COMO EFICÁCIA VERSUS LGPD

Como dantes citado, a LGPD elenca as hipóteses em que o tratamento de dados pessoais poderá ser realizado. Entendemos tratar-se de rol taxativo, elencado em *numerus clausus*, uma vez que o caput prescreve que "somente poderá ser realizado" nas hipóteses que descreve. O inciso II possibilita o necessário tratamento de dados para cumprir obrigação legal ou regulatória do controlador, e o inciso III,[25] por sua vez, disciplina que o tratamento

25 "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e

poderá ser realizado pela administração pública, para o cumprimento de *políticas públicas relacionadas a suas finalidades previstas em leis, contratos ou instrumentos congêneres.*

Ademais, a LGPD possui um capítulo próprio para regramento "Do tratamento de Dados Pessoais pelo Poder Público", o qual contém duas seções, a saber: seção, sobre as regras, e seção II, sobre a responsabilidade. Cabe salientar que a primeira seção não elenca hipóteses em que o tratamento de dados será efetuado pelo poder público, mas sim dita que o tratamento deverá ser realizado para o atendimento "de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", de acordo com o caput do artigo 23 – o qual está intrinsecamente ligado ao inciso II do artigo 7.º, no que se refere à "obrigação legal ou regulatória do controlador". Ou seja, nota-se que o uso de dados pela administração deve estar estritamente ligado à sua finalidade, a qual deverá estar constitucional ou infraconstitucionalmente prevista (BRASIL, 2018).

Imperioso se faz ressaltar que a transparência e a participação social são princípios que cada vez mais devem pautar a gestão pública – Heinen (2020, p. 222) a considera a publicidade "um dever da Administração Pública".

A LGPD traz a previsão de que o Estado pode realizar tratamento de dados, o que implica, necessariamente, o sacrifício ao direito de outrem – tanto que a pessoa natural a quem pertence tais dados não precisa, nessa hipótese legal, consentir. A conduta de tratamento de dados, seguindo a hipótese legal, será legítima. No entanto, pode ocorrer que, por exemplo, tal tratamento não seja informado devidamente,[26] o que acarretará sua ilegitimidade. O mesmo ocorreria se a administração pública se "escapasse" à finalidade específica de suas atribuições legais ou mesmo quando não houvesse a devida observância dos princípios.[27] Nota-se que a conduta, inicialmente, seria legítima, mas fatalmente perderia essa característica.

---

regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei" (BRASIL, 2018).

26 Prescreve o artigo 23, inciso I, para o poder público, que devem ser "informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos" (BRASIL, 2018).

27 "Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei" (BRASIL, 2018).

No entanto, necessário se faz rememorar que a publicidade dos atos é condição de sua eficácia. No RE n. 501010/DF,[28] por exemplo, decidiu-se, conforme trecho da ementa, que "A publicidade é requisito de eficácia dos atos administrativos. A pretendida retroação de ato normativo (Ato da Mesa n. 17/1991), após sua publicação, choca-se contra o art. 5º, inciso XXXVI, da Constituição". Di Pietro (2020, p. 770) afirma que "a publicidade é princípio que decorre do artigo 37 da Constituição e constitui condição para que os atos administrativos produzam efeitos externos". Heinen (2020, p. 222) afirma que:

> [...] a publicidade deve ser compreendida como fio condutor à eficácia do ato administrativo. Caso ausente a publicidade necessária ao ato, este não produzirá efeitos. Há entendimentos, inclusive, no sentido de que a ausência de publicidade poderia conduzir à invalidade do ato administrativo.

É dizer, o fato de o poder público utilizar-se dos dados pessoais de seus jurisdicionados não significa, de plano, a possibilidade de sua divulgação. Antes, sendo a publicidade condição de eficácia dos atos administrativos, o órgão deve restringir-se a veicular somente dados necessários à produção dos efeitos dos atos ou que permitam a identificação do titular de modo a viabilizar-lhe a defesa, a impugnação, ou seja, exercer seus direitos perante a administração pública. Atuando o poder público de acordo com o *múnus* constitucional da publicidade, verificará quais os dados aptos à viabilização da identificação inequívoca e inerentemente necessária às suas finalidades, previamente descritas pelo legislador. Assim, a divulgação de dados deve restringir-se às condições do ato: dar a devida eficácia às decisões.

Ao analisar a possibilidade de conflito de normas, Di Pietro (2020, p. 232, grifos nossos) ainda leciona que:

> Pode ocorrer conflito entre o direito individual ao sigilo, que protege a intimidade, e outro direito individual (como a liberdade de opinião e de imprensa) ou conflito entre o direito à intimidade e um interesse público (como o dever de fiscalização por parte do Estado. Para resolver esse conflito, invoca-se o princípio da proporcionalidade (em sentido amplo), que exige observância das regras da necessidade, adequação e proporcionalidade (em sentido estrito). **Por outras palavras, a medida deve trazer o mínimo de restrição ao titular do direito, devendo preferir os meios menos onerosos (regra da necessidade); deve ser apropriada para a realização do interesse público (regra da adequação); e deve ser proporcional em relação ao fim a atingir (regra da proporcionalidade em sentido estrito).**

28 STF - RE: 501010 DF, Relator: Min. CÁRMEN LÚCIA, Data de Julgamento: 02/08/2010, Data de Publicação: DJe-147 DIVULG 09/08/2010 PUBLIC 10/08/2010.

Mas seria a qualificação necessária à eficácia? O Tribunal de Contas da União, por exemplo, possuía o entendimento de que dados cadastrais não seriam informação pessoal. Aquela corte entendeu, após parecer da consultoria jurídica do órgão, que o uso desses dados não constitui qualquer ofensa à intimidade, honra, vida privada ou imagem de seus jurisdicionados:

> É constante a preocupação de cidadãos quanto à proteção de seus dados e sua segurança pessoal, especialmente no que tange à divulgação do número de registro no CPF (Cadastro de Pessoa Física na Receita Federal), no momento da divulgação dos julgados deste Tribunal, que possuem natureza pública. Entretanto, parecer da Consultoria Jurídica deste TCU (Conjur) indeferiu pedido de retirada do número do CPF do Portal do TCU, opinando no sentido de que a informação quanto ao CPF em deliberação proferida pelo TCU e, portanto, na base de dados disponível na Internet, não constitui informação pessoal nos termos do art. 4ª, IV, da Lei 12.527/2011 (TC 014.610/2014-0). No mesmo sentido, a Conjur consignou que dados cadastrais, em processos de controle externo, de endereço de responsáveis, seja pessoa física ou jurídica, de interessados, de sócios de pessoa jurídica, e de seus respectivos procuradores, para fins de comunicação processual, não deve ser considerado informação pessoal, haja vista que não constitui qualquer ofensa à intimidade, vida privada, honra ou imagem dos jurisdicionados (TC 034.351/2014-0) (GOULART, 2022).

Repise-se que a disponibilização de referido conteúdo data de junho de 2018. Entende-se que, após a LGPD, tal posicionamento não se sustenta, visto que o artigo 5.º, inciso I, de referida lei classifica-os como dados pessoais, sendo "irrelevante, para essa classificação, sua vinculação ou não à honra ou à imagem de seus titulares" (MATOS; RUZIK, 2019, p. 211). No entanto, entende-se que tal tratamento está abrangido pelo art. 7.º, II e III, c/c arts. 23 e 24 da LGPD.

Assim, é preciso que haja a correta delimitação de quais dados pessoais podem ser veiculados. A respeito dos números de CPF e RG, bem como de cadastros profissionais, é preciso ter em mente que:

> [...] [a]inda que sejam dados pessoais, tais números cadastrais são necessários à precisa identificação dos indivíduos que integram a administração, ou com ela contratam, celebram convênios, ou, ainda, se beneficiam individualmente – e voluntariamente – de atos administrativos. Aqueles que contratam com a administração pública, ou a ela se vinculam como agentes públicos, sujeitam-se, voluntariamente, a uma limitação ao espaço de reserva desses dados [...] uma vez que a identificação precisa desses agentes deve integrar a transparência pública (MATOS; RUZIK, 2019, p. 211).

O *Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público*, publicado pela Agência Nacional de Proteção de Dados em janeiro de 2020 (ANPD), assim considerou:

> De forma geral, a análise dessas situações envolve uma ponderação entre direitos: de um lado, o direito à privacidade e o direito à proteção de dados pessoais e, de outro, o direito de todos os indivíduos à informação sobre as atividades do Poder Público. Este último se traduz, por exemplo, na divulgação, com base no interesse público, de informações relativas à execução de políticas públicas e ao exercício de competências legais pelos órgãos e entes públicos que permitam aos cidadãos o exercício do controle social sobre as atividades do Poder Público. **Frequentemente, todavia, para atender ao princípio da publicidade, o Estado é obrigado a divulgar dados pessoais** [...] Em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais (BRASIL, 2022, grifos nossos).

Reza o guia que a finalidade deve estar sempre sendo o eixo condutor, buscando-se sempre a mitigação de riscos. Traz ainda, como possível salvaguarda, "a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa". Para exemplificar, trouxe a decisão do STF quanto à necessidade de divulgação da remuneração dos servidores públicos sem a apresentação completa de números como o CPF e matrícula. No entanto, mister se faz ter em mente que tal exemplo não parece estar ligado à eficácia dos atos – o pagamento é efetuado e eficaz, revelando, antes, a necessária gestão transparente do setor público.

Em seguida, reconhece o guia que há casos em que haverá divulgação de dados pessoais, e recomenda que sejam prevenidos os riscos, de modo a mitigá-los. Traz outro exemplo, no qual se nota a divulgação desses dados pessoais:

> Entidade pública municipal recebe candidaturas de interessados em integrar órgão consultivo na qualidade de representante de organizações da sociedade civil ou de sindicatos de empresas ou de trabalhadores. **Durante o processo seletivo, os currículos dos candidatos são disponibilizados na internet**. **Informações pessoais de candidatos de processos anteriores também permanecem disponíveis na página da entidade**. Um candidato que, há alguns anos, participou do mesmo processo seletivo, solicitou que seu currículo fosse retirado da página eletrônica da entidade. Seguindo orientação da área técnica e da jurídica, a autoridade competente acatou o pedido. Assim, o currículo do titular e os de outras pessoas na mesma situação foram retirados da página da entidade na internet. Além disso, **a entidade municipal passou**

> **a adotar a prática de limitar a divulgação dos currículos apenas durante o período do processo seletivo, mitigando, dessa forma, os riscos decorrentes da exposição pública dos titulares. Para tanto, considerou-se que, embora determinada por lei municipal, a divulgação dos dados pessoais dos candidatos tem por objetivo viabilizar o exercício do controle social, mediante, por exemplo, eventual impugnação de candidatura. Assim, após a conclusão do processo, com a designação dos novos membros do órgão consultivo, a finalidade legal é alcançada**, não mais se justificando a disponibilização dos currículos em transparência ativa (BRASIL, 2022, grifos nossos).

Vislumbra-se, portanto, que, agindo com embasamento legal prévio, com a finalidade corretamente definida, não se afasta, de plano, a divulgação dos dados pessoais nos atos e contratos públicos. A Lei n. 8.666/93, ainda vigente, prevê expressamente, nos artigos 26 e 60, que a publicação é condição de eficácia dos atos. A nova Lei de Licitações, Lei n. 14.133/2021, também traz a divulgação no Portal Nacional de Contratações Públicas (PNCP) como condição indispensável para a eficácia do contrato e de seus aditamentos. Necessário é rememorar que ambas as leis permitem a contratação com pessoa física. Assim, seria incompatível com a LGPD a devida qualificação dos contratados? A não divulgação integral da qualificação do contratado não iria na contramão da publicidade almejada – que visa, também, ao controle social? A resposta parece realmente residir na finalidade. Estando ela prevista, não haveria descompasso na prática, desde que única e precisamente para a eficácia dos atos.

Tal questionamento pode ser feito também em relação ao processo administrativo disciplinar. Em âmbito federal, encontra-se previsto na Lei n. 9.784/1999, que prescreve, na comunicação dos atos, a publicação em edital quando interessados com domicílio indefinido (dentre outras hipóteses) – § 4.º do artigo 26. Ademais, os atos de delegação e revogação também são publicados em meio oficial (art. 14), assim como a ata de trabalhos em decisão coordenada. Entende-se que, delimitadas as finalidades legais, os sujeitos precisarão eventualmente ter dados pessoais expostos, mas somente na esfera do estritamente necessário à sua identificação.

É importante, por fim, salientar que, de acordo com o artigo 16 da LGPD, os dados devem ser eliminados após o término de seu tratamento. No entanto, o mesmo artigo ressalva a possibilidade de manutenção de tais dados para cumprimento de obrigação legal ou regulatória pelo controlador – hipótese essa que pode ser conjugada com o atendimento à finalidade pública que dispensa o consentimento do titular. No entanto, como tais dados permanecem sob tutela do órgão, deverá o poder público observar a diligência em relação à segurança desses dados ininterruptamente, enquanto os mantiver sob seu domínio, de modo a evitar a responsabilidade civil do estado pelo indevido tratamento de dados.

5 CONSIDERAÇÕES FINAIS

É possível deduzir que, para a devida tutela aos dados pessoais (e aos dados pessoais sensíveis), é preciso que seja feita a leitura em conjunto de todo o ordenamento. Como dantes afirmado, a LGPD não é uma panaceia para todos os males, mas vem (se e quando vier) em boa hora na defesa do que tem se convencionado denominar como *direito fundamental de proteção de dados*. Como afirmado no artigo 64, os direitos e princípios expressos na LGPD não "excluem outros previstos no ordenamento jurídico relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte" (BRASIL, 2018).

Sendo a proteção de dados ligada aos direitos de personalidade, a análise da legislação brasileira no tocante ao tema permite concluir pela especialidade da LGPD. Não se trata de uma panaceia para todos os males. Antes, deve ser interpretada em conjunto, no *microssistema de proteção de dados*, o qual abrange leis esparsas, como a LAI, MCI, Lei do Habeas Corpus, Lei dos Registros Públicos, dentre outras. Toda essa leitura e análise, por óbvio, deve estar sempre pautada pelo viés constitucional.

Foi possível notar, a partir dessa visão sistêmica, o dialogo estabelecido inclusive entre a LGPD e LAI. Não há antinomia entre os diplomas. Antes, conjugados, permitem e viabilizam a escorreita proteção daquele que agora é direito fundamental expressamente consignado pelo constituinte reformador. A conjugação da lei com a necessária publicidade e eficácia dos atos e contratos administrativos também foi debatida: como exposto na introdução deste capítulo, o tema ainda gera diversos questionamentos. No entanto, a resposta parece estar na matriz principiológica da LGPD – a finalidade.

Assim, em sua atuação consoante a legalidade ou juridicidade, seguindo estritamente suas atribuições constitucionais e legais, deve o poder público manter a devida gestão dos dados, garantindo a sua segurança, bem como aplicando boas práticas de governança, de modo a sempre mitigar os riscos. Com tais atitudes, garante-se que o cidadão tenha resguardado o seu direito – doravante formalmente fundamental – à proteção de dados.

REFERÊNCIAS

BRASIL. Guia Orientativo. **Tratamento de Dados Pessoais pelo Poder Público**. Brasília: Autoridade Nacional de Proteção de Dados, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 15 jan. 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 18 maio 2020.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 abr. 2020.

BRASIL. **Lei n.º 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 18 abr. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2022.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. Rio de Janeiro: Forense, 2020.

GOULART, Camila Felisberto. Proteção de dados pessoais no setor público e acesso a informação: Duas garantias constitucionais que divergem? **Migalhas**, 14 abr. 2022. Disponível em: https://www.migalhas.com.br/depeso/363954/protecao-de-dados-pessoais-no-setor-publico-e-acesso-a-informacao. Acesso em: 14 jun. 2022.

HEINEN, J. **Curso de Direito Administrativo**. Salvador: Juspodivm, 2020.

LEMOS, Ronaldo. Lei de Proteção de Dados está sendo usada contra transparência. **Folha de São Paulo**, 22 fev. 2022. Disponível em: https://www1-folha-uol-com-br.cdn.ampproject.org/c/s/www1.folha.uol.com.br/amp/colunas/ronaldolemos/2022/02/lei-de-protecao-de-dados-esta-sendo-usada-contra-transparencia.shtml. Acesso em: 1.º mar. 2022.

MATOS, A. C. H.; RUZIK, C. E. P. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. IN: TEPEDINO, G.; FRAZÃO, A. OLIVA, M. D. **Lei Geral de Proteção de Dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 199-218.

MENDES, L. S. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. **Jota**, 10 maio 2020. Disponível em: https://www.jota.info/opiniao-e-analise/

artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 17maio 220.

OLIVEIRA, M. A. B.; LOPES, I, M. P. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, G.; FRAZÃO, A. OLIVA, M. D. **Lei Geral de Proteção de Dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.53-84.

PECK, P. **Proteção de dados pessoais:** comentários à Lei 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

SALVIO, G.G.L.; ROGENFISCH, S.; LADEIRA, R. Privacidade e proteção de dados pessoais: evolução do cenário legislativo no Brasil. *In*: OLIVEIRA, A. C. B. S.; BRANCHER, P. M. R. **Proteção de dados pessoais no Brasil:** uma nova visão a partir da Lei 13.079/2018. Belo Horizonte: Forum, 2019.

TARTUCE, F. **Manual de direito civil:** volume único. 10. ed. Rio de Janeiro: Forense; São Paulo: Método, 2020.

TEIXEIRA, Pedro Eurico de Souza Cruz. **A lei de acesso à informação nos tribunais brasileiros**. São Paulo: Article 19, 2017. Disponível em: https://www.conjur.com.br/dl/relatorio-artigo-19-lei-acesso1.pdf. Acesso em: 12 jul. 2020.

VAIZONF, R. Capítulo I – Disposições Preliminares. *In*: MALDONADO, V. N.; BLUM, R.O**. Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters, 2019, p. 19-178.

6
SEGURANÇA DA INFORMAÇÃO: PROTEÇÃO CONTRA VAZAMENTO DE DADOS

Andrey Guedes Oliveira

1 INTRODUÇÃO

A transformação digital e a interdependência da tecnologia da informação no funcionamento de empresas e governos criaram um cenário complexo e desafiador para o funcionamento dos processos internos, de vendas e produtivos, sem contar com a necessidade de processos de inovação ou mesmo de automação do trabalho.

O emprego de tecnologias conectadas com a internet gerou uma nova realidade nas relações entre empresas e governos, assim como alterou os modelos de serviços e produtos.

No âmbito governamental os serviços ao cidadão levaram à execução do conceito de "governo eletrônico e-Gov" (MESQUITA, 2019). Segundo Dujisin e Vigón (2004, p. 18):

> [...] o uso estratégico e intensivo das tecnologias da informação e comunicação, tanto nas relações do setor público entre si, como nas relações dos órgãos do Estado com os cidadãos, usuários e empresas do setor privado.

Esse novo horizonte alterado pelo advento das tecnologias em *nuvem* ou por *serviços* (CIASULLO; LIM, 2022) gerou novas oportunidades de negócios, automação de serviços, relacionamos com vantagem, desafios e novas oportunidades.

A nova conjuntura interligada por sistemas on-line, com ambientes híbridos que vão desde as redes tradicionais (locais) à interligação com nuvens privadas e públicas, criou um novo contexto, transformando os sistemas que outrora eram centralizados e com poucas variáveis em um modelo complexo, inter-relacionado e heterogêneo. Isto é, uma nova arquitetura tecnológica que, por conseguinte, gera novas oportunidades e ameaças que são traduzidas atualmente por ataques digitais e vazamento de dados.

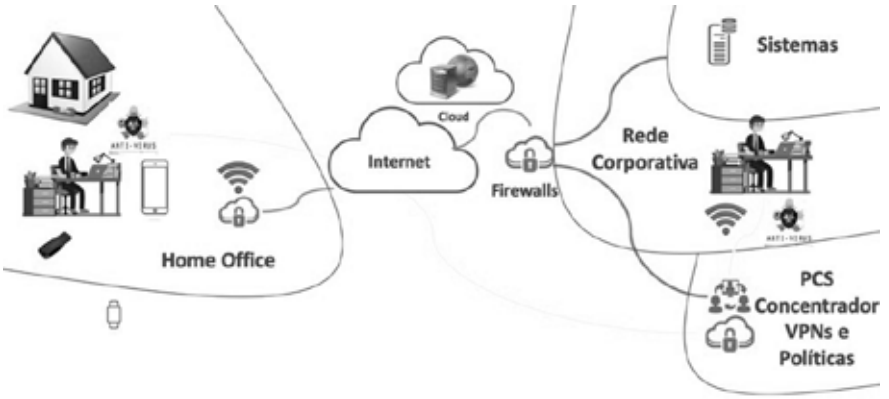
2 SEGURANÇA EM CAMADAS

As redes de computadores, corporativas ou governamentais, eram conectadas à internet por meio de roteadores e com uso de TCP/IP. Elas possuíam características de conexão externa e uma rede interna para serviços básicos, ou seja, duas camadas (externa/interna). A proteção dessas redes era realizada pelos *firewalls*, advindos de sistemas operacionais como Linux e com regras para proteção por ambiente, dando origem à Zona Desmilitarizada DMZ (*Demilitarized Zone*) (KIZZA, 2017, p. 267), à qual pode se ligar uma rede confiável e outra não confiável com endereços válidos ou públicos e privados (RFC1918). Nesse contexto, o *firewall* realizava a segmentação e as regras para acesso externo e interno, assim como a adoção de outras sub redes para os demais serviços.

As DMZ e o papel dos *firewalls* foram sendo transformados ou alterados com a adição de mais funcionalidades, como sistemas de prevenção/detecção de intrusão – IPS/IDS (*intrusion prevention/detection system*) –, antivírus, *webfilters* etc. Se outrora havia pontos de segmentação em uma rede com poucas funcionalidades, atualmente há diversas funções e serviços de interconexões com *clouds* privadas e/ou públicas, com relações de conexões lógicas via VPN (*virtual private network*) (TANENBAUM, 2021).

Esse cenário gerou e levou aos *firewalls* a concentração de serviços diversos de segurança (figura 1): proteção as redes, regras de segurança, verificação de vírus, *sandbox*,[29] VPNs, IPS etc.

Figura 1 – *Firewall* concentrador de serviços de segurança.

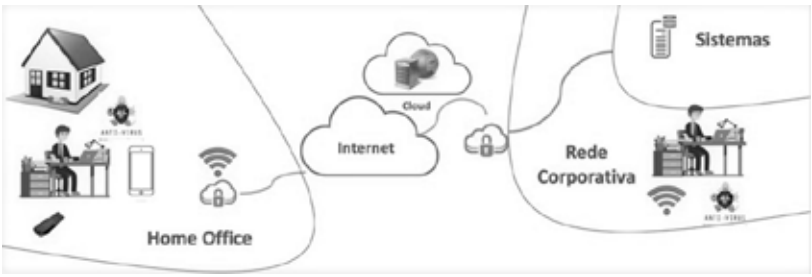


Fonte: elaboração própria.

29 Sandbox é um mecanismo de segurança para separar programas em execução, geralmente em um esforço para atenuar a disseminação de falhas no sistema ou vulnerabilidades de software.

O uso de VPNs para o teletrabalho ou *home office* (figura 2) trouxe uma nova variável para possibliidade de vazamentos de dados, invasões, exploração etc. Isso significa que as conexões remotas de funcionários/colaboradores migraram do presencial para o acesso via internet. Logo, o *firewall* se tornou o "salvador" para o *home office*, pois recebeu a atribuição de concentrar essas redes remotas com a local.

Figura 2 – Uso de VPNs para acesso remoto.



Fonte: elaboração própria.

Outro desafio é a aplicação de políticas de segurança aos usuários, com destaque para a concessão de acesso a sistemas, ou seja, limites para algumas execuções em aplicações ou sistemas, auditoria de uso e privacidade de dados, proteção a dados sensíveis (BRASIL, 2018), gerenciamento do trabalho remoto, uso de equipamentos de terceiros BYO (*bring your own device*)[30] (KIZZA, 2017, p. 6), controle de horas, entre outras funcionalidades.

3 VAZAMENTOS DE DADOS

O vazamento de dados significa, na prática, que dados saíram da organização sem autorização, sendo divulgados na rede pública de computadores e, em consequência, afetando a confidencialidade e acarretando infortúnios e prejuízos.

As informações podem ser classificadas ou etiquetadas de acordo com a sua importância, baseada no provável impacto. Cada organização adota um determinado critério para proteção desses dados (CALDER; MATKINS, 2015).

Os tipos de vazamento podem ser caracterizados como:

- *social intencional*: ação de pessoas interessadas no vazamento;
- *social por acidente ou desleixo*: envio de forma não dolosa ou por descuido;

30 BYO (*bring your own device*): significa que os usuários podem utilizar os seus equipamentos pessoais nas redes corporativas.

• *engenharia social*: indução de indivíduos internos que são levados ao erro por meio de manipulação;

• *furto tecnológico de informações:* extração direta ou indireta por meio de tecnologia que utiliza software para extração e envio aos interessados;

• *espionagem industrial*: tipo de furto de informação para fins específicos que possui, como alvo, indivíduos, empresas e governos, com o intuito de utilização de informações confidenciais para seus próprios interesses;

• *sequestro de dados*: utilização da extração (furto) com a utilização de tecnologia que realiza a criptografia dos dados e promove a extorsão mediante pagamento para liberação do acesso aos mesmos.

3.1 VAZAMENTOS SOCIAIS

Os vazamentos por ações de interação humanas são muito comuns, intencionais ou não. O comportamento eleva o caráter de risco empresarial e governamental, com possibilidade de concretização de uma extração ou despacho de dados a entes que não deveriam ter acesso ao seu conteúdo.

No vazamento intencional, o sujeito ativo movimenta-se por conta própria ou em conluio. Para que haja o fato, os motivos podem ser diversos, e geralmente se caracteriza pelo emprego dos instrumentos tecnológicos internos e privilegiados para que se tenha o envio a um repositório externo.

Algumas ações intencionais podem ser realizadas por ativismo, isto é, alguém que defende algo, podendo ser: doutrina, conceito, filosofia, religião e ideologia, entre outras.

Já o vazamento não intencional *por acidente ou desleixo* caracteriza-se por um ato não doloso, quer dizer, indivíduos realizam uma ação direta como, por exemplo, o envio de um e-mail acidentalmente com uma planilha com dados sigilosos. Outro atributo comum é a falta de conhecimento sobre as ferramentas utilizadas, o impacto gerado por acesso indevido ou mesmo aberto, que venham a ser utilizados ou vazados indevidamente.

3.2 ESPIONAGEM INDUSTRIAL

A espionagem promove a tentativa ou execução do interesse em dados secretos e/ou confidenciais, podendo ter como alvo pessoas físicas, empresas, governos e organizações. Procura-se obter informações que gerem vantagens estratégicas, política, tecnológica etc.

No Brasil temos a legislação que protege segredos industriais, a Lei n. 9.279/1996 (Lei da Propriedade Industrial), que pode ser empregada no caso de comprovação desse tipo de crime.

Alguns exemplos de espionagem são a obtenção de informações de clientes e fornecedores, tecnologias, documentos fiscais e financeiros, especificação de produtos, fórmulas, entre outros.

3.3 SEQUESTRO DE DADOS (*RANSOMWARE*)

O *ransomware* é a expressão que tipifica o conceito de sequestro de dados, em que se realiza a criptografia de dados, por meio de um sequestro digital, com uma chave para a recuperação e disponibilização mediante um pagamento.

Esse tema é importante a todos, pois o método pode ser utilizado para qualquer sistema, corporativo e em ambientes domésticos, sem contar a gravidade que se dá justamente pelo caráter digital que possuímos nos ambientes: pessoal, governamental e empresarial.

A seguir, apresentamos os tipos de *ransomware*, fatores de interesse, "portas de entrada" e modelos de prevenção.

3.3.1 Tipos de ransomware

O *ransomware* é um software malicioso, *malware*, que infecta computadores, servidores e dispositivos computacionais, tendo como premissa a exigência de um pagamento para que as funções originais retornem ao normal. Há diversos tipos, conforme Mohanta, Hahad e Velmurugan (2018), sendo explicados a seguir:

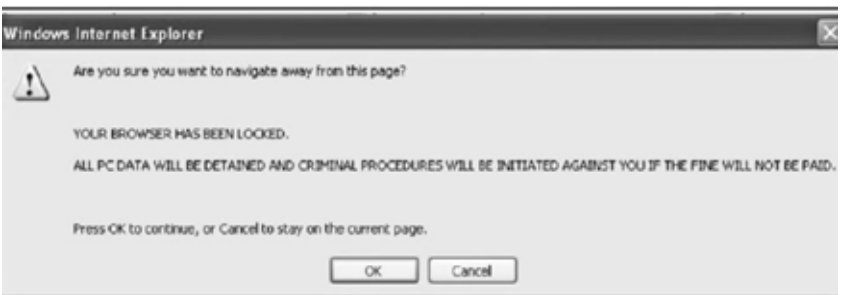
• *Scareware and rogue security software ScreenLocker (scareware e software de segurança desonesto, ScreenLocker)*: o usuário é conduzido a acreditar que existe um problema em seu sistema, induzindo-o a uma ação para que seja instalado o vírus/*malware*. Um exemplo clássico é o antivírus falso (*fake antivirus*) (figura 3);

Figura 3 – Print do antivírus *fake*.

Fonte: Remove... (2011).

• *browser ransomware*: esse tipo de *ransomware* não criptografa, mas congela as funções de navegação;

Figura 4 – Mensagem de bloqueio do navegador MS-Explorer



Fonte: Your browser... (2013).

• *crypto ransomware*: a espécie que criptografa, por meio de chaves complexas assimétricas e simétricas, tendo assim a chave principal em posse do sujeito ativo[31] ou interessado no sequestro do dado;

• *ransomware targeting infrastructure (objetivo na infraestrutura) boot ransomware*: procura explorar, por meio da rede, um ataque lateral,[32] tendo como objetivo os sistemas operacionais vulneráveis, sendo uma porta (*backdoor*)[33] para uma ação remota para criptografia dos dados em sistemas que estão abrigados.

3.3.1.1 As relações com a Darkweb

A relação com a *darkweb* está na preparação de um ataque direcionado ou encomendado; a vítima, então, é escolhida, por meio das relações de grupos que disponibilizam códigos ou mesmo "prestam serviços" para novas variantes de *malware* ou chaves de criptografias.

Outro aspecto é a armazenagem das chaves em servidores "escondidos", ou mesmo o vazamento com comando e controle de dados – esses sendo compartilhados ou vendidos.

A *darkweb* possui um caráter de preparação, vazamento e armazenamento de dados e, após o ataque, é o salvo conduto para o sequestro de dados e até para a tentativa de recebimento do resgate.

---

31 A expressão sujeito ativo refere-se ao conceito jurídico-criminal, segundo o qual o sujeito ativo do crime é aquele que pratica a conduta proibida descrita na lei.

32 O ataque lateral é conceituado como a difusão do *malware* pela rede, testando os sistemas mais vulneráveis e se espalhando.

33 O conceito de *backdoor* é voltado à possibilidade de acesso remoto de um agente não autorizado a rede ou sistemas.

3.3.1.2 As relações com a Lei Geral de Proteção de Dados (LGPD)

Os vazamentos estão associados ao período no qual a empresa percebe o vazamento, de maneira ativa, muitas vezes como vítima, ou sequer nota que já foi invadida e que os seus dados estão na *darkweb*.

Os *ransomware* possuem características de comando e controle[34] prévio, isto é, os dados podem ser vazados mesmo antes do comando de criptográfica. Em linhas gerais, a vítima poderá ter tido dados enviados meses atrás e ser induzida a indicar que esse vazamento ocorreu apenas no ato do ataque.

Caso as empresas não monitorem a *darkweb* por meio ações de segurança preventiva, não saberão quando houve as ações de tentativa ou concretas.

Por fim, mesmo que haja todas as ações de compliance e instrumentos internos, isso não pode garantir que esteja não ocorrendo vazamento (incluso via engenharia social). Em outras palavras, sem o monitoramento externo, as empresas terão apenas parte da visão de risco.

3.3.2 Modelos de proteção: conscientização

O processo de conscientização dos usuários é um tema fundamental para que se mitigue risco de ataques classificados como "sociais", já descritos neste texto. Em outras palavras, quanto mais os indivíduos entenderem as ameaças e os riscos, menor será a possibilidade de fraudes, invasões, coleta de informações, *phishing*, engenharia social e espionagem industrial.

O ciclo modelo, destacado na figura 5, ilustra um processo de treinamentos, palestras e conscientização que dá suporte para avaliação continuada, e testes de conhecimento ou temas que são expostos a maior risco no comportamento dos usuários.

A figura 5 explora cada etapa do ciclo.

3.3.2.1 Plano de Conscientização da Segurança da Informação e Privacidade de Dados

O plano de conscientização passa pelas etapas de trilhas que funcionam como um guia de treinamento e divulgação.

Conforme destacado na figura 6, o primeiro passo, ou mesmo sendo uma premissa para o início do plano, é a avaliação das políticas de segurança e privacidade de dados (LGPD) à qual todos os usuários deverão ter acesso, estando conscientes de seus deveres e direitos.

As políticas geram uma formalidade necessária, diminuindo o risco de comportamentos. Não obstante, em caso de má-fé, serve para que

34 **Comando e controle** significa que um invasor possui capacidade para controlar ou realizar ações remotamente no sistema comprometido.

os postulantes saibam das consequências de seus atos. Sem contar o entendimento de ferramentas de monitoramento de segurança da informação, como SIEM[35] e DLP,[36] que possam proporcionar a detecção ativa de um vazamento de dados. A conformidade às leis e aos regulamentos internos é algo fundamental, devendo ser demonstrados e ratificados por todos os usuários.

Figura 5 – Programa de conscientização aos usuários.

Fonte: elaboração própria.

Os treinamentos e palestras proporcionam a visão básica dos conceitos e, de acordo com a trilha, as informações relevantes para proteção dos usuários.

A continuidade de serviços é parte do modelo e possui o intuito de preparar as equipes em caso de indisponibilidade, assim como aplicar os planos de continuidade de negócios.

3.3.2.2 Treinamentos e palestras

Os treinamentos e palestras devem ter elo com as políticas, de modo que o emprego de conceitos de tecnologia e segurança da informação seja seguida.

Os conceitos aplicados ou avançados devem proporcionar maior utilização das ferramentas internas de empresas ou entidades.

---

35 A sicla a *security information and event management*, que é responsável por aglutinar e correlacionar registros dos sistemas para ataques, riscos, atividades e auditorias.

36 *Data loss prevention* é caracterizado por um software ou um conjunto de softwares que evitam o vazamento ou mesmo monitoram a perda de dados, fruto der violações e transmissões de extração de dados sem autorização.

Não obstante, a utilização de sistemas de gerenciamento educacional – *learning management system* (LMS) ou sistemas de gerenciamento do conhecimento – geram um grau de maturidade para que os gestores acompanhem o desenvolvimento e possam, inclusive, criar modelos de pontuação para participação em testes de conhecimento.

Figura 6 – Plano de conscientização da segurança.

Fonte: elaboração própria.

As práticas de proteção podem ter um caráter didático e com relação de causa e efeito, em especial com foco no comportamento inadequado ou não intencional.

3.3.2.3 Informativos continuados

Os informativos continuados são instrumentos de divulgação rápida, como "pílulas" do conhecimento, boletins, vídeos, informativos, entre outros, que venham corroborar temas importantes sobre segurança e privacidade de dados.

3.3.2.4 Simulações ativas e passivas – ferramentas

As simulações ativas são ações tecnológicas que testam o entendimento e o grau de comportamento dos indivíduos, como campanhas de *phishing* ou instrumentos utilizados pelos fraudadores para implicação de dados ou mesmo instalação de software maliciosos.

As simulações passivas são *feedbacks* de testes ou ferramentas que monitoram o comportamento de pessoas para que se tenha o mapeamento dos grupos ou indivíduos que necessitam de atenção e novos ciclos de conscientização.

3.3.2.5 Resultados e melhoria continuada

Os resultados obtidos pelas simulações acarretam uma melhoria continuada no programa preventivo e dos treinamentos empregados no plano.

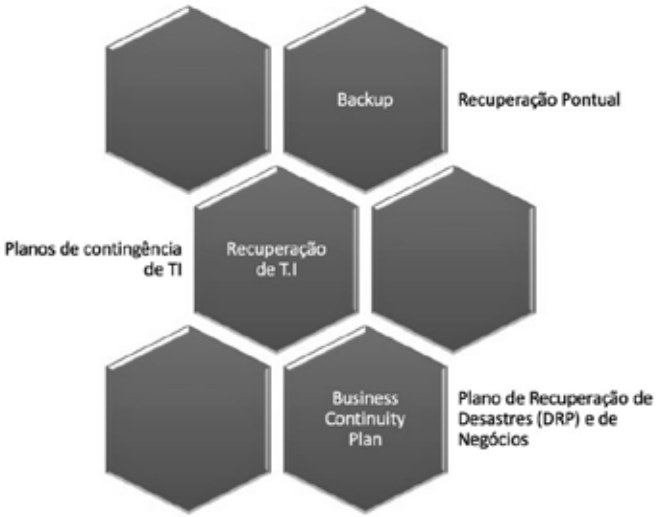
3.3.3 Plano de recuperação

Ameaças como *ransomware* crescem devido ao modelo industrializado do *ransomware as a services* (RaaS), isto é, novos *malwares* ou *zero day*[37] que estão se espalhando exponencialmente, tendo assim grande possibilidade de sucesso em ataques cibernéticos.

O impacto do comportamento do *ransomware* se traduz no *comando e controle*, com o qual o atacante instala um *zero day* e compromete os sistemas operativos, assim como também os sistemas de recuperação.

O Plano de Continuidade de Negócios (*Business Continuity Plan*), figura 7, gera mais um elemento de proteção, levando em consideração o *backup* tradicional, plano de recuperação e de continuidade de negócios.

Figura 7 – Tipos de recuperação.



Fonte: elaboração própria.

37 A expressão *zero day* (ameaça de dia zero) representa uma nova vulnerabilidade desconhecida pelos fabricantes de software, equipamentos, antivírus etc.

3.3.4 Plano de Contingência de TI

O Plano de Contingência de Tecnologia da Informação é um recurso com os seguintes elementos:

• *arquitetura*: infraestrutura, banco de dados, sistemas que proporcionem capacidade de contingência e retorno rápido de um ambiente comprometido;
• cloud *pública e privada:* utilização do ambiente de *cloud computing* como meio de continuidade em caso de um evento grave;
• *alta disponibilidade:* ambientes com redundâncias ou capacidade de retorno rápido, no prisma que vai desde o hardware, software e serviços de *cloud*;
• backup *e restauração*: ambientes que proporcionem cópias de segurança e com possibilidade de restauração rápida para reparação parcial ou total de sistemas;
• *política de contingência de ti*: documento que descreve o plano, com pilares e fundamentos como base a ser seguida pelas equipes técnicas;
• *procedimentos e instruções de trabalho*: documentos que suportam as equipes e realizam os preceitos descritos na política;
• *BIA (business impact analysis)*: documento (análise de impacto nos negócios) que ratifica o impacto ao negócio em caso de ausência de serviços ou da produção; assim dizendo, a inatividade das operações corporativas ou de instituições que levam em conta o plano de execução em caso de indisponibilidade.

3.3.5 Plano de Continuidade do Negócio ou *Business Continuity Plan* (BCP)

O plano consiste em ações técnicas, administrativas e estratégicas para que o negócio não seja impactado por ameaças ou mesmo inviabilize a sua continuidade. Já os planos tradicionais tratavam de ameaças, como desastres naturais ou atreladas a riscos físicos, não obstante elementos como terrorismo e sabotagens.

O plano é uma ferramenta importante e estratégica, não apenas para a contingência, emergência ou desastre, podendo tornar-se um diferencial competitivo, sendo reconhecido por investidores e clientes.

A seguir, apresentam-se partes desse plano:

• *plano de recuperação de desastres (disaster recovery plan –drp)*: ações associadas ao plano de recuperação de tecnologia, somadas às áreas de negócios para que a empresa possa continuar suas operações;
• *classificação de ativos*: identificação de ativos críticos para priorização, tanto para proteção, quanto para recuperação;

• *uso de recursos durante a indisponibilidade*: mitigação das perdas no uso da contingência;

• *processos empresariais*: mapeamento dos processos e que estejam no plano de contingência e recuperação.

3.3.6 Senhas e credenciais

A abundância de sistemas e serviços sempre requer um login (nome do usuário) e uma senha. Se antes tínhamos poucos sistemas, hoje a quantidade de portais/aplicativos gerou uma enorme quantidade de credenciais, criando um problema bem "comum": lembrar de tudo isso!

Outro desconforto é a complexidade, incluindo-se o duplo fator de autenticação,[38] gerando o descontentamento pela dificuldade de uso com caracteres especiais/letra maiúscula e quantidade mínima caracteres. Não obstante, as ações dos usuários para recordação dessas informações se tornaram um novo risco, pois a "lembrança de todas as senhas" cria uma grande barreira, levando-os a utilizar o que há disponível: as chaves "gravadas" em planilhas e/ou documentos no Microsoft Word, ou mesmo a repetição em todos os sistemas – alguns chegam até a anotar em cadernos ou *post-id*.

Um dos maiores fatores de riscos, de fato, são relacionadas às senhas; essa "porta" gera a oportunidade ou mesmo a "certeza" de que o crime cibernético "vale a pena". No fim das contas, o atacante sabe que é "fácil" descobrir ou tentar (via software) saber a senha de outrem, facilitando as invasões aos sistemas, fraudes, roubo de identidades, entre outros crimes digitais.

A utilização de cofres de senha atrelado à conscientização dos riscos se torna um excelente sistema de proteção aos acessos indevidos.

A utilização de *multi factor authentication* (MFA) ou múltiplo fato de autenticação auxilia e protege contra furto de identidades. Em resumo, é proporcionar mais uma camada de checagem sobre o acesso a um sistema, como uma contrassenha por e-mail ou a utilização de sistemas de *token*[39] para validação do acesso.

3.3.7 *Zero trust* – confiança zero

Dado o cenário de *alto risco*, com diversas invasões e sequestros de dados, atrelado ao aumento exponencial de vazamento e falhas em sistemas,

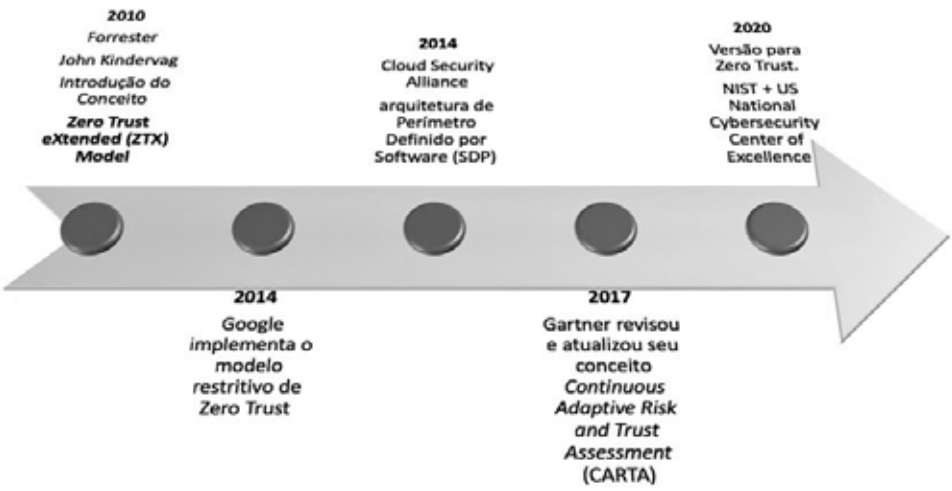
38 Os duplos fatores de autenticação, via de regra, são os mecanismos de confirmação via celular ou e-mail, justamente para "evitar" que alguém utilize o sistema no lugar do usuário.

39 Tokens são softwares que geram códigos dinâmicos e sincronizados para autenticação, comumente usados por aplicativos bancários.

o conceito de *não confiança*, aplicado às camadas de segurança, é hoje um tema altamente discutido no mercado de segurança da informação, sendo, o mais adequado, o modelo **confiança zero** ou z**ero trust**

A ideia nasceu com a publicação do artigo do analista da Forrester[40] John Kindervag, em 2010, que introduziu a expressão *zero trust*" em seu *paper* "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security".[41]

Figura 8 - Histórico da adoção da expressão *zero trust*.



Fonte: elaboração própria.

O próximo passo veio em 2014, dado pela Google, que iniciou a aplicação prática dentro de suas operações/redes, tendo como base a restrição de acesso ou remoção de acessos à rede de produção. Tal ação influenciou fortemente o setor com uma série de artigos documentando sua implementação interna e inovadora.

No mesmo ano, 2014, a Cloud Security Alliance apresentou a arquitetura de perímetro definido por software (SDP – *software defined perimeter*), que fornecia uma especificação concreta para um sistema de segurança compatível com *zero princípios* de confiança.

Já em 2017, empresas de segurança começaram a utilizar o modelo e esse foi ratificado pelo Gartner, que o revisou, incluindo-o no *continuous adaptive*

40 A Forrester é uma empresa norte-americana de pesquisa de mercado que presta assessoria sobre o impacto existente e potencial da tecnologia e segurança da informação.

41 Em tradução livre para português pode ser lido como: "Não há mais centros rígidos: confiança zero um modelo de segurança da informação" (o autor utilizou a expressão borracha e que foi expressa pela palavra "rígido")

risk and trust assessment (Carta) – avaliação de confiança e risco adaptável contínuo –, que possui princípios em comum.

Em 2020, a ênfase de toda a indústria em *zero trust* continuou, com o National Institute of Standards and Technology (NIST), associado ao *U*S National Cybersecurity Center of Excellence dos EUA, que lançaram uma publicação dedicada à *arquitetura zero trust*.

O *zero trust* continua a evoluir à medida que fornecedores e empresas vão adotando e implementando os conceitos, reconhecendo-o como uma mudança fundamental na abordagem da segurança da informação.

4 CONSIDERAÇÕES FINAIS

O processo de proteção e segurança da informação e privacidade de dados pessoais nos leva ao entendimento em camadas, destacado na figura 9, com a adoção do conceito de *zero trust* partindo do dado primário até o ambiente externo denominado *deep* e/ou *darkweb*.

O dado primário está no nível de arquivos e nos sistemas operacionais, tanto para estações de trabalho quanto para servidores em rede. Em seguida temos os sistemas operacionais que são fontes de vazamento e invasões, sem contar o comportamento do usuário. As conexões lógicas propiciam redes de comunicações locais, remotas ou via serviços de *cloud* privadas e públicas, atreladas às aplicações e sistemas, não obstante interconectados e com necessidade de proteção.

Por fim, o ambiente externo que pode ser avaliado pelo interesse de grupos ou pessoas, ou mesmo na ação proativa de monitoramento de marcas, antifraude, de pessoas (redes sociais) e vazamentos pretéritos de dados.

As tecnologias e boas práticas para proteção sugeridas:

- emprego de boas práticas e modelos como destacados nas normas da ISO 27.000;
- conformidade com a LGPD;
- aplicações de políticas de segurança e privacidade de dados;
- programa de conscientização e comportamento seguro;
- aplicação de programas de recuperação de destrates e continuidade de negócios;
- teste de backups
- auditoria interna e externa;
- criptografia de sistemas de arquivos e backup;
- sistemas de restauração de cópias de segurança;
- antivírus;
- *data loss prevention* ou sistema de prevenção de perdas/vazamento de dados;

• microssegmentação com sdp software defined perimeter (perímetro definido por software);

• controle de acesso à rede (*network access control*);

• *identity and access management* (IAM) ou gerenciamento de acesso e identidade;

• Uso de autenticação multifatorial (MFA – *multi factor authentication*);

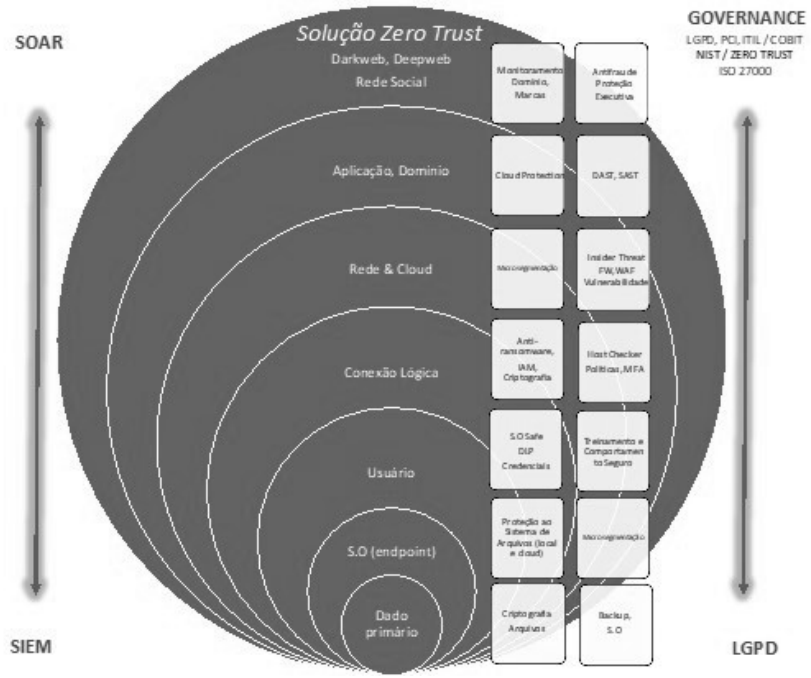
• emprego de *firewalls* com *web application firewall* (WAF);

• WAF uso de *dynamic application security testing* (Dast) – teste de segurança de aplicações dinâmica;

• no desenvolvimento, a execução de *static application security testing* (Sast) – teste de segurança de estático em aplicações e códigos);

• monitoramento antifraude, *deep* e *darkweb*.

Figura 9 – Camadas de proteção.



Fontes: elaboração própria.

Com a utilização da visão em camadas, as entidades governamentais e privadas podem direcionar seus investimentos de acordo com o maior grau de risco e limitações orçamentárias, todavia se recomenda que os temas de comportamento, conformidade com a LGPD e as camadas mais elementares sejam o foco de qualquer organização.

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 jan. 2022.

CALDER, Allan; MATKINS, Steve. **IT Governance: An International Guide to Data Security and ISO 27.001/27.002**. 6. ed. [*s.l.*]: KoganPage, 2015.

CIASULLO, Maria Vincenza; LIM, Weng Marc. Editorial: digital transformation and business model innovation: advances, challenges and opportunities. **Int. J. Quality and Innovation**, v. 6, n. 1, 2022.

DUJISIN, R. A.; VIGÓN, M. A. P. **América Latina Puntogob:** casos y tendencias en gobierno electrónico. Santiago: FLACS, 2004.

KIZZA, Joseph Migga. **Guide to Computer Network Security**. 4. ed. [*s.l.*]: Springer, 2017.

MESQUITA, Camila: A evolução do Governo Eletrônico no Brasil e a contribuição das TIC na redefinição das relações entre governo e sociedade. **Comunicologia**, v. 12, n. 2, p. 159-180, jul./dez. 2019. Disponível em: https://portalrevistas.ucb.br/index.php/RCEUCB/article/view/10900. Acesso em: 4 jan. 2022.

MOHANT, Abhijit; HAHAD, Mounir; VELMURUGAN, Kumaraguru. Preventing Ransomware: Understand, prevent, and remediate ransomware attacks. [*s.l.*]: Packt, 2018.

REMOVE XP Home Security 2012 (Uninstall Guide). **Bleeping Computer**, 5 dez. 2011. Disponível em: https://www.bleepingcomputer.com/virus-removal/remove-xp-home-security-2012. Acesso em: 4 jan. 2022.

TANENBAUM, Andrew. **Redes de Computadores**. 6. edição. [*s.l.*]: Bookman, 2021.

YOUR BROWSER has been locked Ransomware Removal Guide. **Bleeping Computer**, 29 out. 2013. Disponível em: https://www.bleepingcomputer.com/virus-removal/remove-your-browser-has-been-locked-ransomware. Acesso em: 4 jan. 2022.

7
A IMPORTÂNCIA DA GESTÃO DE PROJETOS E GESTÃO DE SERVIÇOS PARA O DPO

Davis Alves
Nilson Brito

Resumo

Esse artigo explora o cenário em que a utilização das boas práticas de gestão de projetos e gestão de serviços para implementar um sistema de gestão de proteção de dados (SGPD) para adequação à LGPD poderá trazer um resultado satisfatório, considerando as fases da gestão de projetos segundo o PMBOK (iniciação, planejamento, controle e execução, encerramento), com as fases do ciclo de vida do serviço (estratégia, desenho, transição, operação e melhoria contínua), relacionando ambas as abordagens com os componentes/fases do SGPD (preparação, organização, implementação, governança e melhoria).

Palavras-chave: LGPD; PMBOK; SGPD; gestão de projetos; governança.

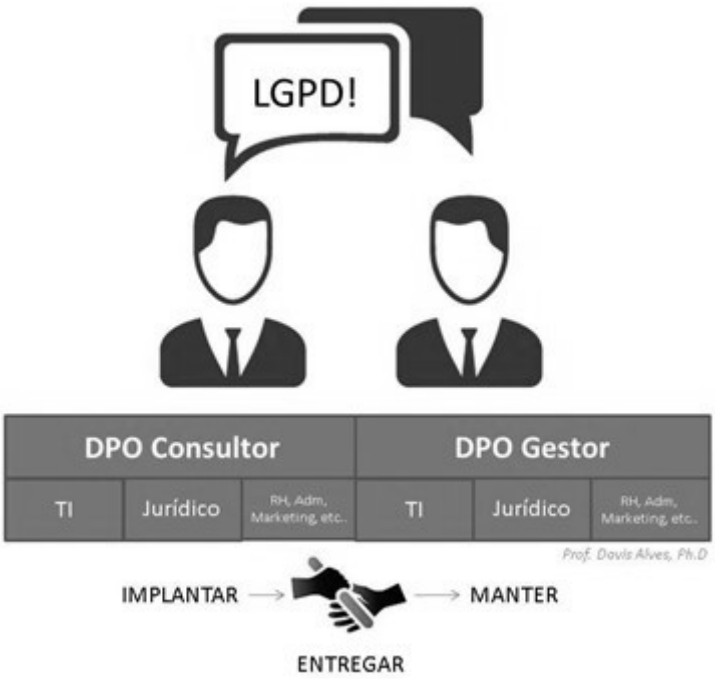
Neste artigo será explorado o cenário em que a utilização das boas práticas de gestão de projeto e gestão de serviços para implementar um sistema de gestão de proteção de dados (SGPD) para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) poderá trazer um resultado satisfatório considerando as fases da gestão de projetos segundo o PMBOK (iniciação, planejamento, controle & execução, e encerramento) e os componentes/fases do SGPD (preparação, organização, implementação, governança e melhoria). A adoção de boas práticas é estimulada por meio do art. 50 da LGPD:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos

> de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

A abordagem parte da visão do *data protection officer* - DPO consultor (gestor de projetos) que irá desenvolver e entregar o projeto de implementação de forma operacional para um DPO gestor (gestor de serviços) conforme apresentado na figura a seguir:

Figura 1 – DPO consultor X DPO gestor.



Fonte: elaboração própria.

Falando de forma bem simples sobre gestão de projetos, deve-se ter em mente a definição de um projeto. Segundo o *PMBOK – Guia de Boas Práticas para Gestão de Projetos* [PMI, 2021), um "projeto" é um esforço temporário para criar um produto, serviço ou resultado. Sendo assim, todo projeto tem início, meio e fim (PMBOK). Quando se refere às boas práticas, fala-se em competências, ferramentas, técnicas e processos aplicados para todas as fases de um projeto (iniciação, planejamento, execução, monitoramento e encerramento).

O SGPD, da sua concepção inicial até seu modelo final, que é operacional, utiliza como padrão o PDCA (*plan*, *do*, *check* e *act*), usado para controle e melhoria contínua de processos e produtos.

O SGPD é um conjunto de boas práticas (*framework*) que tem como objetivo servir como modelo prático para adequação das empresas ao Regulamento Geral de Proteção de Dados europeu (GDPR), mas também aplicável a LGPD para o tratamento dos dados pessoais, desde a coleta até o processamento, armazenamento e descarte. Esse sistema utilizará um ciclo PDCA de cinco componentes/fases desde seu projeto de implementação pelo DPO consultor até o momento em que será entregue operacionalizado como produto final ao DPO gestor.

Veja abaixo os cinco componentes/fases do SGPD visto como ciclo PDCA:

Figura 2 – Fases SGPD.

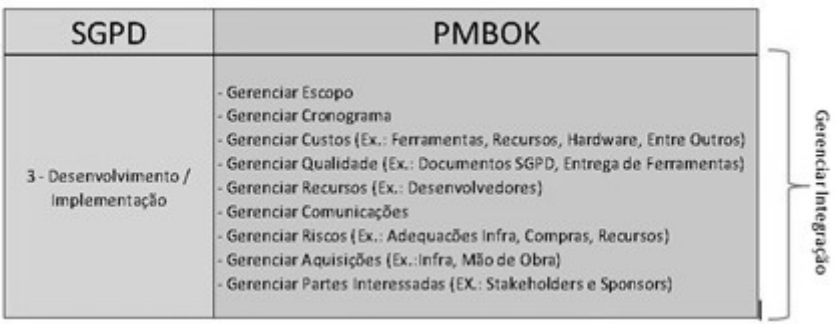
Fonte: Kyriazoglou (2016).

As fases 1, 2 e 3 podem ser conduzidas por um DPO consultor e, após a fase 4, o SGPD pode ser operacionalizado por um DPO gestor. No momento de sua implementação, cada uma das suas fases tem como entrega final documentos (produtos/resultado) com todas as análises, políticas, ferramentas aplicadas, riscos identificados, modelos de como serão reportados os incidentes aos titulares e até mesmo à Autoridade Nacional de Proteção de Dados (ANPD), treinamentos/palestras internas e outros documentos pertinentes à implementação e operação do SGPD na organização.

Cada organização e projeto são únicos. As práticas de gestão de projetos irão auxiliar o DPO consultor em praticamente todas as fases da implementação do SGPD com uma visão apurada de como coletar requisito, definir escopo, desenvolver a equipe, documentar, comunicar, controlar, monitorar, identificar riscos, entre outras práticas. Apesar de auxiliar em

todas as fases da implementação do SGPD, a utilização dessas práticas de forma mais completa será quando o SGPD inicia seu desenvolvimento e implementação, ou seja, na fase 3, que se caracteriza pelo momento em que o próprio nome já diz, o projeto é desenvolvido e implementado. Esse é o momento de "pôr a mão na massa" para efetivar as fases 1 e 2 com tudo que já foi preparado e organizado em documentos para ser realmente implementado e adequado dentro da organização. A figura 3 exibe um quadro que exemplifica uma visão objetiva de como integrar a implementação do SGPD e as práticas de gestão de projetos. De forma bem resumida, pode-se ver como se dá a aplicação prática do PMBOK para estruturar e gerenciar a parte da implementação que estará documentada em um plano de projeto – centrado na execução.

Figura 3 – Exemplo de Integração das práticas de gestão de projetos na implementação do SGPD Fase 3.



Fonte: elaboração própria.

Ao analisar a figura acima, já se tem uma preparação e organização (fases 1 e 2) de proteção de dados e privacidade, e a visão das práticas de gestão de projetos ajudou na coleta de requisitos, definição do escopo, avaliação se haverá custos ou não com recursos e aquisições adicionais, definição de um cronograma de entregas nas documentações, avaliação de riscos iniciais na privacidade dos dados e também comunicação às partes interessadas sobre como está o andamento das fases iniciais (apenas nesses exemplos acima citamos oito das dez áreas de conhecimento do PMBOK que ajudaram nas fases 1 e 2). Agora, ao iniciar a execução, pode-se precisar adequar infraestrutura/software e serão necessários requisitos para cada um dos itens relacionados a eles, e coletar os requisitos precede a definição do escopo do que realmente será necessário e somente o que é necessário para adequação à LGPD, procurar fornecedores e desenvolvedores, gerenciar contratos, contratar mão de obra especializada (recursos), desenvolver a equipe que irá atuar no projeto em conjunto com os funcionários da organização, avaliar riscos relacionados à implantação e desenvolvimento

e ter um plano de respostas que estará dentro do plano de projeto, sendo citada apenas uma parte do conteúdo do plano.

Nesse momento, algumas questões devem ser levantadas: será aceito? Mitigado? Transferido ou eliminado o risco? Quais departamentos precisarão atender primeiro às adequações? Existem possibilidades de fazer ou é preciso comprar? Desenvolver com mão de obra própria ou terceirizar? Qual é o prazo? E se um recurso contratado for compartilhado com outros projetos? Isso é um risco? É preciso ter um plano de contingência? É necessário ter orçamento de contingência? Qual é o custo estimado e em que momento serão aplicados os investimentos? Desenvolver primeiro ou comprar o hardware necessário? Já são conhecidas as visões otimistas e pessimistas do prazo e custo do projeto como um todo? Qual é o caminho de risco do projeto? As entregas de adequação estão com boa qualidade? Existem retrabalhos? Todos os envolvidos estão sabendo sobre como o projeto anda? O projeto está sendo reportado para todas as partes interessadas e de quanto em quanto tempo acontecerá o reporte do andamento? Qual é o perfil do Sponsor? Ele prefere ser reportado de forma detalhada ou resumida?

Imagine-se que a organização tem presença em todo território nacional; nesse caso, será preciso um DPO como PMO central que irá coletar as informações para apresentar os resultados aos executivos na matriz. Como será a presença de um ponto focal? Será necessário um time de DPOs e cada um localizado em regionais espalhadas pelo território nacional? São questões importantes, e tudo isso é parte da implementação do SGPD, e a visão de boas práticas em gestão de projetos irá ajudar o DPO consultor a gerenciar de forma eficaz.

Aqui, é importante lembrar do plano de projeto. Ele terá todas as respostas para as questões colocadas acima, uma vez que tudo estará descrito. Não se deve confundir a aplicação das práticas em gestão de projetos nas fases 1 e 2 com o plano de projeto da fase 3, ele será um documento exclusivo para essa fase.

É possível também a utilização das práticas de gestão de projetos para as fases 4 e 5. Como um exemplo prático, será criado um arquivo de registro para lições aprendidas contendo possíveis descuidos de funcionários, que será colocado em pauta em treinamentos futuros. Isso é governança e melhoria contínua. Práticas em gestão de projetos contribuem para a elaboração de um plano de resposta de violação de privacidade, tendo a contribuição de outros *frameworks* para suportar as operações (gestão de serviços) que serão operacionalizadas pelo DPO gestor.

Após sua implementação pelo DPO consultor, o SGPD se tornará, como um todo, um conjunto de processos e práticas operacionais, entregue ao DPO gestor e à organização. O *framework* do SGPD traz 44 documentos como produtos/resultados/entregas da implementação de um SGPD para

adequação à LGPD. Esses documentos deverão ser periodicamente avaliados e, quando necessário, atualizados, já que o ciclo PDCA é contínuo.

Para visualizar toda a contextualização, a figura 4 a seguir apresenta uma visão bem clara de como o PMBOK + ITIL complementam a implementação do SGPD como um todo:

Figura 4 – Exemplo macro de Integração das práticas de gestão de projetos + ITIL na Implementação do SGPD.

Fonte: elaboração própria.

Portanto, a implementação do SGPD é abrangente e minuciosa, porém é viável e indicado aplicar boas práticas de gestão de projetos e da ITIL, para a gestão de serviços, como facilitadores na implementação e suporte do SGPD, pois o DPO consultor que tem capacitação em gestão de projetos poderá entregar um produto final dentro das adequações necessárias à LGPD, considerando os pilares fundamentais de qualidade, custo e tempo para qualquer organização, independente do seu porte. Entretanto, não se pode esquecer que após a fase 3 do SGPD, é iniciada a operação, que pode ser suportada pela ITIL.

Em suma, é de extrema importância que um DPO tenha também conhecimentos em gestão de projetos e gestão de serviços de TI, mesmo que em nível básico, pois essas duas áreas de conhecimento, aliadas às respectivas

boas práticas (PMBOK e ITIL), contribuem para que o SGPD seja seguido, e consequentemente a empresa esteja adequada a LGPD.

REFERÊNCIAS

KYRIAZOGLOU, John. **Data Protection and Privacy Management System:** Data Protection and Privacy Guide – vol. I. [*s.l.*]: Bookboon, 2016.

PMI Project Management Institute. **PMBOK** – Guia de Boas Práticas para Gestão de Projetos. 7. ed. [*s.l.*]: [*s.n.*], 2021.

8
POLÍTICAS PÚBLICAS MUNICIPAIS DE FOMENTO À PROTEÇÃO DE DADOS PESSOAIS PELO SETOR PRIVADO

Eduardo Tuma
Fernando Antonio Tasso

Resumo

Discute-se, a partir do modelo de atuação para o poder público traçado pela Lei Geral de Proteção de Dados, sobre políticas públicas destinadas a conferir efetividade à proteção de dados pessoais, pelo setor privado, no Brasil. Para tanto, avaliam-se algumas das competências atribuídas à ANPD, sobretudo no campo da instrução social, fomento de boas práticas e governança em matéria de proteção de dados. Defende-se que a atuação do órgão deve servir de norte à atividade regulatória de estados e municípios, a fim de que marco legal de tamanha envergadura seja efetivamente observado. Além disso, sugerem-se possíveis modelos de políticas públicas, especificamente no âmbito municipal, para disseminar a cultura de proteção de dados, valorizando as empresas que atendam aos requisitos da LGPD. O método adotado é o da revisão de literatura narrativa.

Palavras-chave: proteção de dados; poder público; empresa.

1 INTRODUÇÃO

Qualquer mudança legislativa implica consequências para o convívio social. Podemos afirmar que projetos de lei que não contem com ampla participação de diversos setores sociais costumam carrear desafios ainda maiores para a conquista da efetividade social de seus comandos normativos.

A Lei Geral de Proteção de Dados (Lei nº. 13.709/2018 – LGPD) inova, consideravelmente, a forma como a disciplina da privacidade deve ser encarada pelos setores público e privado.

Sem se restringir à proteção de dados em suporte digital, já que igualmente aplicável a situações em que tais elementos se encontrem noutros suportes, inclusive o físico, é certo que a realidade tratada na LGPD está diretamente relacionada com a chamada Era Digital e seus impactos na forma de interseção entre as pessoas e entre estas e as instituições públicas e privadas.

Por mais que grandes agentes do setor privado tenham se adequado para cumprir as novas exigências legais, é sabido que a elaboração de um plano de adequação para proteção de dados pessoais não é prática corriqueira na maior parte dos setores da sociedade brasileira, principalmente quando se trata de empresas de pequeno porte. Trata-se de providência nova e que demanda tempo para ser compreendida e adotada.

Essa realidade impõe ao Estado enorme responsabilidade. Para que a proteção de dados pessoais seja uma realidade, urge a adoção de medidas por todos os agentes de tratamento de dados (controladores e operadores), conforme o art. 5.° da lei, que tratem dados pessoais sensíveis, sendo certo que o Estado, em suas esferas regulatória e fiscalizatória, pode se prestar a fomentar essa consolidação de cultura de proteção de dados no setor privado e, sem prejudicar a cultura de transparência ativa, também o fazer no setor público.

A LGPD está em plena vigência, mas ainda não parece se encontrar dentre as prioridades de determinados setores sociais. Diante dessa situação, é necessário que instituições que integram a administração pública, em todos os níveis federativos, delineiem políticas públicas voltadas ao fomento no cumprimento desse importante marco legal.

Pretende-se apresentar algumas estratégias que possam contribuir com esse objetivo. Cumpre esclarecer que o foco do artigo é a perspectiva pragmática e não dogmática a respeito do conceito eventualmente aplicável a essa ou àquela política pública. O objetivo geral é a reflexão a respeito de como o Estado – compreendidas nessa expressão todas as pessoas políticas – pode atuar para induzir a sociedade ao cumprimento daquilo que se encontra na LGPD.

2 O ESTADO COMO INCENTIVADOR DE BOAS PRÁTICAS NO ÂMBITO DA LGPD

Diante de uma nova realidade normativa, sobretudo quando vinculada à chamada Era Digital, parece-nos que o papel do Estado como incentivador de boas práticas, em busca de majorar a efetividade das normas, é ainda maior. A LGPD não tem aplicação exclusiva a ferramentas de natureza digital, mas decorre do amplo desenvolvimento de tais aplicações e de seu frequente uso para o desempenho das mais corriqueiras atividades sociais, econômicas e políticas com a utilização massiva do tratamento de dados.

Muitos desafios se apresentam contra à efetividade da LGPD. Dentre eles, podemos citar: i) necessidade de maior inclusão digital; ii) publicidade e instrução em relação ao objeto tratado pela lei; iii) apresentação de mínimas diretrizes para elaboração de planos de adequação por parte dos setores público e privado; iv) estabelecimento de cronograma para fiscalização dessa

mesma adequação; v) incentivo estatal para que providências sejam tomadas por agentes públicos e privados, entre outros.

Sabemos que a eficácia social de uma norma jurídica depende da legitimidade que a ela é atribuída por seus destinatários. O trabalho do Estado na divulgação do conteúdo da LGPD e incentivo à adoção de medidas alinhadas à efetividade de seus dispositivos parece indispensável à conquista da referida eficácia social. Nesse sentido, oportuna a lição de Miguel Reale (2002, p. 113, grifo nosso): "O Direito autêntico não é apenas declarado, mas reconhecido, é vivido pela sociedade, como algo que se incorpora e se integra na sua maneira de conduzir-se. A regra de direito deve, por conseguinte, ser *formalmente válida e socialmente eficaz*".

Sem que políticas públicas sejam traçadas, a LGPD não atingirá a almejada efetividade. O debate público a respeito do conteúdo desse importante marco legal é igualmente relevante e inadiável. Nessa esteira, cremos que a Autoridade Nacional de Proteção de Dados (ANPD) apresenta-se como órgão que deve estar no ápice de todo o sistema de proteção de dados pessoais no país. Por mais que se possa discutir a respeito da melhor conformação jurídica para a ANPD – se agência reguladora ou autarquia comum, por exemplo –, é inegável que o legislador lhe entregou competências que apenas reforçam seu papel central em matéria de proteção de dados pessoais.

O art. 55-J da LGPD, em seus vinte e quatro incisos, estabelece as competências da ANPD, destacando-se nesse artigo as que se encontram nos incisos VI a IX. Newton de Lucca e Cíntia Rosa Pereira de Lima (2020, p. 385) explicam o poder regulatório da ANPD e destacam sua importância diante da assimetria de recursos e conhecimento por parte dos destinatários da norma:

Essa função da ANPD deve ser compreendida como um "poder-dever", pois deve ser exercida em prol da defesa dos titulares dos dados pessoais, considerados hipervulneráveis em função da assimetria informacional, jurídica e do poder econômico.

O inciso VI do art. 55-J prevê que cabe à ANPD "promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança" (BRASIL, 2018). A razão para essa previsão alinha-se àquilo que adrede se afirmou. A nova legislação, sobretudo tratando de tema ligado – não exclusivo – à área digital, depende da promoção pública de seu conteúdo, do delineamento e da ampla divulgação de políticas públicas ligadas a esse mesmo objeto. Nesse aspecto, emerge o papel da educação para utilização de ferramentas digitais. Paula Marques Rodrigues e Alessandra Borelli Vieira (2021, p. 15) afirmam:

> Para garantir ampla aplicabilidade do quanto regulado pela Lei, é necessário vencer a resistência quanto ao que é considerado novo (ainda

> que o direito à privacidade não o seja), além de assegurar a compreensão da sociedade sobre os efeitos do direito à proteção dos dados pessoais. Nesse contexto, a educação tem papel imprescindível nessa temática, pois somente com a conscientização e a compreensão do que é privacidade – não somente para o indivíduo, mas também para a coletividade – é que serão possíveis a efetiva proteção da tutela dos dados pessoais e a sua utilização conforme os limites estabelecidos pelo ordenamento jurídico.

O inciso VII do mesmo artigo estabelece que cabe à ANPD "promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade" (BRASIL, 2018). Através desse dispositivo o legislador atribuiu à ANPD o dever de aprofundar-se, por meio de estudos, nas melhores práticas nacionais e internacionais. Tal incumbência reafirma a posição do órgão no ápice do sistema brasileiro de proteção de dados, bem como busca conferir-lhe repertório para o desempenho das demais competências que lhe são destinadas.

Ainda para auxiliar na promoção da proteção de dados pessoais no Brasil, o inciso VII do art. 55-J fixa à ANPD a seguinte competência: "estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis" (BRASIL, 2018). Aqui se encontra atribuição que diretamente servirá de base para que a sociedade civil, por meio de seus mais distintos segmentos, consiga cumprir o desiderato da lei.

Com efeito, a ANPD, inclusive por meio da busca de parâmetros internacionais, deverá fomentar a adoção de padrões de serviços e produtos voltados à facilitação do exercício de direitos por parte dos titulares de dados pessoais. Não devemos nos esquecer que o ambiente digital está repleto de tecnicidade. Assim, impõe-se à ANPD viabilizar a compreensão dos mecanismos de proteção através de linguagem acessível e de acordo com as especificidades e porte dos responsáveis pelo tratamento de dados pessoais.

Nesse contexto, a ANPD criou perfis em algumas das principais redes sociais e passou a oferecer à sociedade canais de acesso a guias orientativos. Um dos exemplos mais recentes é o *Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte*, editado em outubro de 2021. Nele, a ANPD traz apresentação de sua missão institucional, esclarece os principais tópicos ligados à proteção de dados e oferece algumas diretrizes para que agentes de pequeno porte se adequem à lei. A título de consideração final, o material elaborado pela ANPD afirma que:

> [...] que envolvem a política de segurança da informação relacionada a dados pessoais e a segurança em recursos humanos; e medidas técnicas, que tratam, entre outros, do controle de acesso aos dados; segurança nos dados armazenados; manutenção de programa de gerenciamento

> de vulnerabilidades; e segurança das comunicações. Também se deu destaque a medidas relacionadas ao serviço em nuvem (de ordem técnica ou administrativa), tendo em vista a frequência com que esses serviços são utilizados por agentes de tratamento de pequeno porte (VARGAS, 2021, p. 18).

De maneira semelhante à edição do citado guia orientativo, uma das primeiras providências da ANPD foi a publicação do *Como proteger seus dados pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON* (BRASIL, [202-]). Com caráter bem mais geral, apelo visual e linguagem acessível, apresenta-se aos titulares de dados pessoais, isto é, à cidadania como um todo, formas de proteção e boas práticas, sempre com o intuito de se evitar qualquer forma de vulnerabilidade dos direitos garantidos pela LGPD. Dentre diversos conceitos indispensáveis à correta compreensão dos termos legais, encontramos trechos como o seguinte:

> A proteção de dados é importante tanto para o cidadão, como para a economia e para a sociedade como um todo. Ela dá poder ao cidadão para controlar os seus dados e fortalece o exercício da liberdade de expressão, do acesso à informação e dos direitos à intimidade, à honra e à imagem. A lei está atenta também ao desenvolvimento econômico do País, ao incentivar a criação de novas tecnologias em setores estratégicos pelas empresas de pequeno porte, como as microempresas e startups, que possuem regime diferenciado pela lei (BRASIL, [202-], p. 4).

Ademais, no intuito de colocar a ANPD em sintonia com a vanguarda na proteção de dados pessoais, o legislador também lhe atribui competência, através do inciso IX do art. 55-J, para "promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional" (BRASIL, 2018). É conhecida a influência da General Data Protection Regulation (GDPR) europeia nas bases da LGPD brasileira. Sendo assim, é de todo relevante que a máxima autoridade em matéria de proteção de dados no país mantenha relacionamento e firme cooperação com eventuais congêneres ao redor do mundo.

Os incisos citados são apenas alguns daqueles que descortinam papel central à ANPD em matéria de proteção de dados. Sua atuação não há de se dar apenas através do monitoramento das atividades ligadas à proteção de dados pessoais ou por meio da aplicação de sanções àqueles que descumprirem as obrigações previstas na lei, lesando direitos dos titulares. Para além dessa função, cabe à ANPD promover o conhecimento da lei e incentivar a adoção de políticas – públicas e privadas – voltadas à efetividade da LGPD (atuação preventiva). Sendo o órgão máximo da proteção de dados no país, entendemos que cabe à ANPD coordenar, por meio de diretrizes e

orientações concretas, a atuação das demais pessoas políticas na matéria de proteção de dados pessoais.

3 A ATUAÇÃO COORDENADA DA ANPD COM OUTRAS PESSOAS POLÍTICAS (ESTADOS, DISTRITO FEDERAL E MUNICÍPIOS)

Exposta parte das competências atribuídas à ANPD, resta evidente que o órgão foi alçado à condição de principal responsável pelo tema da proteção de dados pessoais no Brasil. Alocada na administração pública federal, a ANPD não poderá deixar de voltar sua atenção à forma como estados e municípios cumprirão a LGPD e fomentarão o respeito à norma pelos agentes privados. Lembremos que o Congresso Nacional aprovou a EC n. 17/2019, a fim de promover a inclusão da proteção de dados pessoais no rol de direitos e garantias fundamentais do art. 5.º da Constituição Federal. Nesse contexto, traçar políticas públicas voltadas à proteção de dados por meio do monitoramento de atividades de agentes de tratamento, através do fomento à adoção de boas práticas, ou de qualquer outra estratégia eficiente, é dever do Estado, sendo a ANPD sua principal face nessa missão.

O art. 55-J, inciso II, da LGPD atribui à ANPD "elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade" (BRASIL, 2018). A nosso sentir, essa incumbência não apenas reforça o papel central do órgão no sistema de proteção de dados do país, como também impõe à ANPD a manutenção de constante diálogo e apoio às pessoas políticas (União, estados, Distrito Federal e municípios) na implementação das diretrizes voltadas às finalidades da legislação.

Em janeiro de 2022, a ANPD editou *Guia orientativo tratamento de dados pessoais pelo poder público* (BRASIL, 2022a). Esse documento reafirma o papel central da ANPD, tantas vezes reafirmado neste artigo. Vejamos:

> 3. Entre outros aspectos relevantes, muitos órgãos e entidades públicos têm questionado a Autoridade Nacional de Proteção de Dados (ANPD) sobre (i) o âmbito de incidência da LGPD e a aplicação de seus conceitos básicos ao setor público; (ii) a adequada interpretação das bases legais que autorizam o tratamento de dados pessoais; (iii) os requisitos e as formalidades a serem observados nas hipóteses de uso compartilhado de dados pessoais; e (iv) a relação entre as normas de proteção de dados pessoais e o acesso à informação pública.
>
> 4. Considerando essas questões, o presente Guia Orientativo busca delinear parâmetros que possam auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD. As orientações apresentadas constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao Poder Público. Por isso, a versão publicada ficará aberta a comentários e contribuições de forma contínua, com o fim de atualizar o Guia oportunamente, à medida que

> novas regulamentações e entendimentos forem estabelecidos, a critério da ANPD. As sugestões podem ser enviadas para a Ouvidoria da ANPD, por meio da Plataforma Fala.BR (https://falabr.cgu.gov.br/) (BRASIL, 2022a, p. 4).

Já na introdução do referido guia, a ANPD expõe alguns de seus desafios e esclarece que muitos órgãos públicos têm apresentado questionamentos a respeito do tratamento de dados pessoais pelo poder público. Ressalte-se que, até este momento, o papel da ANPD tem sido de coordenar a primeira fase para correto cumprimento da lei. A LGPD foi promulgada em 2018 e, mesmo no início de 2022, o órgão responsável pelo tema da proteção de dados no Brasil segue promovendo esclarecimentos aos diversos segmentos sociais acerca do conteúdo e da abrangência da LGPD. Nesse sentido, a ANPD reconhece o papel de coordenar as políticas públicas, num plano mais geral, que versem a respeito da temática que lhe foi confiada.

Talvez por ainda estar diante do primeiro desafio, qual seja, esclarecer aspectos ligados à interpretação e cumprimento da lei pelos setores público e privado, a ANPD ainda não se dedicou à positiva formulação de estratégias para que o poder público fomente o cumprimento da LGPD pelo setor privado. O caminho não será curto ou simples. Ao contrário, a missão da ANPD revela-se árdua. Contudo, há de ir além de esclarecimentos acerca de aspectos conceituais da legislação. A nosso ver, a ANPD terá papel decisivo na abertura do horizonte de estados e municípios, a fim de que possam pensar e delinear políticas públicas, inclusive alinhadas com a ANPD, para que a obediência à LGPD possa ganhar maior adesão e capilaridade na sociedade.

4 POLÍTICAS PÚBLICAS DE INCENTIVO À ADEQUAÇÃO EM MATÉRIA DE PROTEÇÃO DE DADOS

A LGPD conta com capítulo destinado a regular as sanções administrativas para todo aquele que, na condição de controlador ou operador no tratamento de dados pessoais, descumpra alguma das obrigações legais. O art. 52 da LGPD arrola uma série de sanções, muitas das quais bastante significativas.

Destacamos a que tem previsão no inciso II do art. 52: "multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração" (BRASIL, 2018).

Multar qualquer pessoa jurídica no patamar previsto nesse dispositivo legal é algo bastante severo. Nessa esteira, é inegável que a consequência do comportamento violador da norma pode e deve servir de freio às condutas de agentes de tratamento de dados que não estejam alinhadas com a LGPD.

Contudo, para além desse aspecto repressivo, pensamos que é oportuno ao poder público delinear políticas que fomentem a conformidade em matéria de proteção de dados. Assim, cremos que União, Estados, Distrito Federao e municípios devem, com a participação da ANPD, discutir políticas públicas de incentivo a agentes do setor privado que estejam dispostos a se adequar e servir de exemplo a congêneres em matéria de proteção de dados.

Para refletirmos sobre as mencionadas políticas públicas de incentivo, oportuna a lembrança de passagem da obra de Norberto Bobbio (2007). O político e jusfilósofo italiano desenvolveu a noção de "sanção premial" (positiva) na sua obra *Dalla struttura alla funzione: nuovi studi di teoria del diritto*, de 1977, na qual investiga o sentido teleológico do direito, mas sem renegar sua abordagem estrutural presente nas obras anteriores.

A partir de tal conceito, Bobbio (2007) defende a utilização das normas-objetivo e princípios que deixam de ter a estrutura de regras, que pressupõem uma sanção, para designar objetivos de interesse social, de forma que sejam praticadas ações, incentivadas pelo poder público, que beneficiem a sociedade de uma maneira geral. Nesse campo podem entrar as medidas sobre as quais nos propomos a refletir.

Com efeito, é possível ao Estado fomentar comportamentos que produzam benéficos à sociedade como um todo por meio de estímulos ou incentivos. Norberto Bobbio (2007) denomina de sanções positivas ou negativas, que podem atenuar ou agravar, por exemplo, a carga tributária, sempre no intuito de alcançar uma conduta que seja socialmente desejada. Sustenta o autor que há, e não só nos chamados estados do bem-estar social, relação entre economia e o que chama de sanção positiva, no sentido de premial:

> O Estado, à medida que dispõe de recursos econômicos cada vez mais vastos, venha a se encontrar em condição de determinar o comportamento dos indivíduos, não apenas como exercício da coação, mas também com o de vantagens de ordem econômica, isto é, desenvolvendo uma função não apenas dissuasiva, mas também como já foi dito, promocional. Em poucas palavras, essa função é exercida como a promessa de uma vantagem (de natureza econômica) a uma ação desejada, e não como uma ameaça de um mal a uma ação indesejada (BOBBIO, 2007, p. 68).

Determinadas medidas estatais, voltadas para a garantia de benefícios àqueles que praticam condutas anteriormente estabelecidas pelo poder público como desejáveis, são denominadas pelo filósofo italiano de sanção positiva. Percebe-se, portanto, que é possível e até mesmo desejável a utilização da chamada "sanção premial" como instrumento implementador de políticas públicas voltadas para a proteção de dados e privacidade pelo setor privado, como recompensas oferecidas pelo Poder Público àqueles que praticarem condutas condizentes com o previsto na LGPD.

É de todo possível o estabelecimento de consequências positivas à adesão, pelo ente privado, a comportamentos desejados pela coletividade como um todo, consubstanciados no núcleo de uma dada política pública. Assim, viável a retribuição estatal por intermédio de um prêmio, que pode ser denominado de "sanção premial", uma espécie de recompensa pela prática de condutas socialmente desejáveis, que pode ser plasmada no mundo fático por meio de desoneração ou redução de carga tributária, por exemplo, ou via outorga de selos de qualidade, atendidos determinados requisitos.

O intuito deste artigo é desenvolver ideias de políticas públicas que estejam dentre aquelas viáveis ao poder público municipal. Nesse sentido, apresentam-se algumas que nos parecem perfeitamente alinhadas à competência constitucional dos municípios no contexto da República Federativa de 1988. A saber:

a) cadastro ("do bem")[42] de empresas alinhadas às boas práticas estabelecidas na LGPD e por meio de resoluções da ANPD, a partir de critérios objetivos, restando as inscrições ao cadastro abertas a todas as empresas interessadas, legalmente constituídas e com regularidade fiscal;

b) política para aferição e atestado, com base na observância dos planos de adequação das empresas em matéria de proteção de dados, conferindo-se um "selo da empresa amiga da proteção de dados",[43] mediante avaliação mais criteriosa do que a inclusão no "cadastro do bem";

b.1.) diante da obtenção do selo, portanto sob escrutínio mais aprofundado, que neste caso deve ser realizado por estrutura/órgão no âmbito municipal, apresentar possíveis benefícios, tais como os de ordem fiscal, especialmente reduções em taxas municipais ou no imposto sobre serviços (ISS);

c) criação de um canal de apoio às empresas,[44] para implementação e adequação aos critérios trazidos pela LGPD. A ideia é criar um *squad* que tem como objetivo auxiliar as empresas a implementarem todo o processo de

42 Neste ponto, cremos que o delineamento de políticas públicas possa tomar por base a Lei n. 12.414/2011 que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Adaptada para os comportamentos alinhados com boas práticas em matéria de proteção de dados, a municipalidade poderia estabelecer esse cadastro.

43 A Prefeitura da Cidade de São Paulo instituiu alguns selos para entes do setor privado. Um deles se refere ao âmbito da acessibilidade e se encontra disciplinado pelas seguintes espécies normativas: Decreto n. 58.997, de 4 de outubro de 2019, e Portaria n. 28/SMPED-GAB, de 22 de outubro de 2019. Há, também, selo de direitos humanos e diversidade, voltado a boas práticas nessa área (https://www.prefeitura.sp.gov.br/cidade/secretarias/direitos_humanos/selo_direitos_humanos/index.php)

44 Nesse aspecto, o sistema de ouvidorias do município tende a ser o principal canal, desde que com apoio de pastas que se liguem à atividade empresarial e ao monitoramento da proteção de dados no município. Quanto a esse último ponto, cremos que a participação ou orientação do encarregado – segundo conceituação da LGPD – no município seja determinante.

segurança de dados, promovendo guias, workshops, seminários, treinamentos e a disponibilidade de central de dúvidas;

c.1.) nesse canal haveria área específica para as pequenas empresas, já que necessitam de ajuda do poder publico, sendo carentes de informações, muitas vezes na condição de empresário individual ou de empresa familiar que raramente dispõe de verbas para gastos com profissionais adequados e aptos no que tange a adequação em matéria de proteção de dados.

5 O PAPEL DAS EMPRESAS PÚBLICAS DE TECNOLOGIA NA DISSEMINAÇÃO DE BOAS PRÁTICAS

O poder público tem por característica comum, em todos os níveis da federação, o fato de ser um dos maiores controladores de dados pessoais, mercê de sua função e do exercício de sua missão.

Tem por função prestar serviço público que não é feito por máquinas ou algoritmos, mas por pessoas que passam a integrar o corpo funcional de determinado órgão, principalmente pela via do concurso público. Como se sabe, é crescente a procura pela carreira pública em todas as esferas dos três poderes e nos três níveis federativos. Nos diversos certames que buscam recrutar profissionais por rigoroso concurso público de provas ou de provas e títulos, são coletados e tratados dados pessoais dos candidatos no ato de inscrição e, conforme o processo seletivo é concluído, os dados dos candidatos que não foram selecionados são – ou deveriam ser – excluídos da base de dados do ente público, enquanto aqueles que passam a integrar os quadros do órgão público terão seus dados tratados permanentemente até mesmo após eventual extinção do vínculo funcional.

Por outro lado, sob o aspecto do exercício de sua missão legal, a natureza intrínseca do serviço público, que é prestar serviço ao público, resulta na necessária coleta, tratamento, modificação e eventual compartilhamento de dados pessoais dos cidadãos, destinatários de seu serviço.

Exemplificativamente, o Tribunal de Justiça do Estado de São Paulo tem um corpo funcional composto por 2.620 magistrados e 65.179 servidores, e exerce sua missão constitucional prestando jurisdição pela análise anual de aproximadamente 4,5 milhões de novas ações, gerenciando um acervo flutuante de quase 20 milhões de feitos em andamento (BRASIL, 2022b). Esses dados retratam a dimensão do tratamento de dados pessoais exercido por apenas um dos noventa e um tribunais da federação, que encerram apenas um dos poderes do Estado, ao lado do Legislativo e do Executivo.

Não é apenas o fato de ser um grande controlador de dados pessoais que permeia as três esferas federativas, mas também o fato de que o poder público é detentor ou maior acionista de grandes empresas de tecnologia, a exemplo do Serviço Federal de Processamento de Dados (Serpro), da Companhia de Processamento de Dados do Estado de São Paulo (Prodesp) e da Empresa

de Tecnologia da Informação e Comunicação do Município de São Paulo (Prodam).

Reúne, portanto, sob sua batuta e na maior parte das atividades de processamento de dados, as condições de controlador e operador e, nessa qualidade tem potencializada sua reponsabilidade por uma prestação de serviços públicos em estreita conformidade às normas de proteção de dados pessoais.

As empresas públicas de tecnologia submetem-se, indistintamente, aos preceitos constitucionais da ordem econômica,[45] com destaque para sua finalidade de assegurar a todos uma existência digna, conforme os ditames da justiça social, assim como por força da Emenda Constitucional n. 115, de 2022, à observância ao direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.[46]

A concretização desse mandato constitucional se dá mediante a prestação de serviço público consistente no tratamento de dados pessoais e outras informações de modo não apenas responsável, mas proativo, sob os vieses da segurança, da prevenção e da responsabilização, plasmados nos princípios norteadores da proteção de dados.[47]

Com efeito, a atividade das empresas públicas e sociedades de economia mista não se resumem à prestação do serviço de tratamento de informações e dados pessoais segundo as determinações do controlador. Antes, encontram na nova ordem jurídica que permeia a Era Digital uma coleção de novas missões, igualmente relevantes, como a educação em direitos do usuário do serviço público, o constante treinamento e capacitação de seus colaboradores em matéria de proteção de dados pessoais e a devolução à sociedade do conhecimento produzido, como forma de retroalimentar o ciclo de proteção de dados que tem, no cidadão e nas empresas, seus protagonistas e principais destinatários.

Significa dizer que empresas públicas e sociedades de economia mista da área de tecnologia da informação são reconhecidas ilhas de qualidade por reunirem grande quantidade de informação qualificada e serem dirigidas por profissionais de altíssima gama, selecionados dentre os melhores do mercado justamente com a missão de apoiar o poder público, nas diversas esferas, na tomada de decisão quanto às questões de tecnologia e, no atual contexto, da proteção de dados pessoais.

A Serpro foi das pioneiras, antes mesmo da entrada em vigor da Lei n. 13.709/2018, em disponibilizar conteúdo informativo a respeito da Lei Geral de Proteção de Dados. Em seu sítio eletrônico estavam disponíveis desde a promulgação da lei, infográficos, glossário e conteúdo a respeito das bases

45 Art. 170 da Constituição Federal.

46 Art. 5.º, LXXIX da Constituição Federal.

47 Art. 6.º, VII, VIII e X da Lei n. 13.709/18.

legais e princípios de proteção de dados, buscando disseminar conceitos e percepções sobre a novel legislação, despontando como referencial no âmbito público.

A proposta de atuação dessas entidades preconizada neste estudo busca o comprometimento de sua produção de qualidade para com o impulsionamento da conformidade das empresas privadas, para além dos limites da gestão pública.

Sobressai a atuação da Prodam que publicou em seu sítio a *Cartilha LGPD*, em cuja "Mensagem do Presidente" refere-se à LGPD e sua missão nos seguintes termos:

> Mais do que uma lei, a LGPD possui no seu corpo princípios, fundamentos e ações que todas as pessoas, empresas e governos que tratem dados pessoais devem seguir, mas, principalmente, coloca o dono da informação como figura central: o titular dos dados é o foco.
>
> E é justamente com esse foco que a Prodam elaborou esta cartilha, como um direcionador à empresa e à gestão pública municipal, buscando trazer luz aos pontos fundamentais e esclarecimentos aos pontos mais complexos da lei (SÃO PAULO, 2022, grifo nosso).

É tema de reconhecida relevância na doutrina que a absoluta falta de uma metodologia para a implementação de uma norma referencial de proteção de dados é uma dor que acomete todo o setor público, levando, por vezes à mimetização dos *frameworks* do setor privado adotados apenas por empresas de médio e grande porte com capacidade econômica de contarem o assessoramento de empresas de consultoria, mas que guardam pouca ou nenhuma relação com as rotinas administrativas e particularidades do setor público (TASSO, 2021).

Esse mesmo distanciamento e percepção de inadequação é sentido por pequenas e médias empresas privadas, bem assim como por municípios de pequeno porte em que a baixa arrecadação não permite o investimento na contratação de uma consultoria para a adequação à LGPD.

É nesse contexto que o papel das empresas públicas de tecnologia da informação e comunicação, a exemplo das agências reguladoras e da própria ANPD, avulta-se, realçando os vieses administrativos da oportunidade e conveniência de sua atuação em prol da administração pública como um todo e como agente de fomento à conformidade de pequenas e média empresas, mediante a produção e compartilhamento de conteúdo e metodologias com todo e qualquer agente econômico, público ou privado, transpondo a barreira do potencial econômico.

6 REFLEXOS DA ADEQUAÇÃO DAS EMPRESAS E SOCIEDADES CIVIS NA RESPONSABILIDADE CIVIL

O estabelecimento da adequação das empresas e sociedades civis à LGPD como sendo uma política pública tem inegável reflexo positivo sobre a responsabilidade civil.

O grau de diligência da empresa no estabelecimento de medidas elementares de proteção de dados, para além das práticas de segurança da informação, é fator decisivo na aplicação das sanções administrativas previstas no artigo 52 da LGPD e das normas de responsabilidade civil, na eventualidade de incidente de segurança envolvendo dados pessoais.

Afora as hipóteses de não realização de tratamento de dados pessoais e a culpa exclusiva do titular dos dados ou de terceiros, a responsabilidade civil do controlador somente é afastada quando se provar que, embora tenha realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados.[48]

Já se demonstrou que a responsabilidade civil de empresa ou sociedade civil que realiza o tratamento de dados pessoais em sua atividade, excetuadas as hipóteses em que subjaz relação de consumo, é regida pelas normas da responsabilidade civil subjetiva, porquanto verificada na hipótese de uma violação a um dever, qual seja, o de observar as normas de proteção de dados existentes na LGPD (TASSO, 2020).

Todavia, aferição de "violação à legislação de proteção de dados pessoais" demanda complexa atividade interpretativa pelo órgão jurisdicional, uma vez que a Lei n. 13.709/2018 tem caráter essencialmente principiológico e é permeada por termos abertos, numa clara aderência à ideia de tecnorregulação, conforme a lição de Cintia Rosa Pereira Lima e Kelvin Peroli (2019, p. 428), ao referenciar Pierre Lévy:

> Ao se abordar o tratamento automatizado de dados, a tecnologia é um dos *digital influencers*, de constante atualização, como preceitua Pierre Lévy. Assim, o ideal é que os dispositivos sobre proteção de dados tenham um caráter principiológico e com cláusulas gerais para que possam perdurar com o avanço tecnológico, restando à autoridade garante a regulamentação, ao decorrer das atualizações, conforme uma tecnorregulação.

Nesse cenário onde a álea judicial pode resultar em diferentes consequências jurídicas em decorrência do mesmo fato, conforme o órgão julgador, a aderência de empresas às políticas públicas de incentivo à adequação, verificável através de selos e certificações, é um parâmetro objetivo para aferição do dever de diligência do controlador, sendo assim

48 Art. 43 da Lei n. 13.709/2018.

um parâmetro concreto para ensejar a redução ou o afastamento da responsabilidade civil em caso de incidentes de dados pessoais.

Além disso, a elevação da proteção de dados ao patamar de uma política pública em todos os níveis federativos tem o condão de promover o debate e o aperfeiçoamento interpretativo da LGPD, tendente à criação de consensos a respeito de patamares seguros a partir dos quais se possa afirmar ter a empresa ou sociedade civil observado as normas de proteção.

7 CONCLUSÃO

A plena entrada em vigor da LGPD, ocorrida com o aperfeiçoamento da *vacatio legis* das sanções administrativas em 1.º de agosto de 2021, inaugurou no ordenamento jurídico brasileiro o referencial normativo de proteção de dados pessoais, agregando e conferindo uma base principiológica única aos diversos microssistemas de proteção presentes em leis esparsas, como no Marco Civil da Internet, aa Lei de Acesso à Informação e no Código de Defesa do Consumidor.

Trata-se de uma norma de cunho eminentemente principiológico e permeada de termos abertos, propositalmente escolhidos para permitir que a lei tivesse a plasticidade necessária para acompanhar a rápida evolução das tecnologias aplicadas ao tratamento de dados pessoais. É notadamente uma norma dotada de transversalidade, que passa todos os ramos do direito e regulamenta atividades de tratamento de dados do setor privado e do setor público, realizadas em meio físico e digital.

Norma de tamanha abrangência e impacto tem sua aderência ainda incipiente no setor privado, notadamente pelas pequenas e médias empresa. No poder público, a Lei n. 12.527/2011 – Lei de Acesso à Informação – fomentou o aprendizado e a vivência dos entes públicos nas três esferas federativas e em todos os poderes, de modo que o advento da LGPD foi recebido sem a perceptível resistência, bastando, para sua implementação, que entes públicos de mais alto nível hierárquico capitaneassem um crescente movimento de conformidade.

A ausência de metodologias de implementação, somada à carestia de recursos financeiros para investimento em ações de conformidade em decorrência da pandemia de Covid-19, sobretudo no setor privado, desenhou um cenário nacional de tímida adesão às prescrições da lei protetiva.

Nesse contexto, buscou-se demonstrar que não apenas a Autoridade Nacional de Proteção de Dados, mas principalmente o Estado, sob o recorte do poder público municipal, possui responsabilidade social pela implementação de políticas públicas que fomentem ações de conformidade no setor privado da economia.

Para além do incentivo gerado pelas sanções premiais, preconiza-se que tais políticas públicas promovam o compartilhamento da expertise obtida

pelas grande empresa públicas de tecnologia, como forma de proporcionar, sobretudo à pequena e média empresa, uma coleção de conhecimentos acerca da LGPD e uma metodologia de implementação de marcos de conformidade, gerando reflexos positivos à empresa, tanto na questão concorrencial quanto na atenuação da responsabilidade civil por eventual incidente de proteção de dados pessoais.

Vislumbra-se que, assim como o Município de São Paulo estabeleceu, pela Lei Municipal n. 17.481/20, normas de incentivo e proteção à livre iniciativa e ao livre exercício de atividade econômica, autoproclamando-se "capitalista humanista", cada município brasileiro poderá galgar, em futuro próximo e por intermédio das políticas públicas propostas neste artigo, a qualidade de município protetor dos dados pessoais de seus cidadãos.

REFERÊNCIAS

BOBBIO, Norberto. **Da estrutura à função**. Trad. Daniela B. Versiani. Barueri: Manole, 2007.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Tratamento de Dados Pessoais pelo Poder Públic**o. Brasília, jan. 2022a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 7 mar. 2022

BRASIL. **Como proteger seus dados pessoais:** Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Brasília: Ministério da Justiça e Segurança Pública, [202-]. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 7 mar. 2022.

BRASIL. Conselho Nacional de Justiça. **Relatório Justiça em Números 2021**. Brasília: CNJ, 2022b. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/09/ relatorio-justica-em-numeros2021-12.pdf

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 mar. 2022.

LIMA, Cintia Rosa Pereira de; PEROLI, Kelvin. Desafios para a atuação independente da Autoridade Nacional de Proteção de Dados Pessoais brasileira à luz das exigências internacionais para a adequada proteção de dados. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; DEZEM, Renata Mota Maciel (coords.). **Direito e Internet IV Sistema de Proteção de Dados Pessoais**. São Paulo: Quartier Latin, 2019.

LUCCA, Newton de; LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: LIMA, Cíntia Rosa Pereira de (org.). **Comentários à Lei Geral de Proteção de Dados:** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020.

REALE, Miguel. **Lições preliminares de direito**. 27. ed. São Paulo: Saraiva, 2002.

RODRIGUES, Paula Marques; VIEIRA, Alessandra Borelli. Educação como um dos pilares para a conformidade. *In*: BLUM, Renato Opice (org.). **Proteção de dados:** desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020.

SÃO PAULO. **Cartilha LGPD**. São Paulo: Prodam, 2022. Disponível em: http://www.prodam.sp.gov.br/pdfs/Cartilha.LGPD.pdf . Acesso em: 7 mar. 2022.

TASSO, Fernando Antonio Temas relevantes na implementação da LGPD em instituições públicas de grande porte – Estudo de caso do Tribunal de Justiça de São Paulo. *In*: FRANCOSKI, Denise de Souza; TASSO, Fernando Antonio (coord**.). A Lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado: LGPD. São Paulo: Revista dos Tribunais, 2021.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, Escola Paulista da Magistratura, São Paulo, 2020.

VARGAS, Andressa Girotto *et al.* **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 7 mar. 2022.

9
MONETIZAÇÃO DE DADOS POR ENTES PÚBLICOS

Patrícia Peck Garrido Pinheiro
Camila Nascimento
Julia Lonardoni Ramos

1 INTRODUÇÃO

A monetização de dados é um tema altamente discutido nos dias de hoje, principalmente quando o assunto envolve questões de privacidade e proteção de dados pessoais.

No atual cenário, enfrentado por Manuel Castells (2002, p. 108) como a era da sociedade informacional – em que a informação é tida como matéria-prima –, nota-se a presença de uma economia digital em que dados são os principais ativos e, consequentemente, a informação é tida como a principal fonte de riqueza.

Destaca-se, aqui, o fenômeno trazido por Andrew Murray (2010, p. 4) da "precificação das informações", em que os dados possuem caráter econômico. Tal fenômeno transparece na chamada monetização de dados, entendida como a extração de valor econômico dos dados. De forma geral, os dados podem gerar receita de três maneiras: (i) mediante a venda de dados; (ii) mediante a utilização de dados para criação de produtos ou serviços a serem vendidos e oferecidos no mercado; (iii) mediante a inferência de informações obtidas através da acumulação e manipulação de dados (DENNEDY; LEIZEROV, 2017).

Na esfera privada, nota-se a existência de diversas empresas que possuem como modelo de negócio a monetização de dados pessoais, conhecidas como *data brokers*. A Comissão Federal do Comércio dos Estados Unidos (US Federal Trade Commission) as conceituou como:

> Empresas cujo principal negócio é coletar informações pessoais sobre consumidores de uma variedade de fontes e agregar, analisar e compartilhar essas informações, ou informações derivadas a partir dele, para fins diversos como marketing de produtos, verificação da identidade de um indivíduo ou detecção de fraude (EUA, 2014).

Muito embora a monetização de dados venha sendo discutida há tempo na esfera privada, faz-se necessário trazer a discussão à esfera pública e verificar de que forma os entes públicos monetizam os dados pessoais, aspectos de sua legalidade, limites e diretrizes para que os direitos e garantias fundamentais dos titulares de dados pessoais não sejam lesados.

Sabe-se que são constantes as transformações que a tecnologia proporciona à sociedade e, consequentemente, ao ente público. O crescimento das organizações governamentais que disponibilizam serviços na internet é significativo e decorre de iniciativas como a Estratégia do Governo Digital, para atender aos anseios dos cidadãos em um crescente cenário de avanço tecnológico.

Dessa forma, surge-se a indagação a respeito da cobrança de taxas pelo ente público, quando da solicitação de acesso a informações de terceiros por entes privados, como forma de monetização de dados pelo ente público.

Nesse sentido, o presente artigo possui como objetivo analisar a legalidade da cobrança de taxa pelo ente público para o compartilhamento de dados pessoais a pessoas jurídicas de direito privado, os limites da monetização de dados pelos entes públicos, bem como avaliar os deveres e obrigações trazidas pela Lei Geral de Proteção de Dados quando do tratamento dos dados pessoais.

2 DA LEGALIDADE DA COBRANÇA DE TAXA PELO ENTE PÚBLICO

É notório que no ambiente do poder público, todos os serviços têm um custo e que a origem da receita de custeio deve ser lícita. Não se pode, por exemplo, simplesmente elevar a carga tributária para propiciar os serviços de segurança cibernética, bem como não é possível que haja a prestação desse serviço se não houver base orçamentária para a sua disponibilização e execução.

Juntamente com a transformação digital, sobrevêm os deveres e obrigações que o ente público deve cumprir em respeito a garantias de direitos fundamentais da população e, consequentemente, há necessidade de investimento em estrutura e segurança dessas plataformas, principalmente para cumprimento de obrigações legais existentes.

Assim, chega-se ao cerne da questão sobre a cobrança, pelo ente público, de uma taxa para o compartilhamento de dados pessoais de acesso público a pessoas jurídicas de direito privado: referida cobrança é legal e deve ser realizada com o objetivo de economicidade pelo ente público.[49]

49 O princípio da economicidade está previsto no art. 70 da Constituição Federal e constitui-se na minimização dos gastos públicos sem o comprometimento dos padrões de qualidade. Refere-se, portanto, à capacidade de uma instituição gerir adequadamente os recursos financeiros colocados à sua disposição (PRINCÍPIO DA ECONOMICIDADE, [202-])

Com previsão no inciso II do art. 145 da Constituição Federal, a taxa constitui-se num tributo que tem como fato gerador o exercício do poder de polícia ou a utilização efetiva ou potencial de um serviço público específico e divisível prestado ao contribuinte ou posto à sua disposição (art. 77 do Código Tributário Nacional – CTN) (BRASIL, 1966).

Considera-se o serviço público específico aquele que possa ser destacado em unidades autônomas de intervenção, utilidade ou necessidade pública. Já os divisíveis são considerados aqueles suscetíveis de utilização, separadamente, por parte de cada um dos seus usuários (art. 79, inciso II e III, CTN).

Conforme Aliomar Baleeiro (2018, p. 1280):

> O serviço é efetivo, quando ministrado ao contribuinte a qualquer título, isto é, porque lhe interesse ou porque deva sujeitar-se a ele por sua atividade em relação a terceiros. É potencial, quando compulsório, funcione efetivamente à disposição do contribuinte. Compulsório o pagamento, não o uso. É específico, quando possa ser separado em unidades autônomas de intervenção da autoridade ou de sua utilidade, ou de necessidade pública, que o justificou: por exemplo, a existência do corpo de bombeiros para o risco potencial de fogo. É divisível, quando possa funcionar em condições tais que se apure a utilização individual pelo usuário: a expedição de certidões, a concessão de porte de armas, a aferição dos pesos e medidas etc.

Dessa forma, entende-se que a taxa pressupõe um vínculo de causalidade entre o contribuinte e o serviço prestado (BALEEIRO, 2018). Portanto, quando do exercício do direito de acesso a informações de terceiros por entes privados em face do ente público, que presta um serviço específico e divisível, a cobrança de taxa é legítima.[50]

Importa, aqui, entender a natureza da prestação desse serviço público, ou seja, o oferecimento pelo ente público do serviço de acesso a dados pessoais, uma vez que possuem utilidade ou comodidade material desfrutável por aquele que acessa o conteúdo compartilhado.

Com isso, entende-se que a consulta de informações, ainda que sejam consideradas como dados de acesso público, pressupõe uma atividade pública de fornecimento de dados estruturados e legíveis, que demandam um custo ao ente público.

Inclusive, a própria Lei de Acesso à Informação (Lei n. 12.527/2011) traz a exceção da gratuidade do acesso à informação ao prever a possibilidade de cobrança para o serviço de busca e de fornecimento de informação referente

50 Cite-se aqui a exceção prevista no § 5.º do art. 18 da LGPD, que determina que o atendimento ao exercício de direito previstos no art. 18 deve ser realizado sem custos para o titular, nos prazos e nos termos previstos em regulamento (BRASIL, 2018). Não obstante, verifica-se a impossibilidade de cobrança de taxa pelo poder público ao contribuinte quando da obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal, nos termos do art. 5.º, inciso XXXIV, alínea "b", da Constituição Federal.

ao valor necessário ao ressarcimento dos custos dos serviços e dos materiais utilizados quando a consulta exigir reprodução de documentos (art. 12, parágrafo único). Tal dispositivo pode perfeitamente ser interpretado à luz do contexto digital, em que o custo para o fornecimento dos serviços e dos materiais utilizados decorre de investimento em uma base de dados estruturada, em segurança da informação, bem como da interoperabilidade da base de dados em questão.

Cite-se como exemplo a cobrança de taxa pelas repartições cartorárias para a realização de busca com o intuito de emitir certidões, bem como a emissão de certidões por prefeituras na área de habitação e desenvolvimento urbano – como consulta de nome de proprietário e confrontantes do imóvel.

Quanto aos cartórios, conforme entendimento das normas das Corregedorias Gerais de Justiça (PACHECO, 2016), as certidões não podem ser expedidas sem que antes seja realizada uma busca minuciosa nos livros de protocolo e nos livros de registros de indisponibilidades, em razão de disposição da Lei de Registros Públicos (Lei n. 6.015/73). Assim sendo, há realização de um serviço prévio à emissão da certidão. Quanto às certidões emitidas pelas prefeituras, o serviço é cobrado em decorrência do fato de o ente público arcar com os custos das transações e mais, com o custo de manutenção das bases de dados e investimento em segurança da informação. Nesse sentido, a cobrança de taxa, além de necessária, é sustentável, pois não pode o erário arcar unilateralmente com esses custos.

Não obstante, cabe destacar que além de legislações que tratem da segurança da informação por si só, como o Decreto n. 9.637/2018, que institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal, o ente público possui igualmente o dever de cumprir com as obrigações trazidas pela Lei Geral de Proteção de Dados Pessoais.

Sabe-se que manter a conformidade com a Lei n. 13.709/2018 (LGPD), especialmente em relação às medidas técnicas e administrativas de segurança, exige um custo alto. Assim, a cobrança de taxa viabiliza, inclusive, o investimento em práticas de governança em privacidade e proteção de dados pessoais, principalmente quanto à garantia de requisitos mínimos de segurança das bases de dados e plataformas de compartilhamento de dados pessoais do ente público.

Nesse ponto, cabe diferenciar o mero compartilhamento de dados pessoais do chamado uso compartilhado de dados pessoais (BRASIL, 2022). O compartilhamento de dados por si só decorre de um exercício de direito de acesso pelo ente privado (contribuinte) em face do poder público.

Conforme o referido guia, o compartilhamento de dados pessoais verifica-se na "operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública" (BRASIL, 2022, p. 17).

Já o uso compartilhado de dados pessoais é conceituado pela LGPD, no inciso XVI do art. 5.º, como:

> [...] comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (BRASIL, 2018).

O uso compartilhado deve ser feito de acordo com a LGPD, especialmente com os princípios, as bases legais, a garantia dos direitos dos titulares e outras regras específicas aplicáveis ao poder público (BRASIL, 2022).

Importa ressaltar que o guia da ANPD elenca requisitos que devem ser observados quando do uso compartilhado de dados pessoais, quais sejam: (i) formalização e registro; (ii) definição do objeto e finalidade; (iii) atribuição de base legal; (iv) definição da duração do tratamento; (v) mecanismos de transparência e direito dos titulares; (vi) prevenção e segurança; (vii) outros requisitos, a depender do caso concreto, como a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a definição sobre eventual ônus financeiro decorrente da operação (BRASIL, 2022, p. 18-21).

Pois bem, o uso compartilhado de dados pressupõe que ambas as partes, sejam elas entes públicos ou privados, possuam o poder de consultar, inserir, alterar e deletar dados dentro da base. Nesse sentido, esclarece Patrícia Peck Garrido Pinheiro (2018, p. 135):

> Ressalte-se, por oportuno, que na questão dos dados, faz toda diferença em termos conceituais, diferenciar o que é acesso do que é uso, e, por último do que é compartilhamento. Isso porque, um acesso, significa, apenas poder ver (consulta), o uso envolve um nível a mais do que o acesso (significa além da consulta, poder utilizar a informação consultada). E o compartilhamento é o nível com mais poderes, pois abrange também o ato de transferir, de poder extrair dados.

Dito isso, embora o simples compartilhamento de dados pessoais com entes privados não seja considerado como uso compartilhado de dados pessoais – que pressupõe a adoção das medidas acima indicadas –, os requisitos legais previstos pela LGPD devem ser igualmente respeitados.

3 DA CONFORMIDADE DO COMPARTILHAMENTO DE DADOS PESSOAIS PELO ENTE PÚBLICO COM A LGPD

Conforme dispõe a LGPD, o tratamento de dados pessoais pela administração pública poderá ocorrer de forma que o ente público trate e compartilhe os dados necessários à execução de políticas públicas

previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados, desde que sempre atendido o princípio do interesse público.

Nesse contexto, o tratamento de dados pessoais pelos órgãos e entidades do ente público deve respeitar os requisitos de realização em prol da finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, excetuando-se a aplicação da norma de proteção de dados pessoais apenas na hipótese de tratamento de dados pessoais realizados exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou repressão de infrações penais.

Serviço público é todo serviço prestado pelo poder público e seus entes, em prol da coletividade e com a finalidade de promover o bem-estar social. Normalmente se trata de serviço prestado pelo próprio Estado, através de seus servidores, ou pode ocorrer uma delegação, como ocorre no caso das serventias cartorárias e, então, o serviço público passa a ser prestado por um particular que mantém o caráter público daquele serviço.

Com a crescente evolução da informatização dos serviços públicos, deve-se entender, a princípio, a finalidade do compartilhamento de dados, sobretudo pela necessidade de atender ao disposto na LGPD sobre manutenção dos dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Atualmente, muitos serviços públicos são disponibilizados para a população em formato digital ou eletrônico, configurados em sistemas integrados. Esses sistemas realizam o tratamento de dados pessoais com compartilhamento de dados, como ocorre, por exemplo, entre secretarias de estado ou municipais, no caso de serviço de transporte urbano em que há compartilhamento de dados pessoais de servidores entre a secretaria de transportes e secretaria de obras, tendo em vista a necessidade de manutenção das vias públicas em que os meios de transporte transitam. Esse exemplo demonstra que, independentemente do consentimento do titular, há uma finalidade pública no tratamento, para atender a uma finalidade específica de execução de política pública.

O crescimento significativo das organizações governamentais que disponibilizam serviços na internet traz à tona que o Brasil busca utilizar sistemas informatizados em larga há algum tempo, com iniciativas federais como a Estratégia do Governo Digital[51] para atender aos anseios dos cidadãos em um crescente cenário de avanço tecnológico.

51 A Estratégia de Governo Digital para o período de 2020 a 2022 está organizada em princípios, objetivos e iniciativas que nortearão a transformação do governo por meio de tecnologias digitais (BRASIL, 2020).

Isso se deve ao fato de que, no processo de transformação digital envolvido na sociedade contemporânea, é preciso integrar e coordenar iniciativas que sejam comuns ao setor público e ao cidadão, permitindo a sua aproximação e estimulando não só a redução de custos de informatização e digitalização dos serviços, como aumentando a agilidade e alcance da prestação de serviços públicos com a adoção de soluções multifacetadas e obrigatoriamente escoradas nas infraestruturas de tecnologias de informação e comunicação, as conhecidas TICs (MENDES, 2008).[52]

Em se tratando de compartilhamento com uma entidade privada, o ente público apenas poderá compartilhar dados pessoais com algumas reservas, como em caso de execução descentralizada de atividade pública que exija a transferência, exclusivamente, para esse fim específico e determinado e nos casos em que os dados pessoais forem acessíveis publicamente.

O ente público ainda deve indicar um encarregado de proteção de dados, àquele que servirá como elo entre a administração pública, o titular dos dados pessoais e a entidade fiscalizadora, Autoridade Nacional de Proteção de Dados (ANPD), bem como respeitar previsão legal da transferência ser respaldada em contratos, convênios ou instrumentos similares, prevenção de fraudes e irregularidades ou proteger e resguardar a segurança e a integridade do titular dos dados.

Sabemos que a administração pública é submissa aos princípios constitucionais da legalidade, moralidade, impessoalidade, finalidade, publicidade, eficiência, razoabilidade, proporcionalidade, ampla defesa, contraditório, segurança jurídica, motivação e supremacia do interesse público, e que todas as esferas do governo possuem regras orçamentárias. Não é diferente quando se fala em proteção de dados pessoais e conformidade com a LGPD.

A obrigatoriedade de o setor público cumprir as determinações da LGPD desenvolve uma imposição de investimento na segurança da informação, algo que muitas vezes é negligenciado e colocado à margem em comparação a outros serviços públicos. Devemos atentar para o art. 46 da norma de proteção de dados, no tocante ao emprego de medidas de segurança, técnicas, administrativas e organizacionais, a ser seguido por todos os controladores de dados.

Sendo assim, para o compartilhamento de dados pessoais, além de seguir as regras concernentes à execução de políticas públicas e respeitar os princípios dispostos no art. 6.º da LGPD, deve-se preservar e cuidar de executar a atividade de forma segura e de acordo com a finalidade específica.

52 Tecnologia da Informação e Comunicação (TIC) é um conjunto de recursos tecnológicos que, quando integrados entre si, proporcionam a automação e/ou a comunicação nos processos existentes nos negócios, no ensino e na pesquisa científica e etc. São tecnologias usadas para reunir, distribuir e compartilhar informações (MENDES, 2008).

Outro ponto que merece atenção no que diz respeito ao compartilhamento de dados pessoais é o processamento desses dados, ou seja, a estruturação e a organização dos dados compartilhados. Esse processamento nos leva a pensar, inclusive, nas *ferramentas utilizadas e na segurança das operações de tratamento*.

Conforme previsto pelo artigo 18 da LGPD,[53] que traz a previsão dos direitos do titular, há a possibilidade deste solicitar do controlador a relação de dados pessoais tratados, mediante apresentação de requisição expressa, assim como é possível questionar com quais entidades, públicas ou privadas, o controlador realizou compartilhamento dos dados pessoais desse titular, além da possibilidade de solicitação de correção, eliminação ou bloqueio dos seus dados junto ao controlador, o que acarretaria uma reação em cadeia quanto àquele que recebeu e acessou anteriormente o dado pessoal, sem a correção solicitada.

Importante destacar que especificamente no atendimento dessa solicitação do titular, a previsão da LGPD é de que deve ser feita sem

---

53 "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador. § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor" (BRASIL, 2018).

custos. Portanto, estamos tratando neste artigo da previsão de exploração econômica aplicável a solicitações advindas de pessoas jurídicas ou de outras prestações de serviços em que seja justificável inclusive o custeio/ reembolso de despesas incorridas pelo ente público.

É certo que o compartilhamento de dados pessoais e sua disponibilização pelo ente público coaduna-se com a própria transparência pública e denota um aumento da disponibilidade e qualidade dos dados pessoais.

O momento que passamos é de uma mudança cultural e de aprendizado sobre os dados pessoais, e entender as oportunidades e riscos do compartilhamento de dados é parte integrante desse processo, além da responsabilidade envolvida e os limites estabelecidos na Lei Geral de Proteção de Dados Pessoais.

4 CONSIDERAÇÕES FINAIS

Frente à era da sociedade informacional, em que os dados são tidos como os ativos mais valiosos e a informação, como a maior fonte de riqueza, nota-se fortemente a presença de uma economia digital.

O fenômeno trazido por Andrew Murray da "precificação das informações" transparece na chamada monetização de dados, entendida como a extração de valor econômico dos dados. Referida monetização já vem sendo discutida na esfera privada há um tempo, principalmente pelo fato de existirem empresas que possuem, como modelo de negócio, a monetização de dados pessoais, conhecida como *data brokers*.

Entretanto, notou-se a necessidade de trazer a discussão à esfera pública. Dessa forma, o presente texto buscou verificar de que forma os entes públicos podem de algum modo também monetizar os dados pessoais, os aspectos de sua legalidade, limites e diretrizes para que os direitos e garantias fundamentais dos titulares de dados pessoais também sejam atendidos.

Constatou-se o crescimento de organizações governamentais que disponibilizam serviços de atendimento ao cidadão pela internet, em formato digital ou eletrônico, configurados em sistemas integrados é significativo. E juntamente com a transformação digital, sobrevêm os deveres e obrigações que o ente público deve cumprir em respeito a garantias de direitos fundamentais da população e, consequentemente, há a necessidade de investimento em estrutura e segurança dessas plataformas, principalmente para cumprimento de obrigações legais existentes.

Nesse contexto, surgiu a problematização de monetização de dados pessoais, principalmente com o advento da Lei Geral de Proteção de Dados (LGPD). Dessa forma, buscou-se exemplificar que a cobrança de taxa pelo ente público, quando da solicitação de acesso a informações de terceiros por entes privados em face do ente público, é legítima e deve ser realizada com o objetivo de economicidade pelo ente público.

Como aludido, sendo atribuição do ente público garantir a transparência no tratamento de dados pessoais, bem como o acesso à informação, pode-se afirmar que quando do direito de acesso a informações por entes privados em face do ente público, a cobrança de taxa é tida como uma forma legítima de monetização de dados, uma vez que se verifica na cobrança por serviço específico e divisível realizado. Ainda, as taxas cobradas pelo ente público não são calculadas em razão da capacidade financeira do contribuinte e sim em valor fixo e igualitário, geralmente tabelado pelos órgãos públicos.

Isso porque todo serviço prestado pelo ente público tem um custo. A consulta e o compartilhamento de informações, ainda que de dados de acesso público, pressupõe uma atividade de fornecimento de dados estruturados e legíveis. Não obstante, destaca-se a obrigatoriedade do investimento em segurança da informação.

Como visto, além do cumprimento de legislações que tratem da segurança da informação de forma independente, como o Decreto n. 9.637/2018, que institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal, o ente público possui igualmente o dever de cumprir uma série de obrigações trazidas pela Lei Geral de Proteção de Dados Pessoais.

Cite-se o dever de adoção de medidas técnicas e administrativas de segurança no tratamento de dados pessoais, a garantia de transparência e qualidade dos dados, atribuição de bases legais, a nomeação de um encarregado de dados, mecanismos para atendimento de requisições dos direitos dos titulares, entre outras mencionados no presente texto.

Dessa forma, conclui-se pela defesa de que a cobrança de taxa pode ser considerada como monetização de dados legítima por entes públicos, como um meio sustentável de uso das informações, pois não pode o erário arcar unilateralmente com todos esses custos.

REFERÊNCIAS

BALEEIRO, Aliomar. **Direito tributário brasileiro**. 14. ed., rev. atual. e ampl. Rio de Janeiro: Forense, 2018.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Tratamento de Dados Pessoais pelo Poder Públic**o. Brasília, jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 7 mar. 2022.

BRASIL. D**ecreto n. 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358. Acesso em: 06 mar. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em:

BRASIL. **Lei n. 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em:

CASTELLS, Manuel. **Sociedade em Rede:** A Era da Informação – Economia, Sociedade e Cultura. V. 1. Rio de Janeiro: Paz e Terra, 2002.

DENNEDY, Michele; LEIZEROV, Sagy. On monetizing personal information: a series. **IAPP**, 26 set. 2017. Disponível em: https://iapp.org/news/a/on-monetizing-personal-information-a-series/. Acesso em: 28 mar. 2022.

EUA. **Data Brokers:** A Call for Transparency and Accountability. [*s.l.*]: Federal Trade Comission, 2014. Disponível em: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Acesso em: 28 mar. 2022.

MENDES, A. TIC – Muita gente está comentando, mas você sabe o que é? **Imasters**, 27 mar. 2008. Disponível em: https://imasters.com.br/devsecops/tic-muita-gente-esta-comentando-mas-voce-sabe-o-que-e. Acesso em: 06 mar. 2022.

MURRAY, Andrew. **Information technology law**. Oxford: Oxford University, 2010.

PACHECO, Maria Aparecida Bianchin. Sobre a cobrança de buscas em certidões. **Cartório 1.º Ofício Poxoréu**, nov. 2016. Disponível em: https://www.cartoriorgipoxoreu.com.br/novo/wp-content/uploads/2016/11/00024_00182_00007-1-1.pdf. Acesso em: 29 mar. 2022.

PINHEIRO, Patrícia Peck Garrido. **O direito internacional da propriedade intelectual aplicado à inteligência artificial**. 2018. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2018. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2135/tde-23102020-005146/publico/1370412_Tese_Parcial.pdf. Acesso em: 28 mar. 2022.

PRINCÍPIO DA ECONOMICIDADE. *In*: **Glossário de Termos Orçamentários**. Brasília: Congresso Nacional, [202-]. Disponível em: https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-orcamentario/-/orcamentario/termo/principio_da_economicidade#:~:text=Princ%C3%ADpio%20que%20objetiva%20a%20minimiza%C3%A7%C3%A3o,financeiros%20colocados%20%C3%A0%20sua%20disposi%C3%A7%C3%A3o. Acesso em: 28 mar. 2022.

10
MECANISMOS E MEDIDAS PRÁTICAS PARA OBTENÇÃO DE RESULTADO NO TRATAMENTO DE DADOS

Renato Müller da Silva Opice Blum
Bruno Henrique Cordeiro de Souza

Resumo

O presente artigo tem como objetivo promover a discussão no que se refere à adequação do setor público à Lei Geral de Proteção de Dados, especificamente visando a contribuir com argumentos que colaborem para o desenvolvimento de boas práticas nos municípios brasileiros. Nesse sentido, tratou-se da sistemática de implementação da lei, da interseção de outras leis de gênero similar ou correlato, expondo os primeiros acontecimentos da LGPD junto às pessoas jurídicas de direito privado e público, analisando com ênfase a passagem do setor estatal-geral em busca de melhorias para a esfera dos municípios, trazendo também possíveis medidas a se tomar, a fim de que, verdadeiramente, torne-se cultural a seriedade da Lei.

Palavras-chave: LGPD; medidas práticas; setor público; município; adequação.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), aprovada em vias legislativas no ano de 2018, passou a vigorar em setembro de 2020, porém sua vigência plena teve início apenas em agosto de 2021 (ANPD..., 2021),[54] cerca de três anos após sua materialização, trazendo com ela inúmeras novidades e desafios a serem encarados pela sociedade brasileira.

Tão logo iniciada a vigência da LGPD, as empresas, sobretudo as chamadas empresas de grande e médio porte, viram-se com apertado prazo para a necessária adequação, antes de eventual incidência de sanções,

54 Com ressalva à não regulamentação de norma de sanção e dosimetria, o que acontecerá no decorrer do ano de 2022, conforme agenda regulatória da ANPD 2021/2022 e resolução CD/ANPD n. 1, publicada em 28 de outubro de 2021

buscando assim atualização de sistemas, investimento em conhecimento, além de remodelação do conceito de privacidade e proteção de dados, anteriormente encarado como questão coadjuvante.

Além do mais, muito embora o maior foco tenha ficado nas empresas privadas – uma vez que, claro, são a maioria –, o artigo 1.º da LGPD[55] estabelece que a lei dispõe de tratamento de dados pessoais de pessoas naturais ou jurídica e abarca tanto as de direito privado, quanto as de direito público.

A partir desses pontos, faz-se importante uma análise da legislação federal, destrinchando a LGPD no que se refere aos entes públicos, compreendendo não só a União, estados e Distrito Federal, como também os municípios.

Nesse sentido, revela-se fundamental, ainda, que os entes públicos também encarem a Lei Geral de Proteção de Dados Pessoais como uma das prioridades em suas respectivas organizações, com estratégia de tratamento, implementação, adequação, respeito e regulamentação.

Ademais, perseguiremos o objetivo de registrar pormenores dos entes municipais, sua adequação e instruções práticas para adequação à LGPD, refletindo sobre formas de priorizar a efetividade prática da cultura trazida pela LGPD frente à população, garantindo-se melhores condições de transparência e segurança de dados para a sociedade.

2 AS BOAS PRÁTICAS PARA IMPLEMENTAÇÃO E RESPEITO DA LGPD PELOS MUNICÍPIOS E SETOR PÚBLICO GERAL:

2.1 O INÍCIO DA LGPD NO BRASIL

Inegavelmente, a LGPD tem exercido, nos últimos três anos, um fundamental papel quando o assunto é segurança e privacidade de dados no Brasil, sendo ela a principal lei que rege o assunto.

Inspirada na General Data Protection Regulation (GDPR) (UNIÃO EUROPEIA, 2016), a lei europeia que trata de dados, entende-se a importância de olhar para o que nela deu certo, para ser reproduzido em solo brasileiro, ao passo que é necessário observar os insucessos e, igualmente, evitá-los, já que temos nela um ótimo parâmetro.

Após aprovado o texto original da LGPD, uma série de dúvidas e percalços passaram a fazer parte da rotina não só dos operadores do direito,

55 "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios" (BRASIL, 2018).

como também de empresários dos mais variados ramos e funcionários do setor púbico.

Com a sua entrada em pleno vigor, é incontestável que as muitas dúvidas deram espaço à chama de esperança para prática do conceito de proteção e privacidade de dados pessoais, os quais não tinham uma lei específica para tratar de um direito tão importante.

Imperioso ressaltar que a LGPD também tem sido uma forte aliada da segurança jurídica no Brasil, trazendo diversos exemplos de melhoria em um sistema outrora escasso ou mesmo inexistente, como, por exemplo, a criação de um profissional encarregado de proteger dados numa empresa.

Em breve retrospecto, relembramos que a LGPD iniciou sua vigência plena em agosto de 2021 (com ressalva à não regulamentação de norma de sanção e dosimetria, o que acontecerá no decorrer do ano de 2022, conforme agenda regulatória da ANPD 2021/2022) (ANPD..., 2021), sendo essa a data de início da possibilidade de aplicação das sanções administrativas da LGPD, conforme prevê o art. 52, com competência exclusiva da Autoridade Nacional de Proteção de Dados (ANPD).

A figura da ANPD foi fundamental para realização de acordos técnicos, como o acordo com o Ministério Público, com o Conselho Administrativo de Defesa Econômica (Cade) e até mesmo com o Tribunal Superior Eleitoral (TSE).

Além disso, a ANPD começou, no ano de 2021, a chamada agenda regulatória um mecanismo de transparência e acompanhamento de quais serão os próximos passos e medidas que a adotar no decorrer do tempo e, assim, finalmente, reforçando o atendimento a todos os requisitos trazidos pela Lei Geral de Proteção de Dados.

Em 2021, principalmente, houve grande adesão dos entes privados e públicos à LGPD, muito em virtude da flexibilização das medidas de restrição pós-agravamento da pandemia causada pela Covid-19.

Não se pode fechar os olhos ao fato de que a iniciativa privada, por temer a aplicação de multas pela ANPD, deu uma atenção primordial ao que foi solicitado formalmente pela legislação, porém, por outro lado, não tivemos a mesma intensidade vinda do setor público.

Como dito, não se pode negar que a adaptação às pressas dos entes se iniciou, porque também tivemos o início da possibilidade de sanções administrativas pelo já citado órgão responsável: a ANPD. A repercussão foi tamanha pela possibilidade de aplicação da multa prescrita no próprio art. 52 da LGPD,[56] podendo alcançar até 2% do faturamento da pessoa jurídica de

56 "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional" (BRASIL, 2018).

direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a 50 milhões de reais por infração.

Noutro giro, a lei estabelece que as competências da ANPD prevalecerão, no que se refere à proteção de dados pessoais, haja vista o disposto no Art. 55-K da LGPD: "A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública" (BRASIL, 2018).

Ainda assim, sobre as competências correlatas de outras entidades ou órgãos da administração pública, lembra-se que a aplicação das sanções previstas na LGPD não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei n. 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor) e em legislação específica, qualquer que seja.

Por isso, eventual atuação de outros órgãos públicos, como agências reguladoras ou órgãos de defesa do consumidor, deve se dar de acordo com as suas próprias competências, observando suas legislações específicas.

Tratando de órgãos e entidades públicas, deve ser ressaltado o fato de que a LGPD, enquanto aliada social, prevê a possibilidade de responsabilização de agentes públicos, conforme previsto na Lei n. 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público), na Lei n. 8.429, de 2 de junho de 1992 (Lei da Improbidade Administrativa) e na Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Feitas as devidas constatações, podemos dizer que a fase inicial da era da LGPD e o sistema de proteção de dados, em geral, tem sido assunto recorrente, com as mais diversas formas e abordagens de discussão, isso tudo com significativo crescimento constante de uma Lei que passa cada dia mais a integrar, de fato, o ordenamento legislativo e jurídico brasileiro e que roga por adaptação cultural pelas empresas e entes públicos de todas as esferas.

2.2 A LGPD E SUA RELAÇÃO ESPECÍFICA COM OS ENTES PÚBLICOS:

Uma vez estabelecida a importância da LGPD para a sociedade, e considerando-se o Estado enquanto detentor da função de propiciar o bem-estar, a harmonia social, a qualidade de vida e garantia de todos os meios para que a democracia seja exercida, faz-se necessário a adoção de um plano que alcance a proteção da privacidade dos dados de seus cidadãos.

Buscando um conceito com maior toque de modernidade, Marilena Chaui (2006, p. 142) afirma: "O Estado se apresenta como origem da sociedade, como um poder capaz de instituí-la a partir do zero. Matéria sem forma, a sociedade vem à existência pela ação criadora do Estado, que lhe dá organização e se põe como centro e sentido dela".

É nesse contexto que o Estado também se apresenta como um organismo responsável pela ordem e equilíbrio da sociedade. Isso posto, é evidente que as empresas privadas deveriam se espelhar efetivamente nos entes públicos e deveriam se modelar conforme o possuidor de exemplo social se comporta.

Por essa lógica, é bem verdade que, se tivermos um Estado preocupado com a proteção de dados da sociedade, teremos então uma sociedade educada para, no mínimo, também proteger os seus dados.

No intuito de compreender qual o impacto que a Lei Geral de Proteção de Dados terá em cada ente que compõe o setor público, é plausível recorrer às definições fornecidas pelo Direito Administrativo, pois "[...] o ordenamento jurídico brasileiro submete as variadas hipóteses de atuação da administração pública, nos três poderes e em todos os níveis da Federação, ora a um regime jurídico tipicamente de direito público, ora a normas oriundas predominantemente do direito privado" (ALEXANDRINO; PAULO, 2017, p. 11).

Elucidar a natureza jurídica e escolher como agir, nos moldes do interesse público, resgatando sua finalidade, traz as seguintes indagações: como fazer com que a LGPD ingresse de vez no setor público? Como aproveitar os princípios administrativos e complementá-los com os alicerces da LGPD?

Além disso, a introdução da LGPD no setor público se torna abstrusa, mas também palpável, na medida em que é fundamental que se trabalhe com a conciliação dos preceitos constitucionais, como o respeito à privacidade, à inviolabilidade da intimidade, à honra e à imagem, tudo isso em conjunto pleno com os princípios da publicidade, consagrados tanto no artigo 37 da Constituição Federal,[57] quanto no integral texto da Lei de Acesso à Informação (LAI).

Desponta-se que, nos moldes do setor público, especificamente no texto da LGPD, encontramos uma base fundamental para o correto processamento de dados pessoais dentro da funcionalidade pública, a chamada "base de interesse público".

A regulamentação do tratamento de dados pessoais pelo poder público inicia sua jornada, na LGPD, no art. 23, e finda no art. 32, constando regras a serem seguidas, padrões de tratamento, as exceções permitidas e a constatação de responsabilidade (BRASIL, 2018).

Contudo, antes de adentrar às especificações trazidas pela LGPD, no que se refere ao setor público, há de se observar quatro pilares de embasamento da Lei n. 12.527/2011, a chamada Lei de Acesso à Informação (LAI). Os pilares (BRASIL, 2011) são:

57 "Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte [...]" (BRASIL, 1988).

i) o art. 4.º, IV, que define a informação pessoal: "Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável";

ii) a identificação dos princípios do tratamento, no art. 31, caput: "O tratamento das informações pessoais deve ser feito de forma transparente, com respeito à intimidade vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais";

iii) a restrição de acesso, consoante art. 31, § 1,º, I: "Informações pessoais, relativas à intimidade, vida privada, honra e imagem terão seu acesso restrito pelo prazo máximo de 100 (cem) anos".

iv) já o quarto pilar é destacado do quanto disposto no art. 5.º XXXIII da Constituição Federal: "Direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral [...), ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado" (BRASIL, 1988).

Assim, após enraizar os quatro conceitos basilares da LAI, remetem-se seus devidos suportes ao conceito de interesse público, muitas vezes descritos na LGPD, e que podem ser respaldados pelas principais regras, conceitos e princípios que a administração pública deve seguir, observando-se com cautela a inclusão de práticas de políticas públicas.

A evolução e, de certa forma, a inserção do sistema brasileiro de proteção de dados trabalha com os conceitos da LAI – que viabiliza o interesse público, o Marco Civil da Internet (Lei n. 12.965/2014), que se propõe a tratar o consentimento, e, finalmente, a LGPD, que definirá as bases legais do tratamento dos dados.

Como se daria, então, o início do processo de avaliação dos impactos, na hipótese de não observação da LGPD, no caso específico do setor público? Quem, legalmente, representaria o setor público?

Esses questionamentos são, também, um convite para a compreensão do impacto que a LGPD terá em cada ente do governo, sendo assim admissível olhar para as definições fornecidas pelo Direito Administrativo no tocante à sua constituição, repensar a natureza jurídica do ente e em qual interesse age – se no interesse público e em sua finalidade, ou em regime concorrencial. Esses podem ser os primeiros passos para identificar a funcionalidade da legislação de privacidade.

Hospitais, órgãos da segurança pública, entes educacionais são exemplos de pessoas jurídicas de direito público que demandam especial atenção com o tratamento de dados, sendo certo que dispõem de guarda e tratamento de dados sensíveis, passíveis de punições administrativas, pela ANPD, ou mesmo judiciais, pela jurisdição competente.

Pode-se ainda dizer que alguns instrumentos previstos na LGPD, tais como a anonimização[58] ou a pseudonimização,[59] servem de modo muito útil e efetivo ao gestor público, uma vez que permitirão a divulgação de documentos sem, contudo, permitir a identificação de dados pessoais dos indivíduos envolvidos, nos casos em que a publicidade integral não derive de expressa disposição legal.

Tamanha é a importância da proteção de dados pessoais que o Senado Federal aprovou, em 20 de outubro de 2021, a Proposta de Emenda à Constituição (PEC) n. 17/2019, que torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental.

Ainda, rompendo a base territorial brasileira, a LGPD chama atenção para o fato de que tamanha é sua importância frente à legislação ordinária, que casos de tratamentos de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência, devem, ao menos, possuir grau de proteção de dados pessoais adequado à LGPD.

Assim, compreendendo a magnitude e importância que a Lei Geral de Proteção de Dados adota em sua essência, faz-se extremamente necessário olhar para a legislação, seja na perspectiva da pessoa jurídica de direito público, seja na de direito privado, buscando a devida adequação, sem pular etapas ou desconsiderar tudo o que foi, até o momento, construído e conquistado.

2.3 AS MEDIDAS PRÁTICAS QUE ESTABELECEM O DIRECIONAMENTO DA LGPD PARA OS MUNICÍPIOS BRASILEIROS: O DESAFIO DE INTEGRAR A CULTURA DE PROTEÇÃO DE DADOS.

Compreendendo a existência de todo complexo do Estado, em todas as repartições, levanta-se aqui as boas práticas para implementação definitiva e cultural da LGPD nos municípios brasileiros.

Para entender a relevância desse assunto, ergue-se o entendimento de que é preciso montar uma estratégia básica ou, ao menos, um padrão que atenda os 5.570 municípios (IBGE, [202-?]) em todo território nacional,

58 Diz o artigo 5.º da LGPD: "[...] utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (BRASIL, 2018).

59 Artigo 13, § 4º: "[...] tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (BRASIL, 2018).

ponderando sobre a desafiadora missão de implementar a LGPD em cada um deles e que surtam efeitos relevantes.

Não se trata de fórmula mágica, tampouco a persistência de algum método que venha a ser cem por cento eficaz, mas sim da compreensão social dependente de estudo de governança, organização e planejamento. Sem esses componentes, não será possível adequar sequer um município à desafiadora LGPD.

Faz-se proeminente, ainda, a compreensão da importância da governança e do planejamento em cada município, tratando-os respectivamente como a capacidade que os municípios têm de avaliar e o direcionamento de monitoramento da gestão das políticas e serviços públicos, objetivando o efetivo atendimento das necessidades e demandas da população (CAVARIELI, 2020).

Em efeitos práticos, a ordem que rege o conceito de base legal para tratamento de dados, além da teorização e formalização de medidas legais, é o investimento em cibersegurança e o avanço tecnológico dos sistemas de preservação e manutenção de dados pessoais.

Agora que a sociedade brasileira possui um mecanismo legal para elucidar o tratamento de dados, há de ser pensado como os municípios poderão fazer valer a lei e cumpri-la, com ajuda de todo sistema estatal, que precisa, invariavelmente, proporcionar medidas e instrumentos de tratamento de dados.

Nesse escopo, surge uma brilhante elucidação de Fabrício Motta, quando trata do encarregado de proteção de dados (DPO):

"Para a realidade pública, é preciso que exista uma normativa devidamente publicada que descreva as atribuições e os poderes deste profissional. É recomendável que ele se reporte diretamente à autoridade máxima da organização, que tenha acesso irrestrito aos departamentos administrativos para desenvolver os trabalhos relacionados à sua área de atuação e que possua independência funcional suficiente para tomada de decisões sobre os assuntos de proteção de dados" (MOTTA, 2020).

Não só individualizando as atribuições, em relevantíssimo exemplo, confere-se a estipulação de decreto municipal elaborado pelo sistema legislativo do município de São Paulo, o maior do Brasil, revelando as funções do controlador-geral do município, que também figura como o encarregado de proteção de dados pessoais, isto é, sendo a pessoa indicada pelo chefe do Poder Executivo para servir como canal de comunicação entre a prefeitura do Município de São Paulo, os titulares dos dados e Autoridade Nacional de Proteção de Dados (ANPD).

Guardadas as devidas proporções, possíveis exemplos a seguir encontram-se nas medidas tomadas pela Controladoria-Geral do Município de São Paulo, que apresentou em setembro de 2020, oficialmente, as *Diretrizes para o Programa de Privacidade e Proteção de Dados da Prefeitura do Município*

de São Paulo (SÃO PAULO, [202-b]), bem como *Cartilha de boas práticas de proteção de dados e privacidade* (SÃO PAULO, [202-a]).

As *Diretrizes para o Programa de Privacidade e Proteção de Dados da Prefeitura Municipal de São Paulo* consistem num conjunto de orientações para a implementação dos processos referentes às obrigações estabelecidas na LGPD e no Decreto Municipal n. 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal n. 13.709, de 14 de agosto de 2018, no âmbito da administração municipal direta e indireta.

Já a *Cartilha de boas práticas de proteção de dados e privacidade* elucida condutas para proteção de dados e preservação da privacidade no exercício da função pública, de forma a preservar os direitos e garantias dos cidadãos, em conformidade com a lei e o ordenamento jurídico vigente.

Isso significa que o município de São Paulo começa a ter suporte para o acolhimento de denúncias por ilegalidade na gestão pública, por violações às diretrizes da LGPD, bem como aos deveres/princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6.º, da Lei n. 13.079/18,) por meio de seu principal canal de ouvidoria.

E assim, para fazer dar certo a aplicação efetiva da LGPD no âmbito público, sobretudo na competência municipal, é capital traçar planejamento, ou seja, elencar os pontos de base para procedimento, manutenção e tratamento de dados, criar uma cultura de adequação à LGPD, utilizando-se dos conhecidos instrumentos da LAI e do Marco Civil da Internet (MCI), bem como ratificar o treinamento de funcionários, capacitando-os não só para gestão de dados, como também para agir em caso de vazamento de dados.

3 CONSIDERAÇÕES FINAIS

Pelo que foi exposto, a LGPD ainda é, de certa forma, para os entes públicos, uma pedra bruta – e de muito valor – que precisa ser lapidada dia após dia, mas que tem seu caminho de sucesso facilitado por existir forte base na GDPR – a lei europeia – e uma maior movimentação na iniciativa privada.

A lei encontra-se vigente e aplicável aos entes públicos – embora em distintas proporções, também suscetível à aplicação de multas e medidas coercitivas a serem avaliadas pela ANPD. Sua relevância é enorme, haja vista que influencia a evolução tecnológica de todo um sistema público, em que há dados pessoais (e até sensíveis) de toda uma população.

Observando de modo prático, é relevante que os entes públicos, sobretudo os municípios, contem com três pilares intensos para implementação da

LGPD em suas respectivas organizações, sendo eles: planejamento, cultura e treinamento/capacitação.

Para que surtam efeitos sérios na implementação da LGPD nos municípios – e demais organizações públicas –, é vital a cooperação entre a entidade pública e o encarregado de dados responsável, além da implementação de governança estratégica, o planejamento e a valorização dos dados pessoais, como instauração de programas de treinamento.

A cultura de minimização de coleta, a transparência no tratamento de dados da população, com as explicações sobre a finalidade específica para qual o dado é coletado e a transparência ao passar informações, podem ser os primeiros – e mais simples – passos práticos para que um município adote reais intenções de cultivar a proteção de dados.

Os impactos integradores da LGPD na sociedade são desafiadores e merecem uma atenção análoga aos demais direitos fundamentais, mesmo porque vivemos na sociedade da informação; vivemos em constante evolução digital, merecendo, para tanto, uma ágil e forte adequação.

Reitera-se: uma adequação só será possível após a adoção de organização governamental – por meio de políticas públicas e internalização da cultura de proteção de dados, visando à proteção dos cidadãos e à capacitação de encarregados, ofertando instrumento digno e minimamente tecnológico, a ponto de atender a uma sociedade tão complexa.

Por outro lado, não se pode fechar os olhos para maior dificuldade que o sistema público enfrenta frente às instituições privadas, pois detém burocracias, princípios e legislações a serem seguidas – a exemplo de licitações, mas isso não pode servir como justificativa para morosidades infundadas.

REFERÊNCIAS

ALEXANDRINO M.; PAULO V. **Direito Administrativo Descomplicado**. 27. ed. Rio de Janeiro: Forense; São Paulo: Método, 2017.

ANPD divulga relatório semestral de acompanhamento da Agenda Regulatória. **Gov.br**, 2021 disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-relatorio-semestral-de-acompanhamento-da-agenda-regulatoria#:~:text=A%20Autoridade%20Nacional%20de%20Prote%C3%A7%C3%A3o,materializar%20a%20regulamenta%C3%A7%C3%A3o%20dos%20temas. Acesso em: 26 jan. 2022.

BRASIL. Constituição [1988]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 24 jan. 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 18 maio 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jan. 2022.

CAVARIELI, Davi Valdetaro Gomes. Governança de dados e programa de *compliance* digital na administração pública: contribuições da LGPD para a integridade governamental. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e administração pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

CHAUI, Marilena. **Cidadania cultural:** o direito à cultura. São Paulo: Fundação Perseu Abramo, 2006.

IBGE. **População**. [202-?]. Disponível em https://cidades.ibge.gov.br/brasil/panorama. Acesso em: 25 de jan. de 2022.

MOTTA, Fabrício. Estruturação do cargo de DPO em entes públicos. BLUM; Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coord.). **Data Protection Officer**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020.

SÃO PAULO. **Cartilha de boas práticas de proteção de dados e privacidade**. São Paulo: Prefeitura de São Paulo, [202-a]. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/cartilhaboaspraticas2_publicacao_16_02_2021.pdf. Acesso em: 25 jan. 2022.

SÃO PAULO**. Diretrizes para o Programa de Privacidade e Proteção de Dados da Prefeitura do Município de São Paulo**. São Paulo: Prefeitura de São Paulo, [202-b]. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/DiretrizesparaoprogramadeprivacidadeeprotecaodedadosdaPrefeituraMunicipaldeSaoPaulo_publicacao15_02_2021.pdf. Acesso em: 25 jan. 2022.

UNIÃO EUROPEIA. **General Data Protection Regulation**. 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 24 jan. 2022.

11
TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS E COMPLIANCE DIGITAL

Maria Gabriela Grings
Ricardo Campos

Resumo

A transferência internacional de dados pessoais é tema pungente, presente na rotina dos agentes que realizam operações de tratamento de dados. A Lei Geral de Proteção de Dados Pessoais (LGPD) traz hipóteses específicas que permitem a sua ocorrência. Todavia, o compliance digital exigido pode depender de atuação da Autoridade Nacional de Proteção de Dados Pessoais. No interregno, a experiência europeia indica alternativas, como a elaboração de acordos de tratamento de dados pessoais e modelo de cláusulas-padrão.

Palavras-chave: transferência internacional de dados pessoais; Lei Geral de Proteção de Dados Pessoais; Autoridade Nacional de Proteção de Dados Pessoais; compliance digital; acordo de tratamento de dados pessoais; cláusulas-padrão.

1 INTRODUÇÃO

As operações de transferência internacional de dados pessoais (TID) estão no centro das atenções das autoridades de proteção de dados pessoais e dos agentes de tratamento. O intenso deslocamento de pacotes de dados torna as fronteiras nacionais fator de importância diminuta para o funcionamento da internet.

Essa constatação gera considerações acerca da proteção jurídica conferida aos dados pessoais que trafegam na rede, alguns deles classificados pelas legislações nacionais como sensíveis e outros como merecedores de tutela jurídica diferenciada, como aqueles relacionados a hipervulneráveis, como crianças e adolescentes.

Há anos o espectro jurídico busca regular as TIDs tendo como pressuposto a tutela aos direitos dos titulares e a geração de confiabilidade nos processos de tratamento de dados com elementos de estraneidade. O

maior exemplo nesse sentido é o Regulamento (UE) n. 2016/679, a GDPR, que traçou diretrizes sobre a questão que influenciaram outros ordenamentos.

Para os propósitos que aqui interessam, as disposições da LGPD serão analisadas com o intuito de averiguar como os agentes de tratamento poderão realizar TIDs que possam ser consideradas regulares e conformes.

2 TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS (TID)

O fluxo transfronteiriço de dados pessoais é fato jurídico há muito presente no cotidiano, mas que somente passou a receber maior atenção da comunidade jurídica a partir da percepção dos dados pessoais como objeto autônomo de proteção jurídica, descolado de outras figuras já conhecidas e tuteladas, como a privacidade e a intimidade.

A Europa é o nascedouro dessa percepção, pois desde a lei do estado federativo alemão de Hesse, de 1970, e da lei nacional de proteção de dados da Suécia, de 1973, a proteção aos dados pessoais é tema de diversas legislações nacionais.

A edição de uma legislação supranacional regional adveio em 1981 com a Convenção do Conselho da Europa para Proteção dos Indivíduos Face ao Tratamento Automático de Dados, a Convenção 108. Porém, o marco legislativo sobre o tema é a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC) (UNIÃO EUROPEIA, 1995). No texto, a TID já se fazia presente e calcava-se, essencialmente, na verificação do grau de proteção aos dados pessoais fornecido pelo arcabouço legal do país receptor, se condizente com o do Estado de origem dos dados, que posteriormente ficou conhecido como critério do *nível de proteção adequado* – art. 25 (1).

Alguns parâmetros através dos quais o nível de proteção oferecido pelo país terceiro seria avaliado estavam assentados na natureza dos dados, na legislação do Estado receptor e nas medidas de segurança locais – art. 25 (2). Constatada pela Comissão Europeia a ausência de proteção adequada pelo país terceiro, os Estados-membros deveriam tomar as medidas cabíveis para impedir a transferência de dados – art. 25 (4).

A doutrina informa que inovações tecnológicas que permitiam uso de técnicas mais intrusivas de coleta e tratamento de dados, aliadas à baixa uniformidade das legislações nacionais sobre o tema, teriam motivado alterações na Diretiva 95/46/EC, que culminaram na edição do Regulamento (UE) 2016/679, mais conhecido como General Data Protection Regulation (GDPR) (ANTONIALLI, 2017, p. 58).

Em paralelo, nos anos 2000, considerando o aumento da capacidade de tráfego da infraestrutura física de suporte da internet e a sua popularização, a TID foi objeto de texto legal que buscava trazer parâmetros para as transferências de dados de cidadãos situados no continente europeu para os Estados Unidos, sede das maiores empresas globais de tecnologia.

Por esta razão, o Departamento de Comércio Norte-Americano, em parceria com autoridades europeias de proteção de dados, elaborou o Safe Harbor, conjunto de diretrizes principiológicas de tratamento de dados pessoais a serem seguidas por empresas americanas que desejassem receber os dados com origem europeia. A baixa efetividade do arranjo fez com o Tribunal de Justiça Europeu o considerasse inválido, fazendo com que texto mais assertivo e detalhado fosse elaborado em substituição, o Privacy Shield.

A entrada em vigor da GDPR, no contexto das revelações de atos de vigilância estatal sobre o fluxo de dados que trafegava em servidores situados nos Estados Unidos (*deep packet inspection*), fez com que o nível de proteção aos dados pessoais transferidos, ofertado pelas empresas aderentes ao acordo, fosse questionado, o que ensejou a declaração de incompatibilidade do texto com o novo arcabouço legal europeu (UNIÃO EUROPEIA, 2020).

Após quase dois anos de lacuna legislativa, em março de 2022 foi noticiado que um novo pacto transatlântico foi acordado entre a União Europeia e os Estados Unidos sem que, por ora, maiores detalhes tenham sido divulgados sobre o teor do documento, mas apenas que:

> [...] o novo Acordo de Privacidade de Dados Transatlânticos ressalta nosso compromisso compartilhado com a privacidade, a proteção de dados, o Estado de Direito e nossa segurança coletiva, bem como nosso reconhecimento mútuo da importância dos fluxos de dados transatlânticos para nossos respectivos cidadãos, economias e sociedades (FACT..., 2022, tradução livre).

Para além dos efeitos da entrada em vigor da GDPR sobre os acordos que regulamentam a transferência de dados pessoais em nível transatlântico, a influência do novo texto europeu para qualquer legislação de proteção de dados pessoais é inconteste, tendo a Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) buscado inspiração direta e indisfarçável na GDPR.[60]

60 O parecer final da Comissão Especial da Câmara dos Deputados, ao analisar o Projeto de Lei n.º 4.060/2012 deixou claro as bases legais europeias e a importância de alinhamento legislativo com as diretrizes já estabelecidas pelo bloco, pois "Esse ponto, de a legislação do país estar de acordo com a legislação europeia, é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de data centers, mas das próprias empresas de TIC, incluindo as gigantes ponto com. Por isso, a necessidade de o Brasil possuir, sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia" (SILVA, 2018).

3 A TID E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A LGPD indica que a TID possui caráter excepcional, sendo admitida apenas para as hipóteses taxativas previstas nos incisos I a IX do art. 33. A intenção aqui não é realizar estudo minucioso e dissecado de cada uma das previsões legais autorizativas, mas sim apresentar o quadro legal aplicável e os requisitos autorizativos para as transferências internacionais de dados pessoais para que, na sequência, seja possível verificar como o compliance digital se aplica nessa seara.

Inicialmente, cumpre recordar que, para os dados pessoais, prevalece a legislação do seu país de origem (*data origen country*), mesmo depois de transferidos, o que torna a posição geográfica do local de tratamento dos dados pessoais fator de menor relevância, já que deve ser assegurado que os parâmetros que orientam a atividade de tratamento no país em que foram coletados sejam cumpridos pelo agente de tratamento, controlador ou operador.[61]

Apesar das diversas opções legais contidas nos incisos do art. 33 para TID, verifica-se a inexistência de hierarquia entre os dispositivos, o que sinaliza diferença entre a LGPD e a GDPR. Por lá a prolação de decisão de adequação pela Autoridade Nacional faz com que nenhuma salvaguarda adicional tenha que ser assegurada. Na sua ausência, o agente de tratamento deve buscar outros meios legais para justificar a TID, sendo que, ainda assim, entende-se que deve ser assegurado nível de proteção adequado, evidenciando a importância central do critério (MARQUES, 2021, p. 313).

O inciso I do art. 33 consagra o critério internacionalmente aceito do país ou organização internacional com grau de *proteção adequada*. A sua existência dispensa outros requisitos, estando plenamente justificada a transferência.

A avaliação sobre o arcabouço legal do país receptor dos dados, pressuposto para aferição do nível de proteção conferido, é de competência da Autoridade Nacional de Proteção de Dados (ANPD), que deverá levar em conta os critérios elencados nos incisos I a VI do art. 34:

> [...] as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; a natureza dos dados; a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; a adoção de medidas de segurança previstas em regulamento; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e outras circunstâncias específicas relativas à transferência (BRASIL, 2018).

61 Essa característica faz com que os textos legais sobre proteção de dados pessoais sejam classificados como *normas de extensão* ou *leis de aplicação imediata*, dispensando o habitual uso da regra de conflito de Savigny para definição da lei aplicável em demandas internacionais plurilocalizadas (MIAJA DE LA MUELA, 1977, p. 25).

Imagina-se que a ANPD ao analisar o nível de proteção adequado, tendo como parâmetro a LGPD, considere os países pertencentes à União Europeia e aqueles que já obtiveram tal chancela das autoridades de proteção de dados europeias, como Argentina e Uruguai, como adequados, a priori, à legislação nacional.

Na GDPR, a decisão a respeito da adequação de um país é calcada em critérios objetivos, com destaque para o primado do estado de direito (previsão e respeito aos direitos e garantias individuais) e à legislação em geral, a existência de autoridade de controle independente e os compromissos internacionais assumidos pelo país terceiro ou pela organização, especialmente os relacionados à proteção de dados pessoais [art. 42 (2)].

A partir do Caso Schrems (II) entende-se que o "nível de proteção adequado" do país receptor seria o que se apresenta como "substancialmente equivalente", entendido como aquele em que meios administrativos e judiciais eficazes "para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados" estejam à disposição do titular dos dados (UNIÃO EUROPEIA, 2020).

Não constou expressamente na LGPD a possibilidade de revogação da decisão de reconhecimento de existência de nível de proteção adequado, o que nos parece plenamente viável, ante o grau de dinamicidade da legislação de qualquer país receptor de dados que pode, alteradas certas premissas, não mais ser considerada como suficiente para salvaguardar os dados pessoais dos titulares estrangeiros, tendo como premissa avaliativa os direitos e garantias estabelecidos na LGPD.

O parágrafo único do art. 33 possibilita que pessoas jurídicas de direito público possam, de acordo com suas competências legais, solicitar à ANPD que avalie o nível de proteção conferido aos dados pessoais por país ou organismo internacional (BRASIL, 2018).

O inciso II do art. 33 possibilita ao controlador de dados realizar a TID para países que não apresentem "nível de proteção adequado" chancelado via adoção de mecanismos específicos, calcados em instrumentos privados, como a inserção de "cláusulas contratuais específicas para determinada transferência", a elaboração de "cláusulas-padrão contratuais", a observância às "normas corporativas globais" ou a adoção de "selos, certificados e códigos de conduta regularmente emitidos" (BRASIL, 2018).

É certo que tais mecanismos devem estar assentados na principiologia e na observância aos direitos previstos na legislação de referência, a LGPD, sob pena de serem considerados inválidos. A análise de compatibilidade é de responsabilidade da ANPD, como indica o caput do art. 35.

Cláusulas que autorizem TID individualizadas podem se apresentar como mecanismo de difícil aplicabilidade prática, uma vez que qualquer alteração no seu conteúdo deve ser avaliada pela ANPD, gerando morosidade e sobrecarga de trabalho para esse órgão. Não por outro motivo, objeto de

maior atenção nesse tema são as cláusulas-padrão e as normas corporativas globais, as *binding corporate rules* (BCR), da experiência europeia, idealizadas para proporcionarem transferências de dados entre empresas do mesmo grupo econômico.

As cláusulas-padrão foram objeto de atualização pela Comissão Europeia em 2021, que disponibilizou modelo de cláusulas-padrão a serem inseridas em contratos entre controladores e operadores de dados nas hipóteses de tratamento de dados no contexto de TID (UNIÃO EUPEIA, 2021). O European Data Protection Board (EDPB) edita orientações (*guidelines)* para normas corporativas. Ambos os documentos, sem dúvidas, servirão como material orientativo para a Autoridade Nacional, dada a similitude entre os textos legais.[62]

A adoção de selos, certificados e códigos de conduta regularmente emitidos como uma das hipóteses autorizativas de TID foi novidade apresentada pela GDPR em comparação com a Diretiva 95/46/EC. Nela privilegia-se a esfera privada que amplia, amadurece e desenvolve sua autonomia setorial ao fixar standards de proteção de dados, ao mesmo tempo em que atesta à coletividade que os dados estão sendo tratados de uma certa maneira que observa critérios e padrões técnicos pré-determinados.

Por esse motivo, para alguns, tal atuação seria expressão do modelo de autorregulação regulada (SZINVELSKI, 2020, p. 150), dada a existência de padrões legais a serem seguidos e o acompanhamento contínuo da autoridade nacional especializada. A afirmação ganha reforço diante do § 3.º do art. 35 da LPGD, que prevê que a ANPD poderá designar organismos de certificação para estabelecimento das normas privadas autorizadoras da TID, que serão fiscalizadas pela autoridade nacional. Caso sejam considerados como em desacordo com a legislação, poderão ser revistos ou anulados, conforme § 4.º do art. 35 da LGPD.

Imagina-se que as medidas extremas somente serão aplicadas após a instauração de processo administrativo e com direito de exercício do devido processo legal pelo organismo de certificação. Parece-nos salutar que as organizações filiadas que se valeram do procedimento até então certificado e chancelado pela ANPD, caso desejem, possam participar do feito na qualidade de terceiros interessados. Da mesma maneira, importa a definição da eficácia

62 Inexiste impedimento de que, para além das orientações gerais emanadas pelas autoridades nacionais, entidades elaborem cláusulas-padrão específicas para setores altamente especializados e complexos, tendo como premissa as diretrizes gerais das autoridades nacionais. É o que ocorre, por exemplo, a partir da experiencia da Baltic and International Maritime Council (BIMCO) *e a* The Federation of National Associations of Ship Brokers and Agents (FONASBA) dos Estados Unidos, pois "[...] impõe-se na indústria marítima, cuja boa parte dos contratos possuem elementos de internacionalidade, uma especial atenção na transferência internacional de dados e a regulamentação dessa, devendo as instituições respeitarem tais normas" (PAIVA; OLIVEIRA; NABUCO, 2021, p. 2).

temporal do ato administrativo que determine a revisão da previsão dita em desconformidade, ante a necessidade de salvaguardar a segurança jurídica e as justas expectativas dela decorrentes.

Segundo Lachaud (2018, p. 245), a certificação é avaliação de conformidade, a partir da qual as organizações voluntariamente se submetem à entidade externa terceira, um órgão certificador, para obtenção de chancela de certificação. Ainda segundo o autor, ela pode ser expressão da autonomia privada, como também da corregulação entre a esfera pública e a privada (como ocorre com a proteção de dados, em que a autoridade estatal age como aferidor dos parâmetros nos quais se assenta a certificação), existindo ainda a possibilidade de atuação estatal exclusiva.

O emprego de certificações, em sentido amplo, denota adoção de postura proativa e preventiva das organizações que se engajam na obtenção de atestados de adequação a parâmetros reconhecidos e prestigiados, com os emitidos pela International Organization for Standartization (ISO), entre outros. Eles refletem a internacionalização da sociedade e a necessidade de adoção de padrões de alta credibilidade que possam ser mundialmente reconhecidos como de alta eficiência e elevada idoneidade técnica.

Outro aspecto presente quando se fala a respeito de selos e certificações reside na aparência de confiabilidade e na credibilidade que a autoridade certificadora deverá gozar, pois o intuito de uso dessas figuras está intimamente relacionado à geração de confiança sobre a instituição certificadora.

A LGPD inda permite que haja TID quando ela for necessária para cooperação jurídica entre órgãos de inteligência, investigação e persecução, e para atos calcados em acordos de cooperação internacional firmados pelo país (art. 33, III e VI). Ambas as previsões reforçam o compromisso das autoridades brasileiras com os entes de outros países na persecução do interesse público e auxílio mútuo, bases da cooperação jurídica internacional (BRASIL, 2018).

Não se pode imaginar como atos de extradição, de cumprimento de cartas rogatórias e homologação de sentenças estrangeiras poderiam ocorrer sem atos de transferência de dados pessoais entre Estados. Apenas importa rememorar que a LGPD não se aplica ao tratamento de dados pessoais realizado para segurança pública, defesa do Estado ou persecução penal, que será objeto de normativa própria.

Sentido assemelhado, calcado na busca ideal do bem coletivo, é vislumbrado no inciso VII do art. 33, que permite que a TID ocorra para execução de políticas públicas ou atribuição legal do serviço público, mas apenas e somente quando a internacionalização do dado for *necessária*, assegurada a publicização prevista no art. 23, inc. I.

A preservação da vida e da incolumidade pública do titular ou de terceiro foi incluída como uma das hipóteses autorizadoras de TID (art. 33,

IV), ante a natural prevalência da vida e da integridade física sobre outros bens jurídicos, incluindo a proteção aos dados pessoais.

A centralidade da ANPD para as operações de TID é reafirmada pela possibilidade contida no art. 33, V, de que o órgão poderá *autorizar a transferência*. O dispositivo analisado isoladamente parece conferir permissivo genérico para atuação da autoridade nacional para o tema. Contudo, acredita-se que a significativa discricionariedade permitida pode ser mitigada quando da interpretação da LGPD como um todo, em especial a principiologia presente nos incisos do art. 6.º, que determina que o tratamento de dados pessoais deve pautar-se nas diretrizes da *boa-fé, da necessidade, da adequação, da finalidade e da responsabilidade*, as quais se fazem ainda mais importantes e incisivas no contexto de TID, dados os riscos inerentes a esse tipo de operação.

A base legal do consentimento do art. 7.º, I, faz-se igualmente presente como hipótese autorizativa de TID. Para além dos atributos definidos no art. 5.º, XII, aptos a caracterizar o consentimento para tratamento de dados pessoais ("manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"), quando da presença de TID ele deve ser "específico e destacado".[63]

Não é objeto do presente artigo análise detalhada das vicissitudes envolvendo o consentimento como base legal para tratamento de dados pessoais, que renderia estudo em apartado. Vale apenas destacar que a disposição exige participação ativa do titular, que deverá autorizar especificamente a TID, e maiores cuidados do agente de tratamento ao obter tal espécie de consentimento, que poderá ser revogado a qualquer momento, uma vez que também na TID incide o contido no art. 8.º, § 5.º, da LGPD.

As especificidades que rondam o tema do consentimento como base legal para TID fazem com que, operacionalmente, não seja "[...] recomendada a utilização de consentimento como mecanismo de transferência internacional, diante da complexidade de assegurar a continuidade das atividades de tratamento em caso de revogação desse consentimento e da própria obtenção de consentimento válido diante dos múltiplos requisitos legais" (LEONARDI, 2021, p. 296). O consentimento seria fundamento mais teórico do que prático para TID.

Como última hipótese do rol do art. 33, o inciso IX permite a TID quando necessária para "[...] cumprimento de obrigação legal ou regulatória pelo

63 Para Bruno Bioni (2020, p. 189): "uma das maneiras de extrair essa *carga participativa maior* do titular dos dados seria adotar mecanismos que chamasse mais a sua atenção. Deve haver um alerta que *isole* não só o dever-direito de informação, como, também, a declaração de vontade, colando-a à situação na qual é exigido o consentimento específico. Isso vai muito além de cláusulas contratuais destacadas que já são mencionadas como uma forma de obter o consentimento trivial e não específico. Todo o processo de tomada de decisão é (com o perdão de ser prolixo), específico e deve ser *pontual*. Da informação até o aceite do titular do dado".

controlador; para execução de contrato ou de procedimentos preliminares contratuais de interesse do titular, a pedido seu, e para exercício regular de direitos em processos judiciais ou administrativos" (BRASIL, 218), reprisando a redação dos incisos II, V e VI do art. 7.º.

A redação da previsão equivale ao contido no artigo 49, 1(c) e (e), da GDPR, usualmente interpretado de forma restritiva, com recomendação do EDPB de realização do *teste de necessidade*, semelhante ao empregado para verificação de existência da base legal do *legítimo interesse*.

Apenas a existência de conexão substancial e profunda entre os dados e o objeto do contrato permite o emprego dessa base legal, como a operação de TID realizada por um agente de viagens para reserva de hotel ou passeios no local de destino. De acordo com a entidade, essa previsão não poderia ser utilizada como fundamento para as transferências realizadas por entes públicos, ou ainda para fundamentar a transferência de dados pessoais do setor de recursos humanos de uma empresa para terceirizada localizada em outro país, já que a operação não está relacionada com a execução do contrato de trabalho em si (EUROPEAN..., 2016).

4 COMPLIANCE DIGITAL

A apresentação sintética das hipóteses de TID realizada no tópico anterior já foi capaz de indicar dois dos aspectos mais importantes inerentes ao tema: o primeiro é a complexidade que permeia várias das questões envolvendo TID em conjunto com certo grau de incerteza, provocado por tema tão novo no contexto legal brasileiro, quando visto pela ótica da proteção de dados pessoais. O segundo é o papel crucial desempenhado pela ANPD para a efetividade das disposições da LGPD sobre TID.

Parcela significativa das previsões dependem de atuação ativa da autoridade nacional, a quem o legislador atribuiu variados encargos: concessão da chancela de oferecimento de *nível de proteção adequado* para países e organismo internacionais (art. 34); a aprovação de *cláusulas contratuais específicas para determinada transferência*, definição de conteúdo de *cláusulas-padrão contratuais*; verificação de *normas corporativas globais*, *selos*, *certificados e códigos de conduta* (art. 35, caput) e designação de *organismos de certificação*, que sob sua fiscalização continua, realizarão a atividades dispostas no caput do art. 35 (art. 35, § 3.º e 4.º) (BRASIL, 2018).

Apesar de ter sido criada em 2018, a ANPD foi formalmente instituída somente no final de 2020, de forma paulatina, dada a necessidade de estruturação completa da entidade, vinculada à Presidência da República. Com a nomeação dos diretores, antes mesmo do estabelecimento do Regimento Interno e do Regulamento do Processo Administrativo Sancionador, a ANPD divulgou sua agenda regulatória.

A Portaria n. 11, de 27 de janeiro 2021, indicou os projetos a serem desenvolvidos no biênio 2021/2022 e o grau de prioridade de cada um deles, classificados em fase 1, fase 2 e fase 3. A regulamentação da TID foi indicada como integrante dos projetos de fase 2, o que significa que os trabalhos terão início somente a partir do segundo semestre de 2022.

Considerando a conjuntura atual, alguns entendem que os artigos 34, 35, caput e §§ 3.º e 4.º contêm normas de eficácia limitada, "[...] o que na prática significa que os agentes de tratamento somente podem ser cobrados (e punidos) em relação a seus deveres relativos à transferência internacional de dados uma vez que a ANPD tenha aclarado as regras do jogo" (CHAVES, 2021, p. 315).

Efetivamente, sendo as disposições dependentes de edição de regulamentação a ser elaborada por órgão pré-estabelecido e nomeado, conhecido desde a promulgação da LGPD – a Autoridade Nacional de Proteção de Dados Pessoais –, sem que o ente tenha, por ora, editado a normativa que lhe foi atribuída pelo legislador nacional, os agentes de tratamento não podem ser responsabilizados com fundamento em dispositivos não plenamente incidentes.

Dessa forma remanesce a questão: quais as diretrizes a serem observadas para o compliance digital nas operações de transferência internacional de dados?

Inicialmente, cabe recordar que o compliance busca o agir de acordo com conjunto pré-determinado de regras, procedimentos e métodos internos de conformidade. Ainda que, no seu surgimento, o termo estivesse conecto com a área empresarial, e sua transposição para o campo jurídico tenha se iniciado pelo viés do combate à corrupção, atualmente ele atravessa diversos ramos, incluindo o direito digital e a proteção de dados pessoais, tratados em meio físico ou digital.

Na esfera da proteção de dados pessoais, entende-se que o agir em conformidade se relaciona com a noção de responsabilidade, calcada no emprego das melhores técnicas e instrumentos organizacionais internos, definidos a partir de conjunto variado de fatores, tais como a natureza do dado pessoal tratado, as opções tecnológicas disponíveis e os riscos de violação a direitos e garantias fundamentais potencialmente colidentes. Outro aspecto que não pode ser descurado é a necessidade de atualização contínua das técnicas utilizadas, ante a evolução constante dos meios tecnológicos.

A lacuna regulatória, a ser preenchida pela ANPD em breve, não pode ser compreendida como subterfúgio para operações irregulares de TID ou ainda para que operações de transferência internacional necessárias para a rotina de determinado ente deixem de ser realizadas, por excesso de zelo.

O compliance no tratamento digital de dados pessoais pode ser buscado e atingido quando o agente de tratamento se vale das demais bases legais para fundamentar a operação de TID.

Nesse sentido, há possibilidade de elaboração de acordo de tratamento de dados pessoais (*data processing agreement* – DPA) entre controlador e operador, com inserção de dispositivo que indique de maneira expressa que, caso sejam realizadas operações de transferência internacional de dados, elas somente ocorrerão se presentes um dos requisitos legais previstos no rol do art. 33 da LGPD que independem de atuação prévia da ANPD para terem eficácia plena e imediata, como as hipóteses dos incisos III, IV, VI, VII, VIII e IX do art. 33.

A similitude em diversos aspectos entre a GDPR e a LGPD permite que se avente outra possibilidade: o uso das cláusulas-padrão elaboradas e publicadas pela autoridade europeia, a serem inseridas nos contratos firmados entre os responsáveis pelo tratamento de dados e os operadores localizados em outros país que não proporcionem *nível de proteção adequado*, principal mecanismo de TID no sistema europeu.[64] É certo que tal opção pressupõe as devidas e necessárias adaptações do texto sugerido ao contexto legal brasileiro.

A intenção da comissão de apresentar sugestão de modelo que possa facilitar TID, ao mesmo tempo em que são assegurados os direitos dos titulares dos dados transferidos, é notória.

O Considerando 12 indica que "[...] os titulares dos dados devem poder invocar e, quando necessário, fazer cumprir as cláusulas contratuais-tipo enquanto terceiros beneficiários" e "as cláusulas contratuais-tipo devem exigir que o importador de dados informe os titulares dos dados de um ponto de contacto e dê rapidamente resposta a quaisquer reclamações ou pedidos", enquanto que o Considerando 13 determina que "[...] o importador de dados deve poder proporcionar aos titulares dos dados a oportunidade de procurar obter reparação junto de um organismo independente de resolução de litígios, sem custos" (UNIÃO EUROPEIA, 2021).

As dezoito cláusulas sugeridas pela Comissão Europeia, divididas em quatro seções (dispositivos gerais, obrigações das partes, legislação local e obrigações em caso de acesso por parte de autoridades públicas e disposições finais), abordam questões variadas inerentes às operações de TID. Atuam, por exemplo, na densificação de variados princípios elementares para o tratamento de dados pessoais, como *finalidade*, *transparência*, *exatidão e minimização dos dados*, *limitação da conservação* e *segurança do tratamento*, que devem ser observados tanto nas transferências realizadas entre responsáveis (controlador-operador), quanto entre esses e eventuais subcontratados, e entre subcontratados.

64 Importa destacar que as referidas cláusulas são sugestões de encaminhamento para a questão, não havendo impedimento para que as partes elaborem outros dispositivos contratuais, na condição de que não colidam com as cláusulas-padrão e que não impliquem em prejuízos aos direitos e liberdades fundamentais dos titulares dos dados – cláusula 2 (a).

A preocupação com o acesso de autoridades públicas locais aos dados pessoais transferidos reflete o julgado no Caso Schrems II, com a inserção de variadas obrigações a serem suportadas pelo importador dos dados caso receba pedido vinculativo de autoridade pública ou tome conhecimento do seu acesso aos dados transferidos.

Destaque para o dever de notificação ao exportador sobre o ocorrido – cláusula 15.1(a) – e a aceitação, conforme a cláusula 15.2(a), de dever de controle de

> [...] legalidade do pedido de divulgação, em particular a questão de saber se este se mantém nos limites dos poderes concedidos à autoridade pública requerente, e em contestar o pedido se, após uma avaliação minuciosa, concluir que existem fundamentos razoáveis para considerar que o pedido é ilegal nos termos da legislação do país de destino, das obrigações aplicáveis ao abrigo do direito internacional e dos princípios de cortesia internacional.

Entende-se que as apreensões subjacentes à inserção de tais cláusulas (tratamento inadequado de dados pessoais pelos agentes importadores diretos e subcontratados, e acesso de autoridades públicas locais ao material, em desconformidade com os ditames legais incidentes, aqueles que tutelam o titular dos dados pessoais) são compartilhadas por outras autoridades nacionais de proteção de dados pessoais, não havendo empecilho para que a elaboração europeia não possa servir de norte para os agentes brasileiros até que haja pronunciamento da ANPD sobre o tema. Não causará espanto caso o material futuro produzido pela autoridade nacional muito se assemelhe ao modelo europeu, pelas razões já expostas.

5 CONCLUSÃO

Diante da indisfarçável importância da TID na sociedade contemporânea, o estudo das hipóteses legais que no sistema jurídico brasileiro autorizam a sua realização, com especial atenção às disposições do art. 33 da LGPD, é medida que se impõe.

Tendo em vista a necessidade de regulamentação pela ANPD de várias das previsões da LGPD que permitem a transferência internacional de dados pessoais, prevista para ocorrer no futuro próximo, o presente artigo voltou-se para a normativa europeia e sua irrefutável força inspiradora para a legislação nacional de proteção de dados pessoais, na busca por soluções de compliance digital para TID.

A confecção de acordo de tratamento de dados pessoais em que conste expressamente que a TID ocorrerá apenas se em conformidade com a legislação incidente, com destaque para as disposições dos incisos III, IV, VI, VII, VIII e IX do art. 33 da LGPD e o acréscimo de cláusulas-padrão

nos pactuados entre agentes de tratamento de dados pessoais, nos moldes da experiência europeia, são alternativas viáveis até que a ANPD tenha oportunidade de se debruçar sobre o tema e editar as diretrizes necessárias para a eficácia plena de todas as normas versando sobre TID na LGPD.

REFERÊNCIAS

ANTONIALLI, Dennys Marcelo**. A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais**. 2017. Tese (Doutorado) – Faculdade de Direito de São Paulo, Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2134/tde-18112020-144100/pt-br.php. Acesso em: 25 mar. 2022.

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 mar. 2022.

CHAVES, Luís Fernando Prado. Da transferência internacional de dados. *In*: MALDONADO, Viviane; BLUM, Renato (org). **LGPD – Lei Geral de Proteção de Dados Pessoais Comentada**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf. Acesso em: 25 mar. 2022.

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. **The White House**, 25 mar. 202. Disponível em https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/. Aceso em: 26 mar. 2022.

LACHAUD, Eric. The general data protection regulation contributes to the rise of the certification as a regulatory instrument. **Computer Law & Security Review**, v. 34, n. 2, abr. 2018.

LEONARDI, Marcel. Transferência internacional de dados pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (org). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

LIMBERGER, Têmis (em coop). *T*ransnacionalização e selos de qualidade em proteção de dados: um novo campo de estudo na era digital. **Revista dos Tribunais**, v. 1020/2020, out. 2020.

MARQUES, Fernanda Mascarenhas. O regime de transferência internacional de dados da lgpd: delineando as opções regulatórias em jogo. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (org). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MIAJA DE LA MUELA, Adolfo**. De la territorialidade de las leyes e la nueva técnica del derecho internacional privado**. Valladolid: Universidad, 1977.

PAIVA, Marcella; OLIVEIRA, Bianca; NABUCO, Luiza. Proteção de dados e arbitragem marítima internacional: a regulação da transferência transnacional de dados. **Revista de Direito e as Novas Tecnologias**, v. 10, jan./mar. 2021.

SILVA, Orlando. Relatório da comissão especial destinada a proferir parecer ao projeto de lei no 4060, de 2012. **Câmara dos Deputados**, 2018. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%-3D%3E+PL+4060/2012. Acesso em: 24 mar. 2022.

SZINVELSKI, Mártin M. (em coop). Transnacionalização e selos de qualidade em proteção de dados: um novo campo de estudo na era digital. **Revista dos Tribunais**, v. 1020, out. 2020.

THE GLOBAL COMPACT. **Who Cares Wins**. 2004. Disponível em: https://www.unepfi.org/fileadmin/events/2004/stocks/who_cares_wins_global_compact_2004.pdf. Acesso em: 10 ago. 2022.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2021/914 da Comissão de 4 de junho de 2021**. Relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021D0914. Acesso em: 5 set. 2022.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.** Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 5 set. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça da Corte Europeia. **Decisão C311/18, de 16 de setembro de 2020**. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18. Acesso em: 5 set. 2022.

12
APONTAMENTOS ACERCA DA CONSTITUCIONALIDADE DO ART. 52, X, XI, XII E § 3.º DA LEI N.º 13.709, DE 14 DE AGOSTO DE 2018 (LEI GERAL DE PROTEÇÃO DE DADOS): CONSIDERAÇÕES À LUZ DO PRINCÍPIO REPUBLICANO E DA CONTINUIDADE DO SERVIÇO PÚBLICO

Verena Iannino Soares Rolo
Rafael Felgueiras Rolo

"Il diritto è un apparato simbolico che struttura un'organizzazione sociale anche quando si sa che alcune sue norme sono destinate a rimanere inapplicate" (RODOTÀ, 2008).

Resumo

O artigo se propõe a contribuir para o debate a respeito da constitucionalidade das sanções aplicáveis à administração pública, nos termos do art. 52, X, XI, XII e § 3.º, da LGPD. O artigo é dividido em três partes. Primeiramente, apresenta-se contextualização da Lei n.º 13.709/2018 e das sanções introduzidas pela Lei n.º 13.853/2019. Em segundo lugar, apresenta-se algum adensamento acerca dos parâmetros considerados relevantes para a análise da constitucionalidade das sanções aplicáveis ao Estado, nos termos da LGPD. Por fim, analisam-se se as sanções previstas na LGPD são, de fato, compatíveis com os parâmetros normativos considerados.

Palavras-chave: proteção de dados; constitucionalidade; sanções; administração pública.

1 CONSIDERAÇÕES INICIAIS: A LEI GERAL DE PROTEÇÃO DE DADOS E AS SANÇÕES APLICÁVEIS À ADMINISTRAÇÃO PÚBLICA NO CONTEXTO DOUTRINÁRIO.

A Lei Geral de Proteção de Dados, instituída pela Lei n.º 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1.º), possuindo como fundamentos: (a) o respeito à privacidade; (b) a autodeterminação informativa; (c) a liberdade de expressão, de informação, de comunicação e de opinião; (d) a inviolabilidade da intimidade, da honra e da imagem; (e) o desenvolvimento econômico e tecnológico e a inovação; (f) a livre iniciativa, a livre concorrência e a defesa do consumidor; (g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2.º) (BRASIL, 2018).

A proteção de dados pessoais, como dimensão diretamente relacionada ao desenvolvimento e à defesa de direitos de personalidade, ainda mais no contexto da atual proliferação de *hubs* técnico-tecnológicos a partir dos quais dados pessoais são transmitidos e, por conseguinte, tratados, impõe considerar a centralidade da novel legislação para a afirmação, não somente de alguma dimensão intangível de dignidade humana (entendida essa intangibilidade com toda a carga de ambiguidade que lhe pode ser assegurada), mas também, e mais especialmente, para os fins de produção e conformação das subjetividades contemporâneas à luz das possibilidades estruturais oferecidas pela estrutura descentralizada da internet. Ainda que a LGPD não tenha aplicação exclusiva no âmbito das redes digitais, infere-se naturalmente que é no contexto de democratização do acesso à internet que ela ganha seus ares mais dramáticos, isto é, torna-se mais necessária à medida que a informação é desmaterializada (BIONI, 2020, p. 7).

Considerando o hercúleo – e por vezes inglório – objetivo de regulamentar as trocas de dados pessoais, em meio àquilo que Clare Birchall (2017) denomina de *Shareveillance*, isto é, uma economia política da informação a partir da qual o consumo de dados compartilhados e a própria produção de dados para compartilhamento são atividades capturadas em favor de um agenciamento capaz de produzir subjetividades tanto vigilantes quanto vigiadas, tanto produtoras de conteúdo quanto alvos ou vítimas do conteúdo produzido, deve-se reconhecer a profunda mudança de práticas imposta pela Lei Geral de Proteção de Dados.

O grande desafio associado à implementação da LGPD está diretamente vinculado à pluralidade de realidades e contextos sociais nos quais a legislação deverá necessariamente incidir.

A respeito, conferir o pensamento de Souza, Magarini e Ccarneiro (2020, p. 44):

> Fato é que hoje o compartilhamento de dados ocupa um papel de destaque nas mais diversas relações. Em um contrato de compra e venda firmado na obtenção de produtos em uma farmácia, por exemplo, se o atendente requerer o cadastro e o CPF do consumidor, já existem dados sendo coletados, armazenados e utilizados. Caso este armazenamento seja feito em uma nuvem ou em um programa com conexão à Internet, o tratamento dos dados já será on-line. Se pararmos para refletir, são poucas as situações cotidianas em que não ocorre o fluxo de dados.

Tais mudanças afetam o cidadão tanto quanto as grandes corporações ou mesmo o próprio Estado. O conceito legal empregado para a definição dos "agentes de tratamento" (os chamados controladores e operadores) é genérico o suficiente para se subsumir a uma série de diferentes realidades, o que impõe, necessariamente, a devida consideração dos ditames legais, à luz das realidades existentes e da gramática jurídica que cada realidade tanto impõe como pressupõe. Afinal, nos termos da lei em comento, (a) controlador é, genericamente, toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ao passo que (b) operador é, também de modo bastante amplo, toda pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5.º, VI e VII) (BRASIL, 2018).

Assim, qualquer sujeito, seja ele pessoa natural ou jurídica, que se encontrar no contexto de realizar tratamento de dados (assim entendida 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 – art. 5.º, X, LGPD) em face de pessoa física e cuja atividade não se enquadre diretamente nos termos das exceções do art. 4.º da LGPD (exceções que, segundo se entende, devem ser interpretadas restritivamente), sujeita-se necessariamente aos ditames da legislação.

Especialmente naquilo que diz respeito à administração pública, a Lei Geral de Proteção de Dados soma-se mais diretamente à Lei de Acesso à Informação (Lei n.º 12.527, de 18 de novembro de 2011 – LAI) e ao Marco Civil da Internet (Lei n.º 12.965, de 23 de abril de 2014) para compor o marco regulatório aplicável ao poder público naquilo que diz respeito à política informacional aplicada ao Estado e suas relações com os particulares.

Destaque-se que, formando uma espécie de microssistema de proteção de dados, a LGPD, a LAI e o Marco Civil compõem um todo orgânico e que deve ser interpretado em conjunto, inclusive à luz do ordenamento constitucional e das demais disposições legais aplicáveis, com especial destaque, neste momento, para o art. 6.º, do Marco Civil da Internet, cujo teor é o seguinte: "Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet,

seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural" (BRASIL, 2014).

Tendo em mente esse liame de coerência entre, de um lado, a LGPD, a LAI e o Marco Civil, e de outro, a afirmação de um regime jurídico-administrativo que impõe à administração pública certas prerrogativas necessárias ao desempenho de suas funções mais essenciais (MELLO, 2021), causa espécie a severidade das sanções aplicáveis ao Estado, nos termos do art. 52, X, XI, XII e § 3.º, da LGPD.

Nos termos dos dispositivos em comento:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019). [...]
>
> § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019) [...]
>
> § 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)
>
> I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)
>
> II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018).

Ora, ainda que se entenda minimamente correto sugerir a impossibilidade de deferência acrítica às máximas aplicáveis a esse regime de direito administrativo, acerca da "supremacia" e "indisponibilidade" do denominado interesse público, ainda assim não se poderia concordar que a solução recairia na hipótese ingênua (ou, talvez, simplesmente mal-intencionada) de sugerir

que a proteção que se deve conferir à noção de interesse público seria, hoje, algo a ser superado ingenuamente ou a qualquer custo (SANTOS, 2021).

Se assim é, como se poderia pretender uma aplicação adequada das sanções: (a) de suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (b) de suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; ou mesmo de (c) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, em face da administração pública?

Perceba-se a gravidade do tema. Afinal, segundo o art. 53, da LGPD, a Agência Nacional de Proteção de Dados deverá definir, por meio de regulamento próprio e específico acerca das sanções aplicáveis às infrações previstas na Lei n.º 13.709/2018, dependente de consulta pública a respeito, acerca das metodologias que orientarão o cálculo do valor-base das sanções de multa.

Sem adentrar num caso específico, a sequência deste artigo proporá alguns parâmetros, ainda preliminares, para a construção de uma solução hermenêutica conforme a Constituição para o problema associado às sanções previstas no art. 52, X, XI, XII e § 3.º, da LGPD, dentre os quais o princípio republicano e a premissa sistêmica em favor da continuidade dos serviços públicos.

2 PARÂMETROS PARA A CONSIDERAÇÃO DAS SANÇÕES PREVISTAS NO ART. 52, X, XI, XII E § 3.º, DA LGPD: A EXISTÊNCIA DO REGIME JURÍDICO-ADMINISTRATIVO, A CRÍTICA AO CONCEITO DE INTERESSE PÚBLICO E UMA TOMADA DE POSIÇÃO

A sugestão quanto à existência de um regime jurídico-administrativo é nota tradicional do Direito Administrativo brasileiro. Fincada essencialmente na doutrina de Celso Antonio Bandeira de Mello, em especial em seu artigo publicado em 1967 na Revista de Direito Público, intitulado de "O conteúdo do regime jurídico-administrativo e seu valor metodológico", a consolidação dessa noção é tão essencial à disciplina que se deve partir, neste momento, da seguinte consideração seminal:

> Só se pode, portanto, falar em Direito Administrativo, no pressuposto de que existam princípios que lhe são peculiares e que guardem entre si uma relação lógica de coerência e unidade compondo um sistema ou regime: o regime jurídico-administrativo (MELLO, 1967, p. 8; MELLO, 2021, p. 46).

Atendendo à inspiração juspositivista da doutrina de Celso Antonio Bandeira de Mello (SANTOS, 2021, p. 33 e ss.), bem como considerando o momento em que sua principal produção acadêmica em torno do tema é desenvolvida (em pleno estado de exceção compreendido pelo regime militar de 1964 a 1985), compreende-se a necessidade de afirmação da existência de um regime jurídico fechado em si, capaz de sustentar uma lógica imanente, a despeito de todas as ressalvas que os fatos políticos pudessem trazer a respeito. Ou seja, a doutrina administrativista de Celso Antonio Bandeira de Mello, ao propor a concepção de um sistema jurídico próprio ao Direito Administrativo, tentou "blindar", "proteger" e "garantir" a funcionalidade desse ramo do Direito, em face daquilo que poderia ser considerada a política de sua época (uma política evidentemente assentada em declarado estado de exceção.)[65]

Esse regime jurídico-administrativo é fincado em dois princípios, como se sabe, quais sejam: (a) a supremacia do interesse público sobre o privado e (b) a indisponibilidade, pela administração, dos interesses públicos. Todo o sistema pensado para o Direito Administrativo se constrói, nesse sentido, a partir desses dois pilares normativos, regendo como pode ser concebida a relação entre a administração pública e os particulares, seja em função das prerrogativas da primeira, seja em razão dos direitos/garantias em favor dos segundos. Na condição de prerrogativas, todavia, Celso Antonio Bandeira de Mello (2021, p. 83-84) é categórico ao afirmar que não se pode confundi-las com meros privilégios, com espécies de "potestades" absolutas, mas sob o prisma da teoria da função; afinal, "[...] onde há função, pelo contrário, não há autonomia da vontade, nem a liberdade em que se expressa, nem a autodeterminação da finalidade a ser buscada, nem a procura de interesses próprios, pessoais".

Supõe-se que a intenção de Bandeira de Mello é, portanto, resguardar algo da metodologia científica do positivismo contra o estado de exceção vigente quando da publicação de seu artigo seminal de 1967. O Direito Administrativo, ao se separar determinantemente da política (ou melhor,

65 Admite-se a hipótese, inclusive, de que a situação política de Celso Antonio Bandeira de Mello foi, inclusive, muito próxima da condição de Kelsen, quando de sua célebre discussão com Rudolf Smend ou mesmo Carl Schmitt (OLECHOWSKI, 2020, p. 501 e ss). A sugestão de uma ciência do direito que se separa metodologicamente da política com a finalidade de garantir uma racionalidade em meio ao esvaimento de toda e qualquer calculabilidade do fenômeno jurídico em razão da ascensão e consolidação do antissemitismo e do nazifascismo na Europa da primeira metade do século XX pode muito bem ser aproximada da intenção de Bandeira de Mello que, alguns anos após o Golpe de 1964 e ainda antes mesmo da instituição do AI-5, sugeria a necessidade: (a) de diferenciar o interesse público primário e secundário – expressamente inspirado na doutrina de Renato Alessi (MELLO, 2021, p. 55 e ss.); (b) de afirmar que o interesse público não poderia se confundir com o interesse do governoe; (c) de se firmar a ideia de que a"supremacia" e "indisponibilidade" desse mesmo interesse público não o colocava à mercê dos interesses particulares que atuaram nas inúmeras "tenebrosas transações" que marcaram o período.

de uma "certa política" praticada naquela conjuntura) e se afirmar como componente de um sistema lógico-científico capaz de se sustentar por si no encadeamento consequente de normas jurídicas administrativas, deveria partir da afirmação da existência de um "interesse público", ou seja, aquele "[...] interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade como membros da Sociedade e pelo simples fato de o serem" (MELLO, 2021, p. 52).

A noção de interesse público revelada por Celso Antonio Bandeira de Mello, como espécie de "núcleo duro" de sua concepção de um regime jurídico-administrativo, pode ser bastante abstrata, talvez até mesmo intencionalmente abstrata, de modo a merecer uma revisitação contemporânea, como a desenvolvida por Luasses Gonçalves dos Santos (2021). Contudo, é conceito que dificilmente pode ser dispensado. O próprio Luasses dos Santos é categórico ao afirmar que, para além de qualquer intenção ingênua ou meramente iconoclasta, a revisitação da teoria do interesse público na atualidade merece se fazer em termos consequentes com a própria conjuntura, evitando-se que as dinâmicas administrativas fiquem, de hora para outra, à mercê dos critérios de ocasião (SANTOS: 2021, pp. 351/352).

Concorda-se com a tese principal de Luasses Gonçalves dos Santos (2021, p. 100 e ss.) a respeito, uma espécie de crítica contemporânea, tanto ingênua quanto iconoclasta, à noção de interesse público travada por doutrinadores tais como Gustavo Binembojm (2008), Marçal Justen Filho (2017) e Daniel Sarmento (2017). As propostas mencionadas e que, por motivo de espaço, não poderão ser individualmente consideradas neste momento, seriam tão ingênuas quanto iconoclastas, pois, conforme conclui Luasses dos Santos (2021, p. 106), "[a] tendência das críticas formuladas ao regime jurídico-administrativo, em contraposição ao suposto caráter autoritário dos princípios que o sustentam, é de substituir as abstrações e não de superá-las". Ou seja, a partir dessas propostas, substitui-se a noção abstrata de interesse público por outras consideradas igualmente inadequadas, buscando-se, no recurso a termos empregados segundo um alto nível de abstração, tais como direitos e garantias fundamentais, proporcionalidade, ponderação e razoabilidade, o fundamento das práticas administrativas, como se as noções e métodos decisórios respectivos pudessem conduzir a uma maior racionalidade (a uma menor arbitrariedade) da prática administrativa.

Como contraponto a essas soluções pontuais, Luasses Gonçalves dos Santos (2021) sugere, então, a necessidade de orientação no sentido a uma maior "concretude" para o conceito de interesse público. Se o conceito de interesse público, o qual, conceitualmente, é "de todos e de cada um", mascara o fato de o Direito ser instrumento utilizado pelas classes opressoras que compõem a elite da administração, na condição de aparelho ideológico de poder (ALTHUSSER, 1995), a afirmação de um Estado Democrático de

Direito preocupado com a redução das desigualdades sociais e regionais deve ter como princípio a defesa de um interesse do povo, não no sentido do "*Volk*" alemão, que em última instância serviu para a justificação retórica do nazifascismo nos anos 20 e 30 do século passado, por exemplo, mas no sentido dos "oprimidos de uma nação" (SANTOS, 2021, p. 368).

Não é o caso aqui de sugerir a propriedade ou a inadequação do conceito desenvolvido por Luasses Gonçalves dos Santos. Apenas se faz uso de sua doutrina para destacar a importância atual do conceito de interesse público, o qual, apesar de concordar com a necessidade de se lhe conferir maior "concretude", como propõe Luasses, não seria possível, neste breve espaço, identificar quem seria o sujeito (individual ou coletivo) que poderia ser considerado o portador, a fonte ou mesmo o alvo desse interesse. Este estudo singelo furta-se da tarefa de subjetivar o interesse público em questão para simplesmente apontar a importância da construção teórica na qual ele está assentado. Contra as teorias ingênuas ou iconoclastas meramente mencionadas acima, a afirmação de um regime jurídico-administrativo é necessária para que, para além de se conferir critérios ao manejo da ação do Estado, seja possível controlar democraticamente essa atuação, entendendo-a como um "dever-poder" ou como uma "função pública", uma função que se exerce no interesse de outros, e não no interesse próprio.

A tão singela afirmação dessa condição ética da atuação administrativa, a exigir que o administrador seja capaz de promover alguma forma de mentalidade alargada (e talvez essa seja a principal dificuldade da tarefa administrativa, em termos tanto cognitivo-epistemológicos quanto políticos: a incapacidade psicológica e estrutural de se projetar uma espécie que seja de *erweiterte Denkungsart*, no sentido kantiano [KANT, 2005, p. 89-90], conceito que aqui somente pode ser mencionado, mas não aprofundado) pode permitir a consideração crítica a respeito da inconstitucionalidade das sanções previstas nos arts. 52, X, XI, XII e § 3.º, da LGPD.

A mentalidade alargada, no sentido kantiano, está na base tanto da atividade crítica, quanto de qualquer noção de Estado de Direito moderno, republicano e democrático. No sentido que aqui se busca entrever, trata-se da capacidade de se colocar na posição do outro, de representar a condição da alteridade, do absolutamente diferente, como condição de possibilidade de uma política minimamente crítica e racional. A afirmação de que a atividade administrativa está centrada em uma tal exigência, como corolário lógico ante o fato de que todo exercício da função administrativa aponta, na verdade, para o exercício de um "dever-poder", impõe considerar a impossibilidade de suspensão ou proibição do próprio exercício da atividade administrativa. Impõe, por assim dizer, a premissa da continuidade dos serviços públicos.

No tópico seguinte, portanto, partir-se-á da conclusão preliminar avançada acima, pelo que a administração, servindo àquilo que se entende como sendo nota do interesse público primário (por mais criticável que tal

noção tenha se tornado na atualidade, diga-se de passagem), não serve a si própria senão na medida em que atende a interesses de outros. Que esses terceiros sejam cada vez mais (e cada vez mais radicalmente) associados aos tipos oprimidos deste mundo, como de modo louvável propõe Luasses Gonçalves dos Santos (2021), implica um desenvolvimento que, a despeito de absolutamente necessário em termos políticos, não pode ser realizado neste momento, razão pela qual se abstrai dessa condição, com atenção às estritas finalidades críticas desta abordagem.

A suspensão ou proibição do tratamento de dados, nos termos do art. 52, da LGPD, prejudica o próprio exercício da atividade administrativa e, consequentemente, deve ser interpretada *cum granum salis*, conferindo-lhe alguma espécie de "interpretação conforme" a Constituição Federal, em favor da proteção dos interesses e prerrogativas dos administrados em face da administração, principalmente daqueles mais vulneráveis.

3 A RESPEITO DA CONSTITUCIONALIDADE DAS SANÇÕES PREVISTAS NO ART. 52, X, XI, XII E § 3.º DA LGPD: OS PARÂMETROS DO ESTADO DE DIREITO, DO PRINCÍPIO REPUBLICANO E DA CONTINUIDADE DO SERVIÇO PÚBLICO

O art. 52, incisos X, XI, XII e § 3.º da LGPD destaca que os agentes de tratamento de dados, isto é, controladores e operadores, inclusive quando se tratar de entes públicos, estão sujeitos às seguintes sanções: (a) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (b) a suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (c) a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Percebe-se que, entre os incisos X, XI e XII, do referido artigo da lei, está previsto um escalonamento da sanção. Primeiramente, a simples suspensão parcial do funcionamento do banco de dados, sendo que o tratamento de dados, especificamente, pode continuar a ser realizado, havendo mais de um banco de dados com aquela mesma informação. Nesse primeiro caso, ademais, o prazo da suspensão é de 6 (seis) meses, prorrogável por igual período, podendo ser prorrogado sucessivamente até que a atividade de tratamento seja regularizada.

Em seguida, trata-se da suspensão do exercício da atividade de tratamento de dados. Perceba-se que, aqui, não se trata mais de limitar a atividade em face de um banco de dados específico, mas da limitação da própria atividade de tratamento de dados, definida pela própria lei, em seu art. 5.º, inciso X, como sendo:

> [...] 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 (BRASIL, 2018).

Ou seja, não se limita o acesso a uma fonte de dados a serem tratados, nos termos da legislação. Trata-se, ao contrário, de uma limitação generalizada da própria atividade de tratamento, compreendendo todas as atividades mencionadas acima. Nesse caso, o prazo para tanto será de, no máximo, 6 (seis) meses, prorrogável por igual período. Perceba-se que, em função da gravidade da sanção, não é sugerida a possibilidade de sucessivas prorrogações, ao contrário do que admite a parte final do art. 52, X, da LGPD.

Por fim, vislumbra-se a mais grave de todas as sanções aplicáveis, qual seja, aquela de proibição, parcial ou total, do exercício de atividades relacionadas a tratamento de dados. Ou seja, além de se vislumbrar uma punição com alcance mais profundo (afinal, a "proibição" corresponderia a uma espécie de *capitis deminutio* do controlador ou do operador, definidos propriamente pela "capacidade de tratar dados", isto é, como "agentes de tratamento"). Nesse caso, não há previsão de prazo da pena, pelo que é necessário recorrer ao ordenamento constitucional para se afirmar a impossibilidade de uma pena perpétua (art. 5.º, XLVII, "b", da CF/1988). Ademais, a proibição possui o escopo de afetar não somente as atividades de tratamento de dados (já definidas de forma bastante ampla pela legislação), mas também aquelas atividades "relacionadas a tratamento de dados", o que permite denotar um escopo bem maior da punição.

A própria legislação, possivelmente ciente da gravidade das punições previstas nos incisos X, XI e XII, do art. 52, da LGPD, destaca, no § 6.º do mesmo artigo, que tais sanções: (a) somente serão aplicáveis após já ter sido imposta ao menos uma das sanções de que tratam os incisos II, III, IV, V e VI do artigo 52 para o mesmo caso concreto e (b) que, em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, deverão ser previamente ouvidos esses atores administrativos.

É possível perceber claramente que a aplicação dessas sanções a entidades particulares é, sim, preocupante e merece ser aplicada com extrema parcimônia. Como destacam Tarcísio Teixeira e Ruth Maria Armelin (2020, p. 147):

> Insta destacar que foram promulgados pela Lei 13.859/18 os incisos X, XI e XII que haviam sido vetados pela MP 869/2018, de maneira que também a suspensão do banco de dados, das atividades de tratamento ou até mesmo o bloqueio parcial ou total das atividades estão no rol das sanções que poderão ser aplicadas em caso de descumprimento da lei.

> As sanções recentemente incluídas possuem um caráter punitivo considerável, haja vista que certas atividades dependem quase que exclusivamente da utilização de banco de dados ou incrementam as suas atividades a partir de um. A suspensão do banco ou da atividade, mesmo que parcial, pode trazer sérios prejuízos para a empresa e o bloqueio pode até mesmo pôr fim à sua atividade.

No entanto, se tais dispositivos são preocupantes quando pensados para serem aplicados ao setor privado, é necessário assumir que as sanções referidas se tornam *a priori* impraticáveis no âmbito da administração pública.

Sugerindo caminho semelhante, menciona-se a preocupação de Luciano Reis e Rafael Lippman (2020, p. 175-176):

> Chama a atenção, neste caso, a possibilidade de aplicação, à Administração Pública, das sanções tipificadas nos incisos X, XI, e XII do art. 52.
>
> Estes três incisos preveem, respectivamente, como reprimenda à inobservância da LGPD, a suspensão do banco de dados, a suspensão do exercício da atividade de tratamento de dados e a proibição do exercício da atividade de tratamento de dados.
>
> Em que pese a expressa autorização de sua aplicação à Administração Pública, a realidade prática pode tornar inviável ou, então, catastrófica a incidência da sanção em determinados casos.
>
> Imagine-se, por exemplo, que, por uma falha no sistema de segurança, sejam divulgadas pela Receita Federal informações sigilosas constantes de declarações de imposto de renda de parcela da população. Seria possível, neste caso, suspender a utilização do banco de dados (inciso X), ou do exercício da atividade de tratamento de dados (inciso XI), ou mesmo proibir a Receita Federal de tratar dados relacionados aos rendimentos dos contribuintes?
>
> Nitidamente, há um duplo desafio a ser superado: de um lado, dimensionar a aplicabilidade prática das sanções previstas na LGPD à Administração Pública sem que isso resulte em verdadeiro impedimento da consecução da atividade-fim do órgão estatal e, de outro, evitar que a inexistência de sanção legalmente adequada venha a gerar a "impunidade" da Administração por ocasião do cometimento de infração à legislação que regula o tratamento de dados pessoais.

As preocupações são reais, como se percebe. O tema é deveras profundo em suas consequências. A paralisação do tratamento de dados, ainda que prevista como *ultima ratio* na forma do art. 6.º, do art. 52, da LGPD, representaria inegável violação a princípios basilares da República, na medida em que autorizaria o órgão vinculado diretamente à Presidência (no caso, a Agência Nacional de Proteção de Dados – ANPD) a suspender

ou proibir, parcial ou totalmente, por período considerável, a atividade de tratamento de dados exercida por outras unidades orgânicas do próprio Executivo federal, como o caso da Polícia Federal mencionado acima, por Reis e Lippman (o que, todavia, não a torna mais aceitável), mas também de órgãos ou entidades vinculados a outros Poderes (como Legislativo, Judiciário, Ministério Público e Tribunais de Contas), bem como de outras esferas da federação (como estados, municípios e Distrito Federal).

No que tange os limites estreitos do presente trabalho, adota-se a premissa de que a aplicação de tais sanções viola diretamente o próprio fundamento do Estado Democrático de Direito brasileiro, constituindo afronta ao princípio republicano e, consequentemente, à exigência social de garantia da continuidade de prestação dos serviços públicos. A aplicação desses dispositivos está, pois, em patente desconformidade com a própria possibilidade de afirmação de um regime jurídico-administrativo, a partir do qual se poderia afirmar que a administração pública, enquanto no exercício de sua finalidade precípua, exerce função pública, isto é, não está voltada ao atendimento de fins próprios, senão na medida em que são atendidos os fins dos próprios administrados, ou seja, dos outros, aquela alteridade irredutível que afirma, para muito além de uma regra de moralidade, a própria eticidade (estabelece o próprio *ethos*, a própria *Sittlichkeit*) do Estado brasileiro.

As considerações de Reis e Lippman (2020) acerca do "duplo desafio a ser superado" quanto à interpretação das sanções do art. 52, X, XI e XII da LGPD em face da administração pública, correspondem a uma falsa polêmica, uma vez que o entendimento de que tais sanções são inaplicáveis em desfavor da administração pública de modo algum representaria uma "impunidade" do Estado ou de seus respectivos agentes em face dos particulares, considerando que ambos ainda se sujeitariam à série de âmbitos de responsabilização (nomeadamente nas esferas administrativa, civil, controladora e criminal). Não havendo que se falar em defesa da "impunidade" de quem quer que seja, verifica-se que a única preocupação que, de fato, resta é a de que a aplicação de tais sanções venha a inviabilizar o exercício da própria atividade-fim do Estado, em detrimento do interesse público, ou mesmo, nos dizeres de Luasses dos Santos (2021), dos interesses dos mais vulneráveis.

Assumindo o fundamento da existência de um regime jurídico-administrativo brasileiro, ainda que se discuta quem seria a subjetividade idealizada para a justificação e racionalização da atividade administrativa, se aquela envolvida na afirmação de um interesse público, nos termos de Celso Antonio Bandeira de Mello, se aquela do interesse do povo, no sentido proposto por Luasses Gonçalves dos Santos, o fato é que a gravidade da sanção de suspensão ou proibição das atividades de tratamento de dados pela administração, ainda que parcialmente, desautoriza qualquer medida de tolerância que se possa ter com a aplicação dos incisos X, XI e XII do art. 52 da LGPD, em desfavor dos órgãos e entidades que compreendem a própria administração pública.

Afetada por tais sanções não seria tão-somente a própria administração, como se poderia exigir de uma sanção que atenda minimamente ao requisito da pessoalidade e da não transcendência de seus efeitos, mas toda a coletividade, ou, no pior dos casos, afetados seriam, primordialmente, os mais vulneráveis e precarizados. A aplicação das sanções ora em análise viola de modo determinante o princípio republicano, pois impede o amplo acesso aos bens públicos fundamentais, em especial àqueles que mais precisam deles. Daí o corolário republicano da continuidade dos serviços públicos.

A eticidade da atuação da administração pública é garantida na medida em que sua conduta se volta à satisfação das necessidades de outrem, nunca de si própria. Trata-se de uma exigência radical, a qual não pode ser considerada sem uma abordagem minimamente crítica do papel do Estado brasileiro. Estando, portanto, em descompasso com a própria possibilidade do modelo de Estado previsto na Constituição, chega-se à conclusão a respeito da impossibilidade de aplicação das sanções previstas no art. 52, incisos, X, XI, e XII da LGPD (introduzidas pela Lei Ordinária Federal n. 13.859/2018), em desfavor da administração pública, pois tal incidência se revela absolutamente inconstitucional.

4 CONCLUSÃO

Neste breve ensaio, foi proposta a contextualização das sanções previstas nos incisos X, XI e XII do art. 52 da LGPD, introduzidas pela Lei Ordinária Federal n. 13.859/2018, em face de sua possível aplicação em desfavor da administração pública, como permite o § 3.º, do mesmo artigo.

Partindo-se da sugestão de um regime jurídico-administrativo voltado à afirmação de uma função administrativa que extrai seu significado jusfundamental da prestação de algum benefício considerado público, em favor de terceiros que não, imediatamente, a própria administração, sejam eles considerados em termos abstratos, como titulares individuais ou coletivos de prerrogativas em face do Estado, sejam considerados como aqueles indivíduos ou grupos oprimidos, em termos tendencialmente mais concretos, como querem Celso Antonio Bandeira de Mello e Luasses Gonçalves dos Santos, respectivamente, verificou-se que a aplicação das sanções analisadas neste momento não se revela minimamente consequente com o regime constitucional brasileiro.

Ora, caso aplicadas à administração pública, as sanções de (a) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, (b) de suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, ou (c) de proibição parcial ou total do exercício de atividades relacionadas a

tratamento de dados representariam graves prejuízos não somente ao órgão ou entidade que reiteradamente teriam descumprido as regras de proteção de dados pessoais (nos termos do art. 52, § 6.º da LGPD), mas também de toda a coletividade que, bem ou mal, depende da prestação de serviço público (entendido aqui no sentido mais amplo possível) por parte do Estado.

A possibilidade de aplicação das referidas sanções está em descompasso com a lógica do regime jurídico-administrativo brasileiro, bem como em evidente contraposição à premissa republicana da Constituição pátria e de seu corolário mais direto neste tema, qual seja, a garantia de continuidade do serviço público. A aplicação das sanções referidas no art. 52, X, XI e XII, da LGPD, por parte da Agência Nacional de Proteção de Dados, órgão diretamente vinculado à Presidência da República, em desfavor da administração pública, seja ela federal, estadual ou municipal, seja ela afeta a quaisquer dos Poderes do Estado (sabendo-se que também o Judiciário e o Legislativo exercem atividades de administração, ainda que não seja essa a sua finalidade precípua), representa medida por demais gravosa para ser compreendida como aceitável e constitucional.

Por todo o exposto, em exercício de análise consequente do texto normativo, bem como em função das premissas ideológicas e teóricas empregadas ao longo do texto, ainda que não tenha havido orientação dos tribunais pátrios a respeito da matéria, entende-se pela absoluta inconstitucionalidade da aplicação do art. 52, X, XI e XII da LGPD à administração pública.

REFERÊNCIAS

ALTHUSSER, Louis. **Sur la reproduction**. Paris: PUF, 1995.

BINEMBOJM, Gustavo. **Uma Teoria do Direito Administrativo:** direitos fundamentais, democracia e constitucionalização. 2. ed. Rio de Janeiro: Renovar, 2008.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. ed., Rio de Janeiro: Forense, 2020.

BIRCHALL, Clare. **Shareveillance:** The Dangers of Openly Sharing and Covertly Collecting Data. Minneapolis: University of Minnesota, 2017.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 abr. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

JUSTEN FILHO, Marçal. O Direito Administrativo de espetáculo. *In*: ARAGÃO, Alexandre Santos de; MARQUES NETO, Floriano de Azevedo (coord.). **Direito Administrativo e seus novos paradigmas**. 2. ed. Belo Horizonte: Fórum, 2017. Disponível em: https://www.forumconhecimento.com.br/livro/1447/1501/3126. Acesso em: 1.º out. 2021.

KANT, Immanuel. **Critique of Judgment**. New York: Barnes & Noble, 2005.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 35. ed. São Paulo: Malheiros, 2021.

MELLO, Celso Antônio Bandeira de. O conteúdo do regime jurídico-administrativo e seu valor metodológico. **Revista de Direito Administrativo**, São Paulo, n. 2, p. 8-33, out./dez. 1967. Disponível em: https://doi.org/10.12660/rda.v89.1967.30088. Acessi em: 27 set. 2021.

OLECHOWSKI, Thomas. **Hans Kelsen:** biographie eines rechtswissenschaftlers. Wien: Mohr Siebeck, 2020.

REIS, Luciano Elias; LIPPMAN, Rafael Knorr. A Administração Pública na Lei Geral de Proteção de Dados. *In*: PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados:** estudos sobre um novo cenário de Governança Corporativa. Belo Horizonte: Fórum, 2020.

RODOTÁ. **La vita e le regole**: tra diritto e non diritto**.** Milano: Feltrinelli, 2018, e-book.

SANTOS, Luasses Gonçalves dos. **O interesse público sob a crítica da teoria crítica**. São Paulo: Contracorrente, 2021.

SARMENTO, Daniel. Supremacia do interesse público? As colisões entre direitos fundamentais e interesses da coletividade. *In*: ARAGÃO, Alexandre Santos de; MARQUES NETO, Floriano de Azevedo (Coord.). **Direito Administrativo e seus novos paradigmas**. 2. ed., Belo Horizonte: Fórum, 2017, disponível em: https://www.forumconhecimento.com.br/livro/1447/1501/3132. Acesso em: 1.º out. 2021.

SOUZA, Carlos Affonso; MAGARINI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na turela dos dados pessoais. *In*: MULHOLLAND, Caitlin (org). **A LGPD e o novo marco civil normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria G. da Fonseca. **Lei Geral de Proteção de Dados Pessoais:** Comentada artigo por artigo. 2. ed., Salvador: Juspodivm, 2020.

13
CYBERSECURITY E LGPD

Rodrigo Hiroshi Ruiz Suzuki
Vanessa D'Alessio Giarone Suzuki

Resumo

As empresas usam sistemas informatizados para inúmeras finalidades e, inevitavelmente, armazenam e tratam dados pessoais em suas aplicações. Enquanto isso, cresce a quantidade de ameaças cibernéticas que podem provocar danos e até mesmo a divulgação indevida desses dados. Com a vigência da Lei Geral de Proteção de Dados, passa a ser obrigatório atender requisitos de segurança desses dados em sistemas corporativos, serviços de internet e até mesmo em recursos de comunicação, como e-mails. Reconhecer o ciclo de vida da informação, mas também entender quais são essas ameaças, é fundamental para a definição de uma arquitetura adequada de defesa contra esses ataques. Neste artigo são apresentadas as principais ameaças cibernéticas e os recursos tecnológicos e de governança para a defesa de um ambiente corporativo contra esses ataques virtuais, além de recomendações sobre a classificação da informação e a sua proteção, desde a sua captura ou criação até o seu descarte.

Palavras-chave: *cybersecurity*; LGPD; segurança da informação; privacidade; ataques; vulnerabilidades.

1 INTRODUÇÃO

É inegável que a maioria das empresas, independentemente de seu porte e segmento, utiliza serviços que estão conectados à internet, como correios eletrônicos, *websites*, lojas de comércio eletrônico e até mesmo servidores e aplicações virtuais.

Os riscos e ameaças cibernéticas podem afetar diretamente os direitos dos indivíduos, violando requisitos estabelecidos na Lei Geral de Proteção de Dados (Lei n. 13.709/2018 – LGPD). Dessa forma, esses riscos precisam ser corretamente avaliados, reconhecidos e tratados para protegerem os interesses das pessoas e das empresas, evitando multas, sanções e danos reputacionais.

Por não conhecerem o ciclo de vida das informações que usam, muitas empresas assumem riscos indevidos, seja pelo desconhecimento dos requisitos da lei, seja por usarem serviços, técnicas e ferramentas que podem não atender de maneira suficiente à lei. Situações como a transmissão de dados pessoais para processamento fora do Brasil, em países que não tenham uma

lei similar de proteção de dados, o controle inadequado do armazenamento das informações e até mesmo a impossibilidade de atender aos direitos das pessoas são recorrentes não somente no Brasil, mas também em outros países que possuem legislações de proteção de dados pessoais.

Embora a LGPD não faça distinção sobre porte, faturamento ou número de funcionários de uma empresa, seus requisitos devem ser aplicados da mesma forma, pois os direitos das pessoas não variam em função do tamanho da empresa que processa tais dados. E é errada a crença de que apenas grandes empresas estão sujeitas ao rigor da lei.

Em muitas situações é preciso reconhecer que pode haver a transferência de dados de indivíduos entre a empresa controladora (que solicita ou captura os dados pessoais) e esses prestadores de serviços na internet – os processadores de dados. Os direitos dos indivíduos devem ser preservados em qualquer um dos cenários tecnológicos possíveis. O uso de contas de e-mail, servidores virtuais ou outros serviços de nuvem precisam ser avaliados.

Enquanto isso, os riscos cibernéticos aumentam exponencialmente. Cada vez mais surgem notícias de empresas que tiveram seus sistemas comprometidos e os dados obtidos por *hackers* sendo propagados de forma criminosa na *deepweb*, ou seja, em servidores de internet que não são acessíveis de maneira simples e que não estão indexados por ferramentas de busca clássicas, e frequentemente são usados para atividades ilícitas, como fraudes bancárias e golpes com o uso de dados válidos.

Com o advento das leis de privacidade, as bases de dados pessoais das empresas se tornaram valiosas para as atividades criminosas, pois, além de poderem ser usadas para fraudes e golpes, também são usadas para extorquir empresas a pagarem para não terem seus dados divulgados ou para simplesmente recuperar dados criptografados.

Tanto a LGPD quanto a General Data Protection Regulation (GDPR) (UNIÃO EUROPEIA, 2016), uma das mais antigas leis sobre privacidade de dados pessoais, preveem sanções e multas para as empresas que violarem os direitos dos indivíduos. Observa-se que em muitos países a aplicação de multas tem sido frequente, mesmo para pequenas empresas ou para processamento ilegal de um pequeno número de sujeitos.

Considerando esses pontos, o risco cibernético para a LGPD é algo que precisa ser levado em conta, dado o potencial dano que pode resultar de um ataque. Este artigo apresenta quais são os principais riscos cibernéticos que podem resultar em violações à privacidade de dados e técnicas que podem ser aplicadas na prevenção e resposta para esses eventuais ataques.

2 CICLO DE VIDA DA INFORMAÇÃO E A *CYBERSEGURANÇA*

O processo de levantamento de dados e seu fluxo na empresa é uma oportunidade para conhecer e documentar o ciclo de vida da informação

como, por exemplo, onde ela é gerada ou capturada, onde é armazenada, processada, alterada, onde estão suas cópias de segurança e até quando e como deve ser feito o seu descarte, e deve-se observar os serviços de nuvem que possam estar em uso. Essa prática é importante para que os direitos das pessoas possam ser garantidos de acordo com os requisitos da LGPD.

Cada um dos estágios do ciclo de vida traz seus próprios desafios em relação à LGPD e em termos de segurança da informação. Serviços de backup de dados devem levar em conta exigências da lei, como o direito ao esquecimento, a proteção contra acessos indevidos e a própria garantia do sigilo da informação. Outra preocupação é se o dado pessoal transitou por meios não estruturados, como e-mail ou arquivos de trabalho em um servidor – ele, ainda assim, está sujeito aos requisitos da LGPD.

Havendo o conhecimento de onde as informações estão armazenadas e por onde transitam, é possível definir mecanismos mais adequados para a proteção e reação contra ataques cibernéticos.

A prevenção contra os ataques demanda técnicas específicas, desde as camadas mais externas da rede, como links e servidores expostos à internet, até servidores internos, equipamentos de rede e de usuários finais, sem esquecer de redes de clientes, parceiros e unidades remotas que podem estar conectadas e serviços de nuvem.

3 RISCOS TÍPICOS DE SEGURANÇA CIBERNÉTICA (*CYBERSECURITY*)

De acordo com Barrett *et al.* (2020), segurança cibernética é a habilidade de proteger e defender o uso do espaço cibernético contra ataques, em tradução livre. Os riscos mais comuns são aqueles ligados a softwares maliciosos (*malwares*), ataques de engenharia social e até mesmo ataques direcionados, sofisticados, realizados por meio da internet com o objetivo de ultrapassar as proteções corporativas.

Esses ataques podem levar à violação de vários princípios da LGPD, como a indisponibilidade de dados, a revelação pública de dados considerados sensíveis e seu uso indevido. É importante sempre considerar que o controlador de dados é responsável por todo o ciclo de vida do dado pessoal por ele solicitado, obtido e processado – incluindo a eventual contratação de terceiros, e que os processadores de dados podem armazenar ou processar dados pessoais em nome do controlador.

É necessário ressaltar que o controlador de dados pode responder solidariamente por irregularidades cometidas pelo processador de dados por ele contratado, uma vez que a pessoa concedeu acesso ou foi obtido segundo as bases legais da LGPD apenas para o controlador de dados.

Os riscos cibernéticos se manifestam tanto para o ambiente de computação interno da empresa quanto para os equipamentos de usuários e,

além disso, também para os serviços de nuvem que parte das empresas já usa há algum tempo, como o Office 365, Google Apps, Amazon Web Services e Azure, entre outros. Esses serviços podem armazenar dados pessoais, tendo a empresa contratante como o controlador de dados – e é preciso conhecer os termos da prestação de serviço para entender o nível de compatibilidade com os requisitos da lei de privacidade aplicável. É preciso também reconhecer que esses serviços também estão sujeitos aos riscos cibernéticos aqui descritos.

É comum que as empresas que prestam serviços tenham certificações, como a ISO 27001 e SOC 2 Type2, como prova de que seus processos de trabalho e infraestrutura seguem práticas aceitáveis em termos de segurança da informação e privacidade de dados.

Os riscos cibernéticos podem ter origem na internet e até disseminação maliciosa por meio de dispositivos físicos, como drives USB (pendrives) ou a conexão de dispositivos em redes corporativas. Estar ciente desses riscos e das técnicas para lidar com eles é fundamental para a criação de uma arquitetura de segurança da informação que passe por elementos tecnológicos, mas também considere processos de trabalho adequados para a sua manutenção.

4 MALWARES

Um dos principais riscos cibernéticos são os *malwares*, programas maliciosos criados para se espalharem por computadores ou para realizarem ações danosas em um ambiente computacional. Entre as possíveis ações, estão a destruição de arquivos, a abertura de canais de acesso para *hackers* ganharem acesso à rede da empresa e a divulgação indevida de dados, entre outros. Por muitos anos foram conhecidos como "vírus de computadores", que ganharam essa nova nomenclatura para possibilitar a denominação mais adequada de acordo com a maneira que se propagam e atuam.

4.1 MEIO DE DISSEMINAÇÃO DE MALWARES

A disseminação de *malwares* pode ser feita de muitas maneiras, entre elas:

• e-mails de *phishing* – um dos meios mais simples e mais efetivos para conseguir acesso a um equipamento ou rede. Um e-mail é enviado com a finalidade de convencer quem o recebeu a abrir um arquivo anexo, que contém um *malware*, ou a acessar um site que pode fazer o *download* do *malware*. Esse *malware* pode abrir um canal de acesso para que o atacante consiga adentrar o ambiente protegido da empresa. Há e-mails de *phishing* que são distribuídos amplamente, e sem grande critério, para milhares de destinatários, na expectativa de que um certo percentual se converta em

vítimas. Todavia, há também ataques de *phishing* mais sofisticados que são desenvolvidos para uma empresa ou pessoa específica, usando conhecimento mais apurado sobre a vítima para a criação de uma mensagem que seja mais factível e que faça sentido para o recipiente. Esse ataque é conhecido como *spear phishing*;

• exploração de vulnerabilidades no ambiente – sistemas operacionais e aplicações podem conter falhas que possibilitam um atacante a ganhar acesso aos sistemas, seja por meio da internet, seja invadindo a rede corporativa por outros meios. Essas vulnerabilidades podem ser causadas pelo uso de configurações inadequadas em sistemas ou pela falha existente em um sistema ou aplicação. Vulnerabilidades são comumente resolvidas por meio da aplicação de correções publicadas por seus fabricantes ou contramedidas para reduzir o seu impacto. Muitas vezes as correções podem levar de semanas a meses para estarem disponíveis, período em que o ambiente pode ficar desprotegido se contramedidas não forem adotadas;

• conexão de dispositivo USB malicioso – um meio simples e bastante efetivo é convencer uma pessoa a conectar um dispositivo USB contendo um *malware* que é executado automaticamente quando conectado. Há notícias de que *hackers* deixam pendrives USB nas proximidades das empresas que desejam atacar, esperando que um funcionário desavisado o conecte em seu equipamento. O pendrive é configurado para executar um *malware* assim que é conectado a qualquer equipamento da rede;

• sites falsos – *hackers* constroem sites muito parecidos com os verdadeiros, com a finalidade de obter dados pessoais, números de cartão de crédito e de documentos para cometerem fraudes ou para espalharem *malwares*. Em muitas situações são usados em conjunto com um ataque de *phishing*, para a obtenção de dados da vítima. Muitos sites falsos possuem nomes de domínio que se parecem com o domínio real, com letras faltando ou com letras substituídas, o que pode passar despercebido pelas vítimas, acreditando ser um site verdadeiro;

• engenharia social – técnica utilizada por *hackers* e fraudadores para convencer as vítimas a oferecerem informações, executarem comandos ou realizarem acessos, fingindo serem outras pessoas. Alguns ataques de *phishing* usam técnicas de engenharia social. A engenharia social é dos mais antigos e dos mais efetivos métodos de ataque a uma empresa, pois, por meio dela, é possível obter detalhes sobre a operação da empresa, nomes de pessoas e detalhes que podem fornecer informações valiosas para a realização de um ataque direcionado. Muitos ataques se iniciam por telefonemas para funcionários da empresa, tentando obter informações, como usuários e senhas de sistemas, nomes de pessoas-chave da empresa e até mesmo fazendo-se passar por um funcionário da área de suporte de TI solicitando a execução de comandos.

4.2 TIPOS DE MALWARES

Segundo o Cybersecurity & Infrastructure Security Agency (MALWARE..., [201-?]), existem vários tipos de *malwares* que colocam em risco a operação de uma empresa. Tipicamente, os que podem colocar em risco os dados pessoais são:

• *ransomware* – um tipo de *malware* que costuma codificar os dados (criptografar) dos computadores de uma rede, tornando-os ilegíveis e, por conseguinte, inúteis para a empresa. Para obter a chave para decodificar os arquivos é necessário pagar uma quantia, na maioria das vezes por meio de criptomoedas, como um resgate, para que o atacante entregue a chave para a decodificação dos dados. Em muitas ocasiões, os *ransomwares* também copiam os dados obtidos para a *darkweb*, com a finalidade de serem utilizados para extorquir as empresas. Muitos dos grandes vazamentos de dados pessoais ocorridos desde o início da vigência da Lei Geral de Proteção de Dados podem ter sido realizados por *ransonwares*. A proteção contra esse tipo de ameaça é muito importante do ponto de vista da LGPD, pois, potencialmente, dados pessoais de empregados e terceiros podem estar contidos nos arquivos furtados e codificados. A eventual má utilização desses arquivos pode violar os direitos dos indivíduos, e a empresa, segundo a lei, pode ser penalizada por não ter implementado mecanismos suficientes para a proteção dos dados;

• *worm* – um *malware* que, uma vez instalado em um computador, replica-se para os equipamentos próximos. Muitas vezes é instalado por meio de e-mails falsos que tentam convencer o usuário a acessar um *hiperlink* ou abrir um arquivo anexado à mensagem ou se aproveitando de uma vulnerabilidade presente em um equipamento conectado à internet. Uma vez que o *worm* tenha adentrado a rede corporativa, ele se espalha para outros equipamentos e até mesmo se expande para outras empresas por meio de conexões privativas ou até mesmo pela internet. Os danos causados por um *worm* podem ser desde possibilitar o acesso remoto de um atacante até a disseminação de *ransomware* ou vírus e a paralisação de sistemas;

• *rootkit* – tipo de *malware* que abre uma porta de acesso externo para que um atacante obtenha acesso ilegal ao ambiente. Muitas vezes é instalado em um ambiente por meio de e-mails de *phishing* ou é trazido para dentro da rede por download realizado por um outro *malware*, *script* ou *worm*. Costuma ser uma das principais ferramentas que os *hackers* usam para alcançar outros equipamentos na rede, depois de conseguir atravessar os bloqueios corporativos;

• *botnet* – *malware* que normalmente permanece instalado em equipamentos de forma silenciosa, em milhares ou milhões de equipamentos conectados à internet, aguardando uma ordem enviada por *hackers* com a finalidade de que essa rede de equipamentos execute uma atividade, como

ataques volumétricos simultâneos a um *website*, tornando-o indisponível pela quantidade excessiva de acessos simultâneos válidos, ou até mesmo a mineração de criptomoedas. Recebem esse nome porque os equipamentos infectados se comportam como "zumbis", aguardando ordens para realizarem algum tipo de ataque;

• *spyware* – esse tipo de *malware* costuma ser executado de forma silenciosa em um equipamento enquanto coleta dados do usuário, que podem ser relacionados aos hábitos de uso do equipamento, *cookies* e outros dados que são enviados para o atacante remoto. Muitas vezes são utilizados para fazer o download de *rootkits* ou outros *malwares* para compor um ataque mais sofisticado.

5 CONTROLES CONTRA ATAQUES

Pode ser um grande desafio traduzir o controle do ciclo de vida de dados pessoais em sistemas informatizados, mesmo com a evolução das ferramentas de controle. Ataques que possibilitam o vazamento de arquivos colocam em risco direto o atendimento aos requisitos da LGPD e constituem uma das maiores preocupações corporativas sobre dados pessoais.

Várias tecnologias e processos podem ser implantadas para evitar esses ataques ou reduzir o eventual impacto de sua ocorrência, como veremos adiante.

5.1 CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações é importante para possibilitar a correta identificação de confidencialidade e manuseio de dados. Conforme é requisitado pela Norma ISO 27001:2013 (ABNT, 2013), deve haver uma política de classificação da informação corporativa que indique níveis de confidencialidade de dados e possibilite atribuir o nível de controle correto para cada tipo de informação, indicando o manuseio, o processamento, o armazenamento e o descarte das informações. Exemplos típicos de classes de informação são: pública, restrita e confidencial.

Alguns sistemas operacionais e plataformas de armazenamento de dados permitem atribuir controles sofisticados para arquivos que podem ser muito úteis para a proteção de dados pessoais. Esses controles possibilitam limitar o acesso ao conteúdo do arquivo para apenas os usuários que foram designados, usando técnicas de *digital rights management*, muito comuns para garantir que músicas e filmes licenciados para um usuário não sejam visíveis por terceiros e possibilite que o arquivo tenha um período de validade, tornando-se inutilizado depois de certa data. Caso o arquivo seja capturado por *hackers*, seu conteúdo permanece protegido e ainda será possível revogar o privilégio de acesso de maneira centralizada.

A classificação da informação pode ser feita de maneira semiautomática, por meio de ferramentas que leem o conteúdo dos arquivos e sugerem uma classificação de acordo com seu conteúdo ou enquanto o conteúdo é criado. Os funcionários da empresa precisam receber treinamento adequado sobre como identificar a classificação adequada para o arquivo.

A implementação de uma política de classificação de dados, que deve ser seguida por todos os usuários, possibilita configurar soluções como *Data Loss Prevention* e *Cloud Access Secure Broker* para que protejam um arquivo de dados de acordo com a classificação atribuída, evitando que possam ser transmitidos ou copiados de maneira indevida.

A Norma ISO 27001:2013 também estabelece regras para criar rótulos e identificações que podem ser usados para complementar a segurança dos arquivos, e até documentos impressos, para facilitar seu manuseio e fácil identificação.

5.2 PROTEÇÃO DA REDE

As proteções mais clássicas de redes corporativas com o uso de *firewalls*, sistemas de detecção de intrusão (IDS) e sistemas de prevenção a intrusão (IPS) ainda são necessárias e aplicáveis para todas as empresas. Entretanto, sozinhas, não são mais capazes de fornecer a proteção completa da empresa contra ataques cibernéticos, especialmente aqueles mais avançados e que visam a obter dados pessoais ou disseminar *malwares*.

Entretanto, algumas proteções já não tão recentes e que não são largamente difundidas se tornaram importantes para evitar os riscos cibernéticos.

5.3 WEB APPLICATION FIREWALLS (WAF)

Os *web application firewalls*, ou WAF, são equipamentos que monitoram o tráfego de servidores WEB e são especializados em detectar padrões de ataques mais sofisticados, como aqueles que buscam explorar falhas de programação em um site, injetar código malicioso em uma página ou até mesmo realizar download massivo de dados por meio de um servidor web. Esses equipamentos são um misto de *firewall* e *proxy* reverso, realizando a verificação de tráfego de acordo com regras preestabelecidas e verificando se as requisições HTTP/HTTPS estão sendo realizadas de maneira correta. Na eventualidade de qualquer anomalia, o WAF é capaz de bloquear a conexão atual e futuras provenientes daquele atacante.

5.4 ENDPOINT PROTECTION (EPP)

As soluções clássicas de antivírus, que por muitos anos funcionaram apenas monitorando se os arquivos lidos ou escritos pelo sistema operacional

continham uma certa assinatura contida na base de dados da solução. Dessa forma eram capazes de detectar apenas ameaças já conhecidas.

A evolução dessas plataformas passou pela detecção de vírus "mutantes", que são capazes de mudar seu código executável de forma a dificultar a detecção por soluções clássicas, para softwares que podem monitorar o comportamento de qualquer arquivo ou programa, detectando comportamentos anômalos, como a escrita direta ao sistema de arquivos sem passar pelo sistema operacional, realizar a deleção de muitos arquivos, realizar alterações nos parâmetros do sistema operacional ou se conectar a sites de internet e realizar o download de arquivos. Qualquer uma dessas ações pode ser característica de um *malware* sendo introduzido no equipamento.

A soluções de EPP devem ser instaladas na totalidade dos equipamentos de uma empresa, incluindo, quando aplicável e homologado, também os servidores. Muitas soluções de EPP podem fornecer dados para as plataformas de conectividade à rede corporativa, como *switches* e *access points*, para a verificação do nível de atualização do equipamento em relação às políticas corporativas, como por exemplo se o EPP apontar que o equipamento não possui a última atualização de segurança do sistema operacional ou do EPP, pode bloquear a conexão do equipamento à rede corporativa, liberando apenas um acesso controlado para a internet, possibilitando que o equipamento seja atualizado antes de entrar na rede corporativa.

Além desse tipo de proteção, o EPP também monitora as conexões de rede do equipamento, possibilitando identificar tipos de ataques provenientes da internet, com funcionalidades de detecção de intrusão e *firewall*, protegendo contra ameaças provenientes de redes corporativas ou públicas.

5.5 ENDPOINT DETECTION AND RESPONSE (EDR)

As soluções de EDR possuem certa similaridade com as de *endpoint protection*, com a diferença que a detecção de anomalias pode ser mais rápida e pela troca de informações sobre ataques com todos os usuários dessa aplicação, em qualquer lugar do mundo.

Além de detectar anomalias, pode ser usada para bloquear um determinado programa em toda a rede, impedindo rapidamente a disseminação de qualquer ataque ou *malware*. São ferramentas importantes para as áreas de *cybersecurity* e de centros de operação de segurança (SOC).

5.6 CRIPTOGRAFIA DE DADOS

Embora a Lei Geral de Proteção de Dados não faça menção direta ao uso de criptografia como mecanismo de proteção de dados, o artigo 32 da General Data Protection Regulation (UNIÃO EUROPEIA, 2016) estabelece que dados pessoais devem ser pseudonimizados e criptografados.

A criptografia é uma técnica que possibilita tornar dados ininteligíveis, estejam eles em arquivos, fluxos de dados ou em qualquer outro meio digital, e consiste na aplicação de algoritmos matemáticos que, tipicamente, codificam dados em nível binário. Esses algoritmos possibilitam codificar e decodificar dados, usando uma ou mais chaves. As chaves são compostas por sequencias de *bits* e costumam oferecer melhor proteção de acordo com o número de bits que as compõe.

Os cuidados usuais do uso de criptografia devem ser observados: algoritmos reconhecidos e tamanhos de chave que protejam os dados pessoais contra tentativas de decodificação, testando todas as combinações possíveis de chaves – um ataque conhecido como força bruta. Com o poder computacional disponível hoje é possível decodificar mensagens criptografadas com algoritmos mais antigos ou chaves curtas com reduzido tempo de processamento. Ao escolher um algoritmo de criptografia e o tamanho da chave é preciso considerar o provável tempo de processamento necessário para descobrir a chave que possibilita abrir a mensagem.

Sempre que possível e aplicável, recomenda-se criptografar dados pessoais e proteger de maneira adequada as chaves usadas no processo. Soluções como *password vaults* (cofres de senha) e *hardware security modules* (HSM) são as indicadas para geração, guarda e uso de chaves criptográficas.

Para serviços em nuvem é preciso observar o uso de algoritmos de criptografia de transmissão de dados na internet como o *Hyper Text Transfer Protocol Secure* (HTTPS). E da mesma forma que é recomendável criptografar os dados armazenados na empresa, também é preciso requerer que os dados nos serviços em nuvem usem um nível de criptografia em consonância com a política de classificação da informação. Muitos dos provedores de serviços de nuvem garantem em contrato que os dados permanecem criptografados em seus repositórios.

5.7 DATA LOSS PREVENTION (DLP)

Soluções de prevenção à perda de dados (*data loss prevention* – DLP) são bastante efetivas no controle do uso inadequado de dados e possibilitam limitar a fuga de dados em casos de ataques cibernéticos.

Tratam-se de *softwares* que são executados em estações de trabalho de usuários, servidores e até mesmo em segmentos de rede por onde os arquivos podem trafegar. Comumente têm a habilidade de se integrarem com a classificação de confidencialidade de arquivos, seja por meio de *meta tags* – pequenas descrições de cada arquivo que é gerado –, seja pela interpretação do conteúdo.

Por meio de *scripts* é possível programar filtros para identificar dados pessoais como CPF, RG e até mesmo nomes pessoais em arquivos e, dessa forma, aplicar as políticas adequadas que podem ser o bloqueio

da transmissão, a autorização da transmissão mediante uma justificativa, a criptografia automática do conteúdo ou o bloqueio do envio. Cada uma dessas ações pode gerar alertas imediatos para centros de monitoramento.

Além disso, possibilitam também monitorar ou bloquear o uso de dispositivos USB, controlar o uso das funcionalidades de copiar e colar, monitorar a realização de *screenshots* que contenham dados confidenciais, entre outros. As funcionalidades variam de acordo com o fornecedor da solução, embora a maioria das descritas aqui está presente em grande parte dos softwares.

É possível também configurar essas plataformas para armazenar as evidências necessárias para investigações futuras, como a captura do arquivo, e-mail ou mensagem bloqueada para posterior análise.

Muitos serviços disponibilizados por meio da internet possuem funcionalidades de DLP nativas, como o Office 365 e o Google Apps, e podem ser configurados para refletir a política de classificação de dados corporativa e usarem as classificações já atribuídas em arquivos, fornecendo um nível semelhante de proteção entre os ambientes físicos e virtuais. Ao utilizar um serviço de nuvem é preciso levar em conta as funcionalidades de prevenção à perda de dados da plataforma contratada, se estão em conformidade com a política de classificação da informação da empresa.

5.8 SECURITY INFORMATION EVENT MANAGEMENT (SIEM)

A arquitetura tecnológica para implementar o monitoramento e controle do ciclo de vida da informação pode se tornar complexa e difícil de gerenciar, considerando o número de tecnologias envolvidas e a quantidade de eventos de segurança que são gerados a cada segundo.

Muitos ataques não são fáceis de detectar a partir de um único ponto. Às vezes são detectáveis apenas por meio do cruzamento de dados de vários dispositivos da rede corporativa que, analisados em conjunto, podem indicar uma intrusão na rede ou uma disseminação de um vírus. A análise desse tipo de evento não pode ser feita de forma manual, considerando a quantidade de *logs* que precisam ser interpretados em conjunto. O Siem é a plataforma que recebe os *logs* de diversos equipamentos da rede, incluindo servidores, e possibilita correlacionar de forma automática milhares de eventos por segundo (EPS) e identificar comportamentos anormais que podem indicar um ataque.

Considerando que um Siem armazena logs de equipamentos de forma centralizada, torna-se útil também para atividades de investigação de ataques sofridos, pois contém os dados correlacionados e funcionalidades de pesquisa nos *logs* armazenados.

A maioria dos serviços de centro de operações de segurança, os *security operations centers* – SOC –, usa soluções de Siem para possibilitar lidar com

redes complexas e possibilitar rapidez e precisão na detecção de eventos de segurança, facilitando a reação mais adequada, a partir das informações que são fornecidas pelo Siem.

Existem soluções de Siem que podem ser implantadas dentro da própria rede corporativa ou podem ser executadas nas plataformas de nuvem de seus fornecedores. Em ambos os cenários é preciso configurar os dispositivos a serem monitorados para que enviem seus logs de segurança para a solução de Siem.

A inteligência e a eficácia dessas plataformas dependem da criação das regras de correlação (*playbooks*) para que eventos específicos possam ser monitorados como, por exemplo, uma conexão não usual de um empregado na rede (horário e localidade anormal) seguida da execução de um comando suspeito, o que geraria um alerta imediato para o monitoramento do ambiente e até poderia disparar uma ordem para o bloqueio da conta desse usuário, pois indica que o usuário e senha desse funcionário podem ter sido obtidos por meio de um atacante que está tentando ganhar acesso ao ambiente. Essas regras podem ser criadas para refletir os cenários de riscos de cada empresa.

5.9 *CLOUD ACCESS SECURITY BROKER* (CASB)

O monitoramento e o controle de serviços de nuvem, como plataformas de CRM, e-mail, ferramentas de produtividade, armazenamento de dados e tantos outros é necessário para garantir a segurança aos dados corporativos contidos nesses serviços.

Por residirem fora do ambiente da empresa e serem prestados, tipicamente, para diferentes clientes e sua dificuldade de integração com plataformas de Siem, torna-se necessário o uso de plataforma específica para realizar esse controle. O Casb é uma plataforma que realiza o controle de serviços de nuvem capturando dados da navegação dos usuários, por meio do monitoramento de *proxies* (equipamentos ou softwares que intermedeiam a conexão entre os equipamentos de usuários e servidores com os sites de internet), e alguns serviços de nuvem são compatíveis com o monitoramento do Casb.

Essa conexão entre serviços de nuvem e o Casb dá-se por meio de conexão direta entre essas plataformas, tipicamente por meio de *application programming interface* (APIs), que são porções de software desenvolvidas especialmente para permitir a interconexão com elementos externos. As APIs de serviços de nuvem possibilitam que o Casb monitore o funcionamento da plataforma, mas também interaja diretamente com ela, proporcionando o bloqueio de funções, o controle de privilégios e até mesmo o bloqueio de contas de usuário em caso de anomalias.

Não há uma padronização das funcionalidades disponíveis entre Casbs e plataformas de nuvem, e deve-se analisar a escolha da plataforma de Casb

que melhor proporcione visibilidade e controle dos serviços de nuvem em uso.

Como monitoram o tráfego de acesso à internet, os Casbs possibilitam também conhecer quais serviços de nuvem estão sendo usados. Muitas vezes os funcionários de uma empresa começam a usar serviços que podem trazer riscos, como armazenamento de dados online (que pode ser incompatível com a LGPD pela possibilidade de monitoramento do conteúdo por terceiros, pelo armazenamento em países sem uma legislação de privacidade e até pela perda do controle do ciclo de vida da informação), serviços que a empresa não permite que seus funcionários acessem e até mesmo o bloqueio de serviços reconhecidamente inseguros.

O Casb, operando em conjunto com os *proxies*, pode criar limitações ou bloqueios para serviços de internet de forma individual (bloqueando acesso para um site específico), por categoria (por exemplo, sites de armazenamento de dados on-line, jogos ou esportes), ou até mesmo criar regras que possibilitem ao usuário apenas baixar dados de um site de armazenamento, mas não permite o envio de arquivos, apresentando-se como um importante ponto de controle para os arquivos que contenham dados pessoais, com a finalidade de atender à LGPD.

Essas soluções costumam ser licenciadas pelo número de usuários que irão monitorar e pelos conectores (API) licenciados para serviços de nuvem. Tipicamente são oferecidos como um serviço de nuvem.

6 REFORÇANDO A SEGURANÇA DO AMBIENTE

Além dos controles para a contenção das invasões, ainda há tecnologias e processos que podem ser usados para complementar a segurança, criando camadas adicionais de segurança para dificultar a intrusão no ambiente e outros para possibilitar a recuperação dos dados em caso de necessidade.

6.1 MÚLTIPLOS FATORES DE AUTENTICAÇÃO

Uma das maneiras mais eficazes de impedir o uso de credenciais obtidas ilegalmente é o uso de funcionalidades de múltiplos fatores de autenticação (MFA). Esse método costuma requerer a tradicional combinação de usuário e senha e um código adicional que pode ser um código gerado em um *smartkey*, aplicativo de *smartphone* ou código enviado por SMS/e-mail, entre outros meios.

A segurança desse método está em requerer da pessoa que vai realizar o acesso algo além de um usuário e senha que pode ser compartilhado indevidamente ou obtido por atacantes. Como o código é gerado ou enviado para um dispositivo previamente cadastrado, somente a pessoa que tenha o dispositivo em mãos poderá acessar o código adicional de autenticação.

Para habilitar um dispositivo, como por exemplo um *smartphone*, instala-se o aplicativo de MFA em uso pela empresa nesse celular e realiza-se o processo de cadastramento do aparelho em um portal WEB da solução. Na maioria das soluções é enviado um código para o celular e, dessa forma, vincula-se aquele aparelho à aquela conta de usuário. A partir desse momento, o aplicativo do *smartphone* passa a gerar códigos numéricos diferentes a cada 30 ou 60 segundos e que são reconhecidos pelo servidor que solicita a autenticação. Esse código deve ser informado sempre que é realizada uma conexão.

As aplicações de MFA se tornaram populares pelo seu baixo custo operacional para a proteção adicional que proporciona. Aplicações críticas, conexões à rede corporativa e qualquer outra autenticação que requer usuário e senha pode ter a adição de uma solução de MFA.

6.2 USO DE SENHAS SEGURAS

Embora seja algo bastante óbvio, muitas pessoas ainda usam senhas que são fáceis de adivinhar ou usam a mesma senha para vários serviços.

Usar a mesma senha em vários lugares é um grande problema – se houver um vazamento de dados em qualquer um dos serviços e for possível obter os usuários e senhas de uma pessoa, geralmente disponíveis na *deepweb*, um atacante vai procurar dados sobre uma determinada pessoa e testar a senha encontrada. Estatisticamente é bastante provável que, num universo de, por exemplo, 100 usuários, pelo menos um repita a senha em mais de um serviço, colocando em risco a segurança de acesso da empresa.

Por essa razão é necessário ter programas de conscientização dos funcionários para eles criem senhas diferentes para cada sistema, serviço ou aplicação. Dessa forma, se as credenciais de um serviço forem vazadas, os outros acessos não estarão em risco. A maioria dos sistemas operacionais também possui funcionalidades que permitem exigir a construção de senhas complexas, incluindo caracteres maiúsculos, minúsculos, números e caracteres especiais e impedindo que sejam repetidas senhas já usadas. Essas regras de construção de senhas dificulta ataques de tentativa e erro, conhecidos como ataques de força-bruta, em que todas as possibilidades possíveis de senhas são testadas.

6.3 CÓPIAS DE DADOS

Na eventualidade de um ataque ou até mesmo na falha de equipamentos, ter uma cópia dos dados e aplicações é fundamental para restabelecer a operação da empresa.

Dessa forma, é preciso haver uma rotina de cópias de dados, também conhecida como *backup*, que contenha as informações atualizadas em prazos

compatíveis com as necessidades da empresa. Tipicamente as empresas realizam cópias de todos os dados uma vez por semana e cópias incrementais dos dados que são alterados ao longo da semana, economizando recursos de armazenamento.

Serviços de nuvem oferecem cópias automáticas e a replicação de dados entre os *datacenters* da empresa, que possibilitam garantir a disponibilidade dos dados caso a infraestrutura da empresa prestadora de serviços passe por alguma dificuldade técnica. Contudo, se os dados forem apagados ou criptografados nesses serviços, pode não haver maneira de restaurar uma posição anterior à deleção ou encriptação dos dados, dependendo da característica do serviço.

Por essa razão é importante ter cópias dos dados, tanto dos *datacenters* da empresa, quanto dos serviços de nuvem, para proteger a empresa contra eventuais falhas ou ataques. É preciso também garantir que essas cópias estejam íntegras e, principalmente, livres de *malwares* que possam corromper novamente o ambiente na ocasião da restauração dessas cópias.

Manter cópias dos dados em equipamentos que não sejam acessíveis diretamente pela rede é uma prática que protege os dados corporativos em caso de ataques de *ransomware*. Muitos dessas *malwares têm a capacidade de encriptar backups* se eles estiverem acessíveis pela rede ou conectados em equipamentos com acesso à rede. Apesar de haver soluções de *backup* que copiam dados para partições separadas dentro de um *storage*, essas cópias podem ser corrompidas no caso da disseminação de um *malware*. Soluções de *backup* para fitas e outras mídias removíveis ainda são aplicáveis e úteis, pela possibilidade de manter os dados corporativos desconectados de qualquer sistema que possa ser atacado.

6.4 RESTRIÇÃO DE PRIVILÉGIOS

Os sistemas operacionais e aplicações costumam trazer um conjunto de funcionalidades que podem trazer riscos se não usadas de maneira adequada.

Restringir os privilégios de administradores locais de máquinas, remover aplicativos desnecessários de sistemas operacionais, bloquear portas USB, impedir a instalação de programas e restringir a conexão a redes desconhecidas são maneiras simples e muito efetivas na proteção de um ambiente. Algumas vezes um *malware* não consegue se instalar em um sistema se essas diretrizes estiverem configuradas, elevando o nível de proteção do ambiente como um todo.

Algumas empresas optam por limitar o horário de conexão de seus empregados para apenas o horário comercial e desabilitar o acesso aos finais de semana e durante as férias do profissional, como uma maneira adicional de reduzir possibilidades de ataque.

A empresa deve adotar a postura de proporcionar o mínimo privilégio de acesso para seus empregados. Cada privilégio adicional que se fizer necessário deverá ser concedido de forma individual e com as devidas aprovações.

6.5 PRIVILEGED ACCCESS MANAGEMENT (PAM)

Soluções de PAM são conhecidas também como cofres de senha, que possibilitam criar controles para o uso de credenciais de administradores de sistemas, com todo monitoramento e sem que os administradores conheçam as senhas reais dos equipamentos e sistemas.

Ao invés de cada administrador ter uma conta privilegiada em cada equipamento ou sistema, ele terá apenas uma conta no PAM e os acessos são concedidos para ele em cada dispositivo que ele precisa acessar. O acesso ao dispositivo é feito por meio do PAM, como se fosse um proxy ou servidor de acesso. As soluções permitem adicionalmente monitorar e gravar as sessões e até mesmo restringir a execução de determinados comandos, possibilitando criar diferentes níveis de privilégios, mesmo em equipamentos que não possuam essa funcionalidade.

Caso o equipamento a ser administrado não seja compatível com uma solução de PAM, é possível obter uma senha temporária de acesso ao dispositivo que é trocada automaticamente após o uso, garantindo a segurança do ambiente como um todo.

O console de administração do PAM costuma ser integrado com as soluções de MFA disponíveis, possibilitando um elevado nível de segurança para as contas de administração de um ambiente.

6.5 SECURITY OPERATION CENTER (SOC)

Um centro de operações de segurança (SOC) é um serviço que monitora constantemente os alertas gerados pelos equipamentos de segurança de uma empresa, com a finalidade de detectar rapidamente uma ameaça ou ataque, analisá-la e, se preciso, realizar a contenção do ataque, evitando que se espalhe pela rede. Um SOC geralmente usa ferramentas de Siem para realizar esse monitoramento.

Esse serviço pode incluir também a gestão das vulnerabilidades técnicas do ambiente monitorado, atividade executada por meio de ferramentas automatizadas que verificam a presença de vulnerabilidades conhecidas em sistemas operacionais e aplicações, configurações de segurança inadequadas ou a presença de contas com senhas fracas. O SOC pode emitir um relatório das vulnerabilidades encontradas para que o cliente possa realizar as devidas correções para posterior verificação da sua resolução.

Um SOC também pode fornecer o serviço de verificação da segurança do ambiente, simulando ataques (testes de invasão ou *pentests*) no ambiente em busca de fragilidades que poderiam ser exploradas por um *hacker*. Eventuais problemas encontrados, assim como na verificação de vulnerabilidades, são compilados em relatório e entregues ao cliente para que providencie a correção dos problemas encontrados.

Cada empresa pode decidir ter um SOC interno, com infraestrutura e funcionários próprios, ou terceirizar completamente a operação para empresas especializadas. A escolha pelo melhor modelo deve levar em conta a complexidade da operação e o porte da empresa.

7 FALHAS DOS CONTROLES

Se por alguma razão um usuário reconhecer que abriu um arquivo anexo de um e-mail, acessou um site suspeito ou inseriu um dispositivo USB desconhecido, a melhor ação é realizar uma verificação completa no equipamento ou até mesmo reinstalar todo o sistema operacional, se alguma anomalia for notada ou detectada pelos mecanismos de segurança.

De tempos em tempos é preciso realizar uma verificação completa em todos os equipamentos da empresa, usando uma solução de antivírus, *endpoint protection* ou realizando uma atividade de escaneamento de vulnerabilidades. A detecção de qualquer anomalia deve ser prontamente solucionada para evitar a propagação de ameaças no ambiente.

Na ocasião de um ataque que coloque em risco dados pessoais, em especial, é preciso estar atento ao processo de notificação das partes interessadas – proprietários dos dados, agência nacional de proteção de dados e, se aplicável, seguradoras e processadores de dados.

Em ataques do tipo *ransonware*, em que é preciso pagar uma certa quantia para ter a chave de acesso aos dados, a situação precisa ser avaliada à luz das políticas da empresa. Sempre será preferível recuperar os dados por meio dos *backups* realizados do que ceder à extorsão. Caso a empresa decida pagar pelo resgate – que em algumas situações pode se tornar necessário, por não haver outra maneira de recuperar as informações –, é recomendável ter a evidência de que a chave realmente é capaz de abrir os arquivos antes de efetuar qualquer pagamento e ter o compromisso de que os dados serão destruído, bem como não divulgados. Alguns especialistas recomendam avaliar a possibilidade de pedir a evidência da destruição dos dados subtraídos e o compromisso de não divulgação dos dados, ainda que não seja possível confiar totalmente nos golpistas.

8 CONCLUSÃO

Considerando que a maioria das empresas possui seus sistemas informatizados e com algum nível de conexão com a internet, há um elevado risco de dados pessoais contidos nesses sistemas serem comprometidos por ataques cibernéticos, cada vez mais complexos e causando maior prejuízo para as empresas.

O investimento em soluções de segurança que, a princípio, pode parecer alto, justifica-se pelo risco à reputação da empresa em caso de um ataque, sem contar eventuais multas e sanções dos órgãos reguladores e de clientes. A complexidade dos ataques e a dificuldade de detectá-los rapidamente torna-se um grande desafio para empresas menores ou que não disponham de um centro de operação de segurança (SOC) ou similares.

A capacidade de detecção de ataques e saber como reagir a eles é importante para a empresa gerenciar seu próprio risco em relação à LGPD. Apenas o monitoramento constante e configurações adequadas de segurança do ambiente serão capazes de evitar problemas com a perda de informações e o desrespeito aos direitos das pessoas em relação aos seus dados pessoais.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001.** Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. [*s.l.*]: ABNT, 2013.

BARRETT, Matt *et al.* **Approaches for Federal Agencies to Use the Cybersecurity Framework**. Gaithersburg: National Institute of Standards and Technology, 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf. Acesso em: 10 jul. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jan. 2022.

MALWARE tip card. **Cybersecurity & Infrastructure Security Agency**, [201-?]. Disponível em: https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf. Acesso em: 10 jul. 2022.

14
A LGPD COMO NORTEADORA DA CRIAÇÃO DE CIDADES INTELIGENTES

Wallace da Silva Pereira

Resumo

Este artigo tem por objetivo sensibilizar os gestores públicos para a necessidade de harmonização entre as tecnologias fomentadoras das cidades inteligentes e a garantia dos direitos dos titulares de dados pessoais. O texto revela os avanços tecnológicos em prol de uma melhor experiência do cidadão, como também na execução eficaz de políticas públicas. Contudo, traz à superfície, maximizado pela pandemia, o desconhecimento parcial ou total da população por ferramentas digitais, que estão por traz dessa transformação digital. A metodologia utilizada foi pesquisa explicativa e qualitativa aplicada na forma bibliográfica.

Palavras-chave: urbanização; cidades inteligentes; transformação digital; internet das coisas; IoT; pandemia; LGPD.

Não é de hoje que o processo desenfreado de urbanização trouxe ao mundo um dos seus maiores desafios conhecidos. Tal fato traz à luz o tema cidades inteligentes (*smart cities*), a ser estudado com altíssima densidade em relação ao desenvolvimento urbano (GIL-GARCIA; PRADO; NAM, 2016 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021; JOSS *et al.*, 2017 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Assim,"[...] as cidades inteligentes surgem como uma alternativa para mitigar as consequências da urbanização acelerada por meio do uso de tecnologias sensitivas e cognitivas para gerenciar os serviços e infraestruturas das cidades" (apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021, p. 15).

O aparecimento de megacidades – cidades que possuem mais de 10 milhões de habitantes – e as projeções de aumento global da população urbana – em 2020, 4 bilhões, e em 2050, 7 bilhões (ONU, 2018 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021) traz à superfície diversas consequências. Dentre os desafios a serem enfrentados, temos congestionamento de veículos, poluição e degradação ambiental, violência, insuficiência de serviços básicos (água, energia, saneamento etc.), desigualdades sociais e econômicas, e deficiência no acesso a bens culturais e educacionais (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Segundo os dados da consultoria Frost & Sullivan (2019 (apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021), estima-se que em sete anos o mercado global de cidades inteligentes saltará de US $312,4 bilhões, em 2018, para US $1,56 trilhões, em 2025. No Brasil, para o mesmo período, o Plano Nacional de Internet das Coisas – IoT (BRASIL, 2019), juntamente com o BNDES, estimou, graças à IoT um incremento entre US$ 50 e US$ 200 bilhões à economia brasileira, sendo em torno de US$ 0,9 e US$ 1,7 bilhões referentes a cidades inteligentes (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Um panorama traçado pelo Smart City Strategy Index 2019 (ROLAND BERGER, 2019 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021), índice elaborado pela consultoria internacional Roland Berger que analisa cidades inteligentes no mundo, as regiões que apresentam o maior crescimento dessas cidades são América do Norte, Europa e Ásia. Nesse índice, aproximadamente 41% das cidades inteligentes estão situadas na Europa, 27% na Ásia, 24% na América do Norte e apenas 8% em outros continentes. A mesma leitura traz a World Smart City Awards (citada como o maior evento do gênero), o Smart City Expo World Congress e o IESE Cities in Motion (IESE, 2019 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021), eventos importantes sobre cidades inteligentes. Ambos demonstram a supremacia desses continentes contendo as mais bem avaliadas cidades inteligentes do globo.

Com o advento do Decreto Federal n. 9.854/2019(BRASIL, 2019a), que instituiu o Plano Nacional de Internet das Coisas (IoT), o Ministério do Desenvolvimento Regional (MDR) foi impulsionado a propor e liderar o processo de elaboração da Carta Brasileira para Cidades Inteligentes (MARINHO, 2021). O referido decreto tem como base outro marco legal federal, o Decreto n. 9.612/2018 (BRASIL, 2018a), que instituiu a Política Pública de Telecomunicações. Este último especificou que o Programa de Cidades Digitais do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), atualmente desdobrado em Ministério da Ciência, Tecnologia e Inovações (MCTI) e Ministério das Comunicações (MCOM), seria substituído pelo Programa de Cidades Inteligentes. Em 2021, o Decreto n. 9.612/2018 foi alterado pelo Decreto n. 10.799/2021 (BRASIL, 2021), que instituiu, em seu artigo 6.º, que:

> O Ministério das Comunicações promoverá a implantação de infraestruturas destinadas ao desenvolvimento de Cidades Conectadas por meio das seguintes iniciativas: I - implantação de infraestruturas prioritariamente em cidades com inexistência de redes de acesso de alta capacidade, com vistas à promoção da melhoria da qualidade, à oferta de novos serviços aos cidadãos e ao aumento da eficiência dos serviços públicos.

O Programa de Cidades Inteligentes, por sua vez, é fomentado em uma das câmaras temáticas – Câmara das Cidades 4.0 (CÂMARA..., 2019) – do já citado Plano Nacional de Internet das Coisas (BRASIL, 2019), que visa a contribuir para o trabalho dos gestores públicos federais, estaduais e municipais, auxiliando-os a identificar as condições atuais das cidades, as competências e necessidades para avançar em direção a se tornarem cidades inteligentes sustentáveis, a médio e longo prazos (MARINHO, 2021).

A Carta Brasileira para Cidades Inteligentes (MARINHO, 2021), em consonância com a Política Nacional de Desenvolvimento Urbano – PNDU (BRASIL, 2001) –, é fruto de um esforço coletivo do governo Federal para definir uma "estratégia nacional para cidades inteligentes". Foi um importantíssimo passo para que o país canalizasse os seus esforços em direção ao desenvolvimento econômico mitigando as desigualdades sociais. O intento da produção dessa carta é um convite para ser utilizado por pessoas e instituições engajadas com a melhoria na qualidade de vida nas cidades, e tê-la como referência seguindo uma "agenda pública para a transformação digital nas cidades brasileiras". Diversos segmentos da sociedade brasileira que estão envolvidos com os temas ligados ao desenvolvimento urbano, ao meio ambiente e à tecnologia, bem como com à criação e ao adimplemento de políticas públicas e ações de desenvolvimento local, apoiam o discurso da referida carta.

Em 2021, durante a 4.ª Reunião da Câmara das Cidades 4.0 (CÂMARA..., 2019), a Secretaria de Empreendedorismo e Inovação do MCTI lançou a plataforma inteli.Gente MCTI (BRASIL, 2019b). A novidade foi desenvolvida pela Rede Nacional de Ensino e Pesquisa (RNP),[66] conjuntamente com o Centro de Tecnologia da Informação Renato Archer (CTI),[67] que é o responsável pela construção do modelo brasileiro de maturidade de cidades inteligentes e sustentáveis. Com a recém-publicação pelo CTI do livro eletrônico *Cidades Inteligentes Sustentáveis no Brasil* (PEREIRA; MUNIZ; ALVES, 2022), materializa-se a metodologia de avaliação e diagnóstico de cidades inteligentes e sustentáveis utilizada na plataforma. A maturidade é diagnosticada em quatro dimensões (figura 1), sendo elas: meio ambiente,

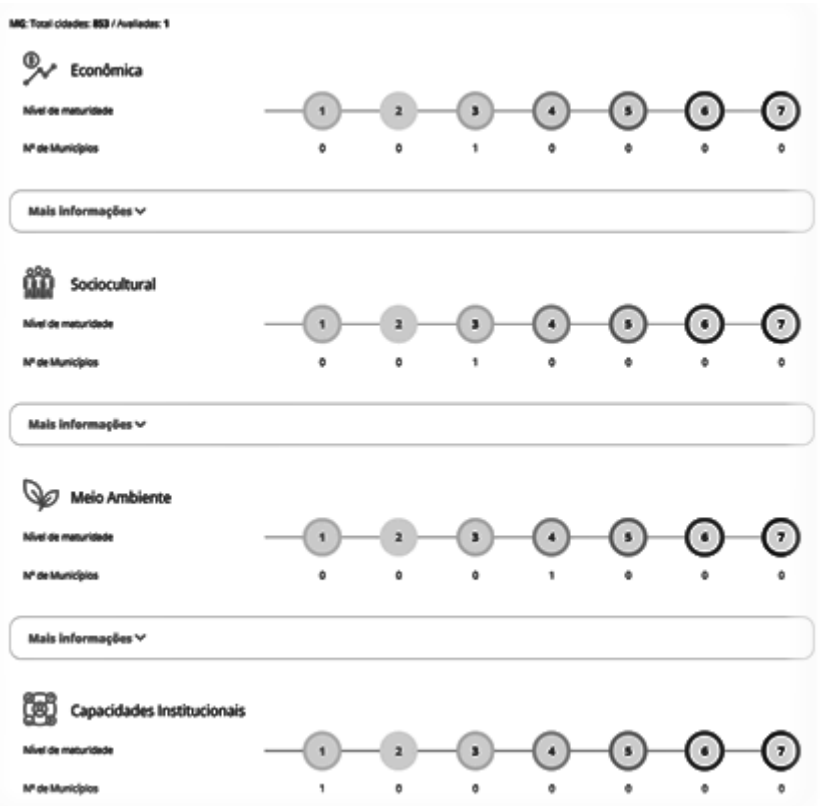
66 A RNP foi criada em setembro de 1989 pelo então Ministério da Ciência e Tecnologia (MCT). Seu objetivo era construir uma infraestrutura nacional de rede de internet de âmbito acadêmico. A Rede Nacional de Pesquisa, como era chamada em seu início, tinha também a função de disseminar o uso de redes no país. Hoje, sua origem e essência pautam-se em ser uma rede brasileira para educação e pesquisa. Disponibiliza internet segura e de alta capacidade, serviços personalizados e promove projetos de inovação.

67 O Centro de Tecnologia da Informação Renato Archer (CTI) é uma unidade de pesquisa do Ministério de Ciência, Tecnologia e Inovações (MCTI) que desde 1982 atua em parceria com agentes do setor privado, da academia e do governo, para promover um ambiente propício à geração de inovações em processos e produtos, visando ao fortalecimento da indústria nacional e ao bem-estar da população (SOBRE..., 2021).

econômica, sociocultural e capacidades institucionais da gestão pública municipal. O livro traz uma síntese dos principais resultados alcançados pelo Sistema de Avaliação de Cidades Inteligentes Sustentáveis – Sisacis (RUMO..., 2021).

A solução da plataforma inteli.Gente MCTI deverá propor diretrizes para a construção da política nacional e municipal para cidades inteligentes sustentáveis. A inteli.Gente MCTI contribui para o trabalho dos gestores públicos federais, estaduais e municipais, subsidiando-os na identificação das condições atuais das cidades, das competências e necessidades para tornarem-se cidades inteligentes sustentáveis, a médio e longo prazos. A plataforma agrega diversos interessados, dentre eles: indústria, instituições públicas e privadas, academia e cidadãos. Com esse ecossistema posto, possibilita a montagem de uma enorme base de conhecimento das cidades com o intuito de canalizar esforços para o aumento da transformação digital e do desenvolvimento urbano sustentável daquela localidade (RUMO..., 2021).

Figura 1 – As quatro dimensões do inteli.Gente MCTI.

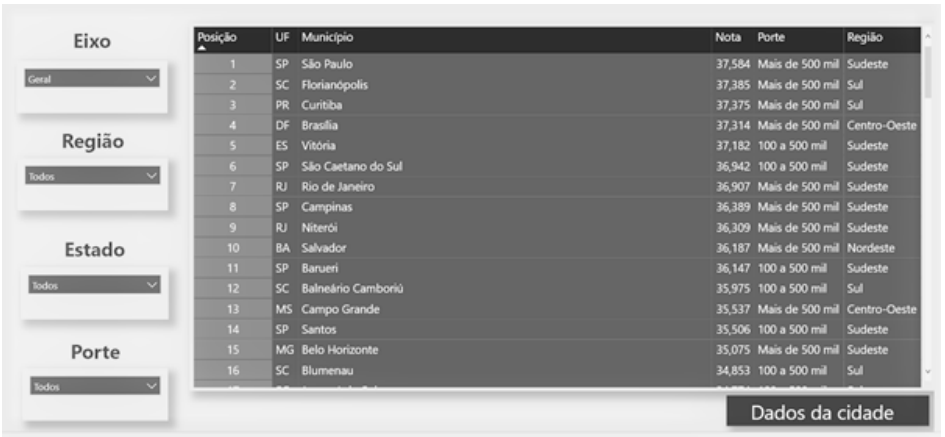


Fonte: Brasil (2019b).

Outras plataformas similares à inteli.Gente MCTI emergem, nesse mundo digital, também na área privada. Elas trazem na sua essência, como objetivo central, contribuir para que a cidade entenda as suas reais vocações – seus pontos fortes, suas cadeias econômicas e suas âncoras de desenvolvimento – e, por outro lado, conhecer os seus pontos fracos – seus *gaps* de infraestrutura e suas fraquezas perante as outras cidades. Dentre as plataformas similares que se destacam, temos a Ranking Connected Smart Cities[68] (figura 2), disponibilizada pela empresa Urban Systems. A empresa é uma consultoria de inteligência de mercado e planejamento urbano, com visão sistêmica e integrada, que auxilia na elaboração de diagnóstico de cidades e no desenvolvimento de planos estratégicos econômicos e urbanos (URBAN SYSTEMS, 2021).

A edição 2021 do *Ranking Connected Smart Cities* coletou dados e informações de todos os municípios brasileiros com mais de 50 mil habitantes (segundo estimativa populacional do IBGE (URBAN SYSTEMS, 2021) em 2019), totalizando 677 cidades, sendo: 48 com mais de 500 mil habitantes, 274 com 100 a 500 mil habitantes e 349 com 50 a 100 mil habitantes. Essa plataforma é composta por 75 indicadores em 11 eixos temáticos: mobilidade, urbanismo, meio ambiente, tecnologia e inovação, empreendedorismo, educação, saúde, segurança, energia, governança e economia (URBAN SYSTEMS, 2021).

Figura 2 - Ranking Geral *Connected Smart Cities* 2021.



Posição	UF	Município	Nota	Porte	Região
1	SP	São Paulo	37,584	Mais de 500 mil	Sudeste
2	SC	Florianópolis	37,385	Mais de 500 mil	Sul
3	PR	Curitiba	37,375	Mais de 500 mil	Sul
4	DF	Brasília	37,314	Mais de 500 mil	Centro-Oeste
5	ES	Vitória	37,182	100 a 500 mil	Sudeste
6	SP	São Caetano do Sul	36,942	100 a 500 mil	Sudeste
7	RJ	Rio de Janeiro	36,907	Mais de 500 mil	Sudeste
8	SP	Campinas	36,389	Mais de 500 mil	Sudeste
9	RJ	Niterói	36,309	Mais de 500 mil	Sudeste
10	BA	Salvador	36,187	Mais de 500 mil	Nordeste
11	SP	Barueri	36,147	100 a 500 mil	Sudeste
12	SC	Balneário Camboriú	35,975	100 a 500 mil	Sul
13	MS	Campo Grande	35,537	Mais de 500 mil	Centro-Oeste
14	SP	Santos	35,506	100 a 500 mil	Sudeste
15	MG	Belo Horizonte	35,075	Mais de 500 mil	Sudeste
16	SC	Blumenau	34,853	100 a 500 mil	Sul

Fonte: Urban Systems (2021).

68 Por haver diversos conceitos de cidades inteligentes, desde os que estão mais apoiados em tecnologia até aqueles que estão mais relacionados ao meio ambiente e à sustentabilidade, elaborou-se um *ranking* nomeado Connected Smart Cities. O estudo considera o "conceito de conectividade" como sendo a relação existente entre os diversos setores analisados. O conceito de *smart cities* considerado entende que o desenvolvimento só é atingido quando os agentes de desenvolvimento da cidade compreendem o poder de conectividade entre todos os setores.

A transformação digital no mundo figura há mais de uma década como item de ponta, alicerçando as iniciativas tecnológicas para as cidades inteligentes. Essas iniciativas buscam no mercado produtos e serviços que visam à redução de custos e a uma melhor experiência para o cidadão nas suas cidades.

A partir da quarta revolução industrial (SCHWAB, 2017 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021) – expressão surgida durante a Feira de Hannover (Alemanha) em 2011 –, fica visível a necessidade mundial com a busca massiva da transformação digital pelas instituições públicas e privadas. A quarta revolução industrial ultrapassa as linhas fabris, criando uma simbiose entre os domínios físico, digital e biológico, nascendo o conceito da Indústria 4.0 (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

A expressão Indústria 4.0 está em crescimento no Brasil e no mundo. Segundo dados publicados em 2018 pela Agência Brasileira de Desenvolvimento Industrial (ABDI),[69] esse conceito tem capacidade para movimentar US$ 15 trilhões nos próximos 15 anos. A Indústria 4.0 está ligada à interconectividade através da Sociedade da Informação e da IoT; a IA (inteligência artificial) através da *machine learning* e da *deep learning*; do *big data* através do *data science* e da análise comportamental; da *cloud computing* através de grandes *data lakes*; entre outros, que, com base em dados e informações de mercado, ajudam a decifrar e a acompanhar as mudanças nos hábitos de consumo e nas demandas dos clientes, tanto em formato B2B (*business to business*) quanto em B2C (*business-to-consumer*) (QUAIS..., [201-?]).

Das tecnologias que despontam na Indústria 4.0, os dispositivos de IoT possibilitam a criação de identidades únicas para máquinas e equipamentos, para pessoas, para objetivos ou para animais. A IoT possibilita a realização de comunicação máquina-máquina e o registro contextual granularizado (temperatura, umidade, rostos, placas etc.). Essa tecnologia relaciona-se com as outras já mencionadas no parágrafo anterior, como processamento de dados em tempo real, aprendizado por máquina (*machine learning*), sistemas embarcados e inteligência artificial, tornando factível administrar pontos longínquos, antes, inimagináveis, das cidades (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Quando se trata do tema cidades inteligentes com o viés tecnológico, as novas ferramentas de tecnologia da informação e comunicação (TIC), como a IoT, coadunadas com novas máquinas e equipamentos, propiciam o monitoramento e a gestão de aspectos variados da vida urbana. Exemplificando a aplicabilidade da IoT a esse contexto, temos o poste de iluminação conectado

69 Tem o objetivo de estimular a transformação digital e a adoção e difusão de tecnologias e de novos modelos de negócios no setor produtivo, seja nas empresas, indústria ou serviços, promovendo o debate entre governo e empresas para qualificar políticas públicas e ações estratégicas voltadas ao aumento da competitividade da economia brasileira frente aos desafios da era digital (TRANSFORMAÇÃO..., [202-?]).

ou inteligente, que também pode fornecer acesso à internet sem fio, anunciar alertas ao cidadão, monitorar o tráfego local de pessoas e veículos, identificar previamente regiões alagadas ou georreferenciar indícios sonoros de tiros (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Waleed Ejaz e Alagan Anpalagan (FALEIROS JÚNIOR, 2021) sugerem outras denominações para a implementação de recursos baseados no conceito de IoT, visando a melhorar a gestão da vida do cidadão, ao nível habitacional (*smart homes*), elétrico/energético (s*mart grids*), econômico (*smart economy*), de mobilidade urbana (*smart mobility and transport*), de atendimento à saúde (*smart healthcare*) e de segurança pública (*smart security*).

A grande volumetria gerada de dados a partir dessa interconectividade das coisas possibilita que o gestor público esteja alinhado à geração de análises preditivas, ao estudo do comportamento do cidadão e a todo o acervo informativo fomentado dentro e fora dos mercados corporativos (*data-driven management*). Essa base de conhecimento gigantesca oriunda dessa interconectividade ganha o status mundial de "novo petróleo do século XXI" (CULTURA..., [202-?]).

A cultura *data-driven* entre as instituições públicas e privadas nasceu na esteira da ideia segundo a qual "quanto mais informação melhor". Contudo a adoção da cultura *data-driven* deverá ser estabelecida por esses organismos como um processo, identificando o *quantum* de informações capturadas pelos dispositivos computadorizados, e se estes estão voltados à finalidade para a qual foram desenhados. É importante trabalhar a mudança do *mindset* entre os gestores dessas bases de conhecimento para evitar conflitos sociotecnológicos em suas ações (CULTURA..., [202-?]).

Doneda (2018) adverte-nos sobre a preocupação da adoção da cultura *data-driven* em larga escala:

> Uma parte relevantíssima, senão a grande maioria, do potencial das *smart cities* consiste em proporcionar um tratamento útil ao emaranhado de informação pessoal coletadas por sensores e pelos diversos sistemas tecnológicos que compõem este ecossistema.

Os primeiros imbróglios sociotecnológicos sobre cidades inteligentes nascem, então, dessa massiva penetração da tecnologia no meio urbano, principalmente na infraestrutura das cidades, com objetivo primário de alcançar o sucesso nas políticas públicas estabelecidas pelo gestor. Esses entes públicos impulsionados por empresas de tecnologias de hardware e software definiram as diretrizes que as cidades inteligentes deveriam seguir. A base tecnológica sozinha, sendo matéria-prima para essa "jornada na criação de cidades inteligentes", cria o paradigma que a inovação nesse setor e é a panaceia para soluções dos problemas das cidades. Nesse contexto, a tecnologia inovadora é o subsídio vital para os agentes públicos que buscam trilhar esse caminho (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Exemplo disso são a IBM e a CISCO, grandes fornecedores de tecnologia para hardware e software, as quais definem como modelos de cidades inteligentes, respectivamente, aquelas que utilizam quaisquer meios de informação para avaliar e gestar processos que utilizem, de forma mais eficiente, os recursos disponíveis (COSGROVE *et al.*, 2011 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021), e aqueles que se apoiam na escalabilidade das soluções da TIC com objetivo de "aumentar a eficiência, reduzir custos, e melhorar a qualidade de vida" (FALCONER; MITCHELL, 2012 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Hall (2000, p. apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021, p. 17) nos brinda com uma definição de cidades inteligentes a partir do enfoque tecnológico:

> A cidade que monitora e integra todas as infraestruturas críticas (estradas, pontes, túneis, metrôs, trens, aeroportos, portos, comunicação, água, energia e grandes edifícios), otimizando o uso de recursos, planejando manutenções preventivas e monitorando aspectos de segurança para maximizar a performance dos serviços oferecidos aos cidadãos.

Na Ásia, os governos também foram na mesma linha dos *players* de hardware e software, utilizando-se do paradigma tecnológico na busca de soluções para sustentabilidade ambiental. A Coreia do Sul utiliza-se do viés tecnológico para catapultar o seu crescimento econômico tangenciando os temas sobre energia limpa e digitalização. Segundo a Japan Smart Community Alliance (JSCA) (EU-JAPAN, 2014 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021), o Japão traz o conceito de cidades inteligentes enraizado na utilização de várias tecnologias de ponta alicerçado a partir de avançados de sistemas sociais integrados e da utilização eficiente de energia e transportes. *Guidance on Promoting Healthy Smart City Development* é o nome do programa em implantação que a China utiliza, lançando mão das mais avançadas tecnologias da informação e comunicação na busca de uma ocupação urbana inteligente, modelos de gestão mais sustentáveis e melhores serviços para os seus cidadãos. Dentre as tecnologias chinesas, destacam-se a computação em nuvem, a IoT e o *big data*, (NDRC, 2014 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Há diversos autores que criticam a utilização isolada do paradigma tecnológico para as cidades inteligentes, modelo esse altamente influenciado por *players* da área da TIC que, muitas vezes preocupados em manter as tecnologias inovadoras em voga, com objetivo de vender cada vez mais para os agentes públicos, esquecem de um dos vértices mais importantes do tripé informacional: as pessoas. Os países que apontam para modelos aplicados a cidades inteligentes que consideram relevantes os aspectos humanos, bem como as dinâmicas socioculturais, alicerce na formação de uma cidade, trazem para o foco do seu planejamento para o cidadão (KOMNIMOS *et al.*, 2013 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Esse cidadão, que a cada dia é exposto às tecnologias inovadoras, a novos meios de comunicação com o mundo digital passando à margem do planejamento das cidades inteligentes, tem que ser, previamente, mais bem preparado para poder fazer parte, de forma segura, desse arcabouço tecnológico inovador. O aumento do analfabetismo digital é um sinal de que um modelo calcado somente no paradigma tecnológico não seria profícuo. A falta da cultura digital da sua população assola muitos países que buscam uma transformação digital. Por isso que, reiteradamente, o analfabetismo digital tem sido colocado na pauta de desenvolvimento de cidades inteligentes, pois cada vez mais é visível o despreparo do cidadão em relação a utilização das tecnologias disponíveis nas *smart cities*. Os benefícios trazidos pela transformação digital ficaram fora do alcance de boa parte da população mundial. Destarte, é de suma importância que conste na agenda positiva das cidades inteligentes a capacitação dos cidadãos objetivando o seu empoderamento como usuário, ao explorar com segurança os potenciais da vida urbana digital. (apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

No Brasil, antes da pandemia, essa nova classe emergente de cidadãos sem o preparo necessário para fazer frente às novas tecnologias – por exemplo, sem os conceitos básicos para navegar pela internet – começa a surgir e incrementar o grupo dos analfabetos digitais, aquelas pessoas que não conseguem compreender as ferramentas do universo digital.

Para contextualizar esse grupo, segundo o site do Indicador de Analfabetismo Funcional (Inaf) (QUEM..., [201-?]), as pessoas podem ser classificadas em cinco níveis de analfabetismo: analfabeto, rudimentar, elementar, intermediário e proficiente. Os dois primeiros, analfabeto e rudimentar, caracterizam um analfabeto funcional, ou seja, pessoas que reconhecem letras e números e que talvez consigam ler pequenos textos, mas não entendem conteúdos mais elaborados ou tem compreensão dele. Até 2018, ainda segundo o Inaf (NÍVEL..., 2018), 8% da população brasileira eram analfabetos e 22% eram analfabetos rudimentares.

Já através da Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua (PNDA..., 2021), apresentada no quarto trimestre de 2019, a informação apresentada é que 75,4% das pessoas entrevistadas que não acessavam internet alegaram não saber usá-la ou falta de interesse.

Nesse cenário, se colocarmos a variável da educação básica, a partir de algumas regiões do nosso país, os problemas do analfabetismo digital são exponenciados. Havendo a deficiência em formar pessoas e, ao projetar um contingente de novos usuários mal instruídos para a vida digital, com a possibilidade de fazer o que quiser no mundo on-line, os abusos e crimes virtuais serão uma realidade cada vez maior, e o que deveria incluir, será motivo de exclusão (RIBEIRO, 2018)

Na esteira legislativa do Brasil, já foram propostas quatro emendas à Constituição, com o fim de incluir o acesso à internet no rol de direitos fundamentais nela previsto. A primeira, PEC n.ç 6/2011 (ROLLEMBERG,

2011), foi arquivada e pretendia inserir o direito de acesso à internet entre os direitos sociais previstos no artigo 6.º da CF. A segunda, de iniciativa da Câmara dos Deputados, desarquivada em 2019 e em tramitação no Congresso Nacional, a PEC n. 185/2015 (ABREU, 2015) busca assegurar a todos o acesso universal à internet entre os direitos fundamentais do cidadão. A terceira, a PEC n. 8/2020 (PASTORE, 2020), de iniciativa do Senado Federal, proposta em março de 2020, também tem o condão de inserir o direito de acesso à internet no rol previsto no artigo 5.º. A quarta, PEC n. 35/2020 (PAIN, 2020), também do Senado Federal, visa a alterar os artigos 5.º, 6.º e 215.º da CF, para inserir o direito de acesso à internet no rol de direitos sociais, assim como o dever de assegurar acesso à internet a todos os residentes no país, tendo sido encaminhada ao plenário do Senado ainda em 2020 (SARLET; SIGUEIRA, 2021).

Senne (2021, p. 26) adverte-nos sobre a necessidade real do acesso à internet como meio de a população buscar a sua cidadania digital: "A Internet deve servir como meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de toda a população".

A emergente Indústria 4.0 nas instituições públicas e privadas e o analfabetismo digital trazem novos desafios à sociedade brasileira quanto ao futuro dos empregos e à criação de novas relações econômicas decorrentes de mudanças substanciais no modo de produção. Esse binômio técnico-social que acarreta mais desigualdade de renda e de emprego faz com que tais assuntos venham a fazer parte dos questionamentos sobre o desenvolvimento das cidades inteligentes (CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Considerando a força da Indústria 4.0, mais cidadãos brasileiros fora da escola, do mercado de trabalho e das relações familiares, inexoravelmente, haverá mais criminosos, valores distorcidos e uma população cada vez mais numerosa sem instrução do universo digital para o físico. Essa visão alarmante é trazida por Ribeiro (2018): "[...] a ideia de se colocar mais gente com critérios deficientes ou valores inexistentes em ambiente digital, vai ser absorvido pela vida real. E o impacto disso vai ser desastroso".

Para ratificar o impacto do analfabetismo digital na tentativa dos gestores públicos de traçarem uma política que envolva a transformação digital, verifica-se a cidade de Filadélfia, localizada no estado da Pensilvânia, EUA. Cidade sempre situada em *rankings* de cidades inteligentes em nível global, enfrentou problemas culturais quando integrou serviços públicos de emergência sob o Programa 311[70]. Diversos entraves sociais também ajudaram a comprometer esse plano de ação: poder e cultura dos órgãos e servidores públicos, exigindo a mudança de práticas, governança e

70 O *contact center* Philly311 é o centro de atendimento ao cliente da Filadélfia para consultas não emergenciais. As solicitações de serviço podem ser enviadas por telefone, aplicativo móvel e aplicativo da web (PHILLY3011, [201-?]).

comportamentos dos agentes e organizações públicas (NAM; PARDO, 2014 apud CARNEIRO; LUDIMILA; LAMOUNIER, 2021).

Aqui no Brasil, como em grande parte do mundo, onde a transformação digital ainda não flui na sua plenitude entre a sua população, o enfrentamento à pandemia, desde 2020, fez a duras penas os cidadãos buscarem, a todo custo, a conectividade com o mundo digital frente às necessidades do mundo real.

Na busca por amenizar os efeitos da pandemia, Senne (2021) descreve a importância do uso da Internet:

> No contexto da pandemia COVID-19 e da adoção de medidas de isolamento social, o uso da Internet tornou-se ainda mais indispensável, seja para comunicar-se, seja para acessar informações, serviços e produtos essenciais. Assim, promover o acesso e uso de tecnologias acessíveis, abertas, diversas e plurais é fundamental para mitigar os efeitos da atual crise sanitária e garantir o acesso à informação.

A partir da publicação, em 2021, pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), do Panorama Setorial da Internet (HENRIQUES; MARTINS JÚNIOR, 2016), pôde-se constatar, em meio à pandemia, as dinâmicas de uso da internet no Brasil. Os dados oriundos do Painel TIC Covid-19, com coordenação do Ponto BR - NIC.br[71] e criado pelo seu Núcleo de Informação, entre junho e setembro de 2020, trouxe um panorama sobre as disparidades na qualidade do acesso, e se esses influenciaram ou não na realização de atividades on-line, bem como se houve ou não o aproveitamento eficiente da adoção da internet por parte da população (SENNE, 2021).

Ainda em meio à crise pandêmica, sobre o crescimento na realização de atividades on-line, é possível notar, nesse pequeno recorte, a manutenção da disparidade de uso da rede segundo as classes sociais (figura 3), o que foi ainda mais evidenciado para as transações financeiras e as atividades de trabalho. Já no caso dos serviços públicos, a distância entre as classes foi reduzida no período, o que está associado à implementação de programas sociais como o auxílio emergencial. O programa do Governo Federal adotou um aplicativo de celular como via preferencial de acesso e movimentação do benefício, programa esse direcionado à população de baixa renda e em situação de informalidade, cuja renda familiar foi fortemente impactada pela crise sanitária. Em resumo, os dados demonstram que houve uma migração de parcelas importantes da população para práticas on-line, o que não foi suficiente para equilibrar as desigualdades digitais quanto ao uso da rede. Não há dúvidas de que tais diferenças ainda podem ter implicações

71 O Núcleo de Informação e Coordenação do Ponto BR - NIC.br foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil – CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da internet no País.

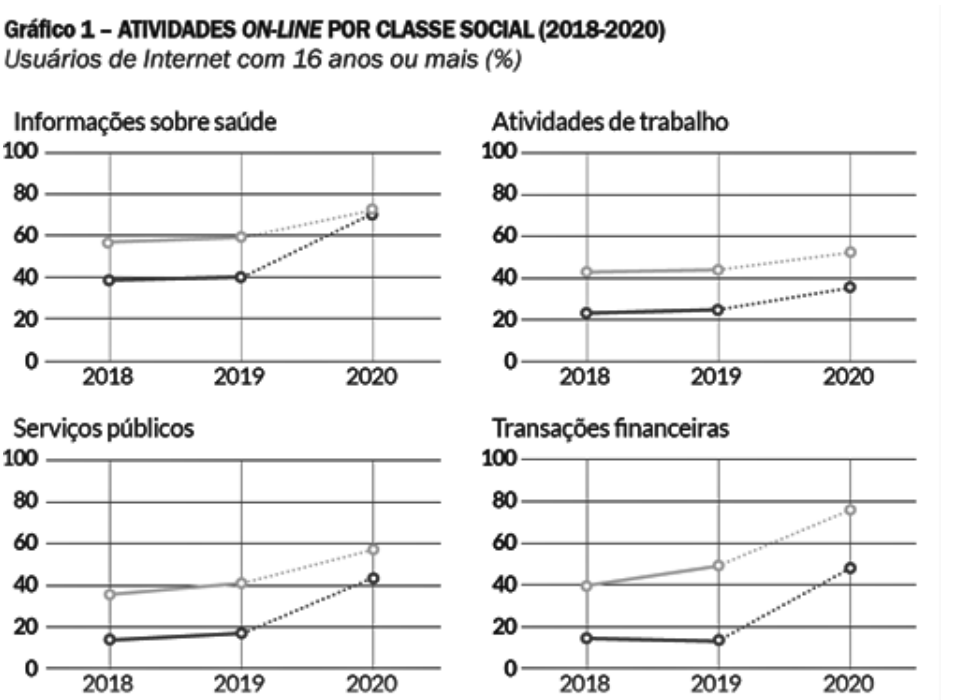
significativas para a capacidade de enfrentamento à Covid-19 e a mitigação de seus efeitos negativos (SENNE, 2021).

Sobre a preocupação constante em termos não somente cidadãos não conectados, mas indivíduos incluídos no mundo digital, principalmente em meio à pandemia, Senne (2021) nos aponta que:

> [...] superar as barreiras da conectividade por si só não é suficiente para o pleno aproveitamento das oportunidades oferecidas pela Internet. As desigualdades digitais devem ser superadas também no nível do uso da rede, para que ela seja usufruída por todas as pessoas, independentemente de hardware, software, idioma, local ou habilidade.

Diante de todo esse poderio computacional integrado, visto até aqui, dados (cultura *data-driven*) e equipamentos (IoT) à disposição das cidades inteligentes, como também de toda essa falta de empatia pelo fortalecimento do conhecimento digital da população, crescem os imbróglios sociotecnológicos quando se apercebe o volume estrondoso de dados pessoais e dados pessoais sensíveis gerados por seus principais usuários, os cidadãos (PINTO, 2022).

Figura 3 - Painel TIC Covid-19 Cetic.br.



Fonte: Painel... (2021).

Doneda (2018) aumenta o coro sobre a preocupação dos problemas sociais que esse poderio computacional integrado pode causar ao cidadão:

> As fontes destes dados pessoais vão desde dispositivos implementados especificamente para este fim – como sensores capazes de identificar transeuntes em um determinado ambiente público, até a utilização de fontes de dados que, cada vez mais, passam a ter seu interesse público reconhecido em atos normativos ou administrativos.

A preocupação dos juristas é que aplicações que capturam informações pessoais de toda sorte dos cidadãos, com a finalidade primária de dar-lhes uma melhor experiência na aquisição de um serviço, seja esse público ou privado (aplicativos de transporte ou de hospedagem), acabam convergindo na busca de informações demasiadas e que são objetos de cobiça por mercados paralelos aos que foram destinados. Os riscos sobre o tratamento indevido de informações pessoais aumentam, numa progressão geométrica, quando da realização de diversos cruzamentos, em bases de conhecimento, apartadas daquela da sua origem, que envolvem sementes residuais de dados oriundos de resultados obtidos enquanto são executadas outras políticas públicas. Os relacionamentos dos domínios informacionais vão para áreas como análise de padrões de consumo de energia elétrica em unidades residenciais, os quais, a princípio, têm o viés de gestar melhor a cobrança do seu consumidor. Contudo ao serem cruzadas com outras bases de conhecimento podem comprometer a privacidade do cidadão (DONETA, 2018).

A assimetria que existe entre a necessidade de o cidadão consumir o serviço, público ou privado, obriga muitas vezes o usuário a não dar a devida importância à confidencialidade dos seus dados pessoais. Sim, é importante que todo cidadão esteja conectado à internet para usufruir das benesses oferecidas pelas tecnologias presentes nas cidades inteligentes, contudo esse usuário deverá ter acesso não somente ao serviço que deseja consumir, mas também aos processos que estão envolvidos e à política pública a que esse serviço está intrinsecamente ligado (FALEIROS JÚNIOR, 2021).

O uso massivo das tecnologias da informação e comunicação na composição das cidades inteligentes e, por conseguinte, a existência de uma sinergia direta com a população urbana e as suas prioridades, leva à necessidade premente de regulações mais próximas dos cidadãos para dar a garantia necessária aos processos que a eles são atribuídos. Doneda (2018) chama atenção para a visão sociotecnológica acerca dessa sinergia desenfreada sem um revestimento legal:

> A integração de dispositivos, sensores, redes e software no contexto das *smart cities* deve, ainda e principalmente, ter seu foco na integração com os cidadãos. Assim, os seus efeitos hão de ser previstos, projetados e mesurados não somente em função de vetores quantitativos pertinentes

> à cada atividade individualmente considerada, porém igualmente em relação ao seu impacto nos cidadãos, em seus direitos e garantias.

Urge, então, que os agentes públicos de transformação instruam esse real protagonista da inovação, o cidadão, para o convívio harmonioso com esse novo mundo digital urbano. A necessidade dessa capacitação dele, em grande escala, já tratada neste artigo, objetivando, também, a tutela dos seus dados pessoais e dados pessoais sensíveis frente a essa nova vida urbana digital, agora encontra, no Brasil, uma base jurídica sólida que implementou direitos sobre as informações a serem custodiadas ora pelo poder público, ora por instituições privadas. Essa base nasceu com a promulgação da Lei n. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, LGPD (BRASIL, 2018b) – e com a recente também promulgação da Emenda Constitucional n. 115 (BRASIL, 2022), que incluiu a proteção de dados pessoais na categoria de direitos e garantias fundamentais, descritas no inciso LXXIX, do artigo 5.º da CF, com a seguinte redação: "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais" (PINTO, 2022).

Se, por um lado, a LGPD traz para o cidadão a segurança necessária para adentrar nesse mundo tecnológico, possibilitando interagir com os serviços que estão a sua disposição dentro das cidades inteligentes, por outro lado, essa lei apresenta aos gestores municipais a obrigação de estarem em consonância com suas políticas públicas, tomando como base os fundamentos listados no art. 2.º e nos princípios elencados no art. 6.º desse marco legal. É de fundamental importância que as atividades de tratamento de dados realizadas por processos advindos dos serviços disponibilizados a seus cidadãos estejam em sintonia com a LGPD (FALEIROS JÚNIOR, 2021).

Na necessária agenda à capacitação ao cidadão a Autoridade Nacional de Proteção de Dados (ANPD), criada a partir da Lei n. 13.853, de 8 de julho de 2019 (BRASIL, 2019c), tem cumprido esse papel. Dentre as publicações realizadas por essa autoridade, o Guia *Como Proteger seus Dados Pessoais* (BRASIL, [202-]) traz ao cidadão esse empoderamento: "Os seus dados pessoais importam!". Houve mudança de *mindset* tão necessária para o convívio em harmonia com os avanços tecnológicos trazidos pelas *smart cities*.

Ainda no viés do aculturamento digital, a ANPD revela aos gestores públicos formas legais de tratamento de dados pessoais dos seus cidadãos. Através do *Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público* (BRASIL, 2022) (arts. 23 e seguintes da LGPD), dá-se um norte para os atuais administradores municipais sobre jeito certo de fazer a "coisa". A utilização de bases legais circunscritas aos princípios da LGPD faz com que os gestores avaliem seus processos de tratamento de dados pessoais, gerando instruções normativas com esse tema para cada serviço disponibilizado. Dessa maneira, os riscos inerentes à custódia de informações

obtidas de maneira fortuita (*big data*), com propósito diverso daquela política pública a qual tinha o seu intento, serão mitigados com a aplicação correta de algoritmos de interoperabilidade.

Desde a Declaração Universal dos Direito Humanos (ONU, 1948), de 10 de dezembro de 1948, consagrou-se que "[...] todo ser humano tem direito a receber dos tribunais nacionais competentes remédio efetivo para os atos que violem os direitos fundamentais que lhe sejam reconhecidos pela constituição ou pela lei". À vista disso, a proteção de dados pessoais, que no Brasil, agora, é um direito fundamental, deverá ser garantida a todos os cidadãos na busca do reconhecimento, com o zelo que o tratamento das informações pessoais dele e do seu próximo merece, por sua alta criticidade. Essa mudança de contexto de cada indivíduo é de suma importância para elevar o sistema protetivo do tema. Só assim, os gestores das cidades inteligentes entenderão a importância de assegurar em suas agendas a harmonia do binômio proteção de dados dos seus munícipes e a transformação digital de suas cidades.

REFERÊNCIAS

ABREU, R. **PEC 185/2015**. Acrescenta o inciso LXXIX ao art. 5º da Constituição Federal, para assegurar a todos o acesso universal a Internet entre os direitos fundamentais do cidadão. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2075915. Acesso em: 29 mar. 2022.

BRASIL. **Como proteger seus dados pessoais:** Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Brasília: Ministério da Justiça e Segurança Pública, [202-]. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 2 abr. 2022.

BRASIL. **Decreto n. 10.799, de 17 de setembro de 2021**. Altera o Decreto nº 9.612, de 17 de dezembro de 2018, que dispõe sobre políticas públicas de telecomunicações. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10799.htm#art1. Acesso em: 29 mar. 2022.

BRASIL. **Decreto n. 9.612, de 17 de dezembro de 2018a**. Dispõe sobre políticas públicas de telecomunicações. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9612.htm. Acesso em: 29 mar. 2022.

BRASIL. **Decreto n. 9.854, de 25 de junho de 2019a**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação

Máquina a Máquina e Internet das Coisas. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 29 mar. 2022.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 29 mar. 2022.

BRASIL. Guia Orientativo. **Tratamento de Dados Pessoais pelo Poder Público**. Brasília: Autoridade Nacional de Proteção de Dados, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 2 abr. 2022.

BRASIL. **Lei n. 10.257, de 10 de julho de 2001**. Regulamenta os arts. 182 e 183 da Constituição Federal, estabelece diretrizes gerais da política urbana e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm. Acesso em: 29 mar. 2022.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018b**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 mar. 2022.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019c**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 2 abr. 2022e.

CÂMARA das Cidades 4.0. **Ministério da Ciência, Tecnologia e Inovações**, 2019b. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/camara-cidades. Acesso em: 29 mar. 2022.

CARNEIRO, L. A.; LUDIMILA, L. DE S. V.; LAMOUNIER, P. **Cidades inteligentes:** uma abordagem humana e sustentável. Brasília: Edições Câmara, 2021.

CULTURA data-driven e a transformação digital nas empresas. **ERQ**, [202-?]. Disponível em: https://digital.brq.com/cultura-data-drive. Acesso em: 29 mar. 2022.

DONEDA, D. Um panorama de proteção de dados para as cidades inteligentes. **Jota**, 4 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/um-panorama-de-protecao-de-dados-para-as-cidades-inteligentes-04072018. Acesso em: 29 mar. 2022.

ESTUDO de internet das coisas. **Ministério da Ciência, Tecnologia e Educação**, 2019. Disponível em: https://www.gov.br/governodigital/pt-

br/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas. Acesso em: 29 mar. 2022.

FALEIROS JÚNIOR, J. L. de M. Cidades inteligentes (smart cities) e proteção de dados pessoais. **Migalhas**, 1.º abr. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342754/cidades-inteligentes-smart-cities-e-protecao-de-dados-pessoais. Acesso em: 29 mar. 2022.

HENRIQUES, V. R.; MARTINS JÚNIOR, J. M. Acesso à Internet no Brasil: desafios para conectar toda a população. **Panorama setorial da Internet**, ano 8, n. 1, mar. 2016. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf. Acesso em: 29 mar. 2022.

MARINHO, R. S. **Carta brasileira para cidades inteligentes**. São Paulo: Livraria da Física, 2021.

NÍVEL analfabeto. **Inaf**, 2018. Disponível em: https://alfabetismofuncional.org.br/nivel-analfabeto/. Acesso em: 2 ago. 2022.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 2 abr. 2022.

PAIN, S. P. *et al.* **PEC n. 35/2020**. Altera os art. 5º, 6º e 215 da Constituição para assegurar a todos os residentes no País o acesso à Internet. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/144848. Acesso em: 29 mar. 2022.

PAINEL TIC Covid-19. **Cetic**, 2021. Disponível em: https://cetic.br/pt/pesquisa/tic-covid-19/. Acesso em: 29 mar. 2022.

PASTORE, S. L. *et al.* **PEC 8/2020**. Altera o art. 5º da Constituição Federal, para incluir o acesso à internet entre os direitos fundamentais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141096. Acesso em: 29 mar. 2022.

PEREIRA, C. D. M.; MUNIZ, C. R.; ALVES, A. M. **Cidades Inteligentes Sustentáveis no Brasil**: uma metodologia para avaliação e diagnóstico de nível de maturidade de cidades. Campinas: Centro de Tecnologia da Informação Renato Archer – CTI: Laboratório de Instrumentos de Políticas para TICS, 2022. Disponível em: https://www1.cti.gov.br/sites/default/files//livro_cidades_inteligentes_sustentaveis_brasileiras.pdf. Acesso em: 29 mar. 2022.

PHILLY311. **City of Philadelphia**, [201-?]. Disponível em: https://www.phila.gov/departments/philly311/. Acesso em: 29 mar

PINTO, D. A proteção de dados alçada a direito fundamental. **Conjur**, 17 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-17/douglas-pinto-protecao-dados-alcada-direito-fundamental. Acesso em: 29 mar. 2022.

PNAD Contínua – Pesquisa Nacional por Amostra de Domicílios Contínua. **IBGE**, 2021. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf. 2 ago. 2022.

QUAIS são os desafios da indústria 4.0 e como se adaptar a eles? **TOTVS**, [201-?]. Disponível em: https://conteudo.totvs.com/ebook-industria-4-0. Acesso em: 29 mar. 2022.

QUEM somos. **Inaf**, [201-?]. Disponível em: https://alfabetismofuncional.org.br/quem-somos/. Acesso em: 2 ago. 2022.

RIBEIRO, M. A. Os novos analfabetos digitais. **Belicosa**, 2018. Disponível em: https://belicosa.com.br/os-novos-analfabetos-digitais/#:~:text=Segundo%20IBGE%20170%20milh%C3%B5es%20de,n%C3%A3o%20sabem%20ler%20ou%20escrever. Acesso em: 28 mar. 2022.

ROLLEMBERG, S. R. *et al.* **PEC 6/2011**. Altera o art. 6.º da Constituição Federal para introduzir, no rol dos direitos sociais, o direito ao acesso à Rede Mundial de Computadores (Internet). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/99334. Acesso em: 29 mar. 2022.

RUMO a cidades inteligentes sustentáveis: plataforma inteli.gente MCTI é lançada. **RNP**, 3 dez. 2021. Disponível em: https://www.rnp.br/noticias/rumo-cidades-inteligentes-sustentaveis-plataforma-inteligente-mcti-e-lancada. Acesso em: 28 mar. 2022.

SARLET, I. W.; SIQUEIRA, A. DE B. O direito humano e fundamental de acesso à internet. **Conjur**, 12 nov. 2021. Disponível em: https://www.conjur.com.br/2021-nov-12/direitos-fundamentais-direito-humano-fundamental-acesso-internet. Acesso em: 29 mar. 2022.

SENNE, P. F. Para além da conectividade: Internet para todas as pessoas**. Panorama Setorial da Internet**, ano 13, n. 2, jun. 2021. Disponível em: https://cetic.br/media/docs/publicacoes/6/20210723132708/panorama_setorial_ano-xiii_n_2_internet_para_todas_as_pessoas.pdf. Acesso em: 29 mar. 2022.

SOBRE o CTI. **Ministério da Ciência, Tecnologia e Inovações**, 6 abr. 2021. Disponível em: https://www.gov.br/cti/pt-br/acesso-a-informacao/institucional/sobre-o-cti. Acesso em: 30 mar. 2022.

TRANSFORMAÇÃO Digital, agora mais do que nunca. **ABDI**, [202-?]. Disponível em: https://www.abdi.com.br/sobre. Acesso em: 29 mar. 2022.

URBAN SYSTEMS. **Sobre o Ranking Connected Smart Cities**. 2021. Disponível em: https://ranking.connectedsmartcities.com.br/#:~:text=A%20edi%C3%A7%C3%A3o%202021%20do%20Ranking,com%2050%20a%20100%20mil. Acesso em: 29 mar. 2022.

COMO CITAR OS CAPÍTULOS DESTE LIVRO CONFORME A ABNT

Capítulo 1

XAVIER, Fábio Correa. Recomendações e boas práticas para a jornada de adequação à LGPD pelos municípios. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 27-48.

Capítulo 2

PAGLIA, Lucas. Governança em privacidade de dados: a LGPD e seu artigo 50. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 49-67.

Capítulo 3

BLIACHERIENE, Ana Carla; ARAÚJO, Luciano Vieira de; NUNES, Fátima L. S. Lei Geral De Proteção de Dados e seus impactos no ciclo de políticas públicas no município. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 68-76.

Capítulo 4

CAMPOS, Andra Robert de Carvalho *et al.* Jornada do Estado de São Paulo para adequação à LGPD. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 77-93.

Capítulo 5

SILVA, Andressa Carvalho da. O direito fundamental à proteção de dados no ordenamento e a transparência administrativa: há convivência harmônica? *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 94-110.

Capítulo 6

OLIVEIRA, Andrey Guedes. Segurança da informação: proteção contra vazamento de dados. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 111-126.

Capítulo 7

ALVES, Davis; BRITO, Nilson. A importância da gestão de projetos e gestão de serviços para o DPO. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 127-133.

Capítulo 8

TUMA, Eduardo; TASSO, Fernando Antonio. Políticas públicas municipais de fomento à proteção de dados pessoais pelo setor privado. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 134-149.

Capítulo 9

PINHHEIRO, Patrícia Peck Garrido; NASCIMENTO, Camila; RAMOS, Julia Lonardoni. Monetização de dados por entes públicos. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 150-160.

Capítulo 10

BLUM, Renato Müller da Silva Opice; SOUZA, Bruno Henrique Cordeiro de. Mecanismos e medidas práticas para obtenção de resultado no tratamento de dados. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 161-171.

Capítulo 11

GRINGS, Maria Gabriela; CAMPOS, Ricardo. Transferência internacional de dados pessoais e compliance digital. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 172-185.

Capítulo 12

ROLO, Verena Iannino Soares; ROLO, Rafael Felgueiras. Apontamentos acerca da constitucionalidade do art. 52, X, XI, XII e § 3.º da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados): considerações à luz do princípio republicano e da continuidade do serviço público. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 186-200.

Capítulo 13

SUZUKI, Rodrigo Hiroshi Ruiz; SUZUKI, Vanessa D'Alessio Giarone. *Cybersecurity* e LGPD. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 201-218.

Capítulo 14

PEREIRA, Wallace da Silva. LGPD como norteadora da criação de cidades inteligentes. *In*: XAVIER, Fábio Correa; PAGLIA, Lucas (coord.). **LGPD;** boas práticas para os municípios brasileiros. Salvador: Mente Aberta, 2022, p. 219-236.

Neste livro, Fábio Correa Xavier e Lucas Paglia reuniram agentes públicos e privados para tratarem das boas práticas para a implementação da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) pelos municípios brasileiros.

Três características tornam esta coletânea essencial e de consulta obrigatória sobre o tema. Primeiro, a qualidade dos autores aqui reunidos, que se destacam como profissionais e acadêmicos e trazem reflexões a respeito de suas vivências e estudos. Segundo, o livro se destaca pelo relato de experiências de entes públicos na implementação da LGPD, o que permite a difusão de ideias e programas governamentais que fomentam a aplicação da Lei n. 13.709/2018. Terceiro, os temas abordados demonstram a abrangência e complexidade envolvidas na gestão de dados pessoais pela administração pública.

A lei está em vigor e o desafio de seu cumprimento pelos órgãos e entidades administrativas está posto. A presente obra contribui para a implementação da norma e o alcance de suas finalidades.

DIMAS RAMALHO
Presidente do Tribunal de Contas do Estado de São Paulo

ISBN 978-85-66960-57-0

MENTE ABERTA

IGCP
INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO

RGB
DA GOVERNANÇA À ESPERANÇA