proteção de dados

contexto, narrativas e elementos fundantes

bruno bioni

laura schertel mendes

pedro martins

mariana marques rielli

renato leite monteiro

prefácio
ricardo villas bôas cueva

márcio moretto ribeiro

maria luciano

marina kitayama

daniel dias

rafael a. zanatta

proteção de dados

contexto, narrativas e elementos fundantes

bruno bioni

laura schertel mendes

pedro martins

mariana marques rielli

renato leite monteiro

márcio moretto ribeiro

maria luciano

marina kitayama

daniel dias

rafael a. zanatta

prefácio
ricardo villas bôas cueva

brunobioni.com.br

Organização
Bruno Bioni

Colaboração
Jessica Silveira Leite

Projeto Gráfico e Diagramação
Daniela Jardim & Rene Bueno

Capa
Maria Cau Levy

Coautores
Daniel Dias
Laura Schertel Mendes
Márcio Moretto Ribeiro
Maria Luciano
Mariana Marques Rielli
Marina Kitayama
Pedro Martins
Rafael A. Zanatta
Renato Leite Monteiro

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Proteção de dados [livro eletrônico] : contexto, narrativas e
elementos fundantes / [organização Bruno Ricardo Bioni]. --
São Paulo : B. R. Bioni Sociedade Individual de Advocacia, 2021.
PDF

Vários autores.
Bibliografia.
ISBN 978-65-995360-0-7

1. Artigos - Coletâneas 2. Direito à privacidade 3. Direito à privacidade - Brasil 4. Proteção de dados pessoais 5. Proteção de dados - Leis e legislação I. Bioni, Bruno Ricardo.

21-70188 CDU-342.721

Índices para catálogo sistemático:
1. Proteção de dados pessoais : Direito 342.721
Cibele Maria Dias - Bibliotecária - CRB-8/9427

À **Maria Aragão**,
sua sabedoria eternamente me inspirará.

À **Cecília**,
por todo o amor e companheirismo.

AGRADECIMENTOS

Ao revisitar os quase últimos 10 (dez) anos da minha produção acadêmica, fiz uma viagem que aguçou vários sentidos da minha ignorância nesse vasto campo da proteção de dados e da privacidade.

O quão (in)visível são meus referenciais teóricos que despertam imagens diferentes a cada novo olhar. É necessário sempre uma releitura, pois há sempre algo despercebido ou não tão bem compreendido. O faro de que esse deve ser um campo intergeracional, pois, apesar da sua novidade, é essencial recuperar os erros e, principalmente, os acertos de outras pesquisas e dialogar com as experiências regulatórias das velhas tecnologias para projetarmos um futuro melhor. A intelectualidade enquanto um processo de audição constante. Foram várias as vezes em que, ao reler um determinado artigo, eu me peguei (re)escutando os coautores desta obra. Enfim, eu senti o gosto da gratidão por quem direta ou indiretamente doou seu tempo para dar sentido aos escritos deste livro.

Como costumo dizer, o conhecimento é sempre coletivo. Dentre os vários espaços que frequentei nesta última década, eu sou particularmente grato aos seguintes. À minha *alma mater*, as Faculdades Metropolitanas Unidas/FMU que me abriu os olhos para o tema da sociedade da informação. À Universidade de São Paulo/USP e à Fundação de Amparo de Pesquisa do Estado de São Paulo/FAPESP que são resistência e instrumento de uma das políticas públicas de maior potencial de transformação social. Sem a rede de ensino público e programas estatais de fomento à pesquisa, eu não conseguiria sequer ter batido à porta da ciência. A todas as pessoas que fazem o Data Privacy Brasil acontecer. Um espaço de interseção entre escola e associação de pesquisa que mobiliza tipos de saberes distintos, porém convergentes para ajudar na formação de uma cultura de proteção de dados. A quem passou e quem está na Bioni Consultoria aonde temos lidado com casos complexos, ajudando a colocar a lei geral de proteção de dados em movimento. A todos os co-autores e co-autoras deste livro que eu tive o prazer de encontrar nesses espaços de colaboração. Muito obrigado!

PREFÁCIO

Com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), passamos a contar com um marco normativo indispensável à nossa integração à economia digital. Já contávamos, por certo, com normas protetivas de grande alcance. Na Constituição Federal já se asseguravam os direitos à intimidade, à vida privada e ao sigilo de dados e prevê o habeas data. No Código de Defesa do Consumidor (Lei nº 8.078/1990) foram enunciados importantes direitos relativos a cadastros de consumidores, como os de acesso, comunicação, correção e limitação temporal, que prefiguraram alguns dos princípios caros às legislações de proteção de dados pessoais. Na Lei do Cadastro Positivo (Lei nº 12.414/2011), na Lei de Acesso à Informação (Lei nº 12.527/2011) e no Marco Civil da Internet (Lei nº 12.965/2014), já se identificavam importantes contribuições à proteção de dados pessoais. Mas a LGPD é a primeira lei no Brasil a tratar de modo sistemático e coerente a proteção de dados pessoais, definindo regras e procedimentos estruturantes dessa nascente área do direito, o que terá grande impacto na vida das pessoas, das empresas e dos entes dos setores público e privado, de modo geral.

Tal foi a importância da promulgação da LGPD, que o Supremo Tribunal Federal, enquanto ainda perdurava a longa vacatio legis, reverteu, em decisão histórica, seu entendimento a respeito da matéria, reconhecendo, nas sessões de 6 e 7 de maio de 2020, o direito fundamental autônomo à proteção de dados pessoais, ao suspender a Medida Provisória nº 954/2020, que obrigava as operadoras de telefonia a repassarem ao IBGE dados identificadores de seus consumidores de telefonia fixa e móvel. O julgamento partiu da constação de que, no mundo atual, com o incessante desenvolvimento da tecnologia informática, não há dados neutros. A relatora, Ministra Rosa Weber, assentou que qualquer dado que

permita identificar um indivíduo pode ser usado para a construção de perfis informacionais, de grande valor para o Estado e para as empresas privadas, que potencialmente ameaçam seu direito à autodeterminação informativa. Além disso, foi ressaltado no voto condutor que os vícios da medida provisória, nomeadamente a inobservância do princípio da finalidade, a ausência de medidas de segurança adequadas e o excesso na coleta de dados, eram agravados pela fragilidade do quadro normativo-institucional, decorrente da demora na criação da Autoridade Nacional de Proteção de Dados, que só veio a ser criada no fim daquele ano, a despeito de sua importância central para a implantação bem sucedida do novo regime jurídico.

É nesse contexto de formação de uma nova dogmática, atenta aos profundos impactos socioeconômicos das agudas transformações do mundo contemporâneo, que se destaca o trabalho de Bruno Bioni como estudioso desse novo ramo do direito. Já em sua dissertação de mestrado, que originou o livro Proteção de dados pessoais: a função e os limites do consentimento (Rio de Janeiro, Forense, 2019), soube entrelaçar ao conceito nuclear de consentimento temas de grande importância, como a crescente complexidade do fluxo de dados, a expansão de assimetrias na economia digital e a noção de privacidade contextual, desenvolvida pela Professora Helen Nissembaum.

Agora, o autor reúne artigos publicados ao longo dos anos, abordando temas fundamentais, como o consentimento, o legítimo interesse, o regime jurídico de proteção de dados pessoais públicos ou manifestamente públicos, entre outros.

Tenho certeza de que a presente obra será de grande valia tanto para os pesquisadores em busca de ideias e abordagens originais como para os aplicadores do direito, que poderão contar com orientação segura para a miríade de dificuldades práticas de implementação da nova lei.

Brasília, 9 de abril de 2021

Ricardo Villas Bôas Cueva

SUMÁRIO

PARTE 2 ELEMENTOS FUNDANTES

INTRODUÇÃO

O campo da proteção de dados pessoais está em ebulição. Primeiro, por conta da realidade inescapável da importância dos dados enquanto o principal ativo para a formulação de políticas públicas e modelagem de negócios. Segundo, em razão da aprovação da Lei Geral de Proteção de Dados/LGPD que lança uma nova e importante peça no ordenamento jurídico brasileiro. Com isso em mente, me encontrei motivado para selecionar e, na medida do possível, revisitar as minhas principais reflexões ao longo de anos de engajamento acadêmico e profissional no campo.

Na primeira parte, intitulada Contexto e Narrativas, os artigos iniciais buscam traçar o pano de fundo em torno da importância do direito à proteção de dados pessoais. Desafiando a lógica de encargos e elevação de custos, analisar esse direito como uma janela de oportunidade e de inovação ainda é uma mensagem potente que dever mais propagada. Com o objetivo de situar no tempo e no espaço tal narrativa, analiso também o cenário jurídico-regulatório antes, durante e depois da entrada em vigor da LGPD. Especial ênfase é dada à conjuntura política que permeou o seu processo de promulgação com o objetivo de jogar luz sobre a materialização desse importante direito fundamental no Brasil em futuro próximo. Essa primeira parte é menos sobre o direito e mais sobre os contornos políticos da proteção de dados

Uma vez sancionada a lei e em plena vigência, abre-se um campo bastante fértil para dogmática jurídica. Isto é, qual é o

sentido que deve ser dado ao conjunto de normas traçado na Lei 13.709/2018, de modo que antecipo as possíveis disputas interpretativas e, sempre que possível, procuro me posicionar. Portanto, nessa parte intitulada Elementos Fundantes, apresento algumas rotas hermenêuticas: **i)** começando pelo atemporal direito-dever de informação; **ii)** chegando no legítimo interesse, que é um novo conceito jurídico indeterminado, na necessidade em se reforçar o direito à proteção de dados como sendo autônomo frente ao da privacidade, no conceito de anonimização, em privacy by design, na obrigação de registro das atividade de tratamento de dados, no impacto econômico e na inovação jurídica trazida pela LGPD, na intersecção com o direito eleitoral e; **iii)** chegando a endereçar questões mais de ordem jus-filosófico, como quais são os aportes do termo ecologia para melhor informar melhor o debate sobre cidades inteligentes, o princípio da precaução para a governança-regulação de inteligência artificial, uma possível releitura da cláusula constitucional do devido processo legal e, por fim, o sentido de equivalência normativa para um futuro acordo de transferência internacional entre Brasil e União Europeia.

A aprovação de uma lei geral de proteção de dados pessoais não marca o final dos debates e a solução dos problemas que a sociedade da informação nos coloca. É necessário construir uma cultura acerca do tema e, no campo jurídico, forjar uma dogmática sofisticada para balancear a proteção de liberdades fundamentais e os interesses econômicos em jogo quando um dado pessoal é manipulado. Esse livro é, assim, um gesto de diálogo com que vier a ser seu leitor e leitora para refletirmos sobre a complexidade do tema. E, por fim, um agradecimento às reflexões travadas com coautores e coautoras que, gentilmente, me autorizaram a republicar os textos.

PARTE 1
CONTEXTO E NARRATIVAS

A CONSTRUÇÃO MULTISSETORIAL DA LGPD: história e aprendizados[1]

Bruno Ricardo Bioni[2] e Mariana Marques Rielli[3]

1 Artigo originalmente elaborada para obra coletiva coordenada por Denise Francoski e Fernando Tasso: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (Orgs.), A Construção Multissetorial da LGPD: História e Aprendizados, *in*: **A Lei Geral de Proteção de Dados Pessoais LGPD**, 1. ed. São Paulo: Revista dos Tribunais, 2021.

2 Bruno Bioni é doutorando em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo. Foi study visitor do Departamento de Proteção de Dados Pessoais do European Data Protection Board/EDPB e do Conselho da Europa, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa. É autor do livro Proteção de Dados Pessoais: a função e os limites do consentimento. É membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS, e também da International Association of Privacy Professionals – IAPP, com Certificação CIPP/E. É diretor fundador do Data Privacy Brasil, um espaço de intersecção entre uma escola de cursos e uma associação de pesquisa na área de privacidade e proteção de dados.

3 Mariana Rielli é advogada, graduada pela Universidade de São Paulo (USP), em 2018. É pesquisadora líder de projetos da Associação Data Privacy Brasil de Pesquisa.

A. INTRODUÇÃO

"A LGPD é uma lição de **democracia participativa**, mas acima de tudo é uma lição de **transigência** de como se constrói política pública de qualidade com **partes antagônicas** motivadas (....) pelo melhor interesse do Brasil", relata Sergio Gallindo, presidente-executivo da Brasscom e um dos idealizadores da coalizão tática-multissetorial em favor da aprovação da lei de proteção de dados. 'Eu não lembro de ter tido um projeto de lei recente que tenha tido **um processo de negociação** (...) numa sala dentro de um gabinete de deputado (...) **à luz do dia** (...) de uma **forma tão aberta**' confessa Marcelo Bechara, diretor de relações governamentais do Grupo Globo e um dos atores mais atuantes no parlamento nesta pauta. "Houve um desprendimento dos vários atores envolvidos que toparam (...) um diálogo para a **construção de consensos**", lembra Renata Mielli, integrante do coletivo Barão de Itararé e uma das fundadoras da Coalizão Direitos da Rede. "De repente tinha gente da sociedade civil, nitidamente com viés de esquerda, escrevendo um texto junto com um representante dos bancos, nitidamente um viés de direita (...) e eu falava num **tom de brincadeira** (...) ou **vamos produzir o texto nós aqui** (...) ou **eu decido sozinho**", rememora o Deputado Orlando Silva, que foi relator do projeto de lei da LGPD. "Foi um processo democrático (...) um processo coletivo (...) de **choque de ideias** (...) para um **denominador comum**", sintetiza Bruno Bioni que na época era pesquisador do GPoPAI-USP e também foi um dos fundadores da Coalizão Direitos na Rede. Essas falas, de representantes do setor privado, terceiro setor, governamental (legislativo) e academia, simbolizam que o **multissetorialismo está no DNA** da Lei nº 13.709/2018 (LGPD, a partir de agora).

Esta é a principal tese deste artigo: a LGPD se caracteriza por um processo multiparticipativo e particularmente bem sucedido

na extração de "consensos pragmáticos"[4] que impulsionaram sua construção, articulação e aprovação em agosto de 2018. Este é um dos achados do projeto de pesquisa "Memória da LGPD"[5] que reuniu mais de 10 (dez) horas de depoimentos, de 18 (dezoito) entrevistados, em uma plataforma multimídia composta por pequenos vídeos intercalados com textos que explicam todo o processo de construção da lei. Ainda, buscando aferir o quão multissetorial, de fato, é a LGPD, a metodologia de pesquisa que deu origem a esse artigo cruza a Memória a um dossiê, composto pelas contribuições dos dois processos de Consulta Pública[6] sobre o Anteprojeto de Lei de Proteção de Dados, bem como as notas taquigráficas e sistematização dos atores que participaram da Comissão Especial da Câmara dos Deputados e as diversas versões do texto da LGPD[7] debatidas nos processos de consultas públicas e no Congresso Nacional.

Leis de proteção de dados são marcos regulatórios de envergadura bastante complexa. Isto porque seu objeto não é um setor específico, mas, pelo contrário, toda e qualquer atividade econômica, abarcando setor público e privado, que se valha de dados

4 GATTO, R. **A perspectiva contratualista na construção do consenso da sociedade na internet**. Orientador: Claudio de Cicco. 2016. 174f. Tese (Doutorado em Direito). Pontifícia Universidade Católica de São Paulo, São Paulo, 2016.

5 ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. **Observatório da Privacidade** - Memória LGPD. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 21 de janeiro de 2021.

6 ASSOCIAÇÃO BRASILEIRA DE MARKETING DIRETO. **Dados pessoais - contribuições das entidades**. 2010. Disponível em: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf. Acesso em: 21 de janeiro de 2021; INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. 2015. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 21 de janeiro de 2021.

7 MACHADO MEYER. **Tabela comparativa - Lei Geral de Proteção de Dados**. Disponível em: https://www.machadomeyer.com.br/images/Alteracoes-na-Lei-Geral-de-Protecao-de-Dados.pdf. Acesso em: 21 de janeiro de 2021.

pessoais para o seu desenvolvimento. Essa transversalidade[8] desperta diferentes interesses e cria uma difícil tarefa na arquitetura de normas para um fluxo informacional apropriado.[9] Daí a pertinência em se investigar o processo de formatação de leis desse tipo. No caso da LGPD, os vestígios desse processo de negociação de múltiplas partes deixaram vestígios públicos, antes e durante a tramitação no Congresso Nacional.

Na primeira parte do artigo, descreve-se como o processo de articulação e eventual aprovação da LGPD se deu pela colaboração e engajamento de diferentes atores. Na segunda parte, dedica-se um olhar pontual sobre algumas partes do próprio texto da lei em que esse processo de negociação alcançou soluções mediadas, a ponto de talhar um desenho normativo bastante peculiar e criativo da lei brasileira. Em sua forma e em seu conteúdo, a história da LGPD nos fornece um rico aprendizado sobre multissetorialismo.

B. MULTISSETORIALISMO NA FORMA DA LGPD

Descrito o conceito de multissetorialismo e a sua conexão primordial com o objetivo regulado pela Lei Geral de Proteção de Dados, passa-se a um exame mais aprofundado de como se deu o processo de construção da norma ao longo do tempo e como o caráter multissetorial desempenhou um importante papel, que, como se verá adiante, reverberou também no conteúdo da lei aprovada.

8 WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luis. (Org.). **Tratado de Proteção de Dados Pessoais**. 1ed. Rio de Janeiro: Forense, 2020, v. 1, p. 375-388.

9 Cf. NISSENBAUM, Helen. **Privacy in context:** Technology, policy, and the integrity of social life. Stanford University Press, 2009.

a. O longo caminho para a construção de uma coalizão multissetorial

Em 13 de julho de 2018, foi lançado, pela Brasscom, o Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais[10]. Nessa ocasião, 80 (oitenta) signatários, a ampla maioria entidades, reuniram-se em torno de um objetivo comum: pressionar o Senado Federal pela aprovação do então Projeto de Lei da Câmara nº 53[11], que veio a se tornar a Lei nº 13.709/2018. O grupo era diverso, composto por empresas de diferentes ramos, pesquisadores, entidades do terceiro setor[12] e até órgãos públicos, como Procons.

Não obstante, essa confluência de interesses materializada no documento não era um dado no início do processo que culminou na Lei Geral de Proteção de Dados, e nem mesmo durante momentos emblemáticos da tramitação do projeto. Como, então, chegou-se à formação de uma coalizão ampla, composta por grupos que, tradicionalmente, não têm afinidade e que, inclusive, disputaram versões diferentes, e até opostas, do texto da lei? Um olhar para os cerca de 8 (oito) anos que se passaram entre os primeiros antecedentes do que veio a se tornar a LGPD e a sua efetiva aprovação, em agosto de 2018, podem trazer pistas sobre esse fenômeno.

10 BRASSCOM. **Manifesto pela aprovação da lei de proteção de dados pessoais**. Disponível em: https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/. Acesso em: 21 de janeiro de 2021.

11 Nesse momento, a formação de uma ampla coalizão foi considerada crucial, pois, após o longo e complexo processo de aprovação do texto na Câmara dos Deputados, que contou com a formação de um consenso provisório dos diversos setores envolvidos, era essencial aprovar o projeto no Senado sem alterações substanciais, pois isso implicaria a volta do texto para a Câmara e um consequente atraso no processo e possível perda do "momentum" para a aprovação final da lei. Ver item 19, Capítulo "Uma Conjunção Astral" da Memória da LGPD, do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

12 A Coalizão Direitos na Rede, formada, à época, por 29 entidades do terceiro setor, assinou o manifesto.

B.1. Antecedentes e consultas públicas

É verdade que o marco normativo da proteção de dados no Brasil vai além de uma lei geral, e que foi construído ao longo das décadas por meio de importantes pilares como a Lei nº 8.078/1990 (Código de Defesa do Consumidor), a Lei nº 12.965/2014 (Marco Civil da Internet), a Lei nº 12.414/2011 (Lei do Cadastro Positivo, alterada pela Lei Complementar nº 166/2019), dentre outras normas setoriais[13].

Entretanto, a relevância de uma norma cujos dispositivos atravessassem diferentes setores e regulassem a matéria de forma ampla já era divisada por certos atores pelo menos desde os anos 70 e 80, conforme demonstram iniciativas legislativas de resposta ao projeto do Registro Nacional de Pessoas Naturais (RENAPE)[14] e ao crescente tratamento de dados pessoais em cadastros e bancos de dados,[15] conforme exemplifica o Projeto de Lei 2.796 de 1980, de autoria da Deputada Cristina Tavares.[16]

13 V. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. p. 45 *In*: BIONI, Bruno, DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

14 VIANNA, Marcelo. Um novo "1984"? **O projeto RENAPE e as discussões tecnopolíticas no campo da informática brasileira durante os governos militares na década de 1970.** Oficina do Historiador, Porto Alegre, Suplemento especial, ISSN 21783748, I EPHIS/PUCRS, 27 a 29 maio 2014, p. 1148-11171. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/oficinadohistoriador/article/view/18998/12057. Acesso em: 21 de janeiro de 2021.

15 Como explica Rafael Zanatta no primeiro episódio da Memória LGPD: "A primeira geração é uma geração que trouxe a discussão sobre dados pessoais durante a ditadura militar. Então houve, por exemplo, um projeto do Governo Federal na época do Geisel de implementação de um sistema nacional de pessoas naturais, chamado RENAPE, o que trouxe uma reação muito grande de lideranças de juristas como Raymundo Faoro, René Ariel Dotti - inclusive, o primeiro projeto de lei sobre dados pessoais no Brasil é de 78, que é do José Roberto Faria Lima (...), uma tentativa fracassada de fazer uma legislação de proteção de dados". Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/. Acesso em: 21 de janeiro de 2021.

16 DONEDA, Danilo. Panorama histórico da proteção de dados pessoais, p. 46. *In*: BIONI, Bruno, DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

Então apenas uma semente, essa ideia só ganhou maior tração a partir de meados dos anos 2000, com a participação do Brasil em negociações internas do Mercosul[17], foro que abrigou movimentos de pressão, por parte de países como a Argentina[18], para a construção de uma norma comum aos países do bloco. Embora nunca se tenha concretizado a ideia de uma regulação de proteção de dados para todos os países integrantes do Mercosul, os debates deflagrados por essa proposta serviram de combustível para a internalização do tema pelo Poder Executivo brasileiro[19].

O processo de materialização desse interesse na criação de uma lei geral teve início na Secretaria de Assuntos Legislativos, em parceria com o Departamento de Proteção e Defesa do Consumidor, ambos do Ministério da Justiça, que, sob a coordenação de Laura Schertel Mendes e com a colaboração do então consultor Danilo Doneda, elaborou uma minuta de Anteprojeto de Lei de Proteção de Dados[20] e, em dezembro de 2010, submeteu o texto a consulta pública,[21] seguindo os moldes da elaboração da Lei nº 12.975/2014 (Marco Civil da Internet).[22]

17 Danilo Doneda explica que o Subgrupo de Trabalho de número 13 (SGT13), referente ao Comércio Eletrônico, recebeu uma proposta da República da Argentina, em 2004, para uma regulamentação comum. A partir desse momento, ocorreu um "discreto, porém crescente" debate sobre o tema pelo governo brasileiro, que teve como um de seus marcos o "I Seminário Internacional sobre Proteção de Dados Pessoais", promovido pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior.

18 A Argentina foi o primeiro país do bloco a aprovar uma lei geral de proteção de dados, a Lei de Proteção de Dados Pessoais 25.326 (PDPA), em 2000.

19 DONEDA, op.cit., p. 52.

20 Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf. Acesso em: 21 de janeiro de 2021.

21 O mecanismo de consulta pública como instrumento de participação política é regulado pela Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal (Direta e Indireta): "Art. 31. Quando a matéria do processo envolver assunto de interesse geral, o órgão competente poderá, mediante despacho motivado, abrir período de consulta pública para manifestação de terceiros, antes da decisão do pedido, se não houver prejuízo para a parte interessada."

22 O Marco Civil, na fase de Anteprojeto de Lei, foi submetido a consulta pública promovida pela Secretaria de Assuntos Legislativos (SAL) do Ministério da Justiça (MJ) por meio do portal Cultura Digital entre abril e maio de 2010. A primeira consulta sobre o →

Nessa ocasião, o sistema recebeu 794 (setecentas e noventa e quatro) contribuições[23], em forma de comentários sobre cada um dos artigos, parágrafos, incisos ou alíneas do Anteprojeto. O conjunto de entidades que participou da rodada já refletia o interesse multissetorial pela matéria, uma vez que estiveram presentes representantes de todos os setores, embora com distribuição desigual[24]: dentro do terceiro setor, opinaram 9 (nove) associações empresariais e congêneres[25], 3 (três) organizações não governamentais[26] e um grupo de pesquisa[27]; no setor privado, 4 (quatro) empresas[28]; no setor público, uma fundação[29] e uma comissão de um ente público *sui generis*[30].

Segundo Danilo Doneda, em entrevista para o projeto Memória da LGPD[31], a consulta pública de 2010 e 2011 "não foi muito

➔ Anteprojeto de Lei de Proteção de Dados, inclusive, aproveitou a plataforma criada para as discussões sobre o MCI.

23 Disponível em: http://culturadigital.br/dadospessoais/. Acesso em: 20 de janeiro de 2021.

24 Tal sistematização foi retirada de relatório da Associação Brasileira de Marketing Direto (ABEMD), disponível em: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf

25 ABEMD (Associação Brasileira de Marketing Direto); ABRAREC (Associação Brasileira das Relações Empresa Cliente); ABA (Associação Brasileira de Anunciantes); QIBRAS (Qualidade da Informação Brasil); Comissão de Informática, Internet e Tecnologia – CIIT da Associação Brasileira de Direito de Informática e Telecomunicações – ABDI; ABTA (Associação Brasileira de Televisão por Assinatura);SindiTelebrasil (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal); Associação Brasileira das Empresas de Cartões de Crédito e Serviços; Confederação Nacional das Instituições Financeiras.

26 IDEC (Instituto Brasileiro de Defesa do Consumidor); Organização Transparência Hacker; PROTESTE (Associação Brasileira de Defesa do Consumidor).

27 Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Universidade de São Paulo.

28 Equifax Brasil; Nokia S.A.; Telemar Norte-Leste S.A. ("Oi"); Morrison & Foerster (MoFo) – Global Privacy Alliance (GPA).

29 Fundação PROCON - SP.

30 Comissão de Ciência e Tecnologia da OAB/SP.

31 Ver item 6 do Episódio 1 "O tema entra em pauta" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/

proveitosa" do ponto de vista técnico, mas revelou, que àquela altura ainda havia um grande estranhamento e desconhecimento dos diversos atores envolvidos em relação ao tema da proteção de dados pessoais.

Os anos que se seguiram a essa primeira iniciativa do Ministério da Justiça foram marcados por uma conjuntura que "atrasou" o avanço substancial de uma lei geral de proteção de dados, mas, ao mesmo tempo, ajudou a construir a base contextual e conceitual sobre a qual essa norma viria a se firmar, anos depois. Assim, entre 2011 e 2015, foram aprovadas outras leis integrantes do microssistema de proteção de dados, como a Lei nº 12.414 (Lei do Cadastro Positivo), a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei nº 12.965/2014 (Marco Civil da Internet), a última impulsionada diretamente pelas revelações feitas por Edward Snowden sobre a vigilância em massa promovida pelo governo americano[32].

Paralelamente, no Legislativo foram propostos, nesse ínterim, dois projetos de lei de regulação geral da proteção de dados pessoais: na Câmara, o Projeto de Lei 4060/2012[33], de autoria do então deputado federal Milton Monti (PR-SP); no Senado, o PL 330/2013[34], do então senador Antônio Carlos Valadares (PSB/SE), que viria a "concorrer" com a proposta que eventualmente foi enviada pelo Executivo.

32 Francisco Brito Cruz descreve como o efeito "Snowden" influenciou diretamente o texto do Marco Civil da Internet quanto à privacidade e proteção de dados. CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital:** A experiência de elaboração legislativa do Marco Civil da Internet. 138 f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 21 de janeiro de 2021.

33 CONGRESSO NACIONAL. **Projeto de Lei 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências**. Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 21 de janeiro de 2021.

34 SENADO FEDERAL. **Projeto de Lei do Senado nº 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências**. Brasília, DF, agosto de 2013. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 21 de janeiro de 2021.

Esse contexto movimentado deixou o Anteprojeto do Ministério da Justiça em segundo plano pelo período e também evidenciou a necessidade de se "trabalhar" o texto e adequá-lo às mudanças normativas e contextuais que vinham ocorrendo. Em âmbito internacional, foi no intervalo de 2012 a 2016 que foi discutido e aprovado, em diferentes níveis, o Regulamento Geral de Proteção de Dados (RGPD) europeu[35], reconhecido como a maior influência da Lei Geral de Proteção de Dados.

Assim, em 28 de janeiro de 2015, o Ministério da Justiça submeteu uma nova versão do Anteprojeto a uma segunda consulta pública[36], que se estendeu até o dia 7 de julho do mesmo ano e recebeu mais de 1800 (mil e oitocentas) contribuições, de três tipos: i) comentários em cada parte do texto (artigos, incisos, parágrafos e alíneas); ii) comentários divididos por eixos temáticos; e iii) contribuições documentais em formato *pdf*. Além disso, o sistema permitia a participação de pessoas físicas e jurídicas[37].

A distribuição setorial nessa ocasião, levando-se em consideração apenas as pessoas jurídicas cadastradas, foi a seguinte[38]: no terceiro setor, 11 (onze) associações empresariais e congêneres[39],

35 Ver linha do tempo em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

36 Disponível em: http://pensando.mj.gov.br/dadospessoais/.

37 Exigia-se, para identificação, e-mail, senha e um nome de usuário.

38 Tal sistematização foi retirada do relatório *O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais*, do InternetLab. INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 21 de janeiro de 2021.

39 ABA (Associação Brasileira de Anunciantes); ABDTIC (Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações); ABEMD (Associação Brasileira de Marketing Direto); ABEP (Associação Brasileira de Empresas de Pesquisa); ABINEE (Associação Brasileira da Indústria Elétrica e Eletrônica); ABRANET (Associação Brasileira de Internet); Associação da Liberdade Religiosa e Negócios; CNI (Confederação Nacional da Indústria); CNseg (Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização); Febraban ➔

4 (quatro) organizações não-governamentais[40] e 2 (dois) grupos de pesquisa[41]; no setor privado, 6 (seis) empresas[42]; no setor público, uma secretaria ministerial[43]. Por fim, destaca-se uma participação mais expressiva, nesse processo, de entidades estrangeiras, representantes de diferentes setores[44].

Com a maturação do tema ao longo dos anos e a sua evidente relevância e horizontalidade, além do fato de se tratar de uma matéria bastante técnica, a segunda consulta pública é considerada "um marco" para os atores que dela participaram, uma vez que se pode observar um movimento de profissionalização, principalmente do terceiro setor e das áreas de *policy* das empresas, necessária para que esses grupos estivessem "à altura" do debate que começou a ser travado.

As duas consultas públicas realizadas pelo Ministério da Justiça em 2010-2011 e em 2015, embora não representem o ápice do multissetorialismo no processo de construção da Lei Geral de Proteção de Dados, foram um primeiro passo importante, compartilhado com outros diplomas normativos, como o Marco Civil da Internet, para reunir as perspectivas de atores de diferentes áreas e setores em um mesmo espaço (virtual, naquele momento), o que repercutiu no conteúdo do projeto, como se verá adiante.

➔ (Federação Brasileira de Bancos); FIESP (Federação das Indústrias do Estado de São Paulo); SindiTeleBrasil (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal).

40 CTS-FGV (Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas); Intervozes; ITS-Rio (Instituto de Tecnologia e Sociedade do Rio de Janeiro) e Proteste (Associação Brasileira de Defesa do Consumidor).

41 GEPI-FGV (Grupo de Ensino e Pesquisa em Inovação da Fundação Getúlio Vargas) e GPoPAI (Grupo de Pesquisa em Políticas Públicas de Acesso à Informação).

42 3M do Brasil; Boa Vista Serviços; Cisco (Cisco Systems, Inc); Claro; Sky e Vivo.

43 SEAE/MF (Secretaria de Acompanhamento Econômico do Ministério da Fazenda).

44 American Bar Association (Associação dos Advogados Americanos/EUA); BSA (The Business Software Alliance); ESA (Entertainment Software Association (EUA); GSMA (Groupe Speciale Mobile Association); Privacy International; US Business Council (Brazil-U.S. Business Council).

B.2. O seminário do Comitê Gestor da Internet

Outro elemento que ajudou a moldar o processo de construção e tramitação da LGPD, e o caráter multissetorial que ele incorporou, foi o Comitê Gestor da Internet (CGI.br) e, especificamente, o seu Seminário de Proteção à Privacidade e aos Dados Pessoais, cuja primeira edição ocorreu em 2010, em parceria com o Grupo de Trabalho Tecnologias da Informação e da Comunicação – GTTIC, do Ministério Público Federal e a Fundação Getúlio Vargas de São Paulo – FGV/SP[45].

O modelo multissetorial do CGI.br, cujo gérmen pode ser encontrado nos primórdios da Internet no Brasil[46], foi logo incorporado pelo Seminário, o qual, ao longo de seus 11 (onze) anos de existência, consolidou-se como o principal espaço de debate sobre privacidade e proteção de dados pessoais no país. O destaque do Seminário não decorre apenas do alto nível das discussões e articulações nele realizadas, mas do fato de que esse conhecimento é produzido coletivamente por representantes de todos os setores afetados pelo tema - setor empresarial, acadêmico, terceiro setor

45 Um antecedente importante do Seminário, que influenciou todo o debate sobre governança da Internet da década seguinte, foi o Decálogo da Internet, lançado em 2009, que contém dez princípios que devem balizar o uso da rede. O item número 1 diz respeito à Liberdade, privacidade e direitos humanos: "O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática."

46 Processo que contou, em diferentes momentos, com o apoio mútuo entre entidades acadêmicas, como a Fapesp, entidades do terceiro setor, como o IBASE, e o governo brasileiro, além das empresas que eventualmente promoveram a distribuição comercial da Internet no país. V. GATTO, R.; GETSCHKO, Demi. **Governança da Internet:** conceitos, evolução e abrangência. 27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2009, p. 37. Disponível em: http://ce-resd.facom.ufms.br/sbrc/2009/081.pdf. Acesso em: 21 de janeiro de 2021.

e governo - uma característica que, inclusive, foi se acentuando conforme o Seminário ganhou fôlego[47].

Como um fórum qualificado de discussão sobre privacidade e proteção de dados, em geral, naturalmente o Seminário do CGI.br abrigou, ao longo dos anos, debates sobre o projeto (e Anteprojeto) que viria a se tornar a Lei Geral de Proteção de Dados, bem como sobre certos aspectos da norma após sua aprovação, em 2018[48]. Assim, tanto painelistas do evento, representativos de diferentes setores, quanto a sua audiência, também bastante diversa, puderam ter contato com as especificidades do processo, e inclusive do texto que vinha sendo construído, enquanto ele se desenvolvia.

47 Na edição de 2020, por exemplo, todas as mesas foram compostas por, pelo menos, um representante de cada setor. Ver https://seminarioprivacidade.cgi.br/

48 Ao longo de suas edições, o Seminário de Privacidade CGI.br e NIC.br abordou o tema da regulação de privacidade e proteção de dados no país em vários debates, incluindo, além da própria LGPD, discussões relativas a seu anteprojeto e PLs. São exemplos os painéis "Palestra Magna – Panorama regulatório da privacidade no Brasil" (2012), "Roundtable VI "Perspectivas global e nacional sobre a proteção de dados pessoais" (2013), "Roundtable V "Bases de dados públicas e privadas: riscos potenciais à proteção da privacidade" (2013), "Seminário II: A operacionalização/aplicação da lei brasileira: imperativos legais em interface com imperativos tecnológicos" (2014), "Seminário III: Riscos e perspectivas à proteção da privacidade e dos dados pessoais" (2014), "Sessão 7: Debate público sobre Projetos de Lei e o APL sobre privacidade e proteção de dados" (2015), "Sessão 3: Seminário Formas de consentimento e Proteção a direitos fundamentais de liberdade" (2015), "Sessão 4: Coquetel de debates: Iniciativas legislativas sobre proteção de dados pessoais" (2016), "Sessão 2: Seminário - Economia do compartilhamento: qual o impacto da proteção dos dados pessoais nesse (novo) modelo de negócio?" (2016), "Sessão 4: Seminário Órgãos reguladores, fiscalização e aplicação das leis de proteção de dados pessoais: um panorama a partir da experiência estrangeira" (2017), "Coquetel de debates: Debate sobre os Projetos de Lei de Proteção de Dados Pessoais" (2017), "Sessão 3: Seminário Proteção de dados pessoais como elemento de inovação e competitividade: os desafios da construção de uma 'Agenda Digital' para o Brasil" (2017), "Painel 3: O papel do setor privado na proteção à privacidade e aos dados pessoais" (2018), "Coquetel de Debates sobre a Conjuntura Brasileira: Modelos Regulatórios para a aplicação e fiscalização de leis de proteção de dados pessoais" (2018), "Painel 1: General Data Protection Regulation e Convenção 108: primeiras impressões e expectativas sobre o processo de modernização das normas de proteção de dados pessoais" (2018), "Coquetel de debates - Perspectivas para a implementação da proteção de dados no Brasil e a experiência estrangeira: cooperação entre regulador, atores regulados e os titulares dos dados" (2019), "Painel 2 - Alocando responsabilidades, direitos e deveres dos agentes do ecossistema de dados: um olhar transversal sobre a LGPD" (2019), "Painel 3 - Garantias de segurança para cumprimento da Lei Geral de Proteção de Dados" (2020).

Não obstante, talvez a influência mais direta do Seminário, e especificamente do modelo multissetorial do Comitê Gestor da Internet (CGI.br), sobre o processo de construção da LGPD tenha se dado sobre a atuação do Relator do projeto na Câmara dos Deputados, deputado federal Orlando Silva (PCdoB - SP), que conduziu os trabalhos de uma forma altamente participativa e, segundo ele mesmo relata, inspirada no formato do evento[49].

B.3. Comissão especial e audiências públicas

Dando continuidade à história cronológica da lei, após a segunda consulta pública promovida pelo Ministério da Justiça, entre janeiro e julho de 2015, o governo apresentou a versão final do texto[50] em 20 de outubro do mesmo ano. O envio para a Câmara dos Deputados, entretanto, ainda demorou e veio a ocorrer apenas em 12 de maio de 2016, como um dos últimos atos da então presidente Dilma Rousseff, antes do seu afastamento definitivo do cargo em razão do processo de *impeachment*.

Esse momento marca o início de um debate mais amplo, profundo e multifacetado sobre o tema no Legislativo, o qual, antes de 2016, estava concentrado nos dois projetos em andamento até então - o PL 4060/2012 e o PLS 330/2015. A "nova" proposta, PL 5276/2016, carregava pelo menos 5 anos de debates prévios, com contribuições de todos os setores, e os grupos e indivíduos que já haviam se engajado no texto por meio das consultas públicas

49 Fala de Orlando Silva na abertura do VIII Seminário de Proteção à Privacidade e Proteção de Dados do Comitê Gestor da Internet (CGI.br). Disponível em: https://www.youtube.com/watch?v=GKMul1c4YYU&list=PLQq8-9yVHyOZVGYJeegT8I-mHrWOPliYh&index=1&t=6s&ab_channel=NICbrvideos

50 MINISTÉRIO DA JUSTIÇA. **MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais**. 2015. Disponível em: http://pensando.mj.gov.br/2015/10/21/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/. Acesso em: 20 de janeiro de 2021.

agora iriam se envolver em uma nova fase de discussão, em um novo fórum, com as suas próprias regras e especificidades.

É nesse momento, inclusive, que entidades da sociedade civil (nem todas atuantes no processo até então), que já tinham vivido a experiência de articulação para a aprovação do Marco Civil da Internet, decidiram formalizar uma rede de incidência em direitos digitais, chamada Coalizão Direitos na Rede[51], que nasceu, em junho de 2016, com a primeira missão de promover os interesses do setor na Lei Geral de Proteção de Dados, então em discussão no Parlamento[52].

A influência da Coalizão e de sua incidência sobre o processo em curso ficou evidente com a articulação promovida por algumas das organizações para a escolha de um relator para o projeto que, ao mesmo tempo, compreendesse a importância da matéria e se dispusesse a ouvir todos os interessados. Tal articulação resultou na designação do deputado federal Orlando Silva (PCdoB - SP) para a relatoria do PL 5276/2016, agora apensado ao PL 4060/2012, ainda no âmbito da Comissão de Trabalho, Administração e Serviço Público (CTASP).

Reconhecendo a necessidade de ampliar e aprofundar o debate com a devida autonomia, o deputado requereu a tramitação do projeto por quatro Comissões, o que, de acordo com o Regimento Interno da Casa, automaticamente deflagra a criação de uma Comissão Especial exclusivamente para discutir a matéria. Assim, a Comissão Especial da Câmara sobre Tratamento e Proteção de Dados Pessoais foi instalada em 26 de outubro de 2016, sob

51 Disponível em: https://direitosnarede.org.br/. Acesso em: 20 de janeiro de 2021.

52 Ver item 2 do Capítulo 2 "O Anteprojeto chega à Câmara" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 20 de janeiro de 2021.

presidência da deputada federal Bruna Furlan (PSDB-SP)[53] e com a manutenção da relatoria de Orlando Silva.

A Comissão Especial, então, tornou-se o novo fórum para essa segunda fase de discussão multissetorial em torno do projeto. Alguns meses após a sua formalização, foi promovida a primeira[54] de um total de 11 (onze) audiências públicas temáticas[55] (sobre temas como conceitos fundamentais de proteção de dados, modelo de regulação, modelo de responsabilidade civil, definição de dados pessoais, sensíveis e anonimizados, base legal do legítimo interesse, dentre outros) e 2 (dois) seminários internacionais, todos eventos que replicaram a lógica multissetorial bem-sucedida

53 Um ponto de destaque é que foram designados, para os postos de 3 vice-presidentes da Comissão Especial da LGPD (art. 39 do Regimento Interno da Câmara dos Deputados) parlamentares muito familiarizados com a temática e, além disso, considerados estratégicos por seu trânsito entre vários partidos e atores, o que facilitou as negociações. Foram eles: 1º Vice-Presidente: André Figueiredo (PDT/CE), 2º Vice-Presidente: Alessandro Molon (PSB/RJ), 3º Vice-Presidente: Milton Monti (PR/SP). Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/conheca-a-comissao/membros-da-comissao

54 No seu plano de trabalho, apresentado em 22 de novembro de 2016, o deputado Orlando Silva apresentou como primeiro item das atividades a serem desenvolvidas pela Comissão: "a) Realizar oitiva de convidados especialistas, servidores públicos e autoridades públicas que possam contribuir para a realização deste trabalho, inclusive membros do Poder Judiciário, do Ministério Público e parlamentares relatores de projetos ligados ao tema; operadores do Direito em geral; e representantes de Organizações da sociedade especializadas na temática, entre outros; (...)". Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/roteiro-de-trabalho-apresentado-em-22-11-2016. Acesso em: 21 de janeiro de 2021.

55 Parte das apresentações dos participantes das 11 audiências públicas pode ser acessada aqui: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-e-eventos. Acesso em: 21 de janeiro de 2021.

do Seminário de Proteção à Privacidade e aos Dados Pessoais do CGI.br[56] [57].

Ao final do ciclo de audiências públicas, em julho de 2017, obteve-se, além de um ganho de conhecimento coletivo sobre a temática (e, inclusive de um certo "nivelamento" em relação aos parlamentares e outros atores que se engajaram na discussão em um momento posterior) também uma redução das tensões entre representantes de ONGs e da academia e representantes do setor privado. Bia Barbosa, também entrevistada pelo projeto Memória da LGPD, explicou que, no decorrer do processo, percebeu-se que o setor privado não era "monolítico" e que, dentro dele, também havia uma miríade de diferentes interesses, sendo absolutamente vital o diálogo aberto com todos para a construção de uma lei, que pela sua própria natureza, a todos afetaria[58].

56 Orlando Silva, em entrevista, afirmou que o multissetorialismo não era apenas uma característica incidental do processo, mas um requisito para cada uma das mesas. Ver Item 14 do Capítulo 2, "O Anteprojeto chega à Câmara", da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 21 de janeiro de 2021.

57 Entre a primeira e a última audiência pública transcorreram cerca de 8 meses e, nesse período, participantes do processo relatam que outras articulações se desenvolveram: do lado da sociedade civil organizada, por exemplo, foi realizada uma campanha para trazer o debate da proteção de dados para mais perto da sociedade como um todo (campanha "Seus dados são você"); ao mesmo tempo, tanto ONGs quanto representantes do setor privado e membros da academia se movimentaram para subsidiar os membros da Comissão com informações, das mais básicas às complexas, sobre o tema; a Brasscom, maior associação de empresas do setor de TICs, nesse período organizou um manifesto (https://brasscom.org.br/manifesto-sobre-a-futura-lei-de-protecao-de-dados-pessoais/), em que buscava resumir suas posições acerca de temas basilares da legislação, como conceito de dados pessoais, consentimento e outras bases legais, modelo regulatório, etc. Nesse momento do debate, Rafael Zanatta afirma que a relação entre ONGs e setor privado/associações representativas das empresas era de discordância e antagonismo, não de articulação. Ver mais em Episódio 2 "O Anteprojeto chega à Câmara" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 21 de janeiro de 2021.

58 Ver Item 17 do Capítulo 2 "O Anteprojeto chega à Câmara" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 21 de janeiro de 2021.

2018: conjunção astral e o movimento coordenado de múltiplas partes para a aprovação da LGPD

Vividas duas "fases" de diálogo multissetorial para a construção de um texto para a LGPD, no final de 2017 ainda não havia perspectiva concreta de aprovação da lei[59]. Foi preciso o que Doneda chama de "conjunção astral" para que isso fosse, de fato, possível.

Resumidamente, essa conjuntura favorável pode ser atribuída a, pelo menos, quatro fatores de destaque, que ocorreram paralelamente no Brasil e no mundo e concorreram para a formação de um cenário fortemente propício à aprovação de uma lei geral de proteção de dados brasileira.

Foram eles: i) o escândalo Cambridge Analytica, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados (RGPD) europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; iii) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável.

Posto esse cenário de verdadeiro "ultimato" para a aprovação da lei, o relator Orlando Silva observou a necessidade de "aparar arestas" e superar discordâncias entre as partes interessadas no

59 Doneda relembra que, "em muitos momentos achava-se que nada ia acontecer", mas que, ao mesmo tempo, hoje considera que esse longo período de debates foi essencial para a maturação da lei. Ver Item 17 do Capítulo 2 "O Anteprojeto chega à Câmara" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 21 de janeiro de 2021.

debate, que até aquele momento inviabilizavam a passagem da lei. Para isso, o parlamentar recorreu a uma "terceira fase" de diálogos multissetoriais sobre o texto propriamente dito, reunindo todos os setores em algumas sessões de discussão, com a seguinte metodologia, relativamente inusitada, descrita por ele mesmo em entrevista: leitura em voz alta de todos os dispositivos do projeto, com destaques de pontos específicos do texto sobre os quais algum participante levantar uma discordância, seguida de defesa contra ou a favor do trecho destacado e votação para decidir a versão final[60].

Sobre esse processo, Marcel Leonardi faz a leitura de que, não fosse a iniciativa um tanto inovadora do deputado, o projeto teria seguido a trajetória tradicional do Congresso: após a apresentação de um texto base pelo relator, cada setor se articularia para ver seus interesses representados em emendas ou outros tipos de alteração do processo legislativo, sem um diálogo ou busca de consensos gerais[61]. Similarmente, Marcelo Bechara, Conselheiro do ABERT, nota que o processo de elaboração do projeto de lei da LGPD teve um nível de abertura incomum, incluindo negociações detalhadas e leitura pormenorizada do texto "à luz do dia" e acessível para quaisquer interessados.[62]

60 Ver Item 11 do Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021. No mesmo item, Sérgio Gallindo, da Brasscom, descreve outra regra do processo estabelecido por Silva: as matérias sem chance de consenso seriam decididas por ele. Também afirma nunca ter presenciado um processo legislativo com "tal grau de transparência e tal grau de democracia interna", opinião compartilhada por Marcelo Bechara, também em entrevista ao projeto.

61 Ver Item 12 do Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

62 "Eu não lembro de ter um projeto de lei recente que tenha tido um processo de negociação dessa forma, numa sala, dentro no gabinete de deputado, à luz do dia, de uma forma tão aberta. Eu não lembro recentemente de ter um projeto que todo mundo sentasse para discutir o texto, na frente um dos outros, artigo por artigo. Não acho que é a primeira vez que aconteceu, espero que não seja a última, mas eu não lembro, ➔

Uma vez finalizada essa última rodada de discussões sobre o texto do projeto na Câmara dos Deputados, ocorreu, por um breve período, uma "disputa" entre essa versão e o projeto que tramitava desde 2013 no Senado (PLS 330/2013), que era, reconhecidamente, mais favorável aos setores que fazem uso mais intensivo de dados pessoais para diversas finalidades. Assim, Marcelo Bechara e Aloysio Nunes relatam que, em paralelo ao aparente consenso obtido na Câmara, havia articulações "por trás das cortinas" para fazer avançar a proposta do Senado[63].

Tal disputa se encerrou provisoriamente em 29 de maio de 2018, com a aprovação na Câmara (e consequente envio ao Senado) do projeto que teve origem, 7 anos antes, na primeira minuta do Ministério da Justiça. Trata-se de um momento crucial para o conjunto diverso de atores que se envolveram em todo o processo que culminou nesse momento: a proximidade da Copa do Mundo e do recesso parlamentar, bem como o peso dos anos de articulações e esforços para obter um consenso mínimo em torno do texto, pressionavam para que não houvesse mudanças substanciais na passagem pelo Senado (o que, por sua vez, levaria a um retorno do texto à Câmara e atrasaria o processo).

Foi nesse exato contexto que, finalmente, surgiu a coalizão tática e multissetorial, materializada no referido manifesto encabeçado pela Brasscom, cujo objetivo era, primordialmente, criar pressão política suficiente para que o Senado aprovasse o texto da LGPD sem mudanças. Para isso, Gallindo aponta que era necessário mostrar aos senadores que a lei tinha passado pelo "crivo do consenso de todas as partes"[64]. Assim, sob a liderança do senador

➔ recente, deste modelo dessa forma, abrindo para todo mundo, todo mundo mesmo, ter acontecido."

63 Ver Item 14 do Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

64 Ver Item 19 do Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade. ➔

Ricardo Ferraço, a matéria foi aprovada apenas com modificações textuais e pôde ser enviada à sanção pelo então presidente Michel Temer.

Todas as iniciativas de recurso aos diferentes setores da sociedade para que contribuíssem com a construção da lei, bem como a sua atuação proativa de defesa de interesses muitas vezes antagônicos, mas que acabaram se acomodando ao longo do caminho, culminaram nesse último movimento conjunto para garantir que os esforços de tantos anos não seriam perdidos perto da linha de chegada.

Já os próximos atos dessa longa trama da disciplina da proteção de dados no Brasil não mantiveram a mesma característica. Exatamente como e por que isso ocorreu ainda são questões a serem estudadas com maior profundidade pela literatura, mas abaixo destacam-se alguns dos fatos que sucederam a aprovação da LGPD no Congresso e como eles evidenciam a quebra da coalizão multissetorial.

B.4. A quebra da coalizão multissetorial após a aprovação da LGPD: vetos, a saga da autoridade e vigência

A vitória da aprovação unânime da lei na Câmara e no Senado (sem modificações substanciais) não sacramentou, entretanto, o fim da "via crúcis" da LGPD. Isso porque ainda havia pelo menos uma etapa no processo para a formulação de leis: a sanção

→ com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021. Andriei Gutierrez, no mesmo item, afirma que, para o setor privado, naquele momento já se haviam esgotados os pleitos e houve uma certa aceitação geral de que, em prol da segurança jurídica que uma lei geral traria, era mais estratégico deixar discordâncias específicas de lado e se unir a outros setores em defesa da aprovação pelo Senado.

presidencial e, nesse caso, por parte de um governo que já não era o mesmo que elaborou o Anteprojeto.

Assim, Miriam Wimmer relata que nesse momento diversos órgãos públicos que não haviam participado do processo de construção da lei reuniram-se para discutir e propor uma série de vetos à lei, em razão de receios sobre como a disciplina da proteção de dados poderia afetá-los[65]. Diante desse movimento, os diversos atores que vinham participando ativamente do processo mobilizaram-se para pressionar Temer[66] e demonstrar a relevância da lei e, inclusive, como ela poderia ser um "legado" do seu governo[67].

Um relato de Orlando Silva sobre o período é emblemático: ele afirma que, a despeito de todo o esforço multissetorial realizado para obter consenso sobre o texto da lei, quando houve a oportunidade de negociar vetos sobre dispositivos específicos, atores que haviam "sentado à mesa" com o mandato e com outros *stakeholders*, pressionaram o governo para obter um resultado mais favorável aos seus interesses particulares[68]. Observa-se que, no intervalo em que se discutiam os possíveis vetos, nem a Coalizão Direitos na

65 Ver Item 22, Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/

66 No item 22, Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados, explica Bechara: "teve uma reação quando projeta avançou de vários Ministérios, inclusive alguns deles pedindo veto integral ao projeto. Aí surge uma figura, que é o Subchefe de Assuntos Jurídicos da Casa Civil à época, doutor Gustavo Rocha, que foi um 'leão'. Ele conseguiu mostrar para o Presidente da República a importância do projeto, e o presidente entendeu a importância do projeto. E praticamente contra tudo e contra todos, o projeto passou, salvo os vetos que eram a questão deles legítima de questionar o Congresso Nacional e criar uma Autoridade dentro do Poder Executivo. (...). O Gustavo foi um cara forte, firme, ele mostrou a relevância, atuou, bancou, teve uma defesa importante em relação à aprovação do projeto. E os poucos vetos que tiveram foram graças a ele, porque senão teria muito mais".

67 Fala de Andriei Gutierrez no item 23, Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/

68 Ver Item 23, Capítulo 3 "Uma conjunção astral" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/

Rede, nem a Brasscom lançaram textos públicos de posição. Nesse caso, as negociações ocorreram "nos bastidores".

Os detalhes sobre o conteúdo dos vetos realizados por Michel Temer à época não são objeto do texto, mas destaca-se que foi nesse momento que a proposta de criação de uma Autoridade Nacional de Proteção de Dados com estrutura de agência reguladora, com autonomia e independência administrativa, funcional e financeira, foi suprimida e substituída por um modelo de órgão subordinado à Presidência da República, conforme desenho da Medida Provisória 869/2018[69].

A próxima "fase" da LGPD foi, então, o debate do Projeto de Lei de Conversão 07/2019, originado da MPV 869/2018, que, para criar a nova Autoridade, alterava a LGPD. De acordo com os ditames constitucionais, as Medidas Provisórias têm força imediata (porém provisória) de lei, mas devem ser analisadas pelo Congresso e convertidas, ou não, definitivamente em lei ordinária[70]. Esse processo permite a alteração do conteúdo da Medida pelo Legislativo, por meio de um projeto de lei de conversão, de forma que uma nova oportunidade de discutir o conteúdo da LGPD se apresentou naquele momento[71].

Ocorre que, em 2019, iniciou-se uma nova legislatura, alterando a composição do Congresso, e já não existia o "*momentum*", ou a "conjunção astral" que marcou a formação da coalizão tática para a aprovação da LGPD. Assim, o relato de participantes do

69 CONGRESSO NACIONAL. **Medida Provisória 869/2018 (Proteção de dados pessoais). 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: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 21 de janeiro de 2021.

70 CONGRESSO NACIONAL. **Entenda a tramitação da Medida Provisória**. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/entenda-a-tramitacao-da-medida-provisoria. Acesso em: 20 de janeiro de 2021.

71 Nessa ocasião, novamente o deputado federal Orlando Silva foi designado relator na Comissão destinada a proferir parecer sobre a Medida Provisória 869/2018 no prazo de 45 dias, sob pena de travar a pauta da Câmara.

processo[72] demonstra que, à exceção do consenso sobre a necessidade de manutenção do caráter independente da Autoridade - que foi, inclusive, objeto de mais um manifesto encabeçado pela Brasscom[73] -, houve novamente uma cisão entre os setores, que defenderam separadamente suas propostas de mudança (ou, pelo contrário, de não alteração) da lei.

B.5. Conclusão parcial

O longo período que antecedeu a aprovação da Lei Geral de Proteção de Dados brasileira, em 2018, e também aquele que a sucedeu e se prolongou até a definição de sua entrada em vigor, em setembro de 2020, foi marcado por um caráter multiparticipativo, que enriqueceu e trouxe maior legitimidade ao processo. Multissetorialismo, entretanto, diz respeito à reunião de diferentes perspectivas e não, necessariamente, à obtenção de consensos. A análise dessa década de debates permitiu identificar que apenas em um momento específico, permeado por uma conjuntura extremamente propícia, houve, de fato, uma coalizão tática em prol da aprovação da LGPD.

Trata-se de uma constatação que não diminui, por outro lado, a relevância da participação de múltiplos setores no processo, já que, além de fortalecer o DNA democrático da lei, o caráter

72 Sérgio Gallindo, por exemplo, afirma o seguinte: "Nesse momento, as representações empresariais acharam por bem defender melhorias na lei, assim como a sociedade civil também defendeu suas melhorias. Então, na tramitação da Medida Provisória 869/2018, não houve uma coalizão per se. As partes resolveram tratar dos temas dentro de sua ótica de aperfeiçoamento." Ver Item 3, Capítulo 4, "A saga da Autoridade" da Memória da LGPD do Observatório da Privacidade e Proteção de Dados. Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

73 BRASSCOM. **Manifesto pela criação imediata da Autoridade Nacional de Proteção de Dados Pessoais – ANPD**. 2018. Disponível em: https://brasscom.org.br/manifesto-pela-criacao-imediata-da-autoridade-nacional-de-protecao-de-dados-pessoais-anpd/. Acesso em: 21 de janeiro de 2021.

multissetorial dos debates também teve consequências sobre o conteúdo da norma gerada.

C. MULTISSETORIALISMO NO CONTEÚDO DA LGPD

Como essa natureza multissetorial e emblemática do processo que culminou na aprovação da LGPD refletiu-se no conteúdo da norma? Tratando-se de uma lei extensa e complexa, esse artigo não pretende examinar tal reflexo sobre todos os seus dispositivos, mas optou por focar em dois aspectos específicos: em primeiro lugar, a disputa sobre um dos "pilares" da lei, as bases legais do art. 7º e, especificamente, o consentimento e legítimo interesse; em segundo, o arranjo institucional criado pela LGPD para promover, dentre outras coisas, o seu *enforcement*.

a. Consentimento e legítimo interesse: forjando o artigo 7º por meio de dissensos e consensos

Um sobrevoo sobre os principais marcos do processo de elaboração da LGPD foi feito no item anterior deste artigo. Nesse momento, passa-se a destacar como duas das bases legais para o tratamento de dados pessoais, o consentimento e o legítimo interesse, foram tratadas durante esse processo e, especialmente, como os debates multissetoriais sobre a lei afetaram esse ponto específico do seu teor.

O primeiro texto submetido à consulta pública, ainda em 2010, previa em seu art. 9º[74] que o tratamento de dados pessoais teria

74 "Art. 9º - O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11."

como regra a obtenção do consentimento "livre, expresso e informado" do titular e que as outras hipóteses[75] nele listadas seriam exceções a essa regra[76]. Não havia, nesse momento, nenhuma previsão de base legal do legítimo interesse e, ao se analisar as contribuições à primeira consulta pública, só foi possível identificar um comentário que corresponde à ideia de legítimo interesse que veio a ser incorporada posteriormente à lei[77].

Nesse primeiro momento, portanto, havia um foco e uma prevalência no consentimento do titular como hipótese legitimadora do tratamento de dados pessoais, abordagem coerente com outras escolhas legislativas internas, como o Marco Civil da Internet[78], mas distante, por exemplo, do modelo adotado na Europa[79].

75 No projeto, estas hipóteses eram: obrigação contratual ou legal, dados de acesso público irrestrito, exercício de funções próprias dos poderes do Estado, pesquisa histórica, científica ou estatística, proteção da vida ou incolumidade física do titular ou terceiro, quando o consentimento não for possível, exercício do direito de defesa ou casos que digam respeito ao inadimplemento de obrigações por parte do titular, nos termos do Código de Defesa do Consumidor.

76 Sobre textos iniciais, menciona-se também a versão do PL 4060/2012, do então deputado federal Milton Monti, que fazia faz menção ao consentimento em dois momentos: quando alude a dados sensíveis e quando trata de dados pessoais de crianças; e a versão do PLS 330/2013, de autoria do então senador Antônio Carlos Valadares, que previa o "consentimento prévio e expresso do titular de dados como requisito à coleta, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado". Afora os dados sensíveis, cujas hipóteses de tratamento são abordadas pelo projeto, a única outra menção a bases legais, ou dispensa delas, consta do art. 4º, inciso V, que prevê a obrigatoriedade de "prévia ciência do titular das informações, quando se tratar de dados para os quais o consentimento expresso é inexigível".

77 Nos termos do relatório: "Por fim, a Nokia ressalta também ser necessário que as hipóteses de dispensa abranjam também os casos em que o tratamento for necessário para fins de interesses legítimos do responsável pelo tratamento dos dados ou de terceiro a quem os dados sejam comunicados, sendo preservados sempre os direitos e liberdades fundamentais do titular". ASSOCIAÇÃO BRASILEIRA DE MARKETING DIRETO. **Dados pessoais - contribuições das entidades**. 2010. Disponível em: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf. Acesso em: 21 de janeiro de 2021.

78 Cujos dispositivos referentes ao tratamento de dados pessoais prevê apenas a hipótese do consentimento, com qualificadoras ainda mais exigentes que as da LGPD: art. 7º, VII, IX.

79 Tanto a Diretiva 95/46/EC, que regulava a proteção de dados no bloco até 2018, e o Regulamento Geral de Proteção de Dados (RGPD) estabelecem um rol de bases legais hierarquicamente iguais para o tratamento de dados pessoais.

A mudança desse cenário ocorreu com a apresentação do primeiro substantivo pelo então senador Aloysio Nunes em referência aos projetos que relatava no Senado, ainda em 2015. Nessa ocasião, pela primeira vez, as bases legais para o tratamento de dados foram incluídas na forma de incisos paralelos, sem preponderância de um sobre o outro, e com a presença da hipótese de legítimo interesse.

Há pistas de que esse movimento tão relevante não tenha ocorrido em um vácuo: no mesmo período transcorria a segunda consulta pública sobre o Anteprojeto de lei do Ministério da Justiça e, diferente da primeira rodada, nessa ocasião houve contribuições significativas não apenas sobre a necessidade de se alterar o regime das bases legais e se incluir uma nova hipótese autorizativa, mas, inclusive, sobre a disciplina específica dessa nova opção (o legítimo interesse). Embora fossem processos distintos, a essa altura já havia diálogos estabelecidos entre o Senado e a proposta que viria a ser absorvida pela Câmara[80].

Assim, com a absorção dos diversos comentários que indicavam a necessidade de adequação do texto às melhores práticas internacionais, a versão do Executivo foi enviada à Câmara com a previsão de nove bases legais hierarquicamente equivalentes, de forma que, a partir de maio de 2016, as versões concorrentes do Senado e da Câmara contavam, ambas, com uma redação bastante diferente daquela que deu início ao processo, isto é, sem a prevalência do consentimento e com a presença do legítimo interesse.

Mais relevante, entretanto, foi a disputa que se seguiu a essa decisão: conforme demonstra um estudo do InternetLab sobre a segunda consulta pública do Ministério da Justiça, houve, nessa ocasião, uma cisão de posicionamentos em relação ao legítimo

80 Uma pista a esse respeito foi a participação do então Senador Aloysio Nunes, relator do PLS 330/2013, no evento de lançamento da versão pós-consulta pública do Anteprojeto de Lei do Executivo, quando afirmou, inclusive, que o texto do Executivo deveria ser encaminhado, com regime de urgência constitucional, ao Legislativo.

interesse, embora não tenha havido entidades que rejeitaram a proposta como um todo.

De um lado, empresas como Claro, Vivo, Sky e associações empresariais como Febraban e Brasscom, dentre outras, defenderam existir uma "fadiga do consentimento", isto é, um peso desproporcional sobre o próprio titular que deveria decidir sobre o tratamento de seus dados em todas hipóteses. Assim, as empresas apontaram o legítimo interesse como hipótese legal facilitadora do tratamento de dados em situações nas quais não haveria impactos indevidos sobre os direitos dos indivíduos, sem, entretanto, entrar em considerações mais aprofundadas sobre esses direitos ou sobre os interesses dos titulares. Outras contribuições, como a de Marcel Leonardi, ressaltaram o fato de o legítimo interesse integrar a legislação europeia sobre o tema desde 1995, de forma que se criaria um descompasso e um atraso caso o Brasil optasse por não seguir esse mesmo caminho.

Representantes de ONGs e da academia, entidades como ITS Rio e o Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI) estressaram o debate: para além de defenderem ou não a conveniência de se incluir o legítimo interesse na legislação, opinaram que, caso se decidisse pela sua inclusão, haveria a necessidade de ela vir acompanhada de um teste de razoabilidade/proporcionalidade, a fim de assegurar os direitos dos titulares de dados pessoais frente a uma situação de flexibilização do seu consentimento. Assim, sugestões como a inclusão da obrigatoriedade de anonimização dos dados como forma de proteção do titular foram feitas[81].

81 INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais.** 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 21 de janeiro de 2021.

Tais contribuições da sociedade civil reverberaram nas escolhas do Ministério da Justiça, uma vez que, apresentado o texto pós-consulta pública, ele trazia, para além da previsão do legítimo interesse como uma base legal para o tratamento de dados pessoais, também uma série de parágrafos que tornaram essa previsão mais robusta e equilibrada, a exemplo da legítima expectativa do titular (art. 10, §1º), de medidas de transparência e possibilidade de oposição por parte do titular (art. 10, §2º), dos princípio da necessidade e anonimização, quando compatíveis com a finalidade do tratamento (art. 10, §3º), e, por fim, da possibilidade de solicitação de relatório de impacto pelo "órgão competente"[82].

Olhando para esse momento da consulta pública de 2015, é possível notar um movimento de consenso, referente aos efeitos deletérios de se manter o consentimento como base preponderante e de não haver uma hipótese mais "flexível" como o legítimo interesse[83], e um movimento de dissenso, ou no mínimo, de claro afastamento entre empresas, de um lado, e ONGs e entidades acadêmicas de outro, tendo essas últimas defendido a imposição de certas constrições à aplicação do legítimo interesse.

Durante o processo legislativo que sucedeu esse período, houve poucas mudanças na previsão do legítimo interesse, mas relatos de quem participou dessa trajetória revelam que a disputa entre parte do setor privado e representantes do terceiro setor sobre o conteúdo do legítimo interesse, atravessou as audiências públicas, rodadas de discussão do texto e chegou até os últimos

82 CONGRESSO NACIONAL. **Projeto de Lei 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 20 de janeiro de 2021.

83 Nesse sentido, mencionam-se contribuições de empresas, academia e ONGs: Centro de Tecnologia e Sociedade da FGV Direito Rio; Marcel Leonardi; Instituto de Tecnologia e Sociedade do Rio (ITS-Rio), Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI) da USP, Centre for Information Policy Leadership, InternetLab, Claro S.A, Telefônica Brasil S.A. (Vivo) e Confederação Nacional da Indústria (CNI).

momentos da tramitação na Câmara dos Deputados, o que sugere que, muito embora tenha havido concessões mútuas durante o processo, a disputa de certos interesses ocorreu até o final em certos fóruns[84].

O presente texto não pretende fazer um exercício de futurologia reversa e prever se o Ministério da Justiça, ou os parlamentares autores e relatores dos projetos de lei, teriam chegado ao mesmo resultado, em termos de texto, não fossem as consultas públicas, especialmente a de 2015, e os debates multissetoriais ocorridos ao longo do processo legislativo. Entretanto, é inegável, e inclusive se trata de algo reconhecido pelas partes envolvidas, que foi essa conformação de múltiplos interesses que informou os atores não-técnicos responsáveis pela condução do processo e resultou em um texto "mais equilibrado".

A disputa sobre consentimento e legítimo interesse demonstra (i) a força de um consenso entre setores tradicionalmente

84 ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. **Memória da LGPD - Capítulo 5, "Como a lei mudou desde 2010"**. Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Acesso em: 20 de janeiro de 2021. Transcrição do depoimento de Beatriz Barbosa, Coordenadora do Intervozes. "Tinha um artigo que tratava de uma das hipóteses de tratamento de dados pessoais e que, para sociedade civil, era uma preocupação grande, que é uma hipótese baseada no legítimo interesse das empresas de tratarem esses dados. Essa sempre foi uma preocupação para a sociedade civil, que essa hipótese não fosse um cheque em branco para as empresas tratarem os dados da maneira como elas quisessem, então a gente queria colocar algumas condicionantes nesse trecho. A gente já tinha ido para a mesa de negociação e não tinha rolado, não tinha conseguido incluir isso porque as empresas não tinham deixado a mesa de negociação, mas tinha setores da sociedade civil muito preocupados. Eu lembro que, uma meia hora antes do deputado Orlando protocolar o texto dele, a versão final do substitutivo depois da rodada de negociação que ia para o plenário, ele estava em comissão discutindo um outro tema, conversando com um consultor da câmara que ia fazer a redação final do substitutivo para ele e eu cheguei e falei para ele "Orlando não vai dar, esse trecho aqui não pode passar desse jeito, se passar desse jeito a sociedade civil vai criticar o seu relatório e vai ser muito ruim ele chegar no plenário com críticas da sociedade civil.". Ele falou: "está bom, como é que vocês querem?" Aí eu arranjei uma folhinha do bloco que tinha na minha bolsa, escrevi correndo, grifei os dois trechos que precisavam incluir e entreguei o papel, quase um guardanapo assim para o Orlando. Aí ele pegou e entregou para o consultor, que fez uma cara não muito feliz, e falou assim "coloca desse jeito" e aí o relatório substitutivo foi para o plenário desse jeito. Ele fez a inclusão a nosso pedido e isso foi um dos trechos da Lei que sobreviveu a todo esse processo."

antagônicos sobre a necessidade de superação da hierarquia do consentimento, (ii) a existência de discordâncias sobre o conteúdo da previsão do legítimo interesse, se mais "protetiva" dos interesses do titular, ou menos, desde a segunda consulta pública até o final do processo legislativo; (iii) o fato de que, a despeito do forte multissetorialismo ao longo de toda a trajetória da lei, a coalizão tática, de fato, se deu apenas em um momento específico e bastante restrito no tempo (a pressão para aprovação sem mudanças no Senado), sendo que, até o final do processo na Câmara e em momentos posteriores, houve tentativas de cada setor de fazer valer seus interesses.

b. Arranjo institucional para o enforcement da LGPD

i. ANPD não tem o monopólio: o processo de materialização da LGPD envolve múltiplas partes

Na primeira Consulta Pública, promovida pelo Ministério da Justiça em 2010 e 2011, havia não apenas um dissenso sobre a necessidade de uma autoridade de proteção de dados,[85] como, também, desconfiança em torno da ideia de a própria lei incentivar e prever que o setor privado pudesse colaborar com o processo de regulação (e.g., códigos de boas condutas).[86]

85 Para Rafael Zanatta, a cultura e o arranjo institucional brasileiros incentivam um processo de competição de instituições na implementação da LGPD, conforme explica no item 12 do episódio "A saga da Autoridade" da Memória da LGPD, no Observatório da Privacidade. Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

86 Ainda no Capítulo "A saga da Autoridade" na Memória da LGPD, acrescenta Doneda, no item 15: "Certamente é perspicácia do Deputado Orlando Silva perceber que era possível fazer uma coisa que não parecia ser possível: botar todo mundo discutindo na mesa para chegar no texto final, legitimado por vários setores, a ponto de passar unânime nas duas Casas, sem encontrar resistência na presidência. Talvez, individualmente, seja de longe a maior contribuição para que ela tenha sido aprovada naquele momento". Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

Já na segunda consulta pública (com um debate mais amadurecido), o setor privado, até então maior opositor da criação da ANPD, e o terceiro setor[87], até então receoso com uma possível privatização do processo de regulação[88], começam a aparar tais arestas. O texto final da LGPD aposta no que se chama de corregulação,[89] justamente uma estratégia que é uma espécie de meio termo entre um processo de fiscalização puramente estatal ou uma regulação inteiramente privada. Por meio dessa escolha, reconhece-se o quão complexa é a tarefa regulatória em questão e a distribui nas mãos de vários atores.

Nesse sentido, o desenho final da LGPD programa que: **a)** ANPD deve cooperar com outros órgãos reguladores (artigo 55-J, incisos IX, XXI, XXII, XXIII e parágrafos 3º e 4º); **b)** o tradicional sistema de tutela de direitos difusos e coletivos brasileiro também poderá ser acionado, tanto em âmbito administrativo como judicial

87 Cf. contribuição apresentada pelo Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPOPAI) à segunda Consulta Pública sobre o Anteprojeto, promovida pelo Ministério da Justiça em 2015. Disponível em: http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/07c449c076fabbb00f3d3b850e063417.pdf

88 Cf. COHEN, Julie E. **Between truth and power: The legal constructions of informational capitalism**. Oxford University Press, USA, 2019; COHEN, Julie E. **Configuring the networked self: Law, code, and the play of everyday practice**. Yale University Press, 2012. No relatório sobre a segunda consulta pública elaborado pelo InternetLab, destaca-se, por exemplo, o dissenso no tocante à operacionalização do tratamento de dados e controle dos dados pessoais pelos cidadãos, visto, pelo setor privado, como possível entrave burocrático, e pelo terceiro setor, como instrumento efetivo de empoderamento. INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. 2016, p. 100. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 21 de janeiro de 2021.

89 WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: BIONI, Bruno, DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021; ZANATTA, Rafael A. F.. A Proteção de Dados Pessoais entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). **Direito e Internet III: Marco Civil da Internet.** 1ª ed. São Paulo: Quartier Latin, 2015, v. 1, p. 447-470.

(respectivamente, Procons e Secretaria Nacional de Defesa do Consumidor e ações civis públicas e coletivas) (artigo 22); **c)** os agentes de tratamento de dados, no âmbito do setor privado e setor público, são incentivados a se auto organizar por meio de códigos de boas condutas (artigos 32, 46, 49); **d)** selos, certificações e outros instrumentos contratuais privados são mecanismos de transferência internacional (artigo 33, II, d; e artigo 35), de modo que essa auto organização dos agentes privados pode ser premiada pela própria ANPD para destravar o fluxo transfronteiriço (artigo 55-J, XIV); **e)** é um dever da ANPD realizar consultas públicas, bem como avaliações de impacto regulatório para que haja uma oitiva - uma espécie de contraditório e ampla defesa - das partes afetadas pelo exercício do seu poder de regulamentação (artigo 55-J, §2º).

Além disso, é importante notar que a versão final do texto da LGPD criou o Conselho Nacional de Proteção de Dados/CNPD. Em um formato multissetorial[90], sendo um assento reservado ao CGI.br, é um órgão consultivo à Autoridade Nacional de Proteção de Dados (ANPD)[91] com poder de propor diretrizes e subsídios e realizar estudos e audiências públicas, bem como de elaborar relatórios anuais da execução das ações da Política Nacional de Proteção de Dados Pessoais da ANPD. Dessa forma, o CNPD está investido com poderes para a materialização da proteção de dados junto aos agentes de tratamento de dados e titulares, bem como sobre o próprio órgão regulador.

90 O Conselho é composto por representantes governamentais (Casa Civil, Ministérios, Gabinete de Segurança Institucional); da sociedade civil (organizações com atuação comprovada em proteção de dados pessoais); da comunidade acadêmica (instituições científicas e tecnológicas); do setor empresarial (relativo à área de tratamento de dados pessoais e entidades sindicais); e um assento reservado ao Comitê Gestor da Internet no Brasil.

91 GOV.BR. **Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 06 de janeiro de 2021.

Em poucas palavras, o arranjo institucional da LGPD não aposta em um sistema de supervisão em que haja uma autoridade única e que centralize todas as ações. Pelo contrário, programa-se um sistema de governança em rede, em que se distribuem competências entre uma série de atores, privados e públicos. Essa é justamente uma das definições de multissetorialismo[92], modelo no qual essa teia de atores se contrapõe a uma estratégia de regulação monopolizada pelo Estado.

D. CONCLUSÃO

Leis de gerais de proteção de dados atravessam os mais diferentes interesses e têm como função encontrar um consenso sobre qual é o fluxo informacional apropriado para as múltiplas partes interessadas. A LGPD tem, dentre todos os seus méritos, o fato de que essa realidade, compartilhada pelas normas de proteção de dados em geral, esteja espelhada diretamente no seu processo de construção, bem como em seu conteúdo normativo.

O processo de articulação da LGPD é um caso bastante rico para se investigar a correlação de forças de diversos atores e a construção de consensos e dissensos antes, durante e depois da sua aprovação. Em especial, foi possível observar a participação ativa dos diferentes setores, representando seus próprios interesses e contribuindo para a elaboração de um texto de equilíbrio, em diversos momentos emblemáticos desse processo e, inclusive, registrou-se a formação de uma coalizão tática para a aprovação da lei no Senado, resultado da confluência de esforços de

92 Cf. DENARDIS, L. Introduction: internet governance as an object of research inquiry. *In*: **Researching internet governance: methods, frameworks, futures**. MIT Press. 2020; AYMOND, M.; DENARDIS, L. **Multi-stakeholderism: anatomy of an inchoate global institution**. Global Commission on Internet Governance, paper series n° 41. September 2016. Disponível em: https://www.cigionline.org/sites/default/files/gcig_no.41web.pdf. Acesso em: 21 de janeiro de 2021.

empresas, associações empresariais, ONGs, entidades acadêmicas e órgãos públicos.

O conteúdo da LGPD também é multissetorial. Nesse sentido, o artigo explorou as disputas sobre o teor das bases legais para o tratamento de dados pessoais (art. 7º, na versão aprovada da lei), especialmente o consentimento e o legítimo interesse, e abordou o que talvez seja o maior exemplo dessa característica no conteúdo normativo da lei: o desenho de cooperação interinstitucional, que envolve setor público e setor privado, para a interpretação e fiscalização da LGPD.

O multissetorialismo na LGPD não tem data para acabar: uma norma que foi elaborada por muitas mãos, forjada por meio de um longo processo de dissensos e eventuais consensos, também terá a sua aplicação, na prática, construída pelo diálogo entre diferentes atores: institucionais, do mercado e da sociedade civil. Trata-se de um arranjo prescrito e encorajado pela própria LGPD.

BIBLIOGRAFIA

ARGENTINA. **Ley 25.326/2000 - Ley de Protección de los Datos Personales. Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales**. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. Acesso em: 21 de janeiro de 2021.

ASSOCIAÇÃO BRASILEIRA DE MARKETING DIRETO. **Dados pessoais - contribuições das entidades**. 2010. Disponível em: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf. Acesso em: 21 de janeiro de 2021.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. **Observatório da Privacidade - Memória LGPD**. Disponível em: https://observatorio privacidade.com.br/memorias/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "O tema entra em pauta" - item 1. Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "O tema entra em pauta" - item 6. Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "O anteprojeto chega à Câmara" - item 2. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 20 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "O anteprojeto chega à Câmara" - item 14. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 20 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "O anteprojeto chega à Câmara" - item 17. Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 20 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 19. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 11. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 12. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 14. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 19. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Uma Conjunção Astral" - item 22. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "A saga da Autoridade" - item 3. Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "A saga da Autoridade" - item 12. Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "A saga da Autoridade" - item 15. Disponível em: https://observatorioprivacidade.com.br/memoria/2019-a-saga-da-autoridade/. Acesso em: 21 de janeiro de 2021.

_____. Memória da LGPD - Capítulo "Como a lei mudou desde 2010". Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Acesso em: 20 de janeiro de 2021.

AYMOND, M.; DENARDIS, L. **Multi-stakeholderism: anatomy of an inchoate global institution**. Global Commission on Internet Governance, paper series n° 41. September 2016. Disponível em: https://www.cigionline.org/sites/default/files/gcig_no.41web.pdf. Acesso em: 21 de janeiro de 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%AAncias.&text=Art.&text=Equipara%2Dse%20

a%20consumidor%20a,intervindo%20nas%20rela%C3%A7%C3%B5es%20de%20consumo. Acesso em: 21 de janeiro de 2021.

_____. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 21 de janeiro de 2021.

_____. Lei nº 12.414, de 09 de junho de 2011. 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 21 de janeiro de 2021.

_____. Lei nº 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: 21 de janeiro de 2021.

_____. Lei nº 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: 21 de janeiro de 2021.

_____. 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: 21 de janeiro de 2021.

_____. Lei Complementar nº 166, de 08 de abril de 2019. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm. Acesso em: 21 de janeiro de 2021.

BRASSCOM. **Manifesto pela aprovação da lei de proteção de dados pessoais**. Disponível em: https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/. Acesso em: 21 de janeiro de 2021.

_____. Manifesto pela criação imediata da Autoridade Nacional de Proteção de Dados Pessoais – ANPD. 2018. Disponível em: https://brasscom.org.br/manifesto-pela-criacao-imediata-da-autoridade-nacional-de-protecao-de-dados-pessoais-anpd/. Acesso em: 21 de janeiro de 2021.

_____. Manifesto sobre a Futura Lei de Proteção de Dados Pessoais. Disponível em: https://brasscom.org.br/manifesto-sobre-a-futura-lei-de-protecao-de-dados-pessoais/. Acesso em: 21 de janeiro de 2021.

CÂMARA DOS DEPUTADOS. **Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 4.060, de 2012, do Dep. Milton Monti, que "dispõe sobre o tratamento de dados pessoais e dá outras providências, e apensos. Comissão de Proteção de Dados. Roteiro de trabalho. Proposta do Relator - Deputado Orlando Silva**. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/roteiro-de-trabalho-apresentado-em-22-11-2016. Acesso em: 21 de janeiro de 2021.

_____. Comissão de Proteção de Dados. Apresentações de palestrantes. Arquivos apresentados pelos palestrantes nas Audiências e Eventos da Comissão Especial. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-e-eventos. Acesso em: 21 de janeiro de 2021.

_____. Projeto de Lei 2796/1980. Assegura aos cidadãos acesso às informações sobre sua pessoa constantes de bancos de dados e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.prop

osicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 21 de janeiro de 2021.

_____. Projeto de Lei de Conversão 07/2019. 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: https://www.camara.leg.br/propostas-legislativas/2201766. Acesso em: 21 de janeiro de 2021.

CDR. **Coalizão Direitos na Rede**. Disponível em: https://direitosnarede.org.br/. Acesso em: 20 de janeiro de 2021.

COHEN, Julie E. **Between truth and power: The legal constructions of informational capitalism**. Oxford University Press, USA, 2019.

_____. Configuring the networked self: Law, code, and the play of everyday practice. Yale University Press, 2012.

COMITÊ GESTOR DE INTERNET NO BRASIL (CGI.br). **Resolução CGI.br/RES/2009/003/P. Princípios para a governança e uso da internet no Brasil**. Disponível em: https://www.cgi.br/resolucoes/documento/2009/003/. Acesso em: 21 de janeiro de 2021.

_____. Seminário de Proteção à Privacidade e aos Dados Pessoais. Disponível em: https://seminarioprivacidade.cgi.br/. Acesso em: 21 de janeiro de 2021.

_____. [IX Seminário de Privacidade] Mesa de Abertura. 2018. (39m05s). Disponível em: https://www.youtube.com/watch?v=GKMul1c4YYU&list=PLQq8-9yVHyOZVGYJeegT8I-mHrWOPIiYh&index=1&t=6s&ab_channel=NICbrvideos. Acesso em: 21 de janeiro de 2021.

CONGRESSO NACIONAL. **Entenda a tramitação da Medida Provisória**. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/entenda-a-tramitacao-da-medida-provisoria. Acesso em: 20 de janeiro de 2021.

_____. Medida Provisória 869/2018 (Proteção de dados pessoais). 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: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 21 de janeiro de 2021.

_____. Projeto de Lei 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 21 de janeiro de 2021.

_____. Projeto de Lei 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 20 de janeiro de 2021.

CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital: A experiência de elaboração legislativa do Marco Civil da Internet**. 138 f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 21 de janeiro de 2021.

DENARDIS, L. Introduction: internet governance as an object of research inquiry. *In*: **Researching internet governance: methods, frameworks, futures**. MIT Press. 2020.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: BIONI, Bruno, DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

EDPS. **The history of the General Data Protection Regulation**. Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 21 de janeiro de 2021.

GATTO, R. **A perspectiva contratualista na construção do consenso da sociedade na internet**. Orientador: Claudio de Cicco. 2016. 174f. Tese (Doutorado em Direito). Pontifícia Universidade Católica de São Paulo, São Paulo, 2016.

GATTO, R.; GETSCHKO, Demi. **Governança da Internet: conceitos, evolução e abrangência**. 27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2009. Disponível em: http://ce-resd.facom.ufms.br/sbrc/2009/081.pdf. Acesso em: 21 de janeiro de 2021.

GOV.BR. **Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 06 de janeiro de 2021.

INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 21 de janeiro de 2021.

MACHADO MEYER. **Tabela comparativa - Lei Geral de Proteção de Dados**. Disponível em: https://www.machadomeyer.com.br/images/Alteracoes-na-Lei-Geral-de-Protecao-de-Dados.pdf. Acesso em: 21 de janeiro de 2021.

MINISTÉRIO DA CULTURA. **Dados pessoais**. Disponível em: http://culturadigital.br/dadospessoais/. Acesso em: 20 de janeiro de 2021.

_____. PL de proteção de dados. Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf. Acesso em: 21 de janeiro de 2021.

MINISTÉRIO DA JUSTIÇA. **Anteprojeto de Lei de Proteção de Dados**. Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf. Acesso em: 21 de janeiro de 2021.

_____. MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais. 2015. Disponível em: http://pensando.mj.gov.br/2015/10/21/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/. Acesso em: 20 de janeiro de 2021.

_____. Proteção de Dados Pessoais. Disponível em: http://pensando.mj.gov.br/dadospessoais/. Acesso em: 21 de janeiro de 2021.

NISSENBAUM, Helen. **Privacy in context: Technology, policy, and the integrity of social life**. Stanford University Press, 2009.

PARLAMENTO EUROPEU. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 21 de janeiro de 2021.

_____. 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: 21 de janeiro de 2021.

SENADO FEDERAL. **Projeto de Lei do Senado n° 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências**. Brasília, DF, agosto de 2013. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 21 de janeiro de 2021.

VIANNA, Marcelo. **Um novo "1984"? O projeto RENAPE e as discussões tecnopolíticas no campo da informática brasileira durante os governos militares na década de 1970**. Oficina do Historiador, Porto Alegre, Suplemento especial, ISSN 21783748, I EPHIS/PUCRS, 27 a 29 maio 2014, p. 1148-11171. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/oficinadohistoriador/article/view/18998/12057. Acesso em: 21 de janeiro de 2021.

WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: BIONI, Bruno, DONEDA, Danilo, MENDES, Laura Schertel, RODRIGUES JUNIOR, Otávio Luiz, SARLET, Ingo Wolfgang (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

ZANATTA, Rafael A. F.. A Proteção de Dados Pessoais entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). **Direito e Internet III: Marco Civil da Internet**. 1ª ed. São Paulo: Quartier Latin, 2015, v. 1, p. 447-470.

O BRASIL NÃO PODE PERDER A CHANCE DE SE TORNAR COMPETITIVO EM UMA ECONOMIA DE DADOS[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **O Brasil não pode perder a chance de se tornar competitivo em uma economia de dados**, Jornal Valor Econômico, 19.07.2018.

Desde 2010 o Brasil discute uma Lei Geral de Proteção de Dados Pessoais. Após consultas públicas sobre o texto de um anteprojeto de lei, a realização de uma série de audiências, sessões temáticas e seminários nacionais e internacionais na Câmara dos Deputados, no Senado Federal e em outros fóruns, nós testemunhamos finalmente a aprovação de um projeto de lei sobre o tema no Congresso Nacional e a consequente promulgação de Lei Geral de Proteção de Dados/LGPD (Lei no. 13.709/2018).

Com isso, o Brasil se juntará ao rol de mais de 100 (cem) países que contam não só com uma infraestrutura legal, mas, também em sua grande maioria, institucional para regular o uso de dados pessoais. Essa é uma questão chave para o desenvolvimento econômico do País.

Antes disso o Brasil contava somente com leis setoriais sobre proteção de dados. Era uma verdadeira colcha de retalhos que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios, bem como desestimulava formulação de políticas públicas e parcerias público-privada.

Além disso, nenhuma das leis setoriais existentes haviam sido desenhadas nem eram vocacionadas para lidar com o fenômeno altamente complexo de uma economia e sociedade cada vez mais movida por dados. É a lei geral que fornecerá organicamente o conjunto completo de direitos e deveres de todos os atores desse ecossistema, conferindo segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados.

Tão importante quanto essa infraestrutura legal é a existência de uma infraestrutura institucional que lhe dê "vida". Por isso, historicamente, sempre houve a criação de autoridades para a aplicação de tais leis, sendo elas a engrenagem principal de um sistema de governança eficiente.

No caso brasileiro, em específico, o texto da lei menciona mais de 50 (cinquenta) vezes esse órgão regulador, de modo que ela seria praticamente inaplicável no caso de sua inexistência. Essa técnica é bastante difundida para que a legislação seja imune ao desenvolvimento tecnológico. Ao invés de fazer referência a um determinado padrão tecnológico, a grande maioria das leis trazem conceitos abertos para que as autoridades os calibrem dinamicamente de acordo com o estado da arte da tecnologia de cada período histórico.

Ao assim fazê-lo, tais autoridades garantem que a própria fiscalização da lei seja uniforme e previsível. Diferentemente do cenário em que diversos setores, com diferentes instâncias regulatórias, fragmentariam a sua interpretação indo ao encontro da que se deseja com uma lei geral de proteção de dados.

Ao se observar como o tema evoluiu na Organização para Cooperação e Desenvolvimento Econômico/OCDE ao longo de mais de três décadas, nota-se justamente a preocupação em torno dessa interdependência legal e institucional. Quando consolidou e atualizou as suas recomendações em 2013, a OCDE recomendou que seus países-membros deveriam ter autoridades "independentes" e com "recursos" e "expertise técnica". A futura autoridade brasileira deve ter esse perfil – autônoma funcionalmente e financeiramente – para que aplique e fiscalize de forma efetiva a lei. São essas instituições que cooperaram entre si para a solução de problemas comuns entre os países-membros acerca da matéria e, com isso, permitir maior integração econômica.

Esse é o mesmo fio condutor para que o Brasil seja futuramente considerado como um país de nível adequado de proteção de dados para fins de transferência internacional, de acordo com o sistema da União Europeia e de outros países ao redor do mundo. Tal tipo de análise leva em consideração não apenas o texto da lei, mas, também, o seu sistema de fiscalização. Até hoje os países que foram reconhecidos como tal pelo bloco econômico europeu, todos eles contam com uma autoridade.

Se pensarmos que outros mecanismos de transferência internacional, como selos de certificação, cláusulas corporativas globais e etc., têm um alto custo operacional por envolver a contratação de consultorias altamente especializadas para destravá-los. Então, a ausência desse órgão consistirá em uma barreira de entrada para boa parte das empresas brasileiras. Isto porque, elas precisariam de um alto grau de investimento para estar na rota de transferência global de dados. Ao contrário de estarem automaticamente nela inseridas, caso o Brasil venha a ser considerado um país com nível adequado de proteção de dados.

Até a entrada em vigor da lei brasileira de proteção de dados pessoais, a figura de uma autoridade é essencial para que empresas e o setor público se adéquem à nova lei. A exemplo do que se viu com o recente Regulamento Europeu de Proteção de Dados Pessoais, o papel do órgão regulador é também de auxiliar todos os atores regulados em identificar a quais obrigações estão sujeitos, o que inclui, até mesmo, o desenvolvimento de metodologias que auxiliem tal processo de conformidade (*compliance*).

A não criação de uma autoridade de proteção de dados pessoais com autonomia funcional e financeira sequer deveria ser ventilada a essa altura, ainda que se discuta a maneira pela qual ela será efetivamente instituída. O Brasil estaria novamente perdendo a chance de se tornar competitivo em uma economia de dados, na medida em que para estimulá-la não basta uma infraestrutura legal, mas, também, institucional.

Somente com esse arranjo regulatório completo, o mercado interno brasileiro reagirá bem e as suas aspirações em se tornar membro da OCDE e um país com nível adequado de proteção de dados serão maximizadas. Em poucas palavras, o esforço de quase uma década na construção de um marco legal será perdido caso não haja a criação desse órgão. Isso não deve ser enxergado como um custo, mas como um investimento para a retomada da economia brasileira. Justamente, no momento em que os brasileiros mais precisam.

MATERIAIS RECOMENDADOS

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

NIST . Disponível em: https://www.nist.gov/privacy-framework

D.E. O'Leary; S. Bonorris; W. Klosgen; Yew-Tuan Khaw; Hing-Yan Lee; W. Ziarko. **Some privacy issues in knowledge discovery: the OECD personal privacy guidelines**. Disponível em: https://ieeexplore.ieee.org/abstract/document/395352/metrics#metrics

COMO O BRASIL PODE TER UM PLANO NACIONAL DE IOT INOVADOR PARA A PROTEÇÃO DE DADOS PESSOAIS?[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **Como o Brasil pode ter um Plano Nacional de IoT inovador para a proteção de dados pessoais?** Gen jurídico, 22.02.2018.

No final de 2016, o Ministério da Ciência, Tecnologia, Inovações e Comunicação e o Banco Nacional de Desenvolvimento Econômico e Social firmaram um convênio para mapear as oportunidades da agenda de Internet of Things (IoT). Em 2017 e 2019 foram realizadas consultas públicas sobre o tema. Ou seja, o governo está atuando de forma coordenada e procurando engajar politicamente a sociedade brasileira nessa pauta.

É sem dúvida um assunto estratégico para o desenvolvimento do país e que vai revolucionar os mais diversos setores da economia. Saúde, mobilidade urbana, agropecuária, mineração e varejo são apenas alguns deles. A ideia é que os objetos ao nosso redor se transformem em sensores capazes de monitorar todas as nossas atividades para a elas agregar inteligência.

Por exemplo, um simples marca-passo poderia registrar todo o ritmo cardíaco de um implantado, o que permitiria diagnósticos e prognósticos mais precisos. Ainda, automóveis poderiam transmitir os dados de seu deslocamento para um melhor gerenciamento das rotas de tráfego.

É intuitiva a preocupação com relação à privacidade. Se George Orwell pensou na figura do *Big Brother* em seu homônimo no livro "1984" e de uma única tela que observaria de forma constante os cidadãos, o cenário de IoT complexifica o romance. A vigilância estaria apoiada em várias micro telas e colocada em curso por vários *little brothers*. Não só a TV e não só o Estado, mas, também, a geladeira, o relógio, o tênis e todos os fornecedores desses dispositivos poderiam estar de vigília.

Por isso, a proteção de dados pessoais é uma questão estratégica e indissociável de um plano nacional de IoT.

Leis de proteção de dados pessoais garantem que sejam fornecidos os conceitos-chave para o desenvolvimento da agenda de IoT no Brasil. Por exemplo, o que são dados pessoais e de que forma a tecnologia (e.g., anonimização) poderia ser aplicada para mitigar os riscos à privacidade dos cidadãos que estão atrás desses dispositivos. Referida regulação poderia conferir uma maior

segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado a respeito de como tais dados deveriam ser coletados, processados e compartilhados.

Tais leis são transversais (multissetoriais) em justaposição a molduras normativas fragmentadas. Do setor automotivo ao da saúde, sempre haveria vácuos não cobertos por legislações setoriais de proteção de dados pessoais. Somente uma lei geral teria a amplitude necessária para enfrentar uma demanda tão multifacetada como é a da IoT.

É necessário, portanto, que haja tal infraestrutura jurídica para reduzir as incertezas em jogo. Somente, assim, a IoT florescerá por estar inserida em um ambiente que catalisa a confiança dos seus atores, especialmente quanto ao fluxo de informações-dados nele trafegado.

Mas, para além desse papel estratégico, de que forma a privacidade poderia gerar uma experiência inovadora no Plano Nacional de IoT?

Via de regra, prevalece atualmente uma mentalidade regulatória punitiva para a proteção dos dados pessoais. Veja-se, de forma aleatória, três exemplos de três culturas jurídico-legais diferentes: **a)** o caso brasileiro em que a empresa "Oi" foi multada em R$ 3,5 milhões por não informar de forma adequada como os dados pessoais dos seus consumidores eram coletados; **b)** o caso paradigmático da unificação das políticas de privacidade em que a Google foi sancionada monetariamente por algumas autoridades garantes de proteção de dados europeias; e **c)** a principal bandeira do órgão regulador americano (*Federal Trade Commission*), o qual tem penalizado diversas empresas por cada uma das promessas quebradas sobre privacidade feitas em seus termos de uso ("*broken privacy promises*").

Em todos estes casos, o Estado, na figura do órgão regulador e em um movimento de regulação de cima para baixo, tem sancionado os atores regulados: uma mentalidade regulatória punitiva e *top-down*.

O plano nacional de IoT poderia ser a oportunidade para o Brasil encampar uma nova estratégia regulatória. Por que não combinar medidas de incentivo a comportamentos desejáveis, ao invés de somente punir práticas reprováveis? Isso seria capaz de desencadear um movimento de regulação de baixo para cima (*bottow-up*) e não só de cima para baixo (*top-down*).

É importante enaltecer que isso não seria a "invenção da roda". O direito ambiental já tem feito isso ao incentivar tecnologias menos poluentes, as quais têm isenções ou benefícios tributários. É o que o jurista italiano Noberto Bobbio professava ao dizer que o direito deve incentivar boas práticas por meio de normas premiais.

O mesmo poderia ser feito com tecnologias que tivessem como valor de concepção a proteção à privacidade, metodologia comumente chamada de "*privacy by design*", em que o projeto de um produto ou serviço é orientado por soluções tecnológicas que sejam pró-privacidade.

Por que também não conceder vantagens fiscais para aqueles sensores de IoT concebidos com esse tipo de preocupação? Não seria o caso da *privacy by design* ser uma condicionante imposta pelo BNDES para o financiamento de empresas nascentes de tecnologia?

Essa estratégia regulatória poderia ter vários desencadeamentos. Um deles, talvez o principal, é que a proteção de dados pessoais passaria a ser encarada como um elemento de competividade e vantagem econômica. Os atores regulados seriam induzidos a cooperarem com o órgão regulador, dando ensejo a um movimento de corregulação. Desde o "chão de fábrica" os efeitos da regulação já seriam notados.

O Plano Nacional de IoT parece ser uma excelente janela de oportunidade para tanto. O Brasil poderia ser disruptivo. Já pensou em uma linha branca *privacy-friendly* de IoT, ganhando mercado por esse ser o seu maior atrativo?

MATERIAIS RECOMENDADOS

TIC Domicílios 2019. Disponível em https://cetic.br/media/analises/tic_domicilios_2019_coletiva_imprensa.pdf

Plano Nacional de Internet das Coisas. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm

Estudo "Internet das Coisas: um plano de ação para o Brasil". Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil

REGULAÇÃO DE DADOS É UMA JANELA DE OPORTUNIDADE[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **Regulação de dados é uma janela de oportunidade**, Jornal Valor Econômico, 29.03.2019.

Ainda é comum se referir à Lei Geral brasileira de Proteção de Dados/LGPD, a Lei no 13.709/2018, enquanto um espantalho. Seria mais uma regulação, dentre tantas as outras já existentes, que travaria a economia e a inovação no país. O pessimismo é destilado através do medo. Quem não estiver em conformidade com a nova legislação amargaria prejuízos de até R$ 50 (cinquenta) milhões de reais, uma das suas penalidades previstas. Deveria ser o contrário, empresas e órgãos públicos precisam enxergar na nova regulação uma janela de oportunidade, refletindo sobre o quanto poderão ganhar e se tornarem mais eficientes ao se adequarem à nova lei.

A LGPD parte da premissa de que toda a organização deve não só conhecer os dados que possui, mas, sobretudo, convertê-los em uma informação útil. Todo o sistema gira em torno da lógica em se criar uma trilha auditável do dado, pela qual o cidadão e os demais agentes econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades econômicas e relações sociais que fazem parte. A nova lei não veio para travar o fluxo informacional, mas, muito pelo contrário, estimulá-lo dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora.

Ao prever, por exemplo, que toda e qualquer atividade de tratamento de dados – da coleta, passando pelo compartilhamento ao descarte – deve, dentre uma outra série de princípios, ter especificada uma finalidade, a nova lei ajudará na organização da informação. Infelizmente muitas entidades ainda têm a mentalidade de coletar a maior quantidade possível de dados sem antes refletir sobre a sua real utilidade. Basta abrir nossos smartphones e notar a série de aplicativos que pedem acesso à lista de contatos, câmera, microfone, dentre outras coisas, que são desnecessários para o modelo de negócio ou serviço público que nele roda. O resultado é além da subutilização desses dados, a sua transformação em um elemento tóxico que, depois de "vazado", ocasionam as catástrofes dessa nova economia movida a dados.

Duas das principais ferramentas de adequação à nova lei seguem essa lógica: mapeamento de dados e programas de governança. Respectivamente, a organização deve fazer um diagnóstico em torno de todo o seu repositório de informações e, em seguida, um prognóstico acerca de quais práticas devem ser mantidas ou modificadas para assegurar a sua conformidade regulatória. Se realizado de forma adequada, é um exercício que trará novas ideias, sobretudo em torno de dados subutilizados com o potencial de informar novas ações tanto no poder público, quanto no setor privado.

O processo de conformidade não deve ser internalizado como um custo, muito menos enquanto uma papelada para formalmente fazer um "*checklist*" das obrigações legais. Pelo contrário, deve ser compreendido como um investimento capaz de otimizar e tornar mais eficiente as atividades dos atores regulados. A partir dessa mentalidade, abre-se espaço para que a nova regulação seja um gatilho para: **a)** a criação de novos produtos e serviços e, até mesmo, a revisão de um modelo de negócio ou de uma política pública, ao invés de servir apenas para a manutenção ou a revisão de produtos e serviços existentes; **b)** geração de valor através de diagnósticos e prognósticos recorrentes e dinâmicos, ao invés de avaliações estanques focadas apenas no risco regulatório. Enfim, o processo de conformidade passa a fazer parte de um plano maior de gestão baseado em inovação, ao invés de se guiar apenas pelo receio da aplicação de sanções em caso de não conformidade à nova regulação.

Para além desse efeito colateral interno positivo, o processo de conformidade pode ser um ponto de virada especialmente para fora da organização em meio a um mercado extremamente competitivo e de escala global. A grande maioria das leis de proteção de dados pessoais, a exemplo do que fez a europeia (GDPR) e a brasileira, criaram um vínculo de solidariedade entre quem é uma espécie de gestor da cadeia de tratamento de dados – o controlador – e quem é o seu terceirizado – o processador. Se há um

eventual dano causado pelo terceirizado, o gestor pode ser acionado diretamente a repará-lo. Nesse sentido, obriga-se, diretamente ou indiretamente, que controladores contratem apenas processadores que estejam em conformidade com as regras de proteção de dados pessoais. Com isso, os próprios atores da cadeia de tratamento de dados mais do que fiscalizaram uns aos outros, tendem a escantear aqueles não *compliants*. Portanto, quem estiver em conformidade passa a ter uma vantagem competitiva frente aos seus pares retardatários, o que pode se traduzir, inclusive, na valorização dos seus serviços e produtos.

Em resumo, usando um exemplo mais próximo do leitor em geral e que costumo recorrer em sala de aula, é o da arrumação de um guarda-roupa. Enquanto essa atividade era executada apenas em virtude da pressão de um castigo a ser imposto pelos nossos pais e mães, a arrumação era algo burocrático e que raramente se extraía valor dela. Diferentemente por parte de quem, a curto, médio ou longo prazo, internalizou a tarefa de forma engajada e organizou cuidadosamente as roupas – os dados, transformando-as em informações que otimizaram o processo de tomada de decisão – se preferir os custos de transação – quanto à vestimenta mais apropriada para as diversas ocasiões do dia a dia. Uma organização que não enxerga valor no processo de conformidade regulatória da LGPD, é como se fosse uma pessoa adulta com um armário desorganizado que, cedo ou tarde, se atrasará para uma reunião ou nela chegará malvestida e terá perdas financeiras e reputacionais.

A nova regulação de dados é uma janela de oportunidade. Quem compreender e catalisar o processo de conformidade como um dos pilares de um plano estratégico de inovação, colocará ordem na casa e colherá frutos que extrapolam o mero estado de *compliance*. É um efeito secundário e desejado da nova regulação, o que os economistas costumam chamar de externalidade positiva. Resta saber por quanto tempo essa janela ainda estará aberta e não congestionada, visando ser, para usar um termo em alta, disruptivo.

INOVAR PELA LEI[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: Bioni, Bruno R. **Inovar pela Lei**, FGV Executivo (Fundação Getúlio Vargas), v. 18 n. 04, jul/agosto 2019.

Em 2017, ficou famosa a capa da The Economist com a mensagem de que o recurso mais valioso do mundo não seria mais o petróleo, mas, sim, dados. A revista inglesa ilustrava as grandes empresas de tecnologia como sendo as estações petrolíferas que extrairiam riqueza desse novo ativo. Um ano depois, em agosto de 2018, o Brasil aprovou a sua lei geral de proteção de dados pessoais (Lei 13.709/2018), mesmo ano em que passou a valer o regulamento de proteção de dados na União Europeia – a General Data Protection Regulation (GDPR). Em 2019, começou a ganhar força o movimento dos Estados Unidos para também criarem uma regulação a nível federal, depois de alguns estados, sobretudo a Califórnia, terem legislado sobre o assunto.

Ao longo desses últimos anos, nós estamos testemunhando uma verdadeira ebulição do tema e, mais especialmente no cenário nacional, estamos vivendo isso à flor da pele com uma nova lei que estabelece definitivamente as regras do jogo. É hora de dar um passo atrás, recuperar os registros do porquê e como se gestaram leis gerais de proteção de dados pessoais. A partir desse diagnóstico, pretende-se apontar possíveis tendências dessa nova agenda: como esse jogo pode e tende a ser jogado no Brasil.

OLHANDO PARA A HISTÓRIA

Olhar no retrovisor faz com que se perceba que a demanda por regular o uso de dados pessoais em si não é nova. Ao construir uma linha do tempo com as diversas gerações de normas sobre a matéria, Viktor-Mayer, professor de Oxford, aponta que as primeiras iniciativas deram errado por tentarem domesticar a tecnologia. Logo se percebeu ser impossível prescrever de antemão uma lista fechada sobre seus usos lícitos e ilícitos. Migrou-se, então, para uma abordagem focada na definição dos direitos do titular da informação, cidadãos-consumidores, e deveres das organizações que processavam tais dados.

Desde a década de 80 até hoje, os chamados princípios e práticas informacionais justas – Fair Information Practice Principles (FIPPs)– são a espinha dorsal das leis de proteção de dados pessoais. Originados no âmbito do departamento de bem-estar social dos EUA, tais princípios foram espelhados nas Diretrizes sobre Privacidade e Livre Fluxo Informacional da Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE) e na Convenção Internacional de Proteção de Dados do Conselho da Europa. OS FIPPs não só capilarizaram tais normas em nível global como também demarcaram o duplo objetivo dessa empreitada regulatória: proteger os direitos e liberdades fundamentais dos cidadãos e, ao mesmo, estimular o desenvolvimento econômico.

Já naquela época havia o diagnóstico em torno da necessidade em se estabelecer as regras do jogo para que fosse nutrida a confiança do cidadão em conceder seus dados para organizações públicas e privadas. Caso contrário, censos demográficos e técnicas de marketing ainda incipientes, que respectivamente nada mais são do que a conversão de dados pessoais do cidadão e do consumidor em estatísticas e informações para a formulação de melhores políticas públicas e bens de consumo, seriam possivelmente represadas.

O Brasil chegou atrasado, mas finalmente entrou para o rol de mais de 120 (cento e vinte) países com leis gerais de proteção de dados pessoais. Espera-se que o novo marco regulatório cumpra o seu objetivo histórico em estimular o fluxo informacional e, com isso, o desenvolvimento socioeconômico dele dependente dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora.

IMPACTO REGULATÓRIO E SOCIOECONÔMICO DA LGPD

O adjetivo "geral" é aqui o elemento chave. A LGPD veio para complementar uma série de leis setoriais de proteção de dados já existentes no Brasil, mas que era uma regulação precária e não vocacionada para lidar com o fenômeno altamente complexo de uma economia e sociedade cada vez mais movida por dados. Na medida em que se tem uma lei de aplicação transversal, elimina-se a assimetria regulatória antes existente por uma abordagem fragmentada. Agora todos os setores da economia estarão cobertos e há uma peça central do quebra-cabeça regulatório que dita um mínimo de uniformidade. Com isso, garante-se segurança jurídica para que se estimule a troca dados, nas mais diferentes situações e momentos, a partir de um regramento e vocabulários de definições comuns.

Não é só, portanto, o setor de tecnologia e de internet que são afetados pela LGPD, como se poderia concluir a partir da citada capa da *the Economist*. Todos os setores da economia o serão, inclusive os mais tradicionais, desde que lidem com dados pessoais. Varejo, saúde, automobilístico, energia elétrica, dentre outros setores, terá que tratar dados dos seus consumidores e colaboradores de acordo com a LGPD. A nova regulação terá possivelmente um impacto muito maior do que foi a edição do código de defesa do consumidor nos anos 90, na medida em que abraça relações de trabalho e, também, do cidadão com o setor público.

A lei adota um conceito amplo de dado pessoal: uma informação relacionada a uma pessoa identificada ou identificável. Muito além daquele conjunto de dados que nos identifica de forma direta e imediata (como nome, RG, CPF ou biometria), também estão debaixo do guarda-chuva da LGPD aqueles dados que nos identificam de forma remota ou indireta (como apelidos, fotos,

endereços de e-mail, endereços residenciais, endereços de IP, dados de geolocalização, etc).

Os tentáculos LGPD são, portanto, enormes, com o potencial de abraçar os mais diversos momentos do nosso cotidiano. É difícil imaginar em que momentos não estamos trocando dados e, sobretudo, quando nossas vidas não são orquestradas com base no que um banco de dados diz a nosso respeito. Da concessão de crédito, passando pelo acesso a benefícios sociais até a timeline da rede social, todas essas atividades são automaticamente personalizadas com base nos dados que geramos. Por isso, regulações desse tipo e nesse estágio equivalem ao nosso próprio contrato social contemporâneo.

DADOS + ORGANIZAÇÃO = INFORMAÇÃO

Apesar de uma nova regulação causar receios em relação aos custos de conformidade (o aumento do "custo Brasil"), a LGPD representa uma janela de oportunidades. Primeiro, porque as organizações terão que colocar "ordem na casa", na medida em que vão precisar conhecer melhor todas as suas bases de dados e lhes atribuir uma finalidade específica – um dos princípios da lei. É um exercício que poderá trazer *insights* para se repensar o próprio modelo de negócio ou política pública e até mesmo para lançar novos produtos e serviços. Segundo, a adequação à legislação pode melhorar a reputação da empresa, na medida em que o tratamento adequado dos dados pode ser explorado no plano de comunicação para reforçar a confiança com o titular da informação. Terceiro, porque a lei traz uma série de exigências relacionadas à segurança da informação no sentido não só de prevenir o "vazamento" de dados, mas, também, de remediá-lo da forma mais eficiente caso ocorra. Tratam-se de medidas cujo saldo final pode agregar valor e competitividade a uma organização, a depender de qual mentalidade orientará o seu respectivo processo de conformidade:

Mentalidades de processos de conformidade à LGPD*	
Uma obrigação legal	**Uma janela de oportunidade**
Manutenção e revisão dos produtos existentes	Criação de novos produtos e revisão de modelo de negócio ou política pública
Análise estanque centrada no diagnóstico de riscos	Análise dinâmica centrada no que a organização pode gerar de valor
Gestão baseada em mitigação de risco	Gestão baseada em inovação
Reputação com base no medo de sanções	Reputação com base em dar mais transparência ao uso dos dados
- inovação - competividade - reputação	+ inovação + competividade + reputação

*Elaborado em coautoria com Maria Cecilia Oliveira Gomes para o artigo de autoria dela intitulado: "Para além de uma obrigação legal: o que a metodologia de benefícios e riscos nos ensina sobre o papel dos relatórios de impacto à proteção de dados"

De forma geral, o processo de mineração de dados, para utilizar um termo da ciência da computação, sempre procura levar a um lugar: a extração de uma informação. Essa é, também, a racionalidade por trás da nova regulação por meio da qual toda a organização deve não só conhecer os dados que possui, mas, sobretudo, convertê-los em uma informação útil. Todo o sistema gira em torno da lógica de se criar uma trilha auditável do dado, um modelo de governança pelo qual o cidadão e os demais agentes econômicos enxerguem a repercussão do uso dessas informações em suas atividades econômicas e relações sociais.

FORMAÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A edição de uma lei é apenas o primeiro passo na formação de uma cultura de proteção de dados pessoais no Brasil. Tomando como exemplo a edição do Código de Defesa do Consumidor na década de 90, demorou certo tempo para que o cidadão, órgãos de fiscalização e os próprios agentes econômicos fizessem a "lei pegar". Após quase 4 (quatro) décadas, é possível dizer que a lei pegou e trouxe "civilidade" ao mercado de consumo com produtos e serviços mais seguros. As organizações que enxergaram no novo marco regulatório uma oportunidade em agregar valor e reputação aos seus produtos, até hoje colhem os frutos e usam isso no seu plano de comunicação.

As organizações que vierem a estabelecer processos de governança de dados, investindo em capital humano e não só tecnológico, tudo isso como parte da sua missão institucional, se anteciparão e capitalizarão em cima do processo da formação de uma cultura de proteção de dados pessoais ainda a ser formada no Brasil. Não seria exagero pensarmos em uma futura capa da The Economist com os protagonistas dessa nova jornada.

MATERIAL RECOMENDADO

The Fair Information Practice Principles. Disponível em: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles

VIII Seminário de proteção à privacidade e aos dados pessoais. Disponível em: https://seminarioprivacidade.cgi.br/2017/

Privacidade Hackeada (The Great Hack). Disponível em: https://www.netflix.com/br/title/80117542

A INFRAESTRUTURA JURÍDICA DA ECONOMIA DOS DADOS:
dos princípios de justiça às leis de dados pessoais[1]

Bruno R. Bioni[2] e Rafael A. F. Zanatta[3]

1 Este ensaio foi escrito entre março e abril de 2019, antes da fundação da Associação Data Privacy Brasil de Pesquisa e nosso trabalho em conjunto como diretores da organização. Uma versão foi publicada no livro de Ladislau Dowbor intitulado "Sociedade Vigiada: Como a invasão da privacidade, por grandes corporações e Estados autoritários, ameaça instalar uma nova distopia", pela editora Autonomia Literária (2020), com o título "Direito e economia política dos dados: um guia introdutório". Somos gratos a Antonio Martins e Ladislau Dowbor pelo estímulo à escrita.

2 Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando em Direito Civil pela Universidade de São Paulo. Mestre em Direito Civil pela Universidade de São Paulo. Foi pesquisador visitante do Conselho da Europa e pesquisador na Universidade de Ottawa. Membro da Rede Latino-Americana de Vigilância, Tecnologia e Sociedade. Contato: bioni@dataprivacybr.org

3 Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando pelo Instituto de Energia e Ambiente da Universidade de São Paulo. Mestre em Teoria Geral do Direito pela Universidade de São Paulo. Mestre em Direito e Economia Política pela Universidade de Turim. *Research Fellow* na The New School (EUA). Membro da Rede Latino-Americana de Vigilância, Tecnologia e Sociedade. Contato: zanatta@dataprivacybr.org

INTRODUÇÃO

É lugar-comum afirmar que "vivemos em uma economia de dados" e que estamos passando por um processo de "transformação digital"[4]. Nas ciências sociais, fala-se de "datificação"[5] - um processo de transformação de todos os aspectos da ação social em dados, fazendo com que essa informação tenha valor pela capacidade de análise preditiva -, ao passo que o Fórum Econômico Mundial, sem as mesmas pretensões acadêmicas, tem utilizado constantemente o termo *digital economy* e enfatizado os potenciais da revolução gerada pela conectividade em massa e serviços que se valem de técnicas avançadas de análise de dados.[6] Com acerto, Evgeny Morozov tem defendido a orientação dos debates nas ciências humanas para o fenômeno do "capitalismo dadocêntrico"[7].

No nível político, planos como o "*Building a European Data Economy*"[8] da União Europeia e a "Estratégia Brasileira para a Transformação Digital"[9] evidenciam interesses, no nível regional e nacional, em buscar "competitividade em negócios digitais, digitalização de serviços públicos, criação de empregos qualificados na nova economia e políticas para uma educação melhor e mais avançada". A centralidade da "datificação" se dá, também, nas

4 SILVA, Nelson. Transformação digital: a 4. revolução industrial. **Boletim de Conjuntura da FGV**, n. 8, p. 15-18, 2018. Para um diagnóstico anterior. cf. IANSITI, Marco; LAKHANI, Karim R. Digital ubiquity: How connections, sensors, and data are revolutionizing business. **Harvard Business Review**, v. 92, n. 11, p. 19, 2014.

5 VAN DIJCK, Johana. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197-208, 2014.

6 Ver https://www.weforum.org/system-initiatives/shaping-the-future-of-digital-economy-and-society

7 MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política.** São Paulo: Ubu Editora, 2018.

8 https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

9 http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf

políticas industriais e nos novos planos de "inteligência artificial", que o Brasil ainda não possui.[10]

A configuração dessa "economia política dos dados"[11] parte de um longo processo de transformação sócio-técnica, chamado por James Beninger, em livro clássico de 1986, de "revolução do controle"[12], decorrente de uma série de inovações no campo da física, das telecomunicações e da computação, que ampliaram a capacidade de controle da informação.[13] Recentemente, livros como *Data and Goliath* (2015), de Bruce Schneier, e *The Age of Surveillance Capitalism* (2019), de Shoshana Zuboff, colocaram em evidência uma especificidade dessa economia após o advento de Google, Alibaba e Facebook: a enorme capacidade de empresas de tecnologia de monetizar e extrair valor do "material cru" composto por nossas relações sociais cotidianas, graças à ubiquidade dos *smartphones*, computadores e barateamento dos custos de coleta e transmissão de informações relacionadas a nossa atuação diante de tais dispositivos e aplicações. Tornou-se evidente, enfim, que a Internet é (e sempre foi) uma rede de controle[14] e

10 LEMOS, Ronaldo. É preciso plano de inteligência artificial, **Folha de São Paulo**, 04/02/2019 (argumentando que inteligência artificial "deve ser vista hoje como parte da infraestrutura de qualquer país, pois é capaz de gerar externalidades positivas para todas as atividades produtivas, tornando-as mais competitivas e eficientes"). O plano pode ser sencontrado aqui: http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf

11 ARRIETA IBARRA, Imanol et al. Should We Treat Data as Labor? Moving Beyond'Free'. **American Economic Association Papers & Proceedings**, v. 1, n. 1, 2017.

12 BENIGER, James. **The control revolution: Technological and economic origins of the information society**. Harvard university press, 2009.

13 O historiador da ciência Bonît Godin demonstrou que o conceito de "information economy", utilizado desde 1945, passou por uma compreensão da informação como conhecimento, depois como informação como "commodity", informação como "atividade industrial" e informação como "tecnologia".

14 Demi Getschko, um dos engenheiros responsáveis pela disseminação da Internet no Brasil, sempre afirma em suas palestras que o conceito de *cybernetics*, tal como desenvolvido por Norbert Wiener (1894-1964), se relaciona ao "estudo científico do controle e da comunicação dos animais e das máquinas". A etimologia da palavra "cyber" vem do grego κυβερνητική, originária da navegação marítima, designando "governança". Nesse sentido, é ilusório acreditar que "cyber" significa algo como espaço etéreo, livre de normas e incontrolável. Wiener emprestou o conceito do cientista francês André →

que a digitalização promove uma espécie de "capitalismo de vigilância"[15], com uma lógica econômica específica. Para os juristas, a reconfiguração dessas economias para um modelo de vigilância gera um conjunto de questões passíveis de aprofundamento.

Primeiro, porque também está havendo a reformatação dos arranjos regulatório à reboque da nova lógica econômica. Por exemplo, ao mirar na construção de um "Mercado Único Digital", a União Europeia ainda está passando por um processo profundo de modernização do seu quadro regulatório sobre proteção de dados pessoais. Após aprovar o Regulamento Europeu de Proteção de Dados Pessoais[16] – norma que Ricardo Abramovay chamou de "a mais vigorosa reação pública ao modelo de negócios dos gigantes digitais"[17] – e uma nova Diretiva que regula o acesso à dados para fins de investigação criminal,[18] ainda está em discussão a reforma da Diretiva sobre comunicações eletrônicas.[19] Enquanto o Brasil, logo após a formulação de um plano

➔ Marie Ampére, que cunhou a expressão "*Cybernétique*" como ciência ou arte do governo, sendo uma sub-ciência da "*Politique*". Ampére, por sua vez, adaptou a expressão de Platão (*kybernetike*). LEVIN, Mariam. **Cultures of Control**. Amsterdam: Harwood Academic Publisher, 2000, p. 252.

15 EVANGELISTA, Rafael. Capitalismo de Vigilância no Sul Global: por uma perspectiva situada, *in*: **5º Simpósio Internacional LAVITS**, Santiago, Chile, 2017, p. 243-253. Disponível em: http://lavits.org/wp-content/uploads/2018/04/08-Rafael-Evangelista.pdf

16 A General Data Protection Regulation/GDPR, Regulamento 2016/679, substituiu a antiga Diretiva 95/46/EC. Diferentemente da Diretiva, o Regulamento tem aplicação direta em todos os países membros do bloco econômico e, ao mesmo tempo, poucas normas podem ser derrogadas ou procedimentalizadas por leis domésticas. Com isso, o Regulamento objetiva unificar e trazer consistência na regulação de proteção de dados em todo o bloco econômico, algo que não foi alcançado pela Diretiva por ser um mecanismo sem eficácia direta e que, ao ser internalizado por leis domésticas, acabou por criar um cenário regulatório conflituoso em cada um dos integrantes do bloco europeu. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>.

17 ABRAMOVAY, Ricardo. Aos dados, cidadãos!, **Revista Quatro Cinco Um**, São Paulo, abril de 2018, p. 6.

18 Trata-se da diretiva 2016/680 que visa não só à proteção dos dados pessoais do cidadão, mas, igualmente, a cooperação entre autoridades para o combate à crimes. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:310401_3>

19 Um dos pontos mais controversos da nova regulação é sobre cookies e outras formas monitoramento de navegação, o que é a base da publicidade comportamental online ➔

nacional de Internet das Coisas que destacava a fragilidade da regulação sobre dados no país,[20] acabou por aprovar uma lei geral de proteção acerca da matéria (Lei 13.709/2018). Muitos outros exemplos ao redor do mundo poderiam ser apontados como exemplo dessa ebulição regulatória puxada pela formatação de uma nova economia.

Neste ensaio, buscamos responder algumas questões, atribuindo sentido a essa discussão regulatória. Qual a relação entre economia política dos dados e proteção de dados pessoais? Que infraestrutura jurídica dá sustentação a essa economia? O que se entende por proteção de dados pessoais no Brasil, em um contexto de "regulação pelo código"[21] e de normatividade gerada pelas próprias tecnologias[22]? O que há de diferente no modelo jurídico criado nos EUA, no sistema europeu e nas reações emergentes em países como o Brasil?

O texto divide-se em três partes. Na primeira, discutimos a evolução do sistema jurídico de *privacy* nos EUA, com seu enfoque predominantemente consumerista e principiológico. Na segunda parte, discutimos a emergência do discurso da proteção de dados pessoais como um "direito fundamental" nos países europeus e a afirmação de um modelo regulatório que combina expertise tecnocrática (a criação de *Data Protection Authorities*) com leis gerais de proteção de dados pessoais. Na terceira, discutimos tendências

➔ que sustenta o modelo de negócio predominante na União Europeia. Disponível em: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>

20 Veja, nesse sentido, o estudo sobre ambiente regulatório: <https://www.bndes.gov.br/wps/wcm/connect/site/e614e9a3-053b-42d4-853a-6b4aa406e31f/produto-3-analise-de-oferta-e-demanda-relatorio-horizontal-ambiente-regulatorio.pdf?MOD=AJPERES&CVID=lWrmVIj>

21 LESSIG, Lawrence. **The constitution of code: limitations on choice-based critiques of cyberspace regulation.** *CommLaw Conspectus*, v. 5, p. 181, 1997. GRIMMELMANN, James. Regulation by software. *Yale Law Journal*, v. 114, p. 1719, 2004. No Brasil, ver ABRAMOVAY, Ricardo. Eficiência e democracia na era digital, Valor Econômico, 04/02/2019.

22 HILDEBRANDT, Mireille; TIELEMANS, Laura. **Data protection by design and technology neutral law.** *Computer Law & Security Review*, v. 29, n. 5, p. 509-521, 2013.

jurídicas que se ganham força no Brasil, inspiradas por Europa e EUA, e as dificuldades de construção dessas molduras regulatórias em uma sociedade marcada por instituições democráticas frágeis e por um lugar ainda periférico no arranjo global de proteção de dados pessoais.

Argumentamos que a proteção de dados pessoais é um componente central da infraestrutura jurídica que dá sustentação a essa economia de dados. A análise histórica da formulação desses arranjos regulatórios evidencia o papel central dado aos *fluxos dos dados*, combinado com uma preocupação de princípios de justiça e direitos fundamentais. Nesse sentido, a "proteção de dados pessoais" ocupa um lugar *sui generis*, sendo, ao mesmo tempo, regulação econômica orientada aos negócios e legislação humanista preocupada com a dignidade das pessoas e contenção de disparidades de poder.[23]

1. O DEBATE ESTADUNIDENSE E A CENTRALIDADE DOS FAIR INFORMATION PRACTICES PRINCIPLES

A década de 1960 foi marcada por grandes debates sobre o "direito à privacidade" nos Estados Unidos da América, em um contexto de crescentes poderes governamentais, de uma prática constante de *wire-tapping* e de suspeitas de vigilantismo e coleta de informações privadas derivada do "macartismo" da década de 1950 (a intensificação de elaboração de bancos de dados de "grupos subversivos" e de monitoramento de comunistas nos EUA).[24] Alan

23 Nesse sentido, ver RODOTÀ, Stefano. **Vivere la democrazia**. Gius. Laterza & Figli Spa, 2019.

24 WESTIN, Alan F. The Wire-Tapping Problem: An Analysis and a Legislative Proposal. **Columbia Law Review**, v. 52, n. 2, p. 165-208, 1952. KING, Donald B.; BATT, Marwin ➔

Westin foi um dos juristas a capitanear essa discussão em uma série de publicações no final da década de 1950.

Paralelamente, o direito estadunidense foi redefinido no campo do direito privado no começo da década de 1960, em especial pela elaboração doutrinária do "direito à privacidade" como proteção contra quatro tipos distintos de delitos (*torts*) pelo Prof. William Prosser, desencadeando um sistema de responsabilização civil.[25] No esquema arquitetado por Prosser em 1960, a violação da privacidade - até então entendida como "direito de ser deixado a sós" - poderia ser entendida em quatro diferentes tipos de torts, diferenciados a partir de ações e interesses distintos: (i) *intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;* (ii) *public disclosure of embarassing private facts about the plaintiff;* (iii) *publicity which places the plaintiff in a false light in the public eye;* (iv) *appropriation, for the defendant's advantage, of the plaintiff's name or likeness*. Essa formulação, apesar de ter se tornado imediatamente influente nas Cortes e a doutrina dominante no direito privado, "ossificou"[26] o debate sobre privacidade em uma matriz de direitos individuais e se mostrou pouco responsiva a um debate mais complexo sobre "fluxos adequados de dados" e proteção de dados pessoais.

➔ A. Wire Tapping and Electronic Surveillance: A Neglected Constitutional Consideration. **Dick. L. Rev**., v. 66, p. 17, 1961.

25 William Prosser apresentou essa sistematização em um artigo muito citado no direito estadunidense, intitulado "Privacy", publicado em 1960 na California Law Review.

26 RICHARDS, Neil'; SOLOVE, Daniel. Prosser's Privacy Law: a mixed legacy, **California Law Review**, v. 98, 2010, p. 1888-1928 ("the privacy torts have struggled to address the collection, use, and dissemination of personal information in computer databases. (...) Several privacy torts - public disclosure, intrusion, and false light - require that the privacy invasion be "highly offensive to a reasonable person". Much of the information that is gathered, used, and disseminated by businesses is done in bits and pieces. (...) The tort of appropriation has also failed to address the collection, use, and dissemination of personal data").

1.1. A transformação do direito estatutário e a construção de princípios de justiça

Como sustentam Daniel Solove e Paul Schwartz, foi no campo do direito regulatório de nível federal (*federal statutory law*) que o desenvolvimento do direito à privacidade foi mais robusto.[27] Seguindo a tradição estadunidense de imposição de limites à atuação governamental, surgiu na década de 1960 um vigoroso debate sobre a determinação de direitos claros que pudessem superar a teoria de "invasão da propriedade", definindo os limites de atuação do governo na execução de políticas públicas.[28] Esse debate ganhou novas dimensões com trabalhos como *Privacy and Freedom* (1967), de Alan Westin, que se dedicou à compreensão da privacidade como *capacidade dos cidadãos de controlar os fluxos de dados gerados*.[29] Como sustenta Priscilla Regan, em 1965 "um novo problema foi colocado na agenda do Congresso e de subcomitês da Câmara [*House*] e do Senado [*Senate*]. O problema foi definido como a invasão da privacidade pelos computadores e evocava imagens de 1984 [livro de George Orwell], do Homem Computadorizado, e de uma sociedade do dossiê"[30]. Durante trinta dias foram realizadas audiências públicas sobre o tema. Essa discussão na esfera pública motivou a elaboração de um influente relatório pelo *United States Department of Health, Education and Welfare* (HEW) em 1972, durante a gestão Richard Nixon, que atacou o problema da privacidade e da coleta abusiva de dados

27 SOLOVE, Daniel; SCHWARTZ, Paul. **Information Privacy Law**. Sixth edition. New York: Wolters Kluwer, 2018, p. 36.

28 LONG, Edward V. **The Right to Privacy: The Case Against the Government.** Louis ULJ, v. 10, p. 1, 1965.

29 WESTIN, Alan F.; RUEBHAUSEN, Oscar M. **Privacy and Freedom**. New York: Atheneum, 1967.

30 REGAN, Priscilla. **Legislating Privacy: technology, social values and public policy**. The University of North Carolina Press, 1995, p. 82.

pessoais por meio da proposição de uma base principiológica (*Code of Fair Information Practices*) estruturada em cinco pilares:

a) Não deve haver sistemas de registro de dados pessoais cuja própria existência seja secreta;
b) Deve haver uma maneira de uma pessoa descobrir quais informações sobre ela estão em registro e como essa informação é usada;
c) Deve haver uma maneira de uma pessoa impedir que informações sobre ela, obtidas para um propósito específico, sejam usadas ou disponibilizadas para outros fins sem o consentimento da pessoa;
d) Deve haver uma maneira de uma pessoa corrigir ou ajustar um registro de informações identificáveis sobre a pessoa;
e) Qualquer organização que crie, mantenha, utilize, ou divulgue registros de dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções para evitar usos indevidos dos dados;

Esses cinco pilares formaram o eixo central dos *Fair Information Practices Principles* (FIPPs), que, na opinião de acadêmicos renomados como Marc Rotenberg (fundador da *Electronic Privacy Information Center*), se tornaram a principal moldura jurídica para estruturação das leis de proteção de dados pessoais nos EUA.[31] Até hoje, os princípios da FIPP são utilizados pela Federal Trade Commission para avaliar casos de práticas abusivas que precisam ser repreendidas pela autoridade.[32]

31 ROTENBERG, Marc. Fair information practices and the architecture of privacy (What Larry doesn't get). **Stanford Technology Law Review**, v. 44, 2001.

32 "Fair Information Practices became the dominant U.S. approach to information-privacy protection for the next three decades". WESTIN, Alan. Social and Political Dimensions of Privacy, **Journal of Social Issues**, v. 59, 2003, p. 436.

1.2. Transformações regulatórias: Fair Credit Reporting Act e Privacy Act

Paralelamente ao desenvolvimento das FIPPs, três fenômenos concretos ocorreram na década de 1970 e formataram grande parte da matriz jurídica de regulação da proteção de dados pessoais nos EUA.[33] Entendê-los é fundamental para uma compreensão clara da relação entre direito e economia política dos dados nos Estados Unidos.

O primeiro deles é o intenso debate sobre "consumer reports" (fichas de consumidores) gerado pela enorme indústria de avaliação de risco no setor de crédito, capitaneada por gigantes como Equifax. Em 1969, Democratas propuseram uma série de audiências públicas sobre o problema discriminatório desses mecanismos de avaliação de risco e a completa opacidade, por parte do cidadão, da possibilidade de compreensão de como as fórmulas de *credit scoring* funcionam e quais informações são utilizadas para compor essas notas. Impulsionado pelo ativismo de Ralph Nader e outras grandes figuras públicas do movimento consumerista,[34] o Congresso aprovou em 1970 uma lei federal chamada *Fair Credit Reporting Act* (FCRA), com um conjunto de direitos básicos assegurados aos cidadãos estadunidenses (direito de informação sobre a existência de um credit report, direito de saber o que um birô de crédito sabe sobre você, direito de obtenção gratuita da pontuação de crédito, direito de contestar informações incompletas e imprecisas, direito de corrigir e deletar informações não verificadas e incompletas, direito de se opor à utilização de informações com

33 Essa análise segue de perto as reflexões de Alan Westin. WESTIN, Alan. Social and Political Dimensions of Privacy, **Journal of Social Issues**, v. 59, 2003, p. 431-453. Disponível em: https://spssi.onlinelibrary.wiley.com/doi/full/10.1111/1540-4560.00072

34 WALLER, Spencer. Consumer protection in the United States: an overview. **European Journal of Consumer Law**, 2011 (destacando o papel de Ralph Nader na publicação de Unsafe At Any Speed, na criação de grupos de voluntários de investigação da regulação nos EUA e na fundação da ONG Public Citizen em 1971).

mais de 7 anos, direito de consentir para que essas informações sejam transmitidas a empregadores)[35]. Na época, a legislação foi celebrada por Sheldon Feldman, diretor assistente de legislação da Federal Trade Commission, como um importante avanço diante dos inúmeros casos de práticas abusivas denunciados em audiências públicas.[36] O FCRA também mudou as regras de responsabilização civil, gerando incentivos econômicos aos birôs de crédito.[37]

O segundo fato relevante foi a aprovação do *Privacy Act* de 1974,[38] na esteira do "escândalo de Watergate", que custou a renúncia de Richard Nixon e expôs ao grande público um aparato de escutas ilegais e coleta de dados - colocado em prática para grampear a Convenção Nacional dos Democratas - contestado internamente pelo próprio *Federal Bureau of Investigation* (FBI).[39] Como sustenta Alan Westin, "em termos políticos, o final dos anos 1960 e 1970 viu a maioria da mudança da opinião pública americana da confiança geral nas instituições para a desconfiança dramática. Os excessos do FBI e da CIA, o episódio de Watergate e outras intrusões da Administração Nixon forneceram exemplos concretos de abuso de poder por parte do governo que tornou politicamente possível a promulgação da Lei de Privacidade federal de 1974"[40].

35 Para um sumário preparado pela Federal Trade Commission, resumindo a FCRA, ver: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

36 FELDMAN, Sheldon. The Fair Credit Reporting Act-From the Regulators Vantage Point. **Santa Clara Lawyer**, v. 14, p. 459, 1973.

37 ULLMAN, Charles M. Liability of Credit Bureaus after the Fair Credit Reporting Act: the need for further reform. **Vill. L. Rev.**, v. 17, p. 44, 1972.

38 "The Privacy Act of 1974, 5 U.S.C. § 552a (2012), which has been in effect since September 27, 1975, can generally be characterized as an omnibus 'code of fair information practices' that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies". Ver https://www.justice.gov/opcl/introduction

39 Sobre o escândalo Watergate e suas repercussões para o direito à privacidade, ver SOBEL, Lester A. (Ed.). **War on Privacy**. New York: Facts on File, 1976.

40 WESTIN, Alan. Social and Political Dimensions of Privacy, **Journal of Social Issues**, v. 59, 2003, p. 437.

1.3. O fortalecimento dos FIPPs na Federal Trade Commission

Por fim, o terceiro elemento concreto foi a designação, por meio do *Privacy Act* de 1974, do "U.S. Privacy Protection Study Commission", que se debruçou à questão da aplicação do *Fair Information Practice Principles* ao setor privado.[41] Esse grupo de trabalho, liderado por David Linowes (1917-2007), trabalhou por três anos e publicou, em 1977, o relatório *Personal Privacy in an Information Society*. No relatório, a Comissão conclui por uma abordagem de "reforma sistêmica", com a devida aplicação dos FIPPs por meio da Federal Trade Commission e a expansão de leis federais para setores regulados específicos (saúde, educação, telecomunicações), buscando um balanço capaz de fomentar o empreendedorismo e as proteções dos direitos dos cidadãos com relação aos seus dados:

> "As conclusões da Comissão revelam claramente um enorme desequilíbrio na relação de manutenção de registros entre um indivíduo e uma organização, e suas recomendações de política visam fortalecer a capacidade do indivíduo de participar desse relacionamento. Isso pode ser feito de três maneiras: proibindo ou restringindo práticas de coleta de informações injustificadamente intrusivas; concedendo os direitos básicos individuais, como o direito de ver, copiar e corrigir registros sobre si mesmo, juntamente com obrigações ou organizações para incorporar proteções à privacidade pessoal em suas operações rotineiras de manutenção de registros; e dando o controle individual sobre a divulgação de registros sobre ele. Ao explorar maneiras de implementar suas recomendações de política, a Comissão foi guiada por três princípios: (1) que os incentivos para a reforma sistêmica devem ser criados; (2) que os mecanismos existentes de

41 Ver https://www.justice.gov/opcl/role-privacy-protection-study-commission

regulação e execução devem ser usados na medida do possível; e (3) que custos desnecessários devem ser evitados"[42].

Como sustenta Alan Westin, esse influente relatório de 1977 incentivou "iniciativas pelo setor privado" e uma abordagem caso-a-caso de repressão, conduzida pela Federal Trade Commission, ao invés de uma Lei Geral de Proteção de Dados Pessoais aos moldes de países como França e Suécia. O relatório de pesquisa *Dimensions of Privacy*, publicado em 1978, demonstrou que, para a maioria dos cidadãos nos EUA, era mais desejável a existência de leis setoriais específicas, protegendo dados mais sensíveis como aqueles coletados em hospitais, clínicas de saúde e farmácias.

Como sustentam acadêmicos como Daniel Solove, Woodrow Hartzog e Chris Hoofnagle, as escolhas políticas de década de 1970 levaram os EUA para uma direção oposta da União Europeia. Ao invés de um modelo de "leis gerais" e Autoridades Nacionais de Proteção de Dados Pessoais, os FIPPs foram internalizados na cultura decisória da Federal Trade Commission, que acabou por criar, ao longo de décadas de atuação, uma espécie de "common law" da privacidade.[43] Esse desenvolvimento jurídico, que apresenta uma história notável e construída casuisticamente,[44] garantiu a FTC um "escopo de autoridade que é essencial ao regime de proteção de dados dos EUA e que deveria ser amplamente abraçado para responder às violações de privacidade que não são atendidas pelo direito contratual e pelo regime de responsabilidade civil"[45].

42 **Personal Privacy in an Information Society**: The Report of the Privacy Protection Study Commission transmitted to President Jimmy Carter on July 12, 1977. Disponível em: https://epic.org/privacy/ppsc1977report/c1.htm

43 SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the new common law of privacy. **Columbia Law Review**, v. 114, p. 583, 2014.

44 Para uma análise completa da história da FTC e o desenvolvimento casuístico em proteção de dados pessoais, ver HOOFNAGLE, Chris Jay. **Federal Trade Commission Privacy Law and Policy**. Cambridge University Press, 2016.

45 HARTZOG, Woodrow; SOLOVE, Daniel J. The Scope and Potential of FTC Data Protection. **George Washington Law Review**, v. 83, p. 2230, 2014.

Esse desenvolvimento histórico da "regulação da privacidade" levou os EUA a um sistema baseado em três pilares. Primeiro, a proliferação de normas setoriais de privacidade, como no campo da educação, da saúde, do crédito, das telecomunicações, etc. Acrescente-se a esse cenário um modelo federativo no qual os Estados (Califórnia, Texas, Oregon, etc) podem também legislar sobre assuntos de privacidade, fazendo com que os EUA tenham atualmente mais de 2.000 leis sobre o assunto. Segundo, um sistema de proteção dos consumidores baseado na atuação da Federal Trade Commission e nos conceitos de "deceptive act" e "unfairness"[46], ou seja, um sistema de análise caso-a-caso no qual a FTC avalia se há lesões aos consumidores ou práticas abusivas, como no caso em que a fabricante de "televisores inteligentes" Vizio foi condenada ao pagamento de mais de 2 milhões de dólares de multa pela coleta de informações de visualizações de canais de mais de 11 milhões de consumidores sem consentimento.[47] Terceiro, uma abordagem consumerista fortalecida na década de 1990 na qual o elemento central é o "notice-and-consent", ou seja, a obrigação de empresas explicitarem quais são as práticas de coletas de dados colocadas em prática e a verificação do consentimento dos consumidores pelas vias contratuais.[48] Apesar das inúmeras críticas - muitas delas internas, produzidas pela própria Federal Trade Commission, sobre a necessidade de um novo Consumer Privacy Protection Principles[49] -, o sistema consumerista e de regulação via FTC ainda se mantém como dominante nos EUA.

46 HOOFNAGLE, Chris Jay. **Federal Trade Commission Privacy Law and Policy**. Cambridge University Press, 2016.

47 https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

48 A cristalização desse modo de pensamento, fundado na crença na capacidade de escolha dos consumidores e nas práticas de autorregulação, está no relatório Privacy Online: a report to the Congress, publicado em 1998: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

49 Ver https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf

2. DOS PRINCÍPIOS ÀS LEIS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS: A ABORDAGEM EUROPEIA

Em 1975, em relatório publicado pela Organização para Cooperação e Desenvolvimento Econômico, observou-se que as diferentes experiências de Suécia, França, Alemanha e outros países integrantes da OCDE[50] na criação de leis de privacidade e proteção de dados pessoais apresentava "similaridade impressionante apesar de ações independentes"[51]. Colin Bennett, em estudo clássico da ciência política sobre "convergência da regulação da privacidade", demonstrou que a experiência europeia foi construída a partir de uma filosofia comum e uma atenção a princípios fundamentais de justiça, muitas vezes chamados de "*Fair Information Practices Principles*" em razão da atuação do governo dos EUA.[52]

Concebido à nível local pelo Departamento da Saúde e Bem-Estar do governo estadunidense,[53] os princípios de práticas informacionais justas são a base de todas as normas transnacionais e nacionais de proteção de dados pessoais.[54] Ao ampliar de cinco[55]

50 Sobre os membros da OCDE e sua história, ver http://www.oecd.org/about/history/

51 OECD, Developments in Data Protection and Privacy by OECD Countries, Survey from OECD'S Computer Utilization Group. Paris: OECD, 1975, p. 2.

52 Para o estudo de Bennett, ver capítulos 3 e 4. BENNETT, Colin. **Regulating Privacy: data protection and public policy in Europe and the United States**. Cornell University Press, 1992, p. 95-155.

53 Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

54 GELLMAN, Robert, **Fair Information Practices: A Basic History**, Rochester, NY: Social Science Research Network, 2017.

55 1. There must be no personal datarecord keeping systems whose very existence is secret. 2.There must be a way for an individual to find out what information about him (or her) is in a record and how it is used. 3. There must be a way for an individual to prevent information about him (or her) that was obtained for one purpose from being used or made available for other purposes without his (or her) consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him (or her). 5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must ➔

para oito princípios,[56] a OCDE acabou por transformá-los na espinha dorsal da grande gama dos regimes jurídicos de proteção de dados ao redor do mundo. O objetivo era justamente estabelecer pilares pelos quais diferentes leis nacionais estariam neles escorados para evitar regras conflituosas, as quais poderiam impor barreiras ao livre fluxo informacional. Em poucas palavras, a moldura normativa de proteção de dados à nível global deveria ser responsiva à demanda de uma economia global que já se apresentava dependente da troca de dados.[57] Esse foi o projeto regulatório pensando pelos europeus, combinando ambições de economia política (construção de um espaço de livre comércio dentro do território europeu) com uma visão forte de direitos fundamentais, teoria que ganhou força na filosofia política do pós-guerra.[58]

2.1. A harmonização jurídica via Convenção Internacional 108 e Parlamento Europeu

O trabalho da OCDE durante a década de 1970 mobilizou uma forte atuação política em sentido de convergência. Após um trabalho de cooperação em nível comunitário conduzido pelo *Committee on*

→ assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

56 Os oito princípios são: a) Limitação de Coleta (Collection Limitation Principle); b) Qualidade dos dados (Data Quality Principle); c) Especificação dos propósitos (Purpose Specification Principle); d) Limitação do uso (Use Limitation Principle); e) Padrões mecanismos de segurança (Security Safeguards Principle); f) Abertura (Openness Principle); g) Participação individual (Individual Participation Principle); h) Responsabilidade (Accountability Principle).

57 BIONI, Bruno Ricardo, A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço, *in*: **Direitos e novas tecnologias: XXIII Encontro Nacional do Conpedi**, Florianópolis: Conpedi, 2014, v. 1, p. 59–82.

58 KERSON, D. L. A. The European Convention for the protection of human rights and fundamental freedoms. **California Law Review**, v. 49, p. 172, 1961. PESCATORE, Pierre. Fundamental rights and freedoms in the system of the European Communities. **American Journal of Comparative Law**, v. 18, p. 343, 1970.

Legal Data Processing,[59] o Conselho da Europa abriu para adesões a Convenção Internacional 108 de proteção de dados pessoais, sendo este o primeiro instrumento normativo transnacional vinculante de proteção de dados pessoais. A exemplo das diretrizes da OCDE, as FIPPs orientam toda a sua estrutura normativa,[60] colocando-se, também, como um mecanismo de uniformização de normas de proteção de dados para não travar o livre fluxo de dados.[61] Nesse sentido, como regra, há inclusive a proibição de que países-membros da convenção imponham restrições uns aos outros, sob o argumento puro e abstrato da proteção da privacidade, no que diz respeito à transferência internacional de dados.[62]

No meio da década de 90, a União Europeia, também se valendo das FIPPs,[63] editou a Diretiva 95/46/EC. Um dos seus principais objetivos era também assegurar um grau mínimo de convergência regulatória, o qual estimularia a integração econômica entre seus países-membros na linha do que previu o tratado de criação

59 "The OECD established its first expert group, the Data Bank Panel, as early as 1969. In 1978, a new Group of Experts on Transborder Data Barriers and Privacy Protection was established and instructed to draft a set of recommendations. The resulting "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (Guidelines) were adopted by the OECD in 1980". BING, Jon. The Council of Europe Convention and OECD Guidelines on Data Protection. **Michigan Legal Studies**, v. 5, p. 271, 1984.

60 GELLMAN, Robert, **Fair Information Practices: A Basic History**, Rochester, NY: Social Science Research Network, 2017.

61 O termo livro fluxo está presente inclusive nas "considerandas" da Convenção: "Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".

62 Trata-se do artigo 12 do Convenção cuja proibição foi mantida na versão revisada de 2018: "A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation."

63 GONZÁLEZ FUSTER, Gloria, **The emergence of personal data protection as a fundamental right of the EU**, Cham: Springer, 2014.

do bloco econômico europeu.[64] Sendo uma *Diretiva*, e não um *Regulamento*, seu conteúdo foi pensado como uma espécie de "sugestão de adaptação" aos Estados-membros da União Europeia, permitindo, ainda, um certo grau de manobra e de variação jurídica entre países como Itália, Espanha, Alemanha e Reino Unido. Os "considerandos" da Diretiva deixam claro essa possibilidade de criações jurídicas nacionais diferenciadas e uma forte preocupação com a harmonização em nível comunitário:

> "(8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objectivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam actualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objectivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma acção comunitária com vista à aproximação das legislações;
> (9) Considerando que, devido à protecção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estadas-membros uma margem de manobra que, no contexto da aplicação da

64 Esse é o conteúdo da primeira consideranda da diretiva 95/46 que cita os tratados de criação do bloco econômico europeu, fazendo alusão à "eliminar barreiras que dividem a Europa" para "assegurar progresso econômico e social".

> directiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a protecção actualmente assegurada na respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da directiva, o que poderá reflectir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade"[65];

A Diretiva de outubro de 1995 da União Europeia estabeleceu um regramento básico, aprofundando o processo de "policy convergence" nos termos de Colin Bennett. Conforme notado por Rita Blum, a Diretiva enfatizou "a importância de cada Estado-membro ter a sua própria legislação para tratar os dados pessoais a qual pode ser concretizada por uma lei geral relativa à proteção das pessoas e por leis setoriais como, por exemplo, as relativa aos institutos de estatística"[66]. A legislação também definiu um conceito unificado de *tratamento de dados* ("qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a coleta, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição"), definindo que o tratamento só pode ocorrer, dentro de um Estado-membro, se for:

a) Objeto de um tratamento leal e lícito;

65 Ver a Diretiva em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN

66 BLUM, Rita Peixoto. **O direito à privacidade e à proteção de dados pessoais**. São Paulo: Almedina, 2018, p. 115.

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades (sendo que o tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas);
c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
d) Exatos e, se necessário, atualizados (sendo que devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou rectificados);
e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente (sendo que os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos).

Nos anos 2000, a carta de direitos fundamentais da União Europeia destacou o direito à proteção de dados pessoais do direito à privacidade.[67] A autonomia desse novo direito fundamental é o ponto de chegada de teóricos europeus, dos quais se destaca o jurista e político Stefano Rodotà, que por trás dele enxergavam um conjunto de direitos que configurariam a nova cidadania do milênio e, em última análise, o cerne das próprias relações sociais.[68]

67 Artigo 8° da Carta de Direitos Humanos Fundamentais.

68 RODOTÀ, Stefano, **Il diritto di avere diritti**, Roma; Bari: Laterza, 2013. p. 321.

2.2. O esforço político para construção do Regulamento Geral de Proteção de Dados Pessoais

Como se percebe, o modelo jurídico construído na União Europeia é marcado por complexidades e um conjunto de fatores que se sobrepõem ao longo do tempo. Primeiro, houve um processo de aprendizado institucional e regulatório por parte da OCDE no final da década de 1970, mobilizando ativamente uma estratégia regional por meio da Convenção 108 sobre fluxos internacionais de dados firmada em 1981. Segundo, houve um processo de harmonização de leis nacionais fortes, durante as décadas de 1980 e 1990, e de teorização da proteção de dados pessoais como direito fundamental, ou seja, como um "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[69]. Terceiro, houve um *processo de diferenciação* do direito à privacidade ao direito à proteção de dados pessoais, fenômeno que não ocorreu com clareza nos EUA e que se cristalizou na elaboração da Carta dos Direitos Fundamentais da União Europeia.[70] Como explica Stefano Rodotà, que por muitos anos foi a Autoridade Garante de proteção de dados pessoais na Itália, "no direito ao respeito à vida privada e familiar se manifesta sobretudo o momento individualista, nele o poder se exaure substancialmente pela exclusão de interferências de terceiros: a tutela é estática, negativa. A proteção de dados, ao invés, fixa regras sobre as modalidades de tratamento dos dados, concretiza-se em poderes de intervenção: a tutela é dinâmica,

69 RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 15.

70 RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 175.

segue os dados em sua circulação.[71] Os poderes de controle e de intervenção, além disso, não são atribuídos somente aos interessados diretos, mas são confiados também a uma autoridade independente"[72]. Essa teorização que motivou experiências como o Código Italiano em Matéria de Tratamento de Dados Pessoais,[73] aprovado em junho de 2003, e uma coordenação estratégica, por parte do Parlamento Europeu, para iniciar um trabalho de revisão da Diretiva de 1995 e construção de uma nova norma jurídica, aplicável a toda a União Europeia, sobre proteção de dados pessoais.

O ano de 2010 é considerado chave para compreensão das origens da *General Data Protection Regulation* (GDPR) e suas negociações políticas em Bruxelas. Uma das origens do Regulamento é o documento "*A comprehensive approach on personal data protection in EU*" publicado por um grupo de experts em proteção de dados pessoais reunidos no European Data Protection Supervisory (EDPS), entidade independente fundada em janeiro de 2004 para supervisão das atividades de proteção de dados pessoais na União Europeia e inicialmente presidida por Peter Johan Hustinx.[74] Nesse documento, constatou-se que "os desafios exigem que a União Europeia desenvolva uma abordagem abrangente e coerente, garantindo que o direito fundamental à proteção de dados para os indivíduos seja plenamente respeitado dentro e fora da UE"[75].

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

72 RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 198-199.

73 DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 16, p. 117, 2003.

74 Hustinx foi membro da Comissão Real de Proteção de Dados Pessoais da Holanda entre 1972 e 1976, membro do Conselho da Europa e presidente do Comitê de Dados Pessoais entre 1985 e 1988, e Presidente da Autoridade de Proteção de Dados Pessoais da Holanda entre 1991 e 2003. Em 2004, foi nomeado Presidente do European Data Protection Supervisor.

75 EUROPEAN COMMISSION, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, **"A comprehensive approach on personal data protection in the European →**

A partir do diagnóstico de que a União Europeia possui uma "forte dimensão de mercado interno", o relatório apontou para a necessidade de simplificação e harmonização das diferentes leis nacionais em torno de um Regulamento, com eficácia vinculante aos Estados-membro. Diferentemente da Diretiva, o Regulamento é uma técnica legislativa que têm eficácia direta, sem a necessidade nacionalização pelos países-membros, e mais prescritiva deixando pouca margem para variação jurídica. Como conclusão, a EDPS afirmou que "na sequência de uma avaliação de impacto e tendo em conta a Carta dos Direitos Fundamentais da UE, a Comissão irá propor legislação em 2011 destinada a rever o quadro jurídico relativo à proteção de dados, com o objetivo de reforçar a posição da UE na proteção dos dados pessoais do indivíduo no contexto de todas as políticas da UE"[76].

Dito e feito. Em 2012, a partir de uma definição de estratégia consolidada e por meio da liderança da Comissária de Justiça, Direitos Fundamentais e Cidadania Viviane Reding,[77] a Comissão Europeia anunciou uma ampla reforma da legislação de proteção de dados pessoais, o embrião da *General Data Protection Regulation*.[78] De acordo com o anúncio feito à comunidade internacional em janeiro de 2012,[79] a reforma consistiria nos seguintes elementos:

→ **Union"**, Brussels, 2010, p. 4. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

76 EUROPEAN COMMISSION, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, **"A comprehensive approach on personal data protection in the European Union"**, Brussels, 2010, p. 18.

77 Viviane Reding é uma política de Luxemburgo, doutora em ciências sociais pela Universidade de Sorbonne e membra do Parlamento Europeu. Entre 2004 e 2010 foi Comissária para Educação e Cultura. Entre 2010 e 2014 foi Comissária de Justiça, Direitos Fundamentais e Cidadania.

78 O anúncio de Viviane Reding, feito em 25 de janeiro de 2012, está disponível online: https://www.youtube.com/watch?v=9binnTteKeA

79 Em artigos acadêmicos, Reding apresentou as linhas gerais da GDPR. Ver REDING, Viviane. The upcoming data protection reform for the European Union. **International Data →**

a) Um conjunto único de regras sobre proteção de dados, válido em toda a UE. Requisitos administrativos desnecessários, como requisitos de notificação para empresas, serão removidos (com economia de cerca de 2,3 bilhões de euros por ano);
b) Em vez da obrigação de todas as empresas de notificar todas as atividades de proteção de dados aos supervisores de proteção de dados - um requisito que resultou em burocracia desnecessária e custa às empresas € 130 milhões por ano, o Regulamento prevê maior responsabilidade e prestação de contas para aqueles que processam dados pessoais;
c) Empresas e organizações devem notificar a autoridade supervisora nacional sobre violações graves de dados o mais rápido possível (se possível dentro de 24 horas);
d) As organizações só terão de lidar com uma única autoridade nacional de proteção de dados no país da UE onde têm o seu estabelecimento principal. Da mesma forma, as pessoas podem se referir à autoridade de proteção de dados em seu país, mesmo quando seus dados são processados por uma empresa sediada fora da UE. Sempre que o consentimento é necessário para que os dados sejam processados, fica claro que ele deve ser dado explicitamente, em vez de ser assumido;
e) As pessoas terão acesso mais fácil aos seus próprios dados e poderão transferir dados pessoais de um provedor de serviços para outro com mais facilidade (direito à portabilidade de dados), aumentando a concorrência entre os serviços;
f) Um "direito de ser esquecido" ajudará as pessoas a gerenciar melhor os riscos de proteção de dados on-line: as pessoas poderão excluir seus dados se não houver motivos legítimos para retê-los;

→ **Privacy Law**, v. 1, n. 1, p. 3-5, 2010. REDING, Viviane. The European data protection framework for the twenty-first century. **International Data Privacy Law**, v. 2, n. 3, p. 119-129, 2012.

g) As regras da UE devem aplicar-se caso os dados pessoais sejam tratados no estrangeiro por empresas que operam no mercado da UE e ofereçam os seus serviços aos cidadãos da UE;
h) As autoridades nacionais independentes de proteção de dados serão reforçadas para que possam aplicar melhor as regras da UE em casa. Eles terão poderes para multar as empresas que violarem as regras de proteção de dados da UE. Isso pode levar a multas de até € 1 milhão ou até 2% do faturamento anual global de uma empresa.[80]
i) criação do European Data Protection Board/EDPB, o qual substitui o antigo grupo de trabalho artigo 29. Com isso, criou-se, um arranjo institucional com o objetivo de garantir "consistência" no plano de aplicação e fiscalização da nova lei de proteção de dados Pessoais. Cabe, por exemplo, ao EDPB[81] emitir opinião quando existir conflito de visões entre Autoridades Nacionais de Proteção de Dados Pessoais, sendo vinculativa a sua respectiva decisão.[82] Atacou-se em dois planos, normativo e institucional, a uniformização da regulação acerca da proteção de dados pessoais.

O trabalho político arquitetado pelos membros do Parlamento Europeu, que enfrentou severos lobbies contrários por parte das grandes empresas de tecnologia (detalhados no filme Democracy[83] dirigido por David Bernet), foi apoiado pela Working Party 29 (grupo de Autoridades de Proteção de Dados Pessoais) em notas

80 EUROPEAN COMMISSION, **A comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses**, EC: Brussels, 2012. Disponível em: http://europa.eu/rapid/press-release_IP-12-46_en.htm

81 https://edpb.europa.eu/about-edpb/about-edpb_en

82 É o chamado mecanismo de resolução de disputa previsto no artigo 65 da GDPR.

83 POWLES, Julia. Democracy: the film that gets behind the scenes of the European privacy debate, **The Guardian**, 14/11/2015 (detalhando os bastidores da negociação e aprovação do GDPR). Disponível em: https://www.theguardian.com/technology/2015/nov/14/democracy-film-european-data-protection-privacy-debate

técnicas publicadas em 2012. Após um período de longas negociações no Parlamento Europeu, o Comitê de Liberdades Civis, Justiça e Assuntos Domésticos, liderado pelo jovem Jan-Philipp Albrecht (Partido Verde da Alemanha) e por Dimitrios Droutsas (Partido Socialista da Grécia), aprovou um texto em outubro de 2013,[84] impulsionados pelos efeitos políticos tectônicos do caso Edward Snowden. Em março de 2014, o Parlamento Europeu votou por esmagadora maioria (621 votos a favor e 10 votos contrários) em favor da proposta de Regulamento relatada por Albrecht e Droutsas. Após a histórica votação do Regulamento, o Parlamento Europeu publicou *press release* com a seguinte declaração de Viviane Reding:

> "A mensagem que o Parlamento Europeu está enviando é inequívoca: esta reforma é uma necessidade, e agora é irreversível. Os parlamentares eleitos diretamente pela Europa ouviram os cidadãos europeus e as empresas europeias e, com esta votação, deixaram claro que precisamos de uma lei europeia de proteção de dados uniforme e forte, que facilite a vida das empresas e reforce a proteção dos nossos cidadãos. A proteção de dados é feita na Europa. Regras rigorosas de proteção de dados devem ser a marca da Europa. Após os escândalos de espionagem de dados dos EUA, a proteção de dados é mais do que nunca uma vantagem competitiva"[85].

Em 2015, o texto recebeu recomendações de mudanças pelo European Data Protection Supervisor (EDPS) - já sob a direção de Giovanni Butarelli[86] -, chegando a um consenso político em

84 Ver http://europa.eu/rapid/press-release_MEMO-14-60_en.htm

85 EUROPEAN COMMISSION, **Progress on EU data protection reform now irreversible following European Parliament vote**, EC: Strasbourg, 2014. Disponível em: http://europa.eu/rapid/press-release_MEMO-14-186_pt.htm

86 Butarelli é um jurista italiano, formado na Universidade La Sapienza (Roma), com experiência de mais de 10 anos na Secretaria Executiva da Autoridade de Proteção de →

dezembro deste ano. Em fevereiro de 2016, a Working Party 29 lançou um "plano de ação" para implementação do novo regulamento e, em 27 de abril de 2016, finalmente ocorreu a aprovação e publicação oficial do Regulamento (EU) 2016/679.[87] Enfim, o projeto capitaneado pelo Parlamento Europeu se tornou uma das normas jurídicas mais importantes do século XXI - ao menos no nível político e discursivo[88] -, projetada para ter efeito vinculante a partir de 25 de maio de 2018.

2.3. Transferências internacionais, o "Mercado Único Europeu" e a co-regulação

Em 2015, o fórum para Cooperação Econômica Ásia-Pacífico/APEC também editou um conjunto de diretrizes sobre proteção de dados buscando a criação de padrões normativos "interoperáveis" para desafogar o fluxo transfronteiriço de dados.[89] Diferentemente dos outros instrumentos transnacionais, a APEC já havia estabelecido antes, em 2005, um sistema de certificação para transferência internacional - Regras Transfronteiriças de Privacidade/CBPR[90] Organizações poderiam aderir voluntariamente a tais regras, sendo certificado os seus respectivos programas de conformidade para viabilizar transferência internacional de dados dentre os países fazem parte do programa.[91]

➔ Dados Pessoais da Itália, onde trabalhou com Stefano Rodotà. Em 2015, substituiu Peter Hustinx na Presidência da EPDS.

87 Para uma análise de diferentes elementos do Regulamento, ver MALDONADO, Viviane (ed.), **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: Thomson Reuters, 2018.

88 ALBRECHT, Jan Philipp. How the GDPR will change the world. **European Data Protection Law Review**, v. 2, p. 287, 2016.

89 Disponível em: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

90 Disponível em: <http://cbprs.org/>

91 Atualmente 08 (oito) países fazem parte do programa: Estados Unidos, México, Japão, Canadá, Singapura, Coreia, Austrália e China

Com exceção da APEC, todos os organismos transnacionais citados revisaram as suas normas de proteção de dados pessoais no curto período de 06 (anos). Para além de uma investigação se há uma nova rodada de convergência regulatória que agora não tende a ser somente calibrada pelas FIPPs, é importante notar que todos os instrumentos internacionais e regionais foram modernizados tendo como um dos seus principais gargalos a expansão dos mecanismos de transferência internacional.

Nesse sentido, o novo Regulamento Europeu de Proteção de Dados Pessoais, a Convenção Internacional de Proteção de Dados do Conselho da Europa e o da OCDE passaram a prever ou reforçar a importância de compromissos voluntários por parte das organizações para fins de transferência internacional. Como uma válvula de escape ao sistema de análise se o país destinatário teria um nível equivalente de proteção de dados, selos e códigos de boas condutas passaram a compor um cardápio mais amplo de opções para destravar o livre fluxo de dados. Nota-se, inclusive, um movimento semelhante no cenário brasileiro acerca do alargamento da caixa de ferramentas para fins transferência internacional:

OCDE	CoE	UE	Brasil
Ao destacar a importância dos programas corporativos de privacidade,[92] acaba por interligá-los ao movimento da APEC, CBPRs, que respalda a transferência internacional de dados em compromissos voluntários[93] firmados pelas organizações e certificados por terceiros.	Ao prever que a transferência internacional de dados poderá se dar de forma *ad hoc* ou mediante salvaguardas padronizadas através de instrumento vinculante por parte, o novo texto da Convenção abre espaço para que códigos de boas condutas e selos sejam veículos para transferência internacional de dados	Enquanto a diretiva reconhecia apenas expressamente cláusulas contratuais-padrão enquanto um compromisso voluntário para respaldar transferência internacional, o Regulamento previu também códigos de boas condutas e selos[94]	Selos e códigos de boas condutas não constavam na versão do então anteprojeto de lei,[95] tendo sido incorporados somente no desenho final da lei aprovada no Congresso Nacional.[96]

Desde a década de 80, há uma tensão permanente em se arquitetar arranjos normativos à nível regional e transnacional convergentes que não restrinjam o fluxo de informações transfronteiriço.

92 OECD, **The OECD Privacy Framework**, 2013. p. 4.

93 OECD, **The OECD Privacy Framework**, 2013. p. 106.

94 Deve-se comparar o artigo 46 da GDPR ao artigo 26 da Diretiva.

95 Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>

96 Artigo 33 da LGPD.

As últimas gerações[97] de leis de proteção de dados pessoais reforçaram essa tônica ao ampliar os mecanismos pelos quais se pode ativar a transferência internacional de dados, criando ou reforçando válvulas de escape com base em compromissos privados de organizações que dependem desse livre trânsito de dados para suas operações. Os próximos anos nos reservam novos capítulos dessa permanente tensão geopolítica, mas sob um novo roteiro que abre espaço para que organizações privadas assuma cada vez mais protagonismo e sejam mais proativas para circulação transfronteiriço da informação.

A União Europeia, por meio do Regulamento Geral de Proteção de Dados Pessoais, avançou um sistema de co-regulação no qual os controladores possuem enormes funções (obrigações jurídicas, documentação de processos e avaliações de impacto) e o próprio setor privado possui a alternativa se organizar mecanismos de certificação, criação de arranjos contratuais protetivos de direitos (os chamados *binding corporate rules*) e a possibilidade de instrumentos privados voltados à transferência internacional de dados. Ao mesmo, os reguladores europeus não deixaram de lado o "porrete" e a velha abordagem de comando e controle. Em casos de descumprimentos das normas e dos direitos fundamentais assegurados na GDPR, as sanções a serem aplicadas podem ser bastante elevadas, chegando a 50 milhões de Euros a um mesmo grupo econômico. Como declarado por Reding, busca-se assim o fortalecimento de uma economia de dados no continente europeu e a proteção de direitos fundamentais afirmados historicamente.

97 MAYER-SCHONEBERGER, Viktor, Generational development of data protection in europe, *in*: AGRE, Philip; ROTENBERG, Marc (Orgs.), **Technology and privacy: the new landscape**, 1st paperback ed. Cambridge, Mass.: MIT Press, 1998, p. 219–242.

3. TENDÊNCIAS JURÍDICAS E DESAFIOS PARA O DIREITO REGULATÓRIO BRASILEIRO

A emergência explícita de um "capitalismo dadocêntrico" tem friccionado as concepções jurídicas dominantes e o próprio modelo construído na União Europeia, visto por muitos críticos como limitado e excessivamente focado nas obrigações jurídicas dos controladores e operadores em um cenário de difícil fiscalização e de controle efetivo de quebra dos "fluxos adequados de dados"[98]. Apesar das altas aspirações e das críticas, experiências como a GDPR e a LGPD são hoje, como nota Ricardo Abramovay, "a mais ambiciosa tentativa de iniciar a mudança no funcionamento do punhado de empresas que dominam o mundo atual"[99]. Concordamos com Abramovay quando afirma que a defesa "do poder dos cidadãos sobre seus dados pessoais" é "um dos importantes fundamentos da vida pública, tanto na economia, como na política"[100]. Essa disputa de poder deve ser vista, também, da perspectiva da construção do direito regulatório e da relação entre softwares, código e algoritmos com a normatividade.[101]

98 A expressão é da filósofa Helen Nissenbaum. Por questões de escopo, não poderemos detalhar os elementos estruturantes da teoria da privacidade como integridade contextual. Ver NISSENBAUM, Helen. **Privacy in context: Technology, policy, and the integrity of social life**. Stanford University Press, 2009.

99 ABRAMOVAY, Ricardo. Aos dados, cidadãos!, **Revista Quatro Cinco Um**, São Paulo, abril de 2018, p. 6.

100 ABRAMOVAY, Ricardo. Aos dados, cidadãos!, **Revista Quatro Cinco Um**, São Paulo, abril de 2018, p. 6.

101 Essa é uma das teses centrais de Future Politics, do cientista político Jamie Sussking, em livro publicado pela Oxford University Press em 2018. Para uma resenha, ver ABRAMOVAY, Ricardo. Sociedade da vigilância em rede, **Revista Quatro Cinco Um**, *São Paulo*, março de 2019 ("Se, durante o século 20, se tratava de saber em que medida a nossa vida era determinada pelo Estado, pelo mercado e pela sociedade civil, agora a questão (que norteia o livro de Susskind) é outra: em que medida a nossa vida será determinada por poderosos sistemas digitais e em que termos esse poder será exercido. A dominação — a capacidade de fazer os outros agirem segundo a vontade do →

Nesta seção, destacamos três tendências e suas limitações para o Sul Global: (i) a emergência do *privacy by design* e a regulação por arquitetura, (ii) a centralidades dos mecanismos de documentação e responsabilização (*accountability*) e o surgimento de (iii) avaliações de impacto à proteção de dados pessoais, em aproximação com um modelo regulatório construído no campo ambiental.

3.1. Privacy by design e normatividade pela programação

A ideia de que a própria tecnologia é um mecanismo de modulação de comportamentos sociais não é nova. Em 1980, em um artigo publicado na revista do Massachusetts Institute of Technology (MIT), o cientista político Langdon Winner já apontava como a arquitetura urbanística reforçava a segregação racial na sociedade norte-americana através da construção de túneis e pontes inacessíveis pelo transporte público - majoritariamente utilizado por pessoas de etnia negra.[102]

Já na década de 90, Lawrence Lessig[103] verticalizou tal abordagem sociotécnica para o campo da internet, investigando especialmente como *softwares* e *hardwares* poderiam reforçar ou esvaziar os comandos legais. Ao cunhar a expressão clássica e intercambiável o "Código é a Lei", o professor de Harvard joga ainda mais luz sobre o poder normativo dos artefatos tecnológicos em contraste ao codificado em leis.

➔ dominador, na célebre definição de Max Weber — cada vez mais estará em códigos a partir dos quais nossos equipamentos trarão a instrução sobre o que podemos e o que não podemos fazer. No lugar das regulamentações escritas virão as prescrições programadas").

102 WINNER, Langdon, Do Artifacts Have Politics?, **Daedalus**, v. 109, n. 1, p. 17, 1980.

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

Mais recentemente, filósofos da informação, como Mireille Hildebrant[104] e Luciano Floridi[105], avançaram nessa análise ao investigar como há uma infraestrutura informacional, além de uma infraestrutura física, que orquestra a vida das pessoas. Um visão ecológica[106], no sentido mais amplo do termo, que leva em consideração a interdependência entre os seres vivos (cidadãos) e não vivos (artefatos) na reconfiguração do meio-ambiente que condiciona o comportamento dos seus habitantes.[107]

Desde a década de 90,[108] também se nota um movimento que enxerga a tecnologia enquanto um mecanismo de melhoramento da privacidade - tradução literal do termo *privacy enhancing technologies/PETs*. O movimento das PETs é o germe do que hoje é conhecido por *privacy by design*, repetido como um mantra[109] para a codificação da proteção dos dados pessoais já na fase de prototipagem de serviços e produtos.

Passadas algumas décadas, a exemplo da LGPD[110] e da GDPR,[111] nota-se uma abordagem recente em torno da positivação do conceito de privacy by design. Isto é os textos da leis passaram a prever expressamente o dever dos agentes econômicos

104 HILDEBRANDT, Mireille, **Smart technologies and the end(s) of law: novel entanglements of law and technology**, Paperback edition. Cheltenham, UK Northampton, MA, USA: EE Edward Elgar Publishing, 2016.

105 FLORIDI, Luciano, **The 4th revolution: how the infosphere is reshaping human reality**, Oxford: Oxford Univ. Press, 2014.

106 SPINA, Alessandro, **Laudato Si' and Augmented Reality - In Search of an Integral Ecology for the Digital Age**, Rochester, NY: Social Science Research Network, 2017.

107 BIONI, Bruno Ricardo, Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes, *in*: BARBOSA, Alexandre F. (Org.), **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro : TIC governo eletrônico 2017**, São Paulo: Comitê Gestor da Internet, 2018, p. 53–62.

108 GOLDBERG, I.; WAGNER, D.; BREWER, E., Privacy-enhancing technologies for the Internet, *in*: **Proceedings IEEE COMPCON 97. Digest of Papers**, San Jose, CA, USA: IEEE Comput. Soc. Press, 1997, p. 103–109.

109 BYGRAVE, Lee A., **Hardwiring Privacy**, Oslo, Noruega: Faculdade de Direito da Universidade de Oslo, 2017.

110 Art. 46, § 2º, da LGPD.

111 Art. 25(1) da GDPR.

em protegerem a proteção de dados pessoais desde a concepção de seus produtos e serviços.[112] Trata-se uma meta ambiciosa que aposta na colaboração de quem está na linha de produção[113] em gerenciar os riscos[114] da sua própria atividade econômica. É uma nova moldura jurídico-teórica[115] que vai muito além da mera positivação em si de *privacy by design*.

Há uma agenda ainda a ser explorada, por acadêmicos e reguladores, que investigue quais são os gargalos para a materialização de um conceito formulado teoricamente na década de 90, mas que apenas, recentemente, foi previsto em leis. Dito de outra forma, quais são os riscos e as oportunidades em virtude da codificação (legal) de *privacy by design*, sobretudo as limitações que são ínsitas à formalização legal de um conceito até então tão evasivo.

No Brasil e na Índia, por outro lado, a ideia de privacy by design ainda é um projeto em construção. O ponto de partida, no que toca ao Brasil, é a Lei Geral de Proteção de Dados Pessoais, que prevê uma dimensão principiológica de precaução. O art. 6º estabelece que, dentre os princípios da legislação, está a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Apesar de não haver uma menção explícita à "privacidade por desenho" (ou *por default*), o capítulo que trata de segurança e boas práticas estabelece comandos normativos de

112 ZANATTA, Rafael A. F., A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet, *in*: **Direito & Internet III: Marco Civil da Internet**, São Paulo: Quartier Latin, 2015, v. 1, p. 447–470.

113 BIONI, Bruno Ricardo, **Entre linhas de Código e de Fábrica: o que a GDPR tem a ver com o ex-presidente americano John F. Kennedy?**, GEN Jurídico, Junho de 2018. Disponível em: http://genjuridico.com.br/2018/06/12/entrelinhas-de-codigo-e-de-fabrica-o-que-gdpr-tem-ver-com-o-ex-presidente-americano-john-f-kennedy/

114 MACENAITE, Milda, The "Riskification" of European Data Protection Law through a two-fold Shift, **European Journal of Risk Regulation**, v. 8, n. 03, p. 506–540, 2017.

115 ZANATTA, Rafael A. F., Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?, *in*: **I Encontro da Rede de Pesquisa em Governança da Internet**, Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, p. 175–193.

estímulo ao setor privado, deixando essa missão em aberto para controladores e operadores.

Está em aberto a questão da efetividade dessas normas e mesmo a possibilidade de o Estado criar mecanismos de "sanções premiais"[116] e de estímulo a essas práticas por meio de políticas tarifárias e tributárias (a possibilidade de isenções fiscais para a demonstração de práticas de *privacy by design*), uso estratégico de intervenção no campo financeiro (a possibilidade de linhas de crédito e de financiamento via BNDES para projetos deste porte) e promoção de "competições de desenvolvimento" e técnicas de *privacy by design*.

3.2. *Accountability* como elemento central dos novos sistemas de proteção de dados pessoais: da GDPR à LGPD

Ao se estabelecer metas[117] como de *privacy by design* aos agentes da cadeia de tratamento de dados, as novas leis de proteção de dados pessoais apostam, cada vez mais, na colaboração de quem está prototipando produtos e serviços para mitigar os riscos das suas próprias atividades. Ao contrário de toda e qualquer atividade de tratamento de dados ser notificado às autoridades fiscalizadores,[118] hoje a regulação europeia só exige algum tipo de comunicação quando tal atividade atrai um risco elevado para os

116 BIONI, Bruno. **Como o Brasil pode inovar na proteção de dados pessoais.** Valor Econômico, 20 mar. 2017.

117 GELLERT, Raphaël, **Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk**, Vrije University Brussel, Bruxelas, 2017.

118 Veja, por exemplo, a obrigação de notificação de qualquer atividade de tratamento de dados pessoais as autoridades europeias na antiga diretiva de proteção de dados. Pessoais, a qual deixou de existir no novo regulamento europeu (artigo 18 da Diretiva 95/46/EC).

titulares dos dados. Todo o sistema é calibrado por esse voto de confiança e por uma série de ferramentas pelas quais os agentes de tratamento de dados demonstram a eficácia das medidas tomadas para estarem em conformidade com as regras de proteção de dados pessoais.

Uma das principais ferramentas são os chamados relatórios de impacto à proteção de dados pessoais,[119] pelo qual o controlador - quem tem poder de tomada decisão na cadeia de tratamento de dados - deve obrigatoriamente executá-los quando houver um *alto risco em jogo*. A regulação europeia além de trazer uma lista exemplificativa dessas situações, exige que os órgãos fiscalizadores sejam comunicados apenas quando o próprio agente econômico não encontrar meios de mitigar os prováveis malefícios da sua respectiva atividade, devendo nesse caso aguardar "luz verde" da autoridade para seguir em frente. Portanto, diferentemente da diretiva onde qualquer atividade deveria ser comunicada, a GDPR estabelece um regime totalmente novo de reunião de informação cujo gargalo é torneado por quem está com as mãos nos dados. Os "considerandos" do Regulamento deixam claro essa mudança da mentalidade regulatória:

> "(89) Diretiva 95/46/EC estipulava a obrigação geral de notificar o tratamento de dados para as autoridades supervisoras (...) essas notificações gerais indiscriminadas devem ser abolidas, sendo substituídas por procedimentos e mecanismos efetivos com foco em quais tipos de operações são de alto risco para os direitos e liberdades fundamentais (...) ao envolver o uso de novas tecnologias"
>
> "(84) (...) quando uma relatório de impacto à proteção de dados pessoais indicar que o tratamento envolve um alto

119 WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

risco, o qual não pode ser mitigado por meio de medidas adequados em acordo com a tecnologia disponível e os custos de implementação, um consulta à autoridade de proteção de dados deve ser realizado antes de processamento de dados."

Nessa mesma linha, códigos de boas condutas e certificações seriam outras ferramentas pelos quais os agentes de tratamento de dados demonstrariam ser responsivos às regras de proteção de dados pessoais. Respectivamente, pares de um mesmo setor verticalizaram normas transversais às realidades e desafios dos seus respectivos setor[120] e, ainda, haveriam terceiros imparciais que certificariam[121] os programas corporativos de privacidade das demais diversas organizações. Todo esses mecanismos seriam um cardápio de opções à disposição dos agentes de tratamento de dados pessoais para demonstrar a sua aderências às normas de proteção de dados pessoais, o que deveria ser obrigatoriamente contabilizado na imposição de qualquer penalidade como resultado das ações de fiscalização.[122]

Na linha da GDPR, a lei brasileira também previu o princípio específico da accountabiliuty,[123] relatórios de impacto à proteção

120 Consideranda 98 da GDPR.

121 Consideranda 77 da GDPR.

122 Regulamento Europeu de Proteção de Dados ressalta que a fixação das penalidade deve levar em consideração as medidas técnicas e organizacionais implementadas para se evitar o dano, especificamente privacy by design e padrões de segurança da informação, bem como a aderência à códigos de boas condutar e selos (Artigo 83, "d" e "j", da GDPR).

123 Artigo 6º, X- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

de dados pessoais,[124] selos[125] e códigos de boas condutas.[126] Tudo isso pode dar roupagem à "boa-fé" dos agentes de tratamento de dados pessoais, o que deve calibrar a imposição de eventuais penalidades.[127] Há, no entanto, uma diferença significativa entre tais legislações e que decorre do próprio tipo de técnica legislativa de uma lei, mais geral, em relação a um regulamento, mais prescritivo. A legislação brasileira *não procedimentaliza minimamente* como tais mecanismos deveriam ganhar vida, deixando para posterior regulação por parte da Autoridade Nacional de Proteção de Dados Pessoais. Enquanto que o Regulamento sistematiza todos eles em capítulos próprios e, em particular no caso dos relatórios de impacto à proteção de dados pessoais, já aponta em quais casos são obrigatórios e em que momento deve estabelecer conversas regulatórias com o órgão fiscalizador.

Apesar, portanto, de um sistema de corregulação, através do princípio da accountability, ser uma tendência que aproxima o modelo brasileiro do europeu; deve-se ter em mente a diferença em torno não só da estrutura normativa em questão, mas, também, principalmente dos contexto socioeconômico que serão aplicados.

Há, por fim, uma diferença *cultural* que deve ser levada em conta. As pressões em Bruxelas para que a GDPR tivesse um grande foco em "accountability" - que podemos traduzir como processos

124 Artigo 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;

125 Artigo 33, I, "d"

126 Artigo 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.

127 Artigo 52, § 1°, II e e IX, da LGPD.

de documentação, transparência e responsabilização - foram mobilizadas por parlamentares de países onde a cultura regulatória de transparência e colaboração é grande, como Holanda, Bélgica e Reino Unido. Em países como Brasil, a simples transferência e importação de regras de accountability pode não resultar no efeito esperado por, pelo menos, três fatores: (i) a ausência de uma tradição de regulação focada em "accountability", mas muito focada em regulação do tipo "comando e controle" por agências integrantes da administração pública, (ii) uma desconfiança, por parte do setor privado, sobre as reais capacidades de colaboração e de expertise técnica por parte do regulador, e (iii) a inexistência de criação da Autoridade Nacional de Proteção de Dados Pessoais, que tem como missão a criação de uma cultura de co-regulação e de uso variado de técnicas de regulação (dosando a abordagem de "cenoura", de geração de estímulos, e de "porrete", focada na sanção e punição)[128].

3.3. Avaliações de impacto: tecnocracia ou possibilidade de participação?

Por fim, como dito anteriormente, uma das tendências no campo regulatório com relação à proteção de dados pessoais é a definição de um sistema de documentação e de mitigação de riscos, inspirados na cultura regulatória ambiental (e os *Enrivonmental Impact Assessment*), cristalizado na obrigação de produção de "avaliações de impacto à proteção de dados pessoais".

Essa "laboriosa tarefa de avaliação de risco pelos controladores", na expressão de Claudia Quelle, funciona como uma espécie de *outsourcing* da tarefa regulatória, colocando ao setor privado a tarefa de avaliação do (i) tipo de tratamento de dados em questão,

128 A expressão é utilizada pelo jurista Diogo Coutinho. Ver: COUTINHO, Diogo. A universalização do serviço público para o desenvolvimento como uma tarefa da regulação, *in*: SALOMÃO, Calixto (org.), **Regulação e Desenvolvimento**. São Paulo: Malheiros, 2002.

(ii) o uso de novas tecnologias, (iii) a natureza e o escopo do tratamento, (iv) e se há possibilidade de tal tratamento resultar em alto risco com relação às "liberdades e liberdades da pessoa natural".

No debate contemporâneo sobre o uso das "avaliações de impacto à proteção de dados pessoais" há diferentes interpretações sobre o quão efetivo pode ser esse instrumento para a contenção de violações aos direitos coletivos e para um real conhecimento, por parte da população, sobre como funcionam as técnicas avançadas de profiling e análise preditiva baseada em dados. De um lado, juristas como Paul de Hert, David Wright e Vagelis Papakonstantitnou enxergam nas avaliações de impacto uma aposta positiva de maior documentação, de internalização de riscos por parte do setor privado e de possibilidade de coleta de informações por parte das Autoridades de Proteção de Dados Pessoais.[129] Juristas como Claudia Quelle e Maria Eduarda Gonçalves, por outro lado, apontam que esse tipo de tecnicismo pode gerar uma interpretação errônea de uma "regulação baseada em riscos", típica do sistema financeiro, colocando em segundo plano a ideia de que o risco serve apenas como instrumento de calibração sobre as obrigações por parte do controlador, sendo essencial a manutenção da linguagem da proteção de dados pessoais como um sistema de proteção de direitos fundamentais.[130] Em outro extremo, juristas como o italiano Alessandro Mantelero apontam que o formato atual das avaliações de impacto, ao menos no formato definido pela GDPR, são excessivas técnicas e fechadas em uma relação de documentação entre controlador

129 DE HERT, Paul; PAPAKONSTANTINOU, Vagelis, The new General Data Protection Regulation: still a sound system for the protection of individuals?, **Computer Law & Security Review**, 32, p. 179, 194, 2016. WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

130 GONÇALVES, Maria Eduarda, The EU data protection reform and the challenges of Big Data, **Information & Communications Technology Law**, 26, 2, p. 90-115, 2017. QUELLE, Claudia, The risk revolution in EU data protection law: we can't have our cake and eat it too, *in*: LEENES, Ronald *et al,* **Data Protection and Privacy: the age of intelligent machines**, Springer, 2017, p. 33-62.

e Autoridade, sendo necessário repensar o papel que a sociedade civil e as entidades especializadas podem ocupar na própria *elaboração participativa* das avaliações de impacto, fazendo com esse processo "inclua as várias partes envolvidas e mecanismos de representação dos interesses coletivos afetados por atividades específicas de tratamento de dados"[131].

No Brasil, o sistema de avaliação de impacto também foi adotado pela Lei Geral de Proteção de Dados Pessoais. O chamado "relatório de impacto à proteção de dados" é definido como "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" (art. 5º, XVII). No entanto, ele não é obrigatório para atividades de alto risco, como definido na legislação europeia. Em termos práticos, isso implica dizer que o modelo brasileiro funciona como uma espécie de *documentação posterior*, que se torna obrigatória somente quando houver pedido expresso por parte da Autoridade Nacional de Proteção de Dados Pessoais. O art. 38 diz que "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". Há regra semelhante quando o controlador utiliza a hipótese de *legítimo interesse* para tratamento dos dados.[132] Nesse caso, poderá

131 MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection, **Computer Law & Security Review**, 32, 2, p. 238-255, 2016.

132 Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas (...)
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

a Autoridade "bater à porta" do controlador e exigir que o mesmo elabore, em certo prazo, a referida documentação.[133]

Como consequência, a mensagem que se passa é que a avaliação de impacto é uma *possibilidade*, mas não uma obrigação regulatória. Não há, também, mecanismos definidos de construção participativa desses relatórios, sendo muito distante o horizonte imaginado por Alessandro Mantelero e outros críticos. Está em aberto a possibilidade de uma inclusão participativa por mecanismos autorregulatórios (as próprias empresas definirem processos de discussão e de participação para elaboração dos relatórios) e da criação de uma espécie de rede social de controle e monitoramento, capaz de discutir publicamente como esses relatórios são criados, com quais metodologias e quais instrumentos de verificação de como liberdades civis e direitos fundamentais são afetados por atividades de tratamento de dados.[134] Esse é um trabalho que, em tese, pode ser desenvolvido por centros de pesquisa e organizações civis como Idec, InternetLab, Coding Rights, Instituto Iris e outros integrantes da Coalizão Direitos na Rede,[135] bem como

133 Já se argumentou no Brasil, em diversas ocasiões e por diferentes autores, que há uma tendência de se debater poluição de dados e avaliações de impacto. "De certo modo, falar de 'dados pessoais' é também falar de ambiente, de direitos humanos e de trabalho. Nosso ambiente 'natural' estará cada vez mais integrado com o 'digital', especialmente em um contexto de Internet das Coisas. Será difícil separar a natureza de nossos artefatos em um cenário de 'inteligência ambiental'. As cidades do futuro terão integração de dispositivos e sensores com sistemas inteligentes de energia, irrigação e controle de poluição, alimentados ou não pela atuação humana. Nessa reinvenção do ambientalismo, ganha força o debate sobre poluição de dados e avaliações de impacto". LEMOS, Ronaldo; DOUEK, Daniel; LANGENEGGER, Natalia; ZANATTA, Rafael. **O dia internacional da proteção de dados pessoais**, Jota, 25/01/2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dia-internacional-da-protecao-de-dados-pessoais-28012019

134 Essas possibilidades foram discutidas em texto de um dos autores. Ver ZANATTA, Rafael. **Regulatory Studies, Post-Normal Science and Personal Data Protection: rethinking complexity and uncertainty in the 21st century**, Paper prepared for the course New Legal Theories, University of São Paulo Faculty of Law, 2018. Disponível em: https://www.researchgate.net/publication/327433867_Regulatory_Studies_Post-Normal_Science_and_Personal_Data_Protection_rethinking_complexity_and_uncertainty_in_the_21st_century

135 https://direitosnarede.org.br/

outras organizações da sociedade civil que integram o campo dos "direitos digitais".

CONCLUSÃO

A formulação de instrumentos regulatórios e princípios de justiça à proteção de dados pessoais datam de mais de meio século e apresentam uma tendência de convergência, apesar de existirem claras distinções e opções jurídicas e políticas em regiões como Estados Unidos da América e União Europeia. Apresentamos, neste texto, como se deu a formulação dos *Fair Information Practices Principles* nos EUA e como uma preocupação voltada às limitações dos poderes governamentais foi transporta ao setor privado, por meio de uma estrutura de fiscalização e repressão colocada em prática pela Federal Trade Commission. Os países europeus, por outro lado, valeram-se da formulação destes princípios para avançar uma estratégia regional de harmonização jurídica, impulsionada pelos trabalhos técnicos da Comissão Europeia e da OCDE e por uma forte cultura de afirmação de direitos fundamentais e constituição da proteção de dados pessoais como um direito autônomo e distinto do direito à privacidade.

Demos destaque à inter-relação entre direito e política tanto na experiência estadunidense das últimas décadas quanto na rica experiência europeia, em especial o esforço de criação de novos direitos e instrumentos regulatórios por meio da General Data Protection Regulation (GDPR). Como sustentado, a estratégia europeia deve ser lida também por uma lente geopolítica de constituição de um "mercado europeu único" e de aplicação extraterritorial de suas normas, gerando uma espécie de "modelo de exportação" para outros países. Sem dúvidas, a União Europeia tem como pretensões criar um modelo jurídico de referência para a proteção de dados pessoais, fundamentada em fortes obrigações aos controladores, novos direitos aos titulares de dados,

processos de accountability e fiscalização técnica por meio das Autoridades Nacionais de Proteção de Dados Pessoais.

Apontamos três tendências jurídicas dominantes e seus desafios ao Brasil, para além da já criada Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). Primeiro, a construção de incentivos e de uma cultura adequada de *privacy by design*. Segundo, o fortalecimento de uma cultura de documentação, transparência e responsabilização, fundamentada em uma espécie de "regulação colaborativa" por meio da Autoridade Nacional de Proteção de Dados Pessoais. Terceiro, a possibilidade de que as avaliações de impacto fujam de uma perspectiva tecnocrata e fechada entre empresas e autoridades, fortalecendo uma cultura cívica participativa e de maior compreensão sobre os "detalhes internos" de funcionamento de um capitalismo dadocêntrico. Esperamos que esse guia sirva de incentivo a mais pesquisas e ações práticas nesta área, reforçando o diálogo entre juristas e economistas que se mostra cada vez mais necessário para dimensionarmos a nova lógica econômica e regulatória em questão.

REFERÊNCIAS

ABRAMOVAY, Ricardo. Aos dados, cidadãos!, **Revista Quatro Cinco Um**, São Paulo, abril de 2018.

ABRAMOVAY, Ricardo. Sociedade da vigilância em rede, **Revista Quatro Cinco Um**, *São Paulo*, março de 2019.

ALBRECHT, Jan Philipp. How the GDPR will change the world. **European Data Protection Law Review**, v. 2, p. 287, 2016.

ARRIETA IBARRA, Imanol et al. Should We Treat Data as Labor? Moving Beyond'Free'. **American Economic Association Papers & Proceedings**, v. 1, n. 1, 2017.

BENIGER, James. **The control revolution: Technological and economic origins of the information society**. Harvard university press, 2009.

BING, Jon. The Council of Europe Convention and OECD Guidelines on Data Protection. **Michigan Legal Studies**, v. 5, p. 271, 1984.

BIONI, Bruno Ricardo, A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço, *in*: **Direitos e novas tecnologias: XXIII Encontro Nacional do Conpedi**, Florianópolis: Conpedi, 2014, v. 1, p. 59–82.

BIONI, Bruno Ricardo, Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes, *in*: BARBOSA, Alexandre F. (Org.), **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro : TIC governo eletrônico 2017**, São Paulo: Comitê Gestor da Internet, 2018, p. 53–62.

BIONI, Bruno Ricardo, Entre linhas de Código e de Fábrica: o que a GDPR tem a ver com o ex-presidente americano John F. Kennedy?, **GEN Jurídico**, Junho de 2018.

BIONI, Bruno. Como o Brasil pode inovar na proteção de dados pessoais. **Valor Econômico**, 20 mar. 2017.

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

BLUM, Rita Peixoto. **O direito à privacidade e à proteção de dados pessoais**. São Paulo: Almedina, 2018.

COUTINHO, Diogo. A universalização do serviço público para o desenvolvimento como uma tarefa da regulação, *in*: SALOMÃO, Calixto (org.), **Regulação e Desenvolvimento**. São Paulo: Malheiros, 2002.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis, The new General Data Protection Regulation: still a sound system for the protection of individuals?, **Computer Law & Security Review**, 32, p. 179, 194, 2016.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 16, p. 117, 2003.

EVANGELISTA, Rafael. Capitalismo de Vigilância no Sul Global: por uma perspectiva situada, *in*: **5º Simpósio Internacional LAVITS**, Santiago, Chile, 2017, p. 243-253.

EUROPEAN COMMISSION, **Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions**, "A comprehensive approach on personal data protection in the European Union", Brussels, 2010.

EUROPEAN COMMISSION, **A comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses**, EC: Brussels, 2012.

EUROPEAN COMMISSION, **Progress on EU data protection reform now irreversible following European Parliament vote**, EC: Strasbourg, 2014.

FELDMAN, Sheldon. The Fair Credit Reporting Act-From the Regulators Vantage Point. **Santa Clara Lawyer**, v. 14, p. 459, 1973.

FLORIDI, Luciano, **The 4th revolution: how the infosphere is reshaping human reality**, Oxford: Oxford Univ. Press, 2014.

GELLERT, Raphaël, **Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk**, Vrije University Brussel, Bruxelas, 2017.

GELLMAN, Robert, **Fair Information Practices: A Basic History**, Rochester, NY: Social Science Research Network, 2017.

GONÇALVES, Maria Eduarda, The EU data protection reform and the challenges of Big Data, **Information & Communications Technology Law**, 26, 2, p. 90-115, 2017.

GONZÁLEZ FUSTER, Gloria, **The emergence of personal data protection as a fundamental right of the EU**, Cham: Springer, 2014.

HILDEBRANDT, Mireille; TIELEMANS, Laura. Data protection by design and technology neutral law. **Computer Law & Security Review**, v. 29, n. 5, p. 509-521, 2013.

HOOFNAGLE, Chris Jay. **Federal Trade Commission Privacy Law and Policy**. Cambridge University Press, 2016.

IANSITI, Marco; LAKHANI, Karim R. Digital ubiquity: How connections, sensors, and data are revolutionizing business. **Harvard Business Review**, v. 92, n. 11, p. 19, 2014.

KERSON, D. L. A. The European Convention for the protection of human rights and fundamental freedoms. **California Law Review**, v. 49, p. 172, 1961.

LEMOS, Ronaldo. É preciso plano de inteligência artificial, **Folha de São Paulo**, 04/02/2019.

LEMOS, Ronaldo; DOUEK, Daniel; LANGENEGGER, Natalia; ZANATTA, Rafael. **O dia internacional da proteção de dados pessoais**, Jota, 25/01/2019.

LESSIG, Lawrence. The constitution of code: limitations on choice-based critiques of cyberspace regulation. **CommLaw Conspectus**, v. 5, p. 181, 1997.

LEVIN, Mariam. **Cultures of Control**. Amsterdam: Harwood Academic Publisher, 2000.

MACENAITE, Milda, The "Riskification" of European Data Protection Law through a two-fold Shift, **European Journal of Risk Regulation**, v. 8, n. 03, p. 506–540, 2017.

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection, **Computer Law & Security Review**, 32, 2, p. 238-255, 2016.

MAYER-SCHONEBERGER, Viktor, Generational development of data protection in europe, *in*: AGRE, Philip; ROTENBERG, Marc (Orgs.), **Technology and privacy: the new landscape, 1st paperback ed**. Cambridge, Mass.: MIT Press, 1998, p. 219–242.

MOROZOV, Evgeny. **Big Tech:** a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

OECD, **Developments in Data Protection and Privacy by OECD Countries**, Survey from OECD'S Computer Utilization Group. Paris: OECD, 1975.

POWLES, Julia. Democracy: the film that gets behind the scenes of the European privacy debate, **The Guardian**, 14/11/2015.

QUELLE, Claudia, The risk revolution in EU data protection law: we can't have our cake and eat it too, *in*: LEENES, Ronald et al, **Data Protection and Privacy: the age of intelligent machines**, Springer, 2017, p. 33-62.

READING, Viviane. The upcoming data protection reform for the European Union. **International Data Privacy Law**, v. 1, n. 1, p. 3-5, 2010.

READING, Viviane. The European data protection framework for the twenty-first century. **International Data Privacy Law**, v. 2, n. 3, p. 119-129, 2012.

REGAN, Priscilla. **Legislating Privacy: technology, social values and public policy**. The University of North Carolina Press, 1995.

RICHARDS, Neil'; SOLOVE, Daniel. Prosser's Privacy Law: a mixed legacy, **California Law Review**, v. 98, 2010, p. 1888-1928.

RODOTÀ, Stefano, **Il diritto di avere diritti**, Roma; Bari: Laterza, 2013.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

ROTENBERG, Marc. Fair information practices and the architecture of privacy (What Larry doesn't get). **Stanford Technology Law Review**, v. 44, 2001.

SPINA, Alessandro, **Laudato Si' and Augmented Reality -** In Search of an Integral Ecology for the Digital Age, Rochester, NY: Social Science Research Network, 2017.

SILVA, Nelson. Transformação digital: a 4. revolução industrial. **Boletim de Conjuntura da FGV**, n. 8, p. 15-18, 2018.

SOBEL, Lester A. (Ed.). **War on Privacy**. New York: Facts on File, 1976.

SOLOVE, Daniel; SCHWARTZ, Paul. **Information Privacy Law**. Sixth edition. New York: Wolters Kluwer, 2018.

SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the new common law of privacy. **Columbia Law Review**, v. 114, p. 583, 2014.

ULLMAN, Charles M. Liability of Credit Bureaus after the Fair Credit Reporting Act: the need for further reform. **Vill. L. Rev.**, v. 17, p. 44, 1972.

VAN DIJCK, Johana. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197-208, 2014.

WESTIN, Alan F. The Wire-Tapping Problem: An Analysis and a Legislative Proposal. **Columbia Law Review**, v. 52, n. 2, p. 165-208, 1952.

WESTIN, Alan F.; RUEBHAUSEN, Oscar M. **Privacy and Freedom**. New York: Atheneum, 1967.

WESTIN, Alan. Social and Political Dimensions of Privacy, **Journal of Social Issues**, v. 59, 2003, p. 431-453.

WINNER, Langdon, Do Artifacts Have Politics?, **Daedalus**, v. 109, n. 1, p. 17, 1980.

WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

ZANATTA, Rafael A. F., A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet, *in*: **Direito & Internet III: Marco Civil da Internet**, São Paulo: Quartier Latin, 2015, v. 1, p. 447–470.

ZANATTA, Rafael. Regulatory Studies, Post-Normal Science and Personal Data Protection: rethinking complexity and uncertainty in the 21st century, **Paper prepared for the course New Legal Theories**, University of São Paulo Faculty of Law, 2018.

PARTE 2
ELEMENTOS FUNDANTES

O DEVER DE INFORMAR E A TEORIA DO DIÁLOGO DAS FONTES PARA A APLICAÇÃO DA AUTODETERMINAÇÃO INFORMACIONAL COMO SISTEMATIZAÇÃO PARA A PROTEÇÃO DOS DADOS PESSOAIS DOS CONSUMIDORES: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo "Lulu"[1]

Bruno Ricardo Bioni

1 Originalmente publicado como: BIONI, Bruno R. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo "Lulu", **Revista de Direito do Consumidor**, ano 23, vol. 94, p. 283-326, 2014.

RESUMO

A privacidade dos consumidores na sociedade da informação compreende-se por uma tutela dinâmica atinente a perspectiva de controle sobre seus dados pessoais, surgindo daí o referencial normativo de que o indivíduo autodetermine o fluxo de suas informações pessoais (autodeterminação informacional). A presente monografia debruçar-se-á, então, como tal parâmetro regulatório para a proteção dos dados pessoais pode ser aplicado no atual ordenamento jurídico vigente, uma vez que o Brasil não tem uma lei geral de proteção de dados pessoais. Recorre-se, assim, ao dever de informação permeado pelo princípio da transparência e a teoria do diálogo das fontes para que seja sistematizada a proteção dos dados pessoais dos consumidores a partir da autodeterminação informacional. Após terem sido estabelecidas tais premissas teóricas-normativa, passa-se ao estudo da notória ação coletiva promovida contra o Facebook e o aplicativo "Lulu", empregando uma abordagem concreta e dinâmica da propugnada sistematização para identificar convergências e divergências entre o quadro normativo proposto e como tal processo foi conduzido.

PALAVRAS-CHAVE

Autodeterminação informacional - proteção de dados pessoais - dever-direito de informação - privacidade - transparência.

ABSTRACT

Consumer´s privacy is understood by dynamic protection in the information society. It is consequence of normative framework that the individual should self-determine his flow personal information (informational self-determination). Thus, the present monograph will analyze how this framework regulatory of personal data protection can be applied to the current prevailing legal system, because there is not general law of data protection in Brazil. The duty of information and transparency principle which orient consumption relations and dialogue of sources that are used to systematize consumer data protection by informational self-determination. After It was established these theoretical-normative premises that goes to study the notorious class action against *Facebook* and "Lulu" application/app. By this methodology, it was possible to identify divergences and convergences considering how class action was conducted, creating concrete and dynamic approach of advocated systematization.

KEY-WORDS

informational self-determination - personal data protection - duty-right of information - privacy - transparency

SUMÁRIO

1. INTRODUÇÃO

O presente artigo visa apresentar uma proposta de regulação dos bancos de dados eletrônicos por meio da denominada autodeterminação informacional, pretendendo-se, pois, alcançar uma tutela dinâmica dos direitos da personalidade dos consumidores em meio à denominada sociedade da informação.

Assim, esclarece-se, desde logo, que a investigação proposta está restrita a essa anunciada seara cadastral, perquirindo-se a respeito da autodeterminação do consumidor em face às novas tecnologias.

Parte-se, então, da análise de uma premissa necessária para tanto, qual seja, um processo de interação entre o detentor dos bancos de dados e aquele que é o titular dos dados pessoais, analisando-se o direito-dever informacional entre tais sujeitos que polarizam tal relação jurídica.

Desta feita, iniciar-se-á a análise da própria evolução do conceito de obrigação, chegando-se à concepção dinâmica do complexo obrigacional que é donde, sobretudo, foi concebido o dever-direito de informação oriundo dos denominados direitos anexos, satelitários, secundários ou gravitacionais criados pela boa-fé objetiva.

Em seguida, passar-se-á a sua análise no plano do microssistema legislativo consumerista, verificando-se que o dever-direito de informar formata todas as suas normas, e, por conseguinte, todo o desenvolvimento das relações de consumo.

Posteriormente, contextualizar-se-á o citado dever-direito de informação na denominada sociedade de informação para o desiderato, como dito, de uma possível regulação para os bancos de dados eletrônicos dos consumidores, concluindo-se, por fim, que a autodeterminação informacional consistente, em apertada síntese, no direito do indivíduo controlar seus dados pessoais passa, necessariamente, pelo espectro do dever-direito informacional, sendo, justamente, o elemento que a racionaliza, tornando-a factível e tutelável pelo ordenamento jurídico brasileiro.

Considerar-se-á, ainda, as normas contidas no Marco Civil da Internet (12.965/2014), as Leis do Cadastro Positivo (12.414/2011) e Habeas Data (9.507/1997), e, por fim, os Decretos 6.135/2007, 6.425/2008 e 6.523/2008, que, mediante o diálogo das fontes, servem como um método sistemático para organizar e coordenar as fontes normativas legais e infralegais supracitadas que traçam princípios conformadores da autodeterminação informacional.

Por derradeiro, para validar e testar todo esse percurso teórico-normativo, analisar-se-á o notório caso da ação coletiva promovida pelo Ministério Público do Distrito Federal e dos Territórios em face da rede social *Facebook* e o aplicativo 'Lulu", a qual será dívida em duas partes: i) narrativa: mediante a descrição dos fatos que circunstanciaram o caso, notadamente como se aperfeiçoou a parceria comercial entre os Réus da ação que é donde se desdobra todo suporte fático do litígio; ii) apreciação técnica: análise do caso da petição inicial da ação coletiva e da decisão de segunda instância que concedeu o pedido de tutela antecipada para, dentre outros pedidos, cessar o compartilhamento dos dados pessoais dos consumidores.

Deste modo, será possível constatar convergências e divergências das premissas teóricas-normativa traçadas na primeira parte desta monografia, empregando-lhe uma abordagem mais concreta e dinâmica, refletindo-se sobre a própria racional da petição inicial da ação coletiva e da decisão judicial supracitada, confrontado, em última análise, a propugnada sistematização da proteção dos dados pessoais dos consumidores que se revela e se apresenta como a grande conquista, ainda em construção, da proteção do consumidor no século XXI.[2]

2 Esse é o temário do III Concurso de Monografias realizado pelo Instituto Brasileiro de Política e Defesa do Consumidor/Brasilcon: "Avanços e conquista da Proteção do Consumidor no século XXI".

2. A OBRIGAÇÃO COMO PROCESSO: CONCEPÇÃO DINÂMICA E COMPLEXA DA OBRIGAÇÃO COMO UM FEIXE DE DIREITOS E DEVERES DO VÍNCULO OBRIGACIONAL

A obrigação no clássico conceito de Clóvis Beviláqua: "é a relação transitória de direito, que nos constrange a dar, fazer ou não fazer uma coisa, em regra economicamente apreciável, em proveito de alguém conosco juridicamente relacionado".[3]

Veja-se que o supracitado conceito clássico condensa o vínculo obrigacional sob a sua perspectiva estrutural: elementos subjetivos - credor e devedor; elemento objetivo: a prestação; e, por último, o denominado elemento virtual/espiritual: o vínculo jurídico que conecta credor e devedor.[4]

Por tal construção, com enfoque sobre o elemento objetivo da obrigação, chegou-se à classificação de que as obrigações poderiam ser simples ou complexas, esta última também chamada de conjuntivas. A obrigação simples seria aquela que concentraria, tão somente, uma única prestação. Ao passo que, a obrigação complexa/conjuntiva/cumulativa compreenderia a prática de mais de um ato - um dar e fazer -, ou mesmo, sob a qual poder-se-ia recair sobre mais de uma coisa.[5]

3 BEVILAQUA, Clovis. **Direito das obrigações**. Rio de Janeiro: Livraria Francisco Alves, 1945. p. 14.

4 DELGADO, Mário Luiz. Comentários à Parte Especial – artigos 233 a 420 do Código Civil. **In Código civil comentado**. Regina Beatriz Tavares da Silva. (Org.). São Paulo: Saraiva, 2012. p. 277: "São três os elementos constitutivos da obrigação: o elemento subjetivo ou pessoa representado pelos sujeitos ativo (credor) e passivo (devedor); o elemento objetivo ou material, representado pelo objeto da prestação; e finalmente o elemento espiritual, ou imaterial, representado pelo vínculo jurídico ou liame que conecta os sujeitos".

5 MONTEIRO, Washington de Barros. MALUF, Carlos Alberto Dabus. **Curso de direito civil**, vol. 4: direito das obrigações, 1ª parte: das modalidades das obrigações da →

Tal classificação é uma amostra da *concepção estática da obrigação* que se concentrava numa análise, meramente, dual, em que cabia ao credor receber o pagamento, e, por outro lado, o devedor prestá-lo. A complexidade era erigida, tão somente, ao elemento estrutural objetivo, não se cogitando a respeito de outros deveres e direitos existentes na relação jurídica obrigacional entre credor e devedor.

Contudo, com o advento do imperativo ético obrigacional, ora plasmado pela boa-fé objetiva,[6] criaram-se os denominados deveres acessórios, secundários, gravitacionais ou satelitários,[7] redimensionando o próprio vínculo obrigacional para além de uma simples perspectiva simétrica entre crédito e débito - dar e receber, por exemplo, nas respectivas figuras de devedor e credor -, mas para uma plêiade de direitos e deveres, de forma cruzada, entre credor e devedor, cuja incidência é *ex lege*.[8]

Destes deveres anexos: fala-se em dever de sigilo, de advertência, de proteção, de cooperação, de lealdade, de informação que,

→ transmissão das obrigações. São Paulo: Saraiva, 2012. p. 68: "**Obrigações simples e conjuntas** - Ainda quanto ao seu objeto, as obrigações podem ser simples e conjuntas. São simples quando a prestação abrange um único ato, ou uma só coisa, singular ou coletiva (Cód. Civil de 2002, art. 89): construir um muro, pagar determinada quantia, restituir certo objeto. São conjuntas, também chamadas cumulativas, quando recaem sobre muitas coisas e todas devem ser pagas ou cumpridas."

6 MENEZES CORDEIRO, António Manuel da Rocha e. **Tratado de direito civil** das obrigações. 2°: Direito das obrigações, 1° t: Introdução, sistemas e direito europeu, dogmática geral. Coimbra: Almedina, 2009. p. 467: "Em síntese, podemos dizer que, através da *bona fides*, o Direito romano aperfeiçoou o sistema geral das obrigações, de modo a permitir que o juiz, em vez de se ater a formalismos estritos, pudesse, através de certos expedientes, descer à substância das questões."

7 TEPEDINO, Gustavo; SCHREIBER, Anderson. **Código civil comentado**: direito das obrigações: artigo 233 a 420, volume IV. São Paulo: Atlas, 2008. p. 5: "A cláusula geral da boa-fé objetiva impõe deveres anexos às convenções, como o dever de informação e o dever de colaboração, que recaem também sobre o credor, fazendo-o a um só tempo titular de direitos e deveres frente à contraparte e mesmo a centros de interesses que não integram diretamente o vínculo obrigacional".

8 MENEZES CORDEIRO, António Manuel da Rocha e. **Da boa fé no direito civil**. Coimbra: Almedina, 2011. p. 586: "A complexidade intra-obrigacional traduz a ideia de que o vínculo obrigacional abriga, no seu seio, não um simples dever de prestar, simétrico a uma prestação creditícia, mas antes vários elementos jurídicos dotados de autonomia bastante para, de um conteúdo unitário, fazerem de uma realidade composta."

como dito, incidem tanto para o credor e devedor em decorrência da lei: a cláusula geral de boa-fé.

Daí porque, assevera-se que mesmo as obrigações unas ou simples são complexas, isto porque, não são compostas por um único substrato - o dar, fazer ou não fazer -, mas por múltiplos componentes: os deveres acessórios.[9]

Nesse sentido, decorre, também, a desconstrução das terminologias cunhadas de sujeito ativo e passivo da obrigação, pois a concorrência de deveres e direitos impediria tal classificação, já que ambos são pacientes de deveres e direitos.[10]

Constrói-se, assim, uma *estrutura dinâmica*[11] do complexo obrigacional em que as partes, que o compõem, cooperam para a consecução de seus interesses contrapostos concentrados sob um fim último: o pagamento, pois é tal ato que extingue a obrigação, conformando o seu próprio conceito, o de uma relação transitória.

Há, portanto, uma coordenação recíproca que remete à ideia de processo: de uma prática de atos coordenados em que o vínculo

9 VARELA, João de Matos Antunes. **Das obrigações em geral**: vol. 1. Coimbra: Almedina, 2012. p. 68: "Note-se, porém, que a doutrina moderna das obrigações tem salientado, com razão, a *complexidade* das próprias obrigações *unas* ou *simples*. A complexidade assim entendida reflecte-se no vínculo obrigacional em geral e traduz-se na série de *deveres*, *secundários* e de *deveres acessórios* de conduta que gravitam as mais das vezes em torno do dever principal de prestar e até do direito à prestação principal." (destaques do original)

10 TEPEDINO, Gustavo; SCHREIBER, Anderson. *Op. Cit*. p. 5: "A designação de sujeito ativo ou passivo, embora usual do ponto de vista didático, mostra-se insuficiente e reducionista, já que limitada a traduzir a estrutura estática do vínculo obrigacional, em que o poder de exigir se mostra concentrado na figura do credor. A perspectiva funcional acima aludida sublinha a complexidade de interesses e deveres recíprocos presentes na relação obrigacional, impondo a mútua colaboração em torno do escopo comum, e tornando questionável aquela terminologia."

11 MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1999. p. 394: "Ora, como efeito da apreensão da totalidade concreta da relação obrigacional, percebe-se ser a mesma um vínculo dinâmico - porque passa a englobar, num permanente fluir, todas as vicissitudes, "casos" e problemas que a ela possam ser reconduzidas - que se movimenta processualmente, posto criado e desenvolvido à vista de uma finalidade, desenvolvendo-se em fases distintas, a do nascimento do vínculo, do seu desenvolvimento e adimplemento."

obrigacional se extingue-se desenvolve, contribuindo os dois polos da relação obrigacional para todo esse desencadeamento.[12]

Em síntese, seja qual for a nomenclatura: obrigação como organismo (Heinrich Siber e Savingy),[13] relação-quadro,[14] complexidade intra-obrigacional, obrigação como processo, *concepção dinâmica* da obrigação ou regra moral nas obrigações[15], há uma convergência da doutrina que se afasta de uma análise rarefeita, simples e estática do plexo obrigacional para uma concepção dinâmica em que há um feixe de direitos e deveres entre os polos da relação obrigacional conclamados para a extinção do vínculo obrigacional.

E, por se buscar o pagamento - a causa normal da extinção do vínculo obrigacional -, ínsita está nessa abordagem a própria ideia de não se causar danos a outrem, já que o inadimplemento de uma obrigação gera, inevitavelmente, perdas e danos.[16]

12 SILVA, Clóvis do Couto e. **A obrigação como processo**. Rio de janeiro: Editora FGV, 2006. p. 20: " Os atos praticados pelo devedor, assim como os realizados pelo credor, repercutem no mundo jurídico, nele ingressam e são dispostos e classificados segundo uma ordem, atendendo-se aos conceitos elaborados pela teoria do direito. Esses atos, evidentemente, tendem a um fim. E é precisamente a finalidade que determina a concepção da obrigação como processo."

13 MENEZES CORDEIRO, António Manuel da Rocha e. Tratado de...*Op. Cit*. 291: "Heinrich Siber vem a descobrir, nele, diversos elementos acabando por recuperar uma locução já usada por Savigny, referir o vínculo obrigacional como um organismo.

14 *Idem*. p. 290.

15 RIPERT, Georges. **A regra moral nas obrigações civis**. Campinas: Bookseller, 2009. p. 23: "Até que ponto o mundo jurídico se poderá organizar fora de toda a preocupação moral, sobre os dados práticos e irracionais? Quando se trata de regrar os efeitos legais das vontades e das atividades, de organizar a troca de capitais e de serviços, poder-se-á sobre um ideal bastante vago ou necessidade econômica fazer construções abstratas, e depois divertir-se a escrever equações de relações jurídicas e a transformá-las? Não é, pelo contrário, preciso ter presente que o credor e o devedor, ligados um ao outro pela relação de direito, são homens que fazem parte da mesma comunidade, que uma moral sublime chama irmãos e que não podem ter, um os direitos, outro as obrigações senão na medida em que a lei moral permite tirar de alguém proveito e serviços, ou não o impede em todo o caso de o prejudicar."

16 SILVA, Clóvis do Couto e. *Op. Cit*. p. 40: "Há, no contrato, o dever bilateral de proteção, que impede que uma das partes cause à outro algum dano, em razão de sua atividade. Existem, assim, deveres do credor, que não são deveres para consigo mesmo, mas sim deveres jurídicos. Muitos deles consistem em conduta determinada, em comunicar ➔

Essa última ideia será muita cara ao objeto deste trabalho, partindo-se do pressuposto de que quando há vínculo obrigacional deve-se cooperar para com o outro (alteridade), a fim de que não lhe sobrevenha danos.

Nessa altura, cabe esclarecer que tal perspectiva não se limita às relações contratuais, mas a todas relações travadas na sociedade,[17] extraindo-se o máximo alcance da locução *contato social*.[18]

Em conclusão, conclui-se haver uma clara evolução da própria fonte do direito obrigacional (*ex lege: da cláusula geral da boa-fé*), a iniciar por sua incidência mediante um simples contato social que, a partir de então, pari uma série de deveres obrigacionais de consideração para com o outro,[19] a fim de não lesá-lo; o que parece ter sido uma clara opção adotada pelo Código de Defesa do Consumidor, especialmente no tocante ao dever-direito de informar e o seu resultado consectário: a transparência nas relações de consumo.

➔ algo, em indicar alguma circunstância, em fornecer informações, cuja omissão pode causar dano ao outro figurante."

17 É o que se pode extrair da culpa *in contrahendo* e da terceira via da responsabilidade pela confiança.

18 MARTINS-COSTA, Judith. *Op. Cit*. p. 400: "É justamente esta a razão pela qual, na elaboração da doutrina dos atos existenciais, adverte-se que as duas fontes "clássicas" de criação de relação jurídica obrigacional, a lei e a vontade (ou contrato, ou negócio jurídico) - das quais defluem, como irmãos siameses, os dois diversos fundamentos da responsabilidade para o caso de seu inadimplemento - têm-se mostrado insuficientes para explicar a questão da origem da criação da relação obrigacional. A fim de superar essa insuficiência, Clóvis Couto e Silva propõe que se situe a origem da relação obrigacional, em qualquer de suas espécies, na categoria do contato social, fattispecie de maior grau de abrangência, por forma a se alocar como uma "*fattispecie* comum aos contratos e aos delitos, lhes conferindo um grande valor sistemático, constituindo, por igual, a categoria à qual podem ser reconduzidos os atos existenciais produzidos no âmbito das condutas socialmente típicas."

19 MENEZES CORDEIRO, António Manuel da Rocha e. Tratado de...*Op. Cit*. p.477: "No tocante à constituição: os deveres assessórios têm as mesmas fontes das obrigações. Todavia, eles surgem de modo mais amplo e não necessariamente coincidente com elas. O simples início de negociações pode originar deveres acessórios que, depois, irão se manter. Na constituição de deveres acessórios, jogam relações de proximidade típica e de confiança real.

3. O DEVER-DIREITO DE INFORMAR E TRANSPARÊNCIA NAS RELAÇÕES DE CONSUMO

3.1. O papel central da informação e da transparência no CDC

A legislação consumerista ao prever o princípio da transparência no artigo 4°, *caput*, do CDC, como vetor da Política Nacional do Consumo, bem como o direito à informação contemplado pelo artigo 6°, inciso III, do CDC, como direito básico do consumidor, erigiu a informação como pedra de toque para todas as práticas adotadas no mercado de consumo.

Prescindível, destarte, que conduta do fornecedor do bem de consumo importe num ato de consumo, e, por conseguinte, numa relação contratual. O direito-dever de informação alcança todo e qualquer *contato social* proveniente no mercado de consumo.[20]

Por tal razão, o dever de informar perpassa o capitulo VI do CDC - a proteção contratual do consumidor, como no caso da necessária oportunização do consumidor ter conhecimento das disposições contratuais (art. 46 do CDC) e da própria redação empregada do texto contratual que lhe deve propiciar uma adequada compreensão (art. 54 do CDC) -, alcançando, sobretudo, o primeiro

20 MIRAGEM, Bruno. **Direito do Consumidor**: fundamentos do direito do consumidor: direito material e processual do consumidor; proteção administrativa do consumidor; direito penal do consumidor. São Paulo: Editora Revista dos Tribunais, 2008. p. 123: "Na doutrina estrangeira, há os que dividem o dever de informar em dois momentos; o primeiro pré-contratual, e o segundo de natureza contratual. Existiriam, assim, uma obrigação pré-contratual de informação. A técnica do legislador brasileiro, ao estabelecer o direito básico à informação do consumidor e, deste modo, o dever de informar do fornecedor, parece mais abrangente. A violação do dever de informar, neste sentir, se dá em qualquer fase da relação entre consumidor e fornecedor, havendo ou não contrato e, mesmo, na fase pós-contratual. A violação do mesmo do dever de informar, neste sentido, configura violação de dever legal, e por tal razão, desde logo pode ser sancionado".

contato de uma relação de consumo - capítulo V do CDC: Práticas comerciais (oferta e publicidade), em que se visa a garantir uma assimilação correta do produto ou serviço para que o consumidor não seja enganado, podendo, ao final, praticar um "bom negócio".

Nesse sentido, o Código de Defesa do Consumidor rompe com a bipartição da responsabilidade civil (contratual e extracontratual), sendo, pois, um indicativo da prescindibilidade do contrato para emergir o dever-direito de informar.

A responsabilidade civil está estruturada num novo sistema plasmado pelo fato (artigos 12 a 14 do CDC) ou pelo vício do produto ou serviço (artigos 18 a 26 do CDC). Nesse cenário, aliás, a informação é um dos elementos de ambos os regimes, pois o fornecimento de uma informação inadequada ou insuficiente sobre a utilização ou os riscos do produto ou serviço pode resultar em um acidente de consumo: a quebra da legítima da expectativa de segurança (interpretação sistemática do *caput* e §1°, do artigo 12, do CDC); e, também, a informação inadequada e insuficiente pode acarretar um vício de qualidade ou quantidade do bem de consumo (artigos 18 a 20 do CDC).

Tal construção, portanto, reforça a ideia pretérita de que em todo e qualquer tipo de contato social estarão presentes os deveres anexos, notadamente o dever de informar desde o primeiro contato com o início do desenvolvimento de uma relação de consumo (capítulo V do CDC: Práticas comerciais - oferta, publicidade), até à própria proteção contratual do consumidor (Capítulo VI do CDC), e, por fim, o sistema de responsabilidade civil.

Tamanha é a importância da informação que se aduz que ela é um direito fundamental do consumidor, escapando do seu enquadramento dentre os deveres satelitários da boa-fé, sendo algo que compõe a própria licitude da atividade do fornecimento de produtos ou serviços.[21]

21 LÔBO. Paulo Luiz Netto. A informação como direito fundamental do consumidor. *In* **Coleção doutrinas essenciais do Direito do consumidor**: proteção da confiança e práticas comerciais; v. 3 / Claudia Lima Marques, Bruno Miragem organizadores. São →

Compreende-se, assim, por todo exposto, porque Eros Roberto Grau considera a transparência, e, por via reflexa, a informação como uma norma-objetivo[22] que se esparrama por toda a sistemática do CDC, demonstrando, dado esse aspecto central, a sua própria autonomia.

Tal foco, pode-se dizer dá-se pelo fato de que o microssistema jurídico consumerista parte do pressuposto de que a relação jurídica a ser regulada, as relações de consumo, já são *per si* perturbadas, isto é, desiguais, senão o próprio artigo 4°, inciso I, do CDC, não preceituaria a respeito do "reconhecimento da vulnerabilidade do consumidor no mercado de consumo".

Logo, nesse contexto, o fornecedor do bem de consumo possui, por sua própria expertise profissional, um conhecimento muito maior do que o consumidor, donde se constata um *deficit informacional*[23] que se procura equalizar.[24]

➔ Paulo: Revista dos Tribunais, 2011. p. 602:"Contudo, o dever de informar não é apenas a realização do princípio da boa-fé. Na evolução do direito do consumidor assumiu a feição cada vez mais objetiva, relacionado à atividade lícita de fornecimento de produtos e serviços. A teoria contratual também construiu a doutrina dos deveres anexos, deveres acessórios ou secundários ao da prestação principal, para enquadrar o dever de informar. O desenvolvimento do direito do consumidor foi além, transformando-o no correspectivo do direito à informação, como direito fundamental, e o elevando a condicionante e determinante do conteúdo da prestação principal do fornecedor. Não se trata apenas de dever anexo."

22 TOMASETTI JÚNIOR, Alcides. O objetivo da transparência e o regime jurídico dos deveres e riscos da informação nas declarações negociais para consumo. **Revista de Direito do Consumidor**. São Paulo: Revista dos Tribunais, n.4, p. 59, 1992. p. 59: "Um influente professor da faculdade de Direito da Universidade de São Paulo tem chamado a atenção para a importância prática do enquadramento no art. 4.° do Código de Proteção e Defesa do Consumidor na categoria por ele nomeada norma-objetivo, temática esta que vem ele elaborando em sucessivos trabalhos. A diferença específica da norma-objetivo verticaliza-se na sua particular eficácia teológica sobre o manejo de ordenamentos jurídicos."

23 MARQUES, Cláudia Lima. BENJAMIN, Antônio Herman V. MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2.010. p. 248: "O direito à informação, assegura igualdade material e formal (art. 5°, I e XXXII da CF/1988) para o consumidor frente ao fornecedor, pois o que caracteriza o consumidor é justamente seu deficit informacional, quanto ao produto e serviço, suas características, componentes e riscos e quanto a próprio contrato, no tempo e conteúdo."

24 MIRAGEM. Bruno. *Op. cit*. p. 123.

É, portanto, essa assimetria[25] de informações que revive a transposição da regra *caveat emptor*[26] (o devedor que se cuide ou se acautele) para a regra o *caveat venditor* (o vendedor que se cuide ou se acautele),[27] o que, decisivamente, foi acolhido pelo CDC.

Pretende-se, assim, estabelecer uma relação mais sincera e menos danoso entre consumidor e fornecedor de bens de consumo.[28]

Contudo, qual é essa informação, e, por conseguinte, a composição deste elemento para adimplir o dever de informar?

3.2. O Adimplemento do dever de informar: qual deve ser a composição de uma informação?

De início, buscando o significado linguístico, poder-se-ia dizer na sinonímia que informação é noticiar, fazer, dar conhecimento ou ciência e instruir.[29] Ou, como preceitua Cláudia Lima Marques, decompondo a palavra "informar é "dar" forma, é colocar (in) em

25 TOMASEVICIUS FILHO, Eduardo. **Informação assimétrica, custos de transação, princípio da boa-fé**. São Paulo: USP-SP, 2007. Tese (Doutorado), Universidade de São Paulo Faculdade de Direito. p. 308: "A doutrina em geral reconhece que uma das condições para que surja o dever de informar é a existência de informação assimétrica. Fabre-Magnan sustenta que o fundamento do dever de informar está desigualdade entre as partes. Para Llobet, a obrigação de informação encontra sua razão de ser no desequilíbrio de conhecimentos entre os contratantes, que pode ter duas causas: a própria técnica da formação de contrato, ou pelas circunstâncias."

26 LISBOA, Roberto Senise. **A obrigação de informar**. São Paulo: Almedina, 2012. p. 44.

27 TOMASEVICIUS FILHO, Eduardo. *Op. Cit*. p. 280: "Esta ideia foi sendo absorvida pelo incipiente *common law* em 1535 no julgamento de uma venda de um cavalo. O argumento suscitado para livrar o vendedor da responsabilidade era o de que não se podiam reduzir qualidades de cavalos a um modelo padrão. Por isso, cabia ao comprador tomar cuidado, isto é, *caveat venditor* ("o comprador que se cuide").

28 MARQUES, Cláudia Lima. **Contratos no código de defesa do consumidor:** o novo regime das relações contratuais. São Paulo: Editora Revista dos Tribunais, 2011. p. 745: "A ideia central é possibilitar uma aproximação e uma relação contratual mais sincera e menos danosa entre consumidor e fornecedor."

29 HOUAISS, Antônio. VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa**. Rio de janeiro: Objetiva, 2009. 1.082.

uma "forma", aquilo que um sabe ou deveria saber (o *expert*) e que o outro (leigo) ainda não sabe (o consumidor), donde se constata dois substratos iniciais para dissecar o objeto de análise - a informação.[30]

Se informar é "dar" *forma*. Logo, o pretenso ato de comunicação deve ser *ostensivo*, isto é, *perceptível* ao consumidor para que ele possa constatá-lo. Se a informação é o ato de levar ou de instruir, a forma como se inicia tal prática é de extrema relevância, sendo antecedente *natural* para a sua compreensão.

O segundo elemento é a *utilidade* da informação. Sob esse aspecto a informação deve se mostrar *imprevisível* e *original*[31] para, justamente, colmatar a exposta assimetria ou deficit informacional.

Ela deve *acrescer*, portanto, conhecimento ao consumidor, dispensando-lhe novos elementos para *racionalizar* as suas decisões, permitindo-lhe ter uma *perspectiva crítica*.[32]

Por isso, a informação não é, apenas, aproximação, mas, mediante essa apreensão crítica, ela possibilita ao leigo uma autoproteção.[33]

30 MARQUES, Cláudia Lima. et al. Comentários...*Op. Cit*. p. 249.

31 LISBOA, Roberto Senise. *Op. Cit*. p. 28: "O emitente deve buscar o equilíbrio ideal entre os elementos da mensagem, transmitindo a informação em um grau de originalidade e imprevisibilidade que, ao mesmo tempo, desperte a atenção do receptor e possibilite a sua compreensão. Agindo desta maneira, o emitente da informação terá maior êxito no processo comunicativo, podendo inclusive exercer legitimamente o convencimento necessário para que o destinatário adote a conduta dele esperada. A comunicação adequada e eficiente provoca a reação no destinatário da mensagem"

32 TOMASETTI JÚNIOR, Alcides. *Op. Cit*. p. 58: "O instrumento teorético denominado modelo supõe entretanto uma racionalização dos comportamentos, o que equivale a entender que exista uma certa possibilidade de previsão da realidade, mediante a apreensão crítica das constâncias de seus fenômenos e da repetição das relações estruturais correspondentes, de modo que, para além da previsão, haja também, embora ilimitadamente, possibilidade de interferência sobre a realidade mesma, com o objetivo de modifica-la."

33 BARBOSA, Fernanda Nunes. **Informação**: direito e dever nas relações de consumo. São Paulo: Revista dos Tribunais, 2008. p. 35: "Assim, poderíamos dizer, com os autores argentinos e a doutrinadora brasileira, que comunicar, no sentido que para nós interessará, significa uma aproximação, ao passo que informar, uma forma de proteção "

Assim, sob o ponto de vista do substancial (*qualitativo*), a informação deve *somar*, deve *acrescer*, deve preencher o vazio da assimetria ou do deficit informacional do consumidor, equalizando-o.

É óbvio, no entanto, que para o consumidor é impossível alcançar o patamar informativo do fornecedor. Até porque, para ele é desnecessário saber, por exemplo, como se dá o processo fabril, a concepção do produto ou mesmo a técnica da prestação de um serviço.

Dada a racionalidade limitada (*bounded rationality*) do ser humano,[34] o excesso de informação, também, desinforma (*overloaded information*),[35] razão pela qual a informação adequada[36] é aquela que permite ao consumidor saber das qualidades e características do bem de consumo, e, ainda, a sua utilização atenta aos riscos que lhe pode sobrevir.

Verifica-se, dessarte, que a quantidade de informações pode prejudicar a qualidade da informação transmitida. Contudo, tais critérios não se confundem, ainda que haja um ponto de contato entre eles.

34 MARZAGÃO, Nelcina C. de O. Tropardi. **Da informação e dos efeitos do excesso de informação no direito do consumidor**. São Paulo: USP-SP, 2005. Tese (Doutorado em Direito), Universidade de São Paulo Faculdade de Direito. p. 198: "Para responder tais questões, precisamos analisar a capacidade humana de armazenar e processar informações. Para tanto, diversos autores utilizam o conceito de *bounded rationality*, que traduz a noção de racionalidade limitada e postula que os indivíduos não têm capacidade para receber, armazenar e processar grande volume de informações."

35 MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. *In* **Coleção doutrinas essenciais de Responsabilidade civil**: direito à informação; v. 8 / Nelson Nery Júnior. Rosa Maria de Andrade Nery (organizadores). São Paulo: Revista dos Tribunais, 2010. p. 27: "Estudos sobre o conceito de racionalidade limitada (*bounded rationality*) e sobrecarga de informação (*overloaded information*), têm evidenciado que a equação: maior informação = maior capacidade de decisão consciente (e, portanto, livre) frequentemente não corresponde à realidade"

36 LÔBO. Paulo Luiz Netto. *Op. Cit*. p. 603: "A adequação diz com os meios de informação utilizados e com o respectivo conteúdo. Os meios devem ser compatíveis com o produto ou o serviço determinado e com o consumidor destinatário típico. Os signos empregados (imagens, palavras, sons) devem ser claros e precisos, estimulantes do conhecimento e da compreensão. No caso de produtos, a informação deve referir à composição, aos riscos, à periculosidade."

Pode-se dizer, retomando, o que já foi dito, que o critério qualitativo se liga à ideia de uma informação original e imprevisível que equaliza a disparidade informacional entre consumidor e fornecedor.

A posteriori, deve-se conectar - num *segundo plano* - a *quantidade* de informações transmitidas, se suficientes[37] ou não para revelar ao consumidor um conteúdo para uma apreensão crítica. Não adianta atentá-lo sobre algo que lhe é útil, se o conteúdo informativo não é completo suficiente para nela desencadear uma compreensão completa, e, por último, racionalizar uma tomada de decisão - poder de decisão.

Percorrida toda essa composição da informação, pode-se concluir que informar não é, apenas, uma aproximação, deve-se, efetivamente, alcançar um *diálogo* que elimine qualquer tipo de opacidade e obscuridade, daí porque a transparência lhe é um valor consecutivo: o resultado ótimo/esperado do dever de informar.

Em síntese, o preenchimento de tais substratos da informação deve resultar, necessariamente, nesse resultado ótimo: a transparência, sob pena do consumidor não ter satisfeito tal direito. Tamanha é a correspondência entre a informação e transparência que se poderia afirmar que são irmãs siamesas, pois uma depende da outra para a respectiva completude.

Com base ao que foi exposto, constrói-se um quadro sintético, em escala progressiva, para decompor o dever de informar, e, por

37 Ibidem. p. 604: "A suficiência relaciona-se com a completude e integralidade da informação. Antes do advento do direito do consumidor, era comum a omissão, a precariedade, a lacuna, quase sempre intencionais, relativamente a dados ou referências não vantajosas ao produto ou serviço. A ausência de informação sobre prazo de validade de um produto alimentício, por exemplo, gera confiança no consumidor de que possa ainda ser consumido, enquanto a informação suficiente permite-lhe escolher aquele que seja de fabricação mais recente. Situação amplamente divulgada pela imprensa mundial foi a das indústrias de tabaco que sonegaram informação, de seu domínio, acerca dos danos à saúde dos consumidores. Insuficiente é, também, a informação que reduz, de modo proposital."

conseguinte, o seu adimplemento: a transparência que revela o seu caráter de eficiência.[38]

Formal	Perceptível/Compreensiva (CDC: ostensiva/clara)
Qualitativo	Original/Imprevisível (preencher o deficit/assimetria informacional) (CDC: Adequada/Inadequada)
Quantitativo	Completude/Incompleta - Racionalidade Limitada, Excesso de informações (suficiência/Insuficiência)
Resultado	Eficiência/Deficiência (Transparência): apreensão crítica/racionalização das decisões

À guisa de conclusão, o dever-direito de informação traduz-se na igualdade material entre consumidor e fornecedor sob o ponto de vista da *vulnerabilidade informacional*, propiciando ao elo mais fraco (consumidor) elementos suficientes para que tenha uma percepção crítica, desde o próprio ato de consumo, como, igualmente, a utilização do próprio bem de consumo, desenvolvendo o seu poder de tomada de decisão (racionalização), concretizando a tônica de prevenção de danos, já que fazer um mau negócio e/ou a utilização errônea de um bem de consumo acarreta-lhe, invariavelmente, danos.

38 TOMASETTI JÚNIOR, Alcides. *Op. Cit.* p. 58: "O modelo de transparência implica não só a difusão da informação, mas também a eficiência da mensagem informativa. Pode, dizer-se eficiente a informação que enseja de maneira apropriada (total ou altamente satisfatório) a consecução do objetivo de transparência, propiciando ao consumidor atuar segundo a ponderação e a ordenação das cinco variáveis de racionalidade comportamental consideradas, aqui, modelarmente decisivas para a implantação da Política Nacional das relações de Consumo em direção à qual avança a Lei 8.078, de 11.9.90."

4. BREVES NOTAS SOBRE A SOCIEDADE DA INFORMAÇÃO: O MERCADO INFORMACIONAL E A PRIVACIDADE DO CONSUMIDOR

É indubitável que há hoje uma nova textura social decorrente das recentes evoluções tecnológicas advinda, notadamente, da *internet*[39] que propiciou uma capacidade e velocidade (antes jamais imagináveis) de se processar e armazenar informações.

Trata-se da denominada *sociedade da informação*, na qual a informação assume papel de bem econômico[40] e elemento estruturante para o desenvolvimento das relações sociais, sendo, pois, o signo maior desta anunciada e consolidada revolução socioeconômica.

No que concerne ao primeiro aspecto - *bem econômico* -, fala-se em "mercado de informação",[41] "economia da informação",[42] economia informacional ou "capital-informação",[43] pois o novo paradigma tecno-econômico[44] da tecnologia da informação rompe com o modelo fordista, cujos fatores de produção eram máquinas e materiais. Inaugura-se um novo padrão econômico, sobretudo um novo fator de produção, que é, justamente, a famigerada informação que passa a ser o *meio dominante* para o tráfego econômico.

39 CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 7.

40 MURRAY, Andrew. **Information tecnology law**. Oxford: Oxford University Press, 2010. p.4.

41 GONÇALVES, Maria Eduarda. **Direito da Informação**. Coimbra: Almedina, 2003. p. 129.

42 BRAMAN, Sandra. A economia representacional e o regime global da política da informação. *In* **Informação, conhecimento e poder**: mudança e inovação social. Org. MACIEL, Maria Lucia; ALBAGAJI, Sarita. Rio de Janeiro: Garamound, 2011. p. 47.

43 DANTAS, Marcos. **A lógica do capital-informação**: a fragmentação dos monopólios e a monopolização dos fragmentos num mundo de comunicações globais. p. 144.

44 LASTRES, Helena Maria Martins; FERRAZ, João Carlos. Economia da Informação, do conhecimento e do aprendizado. *In* **Informação e globalização na era do conhecimento**. Org. LASTRES, Helena M. M.; ALBAGAJI, Sarita. Rio de Janeiro: Campus, 1999. p. 47.

Com efeito, numa sociedade globalizada e voltada para o consumo, o manejo de *informações estratégicas* é o que determina o modelo organizacional dos atores no cenário econômico, estabelecendo-se uma *comunicação produtiva* que *precifica* e *monetiza* a informação, circundando quiçá o próprio comportamento dos consumidores em esfera global.[45]

Mais do que isso, a rede global de conexões permite que consumidores disseminem suas opiniões sobre determinados produtos ou serviços, de tal modo que são os próprios destinatários finais que definem o bem de consumo, confirmando, destarte, a caracterização da informação como um bem econômico em sede das relações de consumo.

Atenta-se, outrossim, que a informação, como um bem econômico, perpassa não só o valor social da informação, analisada sob o ponto vista comportamental do consumo, como, também, a própria transformação das pessoas (consumidores) em mercadorias, utilizando-se aqui da expressão de Zygmunt Bauman,[46] haja vista a prática notória de comercialização[47] dos dados pessoais dos consumidores.[48]

45 MATTOS, Karla Cristina da Costa e Silva. **O valor econômico da informação nas relações de consumo**. São Paulo: Almedina, 2012. p. 147.

46 BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

47 Os dados pessoais estão, efetivamente, monetizados, consistindo na moeda de troca - o *tradeoff* - da maioria dos modelos de negócio na internet, os quais são rentabilizados pela publicidade direcionada que se vale, justamente, das informações pessoais dos usuários para lhes direcionarem anúncios publicitários. É, portanto, o caráter econômico das informações pessoais dos usuários que soluciona a equação econômica dos bens de consumo em meio a sociedade da informação, remunerando-os indiretamente. Nesse sentido, aprofundando tal questão: CUSUMANO, Michael A. GOELDI, Andreas. New Businesses and new business models. *In* **The oxford handbook of internet studies**. William H. Dutton (Organizador). United Kingdom: Oxford University Press, 2012. p. 252; STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect (October 1, 2013). 2013. **NYU School of Law, Public Law Research Paper** No. 13-62; NYU Law and Economics Research Paper No. 13-34. p. 163.

48 Veja a capa da revista Veja, edição 2321 - ano 46 - n° 20: "**Entenda o que é Big Data:** o megafenômeno digital que transforma em riqueza dados pessoais, posts, tuítes, e-mails e até cliques". p. 71-81.

Com efeito, quando os dados estão atrelados a um sujeito de titular de direitos, eles representam uma parcela da individualidade daquele, passando, portanto, a compor a sua própria privacidade, e, por conseguinte, um atributo dos direitos da personalidade.[49]

Por isso, que a privacidade sob o ponto de vista de ser deixado sozinho (*right to be alone*) e salvo de interferências alheias não satisfaz mais a proteção dos direitos da personalidade em meio a denominada sociedade da informação, o que reclama uma tutela dinâmica[50] ou plural[51] atinente ao "controle da coleta e da utilização dos próprios dados pessoais".[52]

Como bem definiu Stefano Rodotà, a privacidade antes estabelecida pelo eixo "pessoa-informação-segredo" passa, agora, a outro: "pessoa-informação-circulação-controle",[53] consistindo, pois, numa *liberdade positiva*: controle sobre as informações pessoais.

Como bem atenta Anderson Schreiber, o destino de uma pessoa pode ser decidido com base em seus dados pessoais coletados na *internet*, podendo ser eliminada de um certo processo seletivo por conta da sua opção política, partidária, religiosa ou das mais variáveis.[54]

49 CATALA, Pierre, "Ebauche d´une théorie juridique de l´information", p. 20, *apud* DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Saraiva, 2006. p. 157: " Mesmo que a pessoa em questão não seja a ´autora´ da informação, no sentido de sua concepção, ele é titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um direito da personalidade".

50 RODATÀ, Stefano. **A vida na sociedade da vigilância**. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 17: "Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece regras sobre os mecanismos de processamento de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas - i.e. é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos."

51 LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p. 78-90.

52 SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011. p. 131.

53 RODOTÀ (2008). *Op. Cit*. p. 93

54 SCHREIBER, Anderson. *Op. Cit*. p. 132.

Ou, como prefere Daniel J. Solove, há uma verdadeira biografia digital, um verdadeiro dossiê mais abrangente ou redutor de nossa personalidade.[55]

Fato é que esse fluxo de dados pode repercutir das mais variadas formas, impedindo-nos de entrar em um determinado país ou tomar um avião por conta de nossos hábitos alimentares ou outros dados pessoais que conformariam um estereótipo de um terrorista,[56] o risco de um tomador de crédito ser inadimplente para calibrar o processo de concessão ou não do mútuo;[57] ou, ainda, quais os segurados que tendem a ter maiores riscos ao seus respectivos estados saúde para daí aumentar o pagamento do prêmio.[58]

Assim, verifica-se um claro embate entre o anunciado mercado informacional e os direitos da personalidade, especialmente, o direito à privacidade dos consumidores, cuja solução passa, necessariamente, pelo dever de informar funcionalizando aquilo que se convencionou a chamar de autodeterminação informacional.

55 SOLOVE, Daniel J. **The digital Person**: technology and privacy in the information age. New York: New York University Press, 2004. p. 46.

56 Faz-se referência à troca de dados pessoais de passageiros aéreos entre União Europeia e Estados Unidos sob o fundamento de que se combateria o terrorismo (*Passager Name Record*). A reportagem na íntegra está disponível em: http://www.migalhas.com/mostra_noticia.aspx?op=true&cod=154037 (acesso em 14/04/2013).

57 World Economic Forum. **Big data, big impact**: new possibilities for international development. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigData BigImpact_Briefing_2012.pdf>. Acesso em 08 de março de 2014.

58 MAYER-SCHONEBERGER, Viktor. CUKIER, Kenneth. **Big Data**: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013. p. 160.

5. O DEVER/DIREITO DE INFORMAÇÃO COMO ELEMENTO DE FUNCIONALIZAÇÃO DA AUTODETERMINAÇÃO INFORMACIONAL E A TEORIA DO DIÁLOGO DAS FONTES PARA A NORMATIZAÇÃO DE UM SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO VIGENTE

A *autodeterminação informacional*[59] pode se apresentar como resposta para solucionar tal problemática, devendo toda a acumulação, transmissão, modificação e cancelamento de dados ser orientada pelo dever informacional, tal como por um *consentimento gradual*, empregando, assim, maior aplicabilidade ao artigo 43 do Código de Defesa do Consumidor,[60] frente ao exposto *fluxo informativo* que é inerente à realidade atual.

59 A autodeterminação informacional consiste, em suma, na perspectiva de que o indivíduo deve controlar (autodeterminar) os seus dados pessoais (informações pessoais: autodeterminação informacional), exigindo-se, por isso, o consentimento do titular das informações pessoais para que elas sejam coletadas, processadas e compartilhadas. A terminologia surgiu no julgamento paradigmático do Tribunal Constitucional Alemão, em 1983, que considerou, parcialmente, inconstitucional a lei de recenseamento que não delimitava a finalidade para a qual os dados pessoais dos cidadãos seriam utilizados, permitindo-se, ainda, o seu cruzamento com dados de registros públicos e a sua transferência para outras unidades da administração pública, esvaziando, assim, qualquer perspectiva de controle por parte dos cidadãos sob seus dados pessoais. O julgado está traduzido na obra: MARTINS, Leonardo. **Introdução à jurisprudência do Tribunal Constitucional Federal Alemão**. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.Organização e introdução: Leonardo Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005. p. 233-245.

60 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil →

A questão, contudo, que assola e desafia a solução proposta, cinge-se à maneira pela qual se deve propiciar, ao menos, o indigitado controle dos dados pessoais.

Desta feita, sobrevém o dever-direito informacional a ser abordado, ontologicamente, como uma escala necessária para um processo de *interação* que efetive o controle espacial, contextual e temporal dos dados pessoais.[61]

Em outros termos, deve haver uma *tutela dinâmica*, pela qual a fluidez do ambiente eletrônico não deixe para "trás" o sujeito de direitos da personalidade a que estão atrelados os dados pessoais, seguindo-se os dados em todos os seus movimentos.[62] Tal sujeito deve determinar, repita-se, em quais locais (espacial), para qual finalidade (contexto) e em que momento (temporal) tais informações serão utilizadas.

Para tanto é necessário, como parecer ser até intuitivo, instaurar um *processo comunicativo* entre o detentor do banco de dados

➔ compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor. § 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. § 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.

61 Enunciado 404 da V Jornada de Direito Civil do Conselho da Justiça Federal: "A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas."

62 RODOTÁ, Stefano. *Op. Cit*. p. 17: "um tipo de proteção dinâmica, que segue o dado em todos os seus movimentos".

e a pessoa estigmatizada, revelando-se a informação, novamente, como a pedra de toque para o enredo proposto. É a informação, como dito, a premissa para tal relação intersubjetiva, eis que, é ela (a informação) que emprega forma e conteúdo à troca das mensagens necessárias para tal interação.

Nesse sentido, a própria Lei do Cadastro positivo estabelece tal conexão entre o controle dos dados pessoais acoplado ao dever de informar, quando pontua, em seu artigo 4°,[63] que a abertura do cadastro (entenda-se a coleta dos dados) exige consentimento informado.[64]

Nessa mesma toada, o Marco Civil da Internet, lei sancionada pela presidente Dilma Rousseff no evento de governança mundial da internet NetMundial,[65] também se vale do termo "consentimento informado"[66] para que os dados pessoais dos usuários possam ser coletados, transmitidos e processados em sentido amplo.

Vale dizer, é a prestação da dita informação que cientificará seu receptor, *in casu* aquele afetado pelo fluxo informativo, a respeito

63 "Art. 4° A abertura de cadastro requer autorização prévia do potencial cadastrado mediante *consentimento informado* por meio de assinatura em instrumento específico ou em cláusula apartada." (destaque)

64 Em sentido análogo acenando para o diálogo das fontes entre CDC e a Lei do Cadastro Positivo: BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12,414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011. p 101-102: "O principal aspecto do consentimento decorre do adjetivo *informado*. Como já adiantado, essa característica diz respeito ao farto fornecimento de informações ao consumidor por ocasião da manifestação do consentimento." Nesse mesmo sentido: COSTA, Carlos Celso Orcesi. **Cadastro positivo**: lei n. 12.414/2011. São Paulo: Saraiva, 2012. p.145.

65 **Dilma sanciona Marco Civil na abertura do NETMundial**. Disponível em: <http://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml>. Acesso em 23 de abril de 2014.

66 "Artigo 7°, inciso VII: ao não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante *consentimento livre, expresso e informado* ou nas hipóteses previstas em lei; inciso VIII – a *informações claras e completas* sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justificaram sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços. inciso IX – ao *consentimento expresso* sobre a coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais." (destaque)

da mera possibilidade de controlar seus dados pessoais, o que perpassa desde o ato inaugural de coleta dos dados (dimensão procedimental) até a sua destinação, eliminação e/ou retificação (dimensão substancial).[67]

Assim, na dimensão procedimental toda e qualquer ferramenta tecnológica utilizada para a coleta de dados deve ser cientificado ao consumidor.

No caso, por exemplo, dos *cookies* que são programas instalados no navegador do usuário, identificando-o toda vez que ele acessa a internet para registrar todo o seu comportamento na rede (sites visitados, termos de busca e etc). Eles devem ser, necessariamente, comunicados ao consumidor para que ele possa optar, *ab initio*, pela ativação ou não de tal ferramenta para a coleta de seus dados.[68]

De igual forma, as chamadas etiquetas de pixels se encontram num *web site* ou, até mesmo, em e-mails para registrar os passos do usuário na rede.

Seja qual for a ferramenta utilizada para a coleta de dados, deve-se cientificar o consumidor/usuário da sua existência, permitindo-lhe expressar seu consentimento quanto à prática ou não de tal atividade.

Por isso, mostra-se adequado para um tratamento geral da matéria, o denominado sistema *opt-in* pelo qual não se deve haver a coleta de dados sem o consentimento do indivíduo. Ao contrário, do sistema *opt-out* pelo qual a coleta de dados ocorre já de início, independentemente, de consentimento, devendo o consumidor

67 SCHREIBER, Anderson. *Op. Cit*. p. 132/134.

68 MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. São Paulo: Revista dos Tribunais, 2008. p. 231; CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *In* **Coleção doutrinas essenciais do Direito do consumidor**: proteção da confiança e práticas comerciais; v. 3 / Claudia Lima Marques, Bruno Miragem organizadores. São Paulo: Revista dos Tribunais, 2011. p. 951-952.

para barrá-la fazer uma escolha, *a posteriori*, a de estar fora do coletamento.[69]

Nesse sentido, a Diretiva da União Europeia 2002/58 prevê, expressamente, em seu artigo 5.3,[70] que o armazenamento de informações só é legítimo, após o usuário ter sido informado de maneira clara e adequada a seu respeito. Aliás, o debate que se instaurou a respeito da aplicação/interpretação de tal dispositivo é, justamente, se o usuário deveria consentir expressamente em torno da coleta de seus dados pessoais, ou, se, por outro lado, a própria utilização de um navegador (*browser*), cuja configuração permitiria a instalação de *cookies* externaria um consentimento válido para tal prática.[71]

Nesse contexto, veja-se a importância da teorização dedicada ao dever-direito de informação (vide: item 3.2), pois ao se considerar que a informação deve ser prestada de maneira ostensiva, causando uma reação ao seu destinatário para que ele possa racionalizar uma decisão, é clarividente que tal situação não alerta, cientifica ou comunica o usuário sobre a coleta de seus dados pessoais, não se superando sequer o *aspecto formal* para a prestação de uma

69 Em apertada síntese, o sistema *opt-in* exige, para que sejam coletados, armazenados e transmitidos dados, tal como para o próprio envio de mensagens de marketing, a expressa e prévia autorização do usuário. Ao passo que, o sistema *opt-out* prescinde de qualquer tipo de consentimento para tais práticas. TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions. **Rev. Online. Stanford**, n° 63. fev, 2012. p. 68.

70 "Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario."

71 Resumindo os argumentos favoráveis e desfavoráveis sobre a (i)legalidade do consentimento implícito para a coleta de dados, mediante a simples atividade do usuário/consumidor navegar por um determinado tipo de browser: BORGESIUS, Frederick Zuiderveen. Segmentação comportamental: *Do not track* e o desenvolvimento jurídico europeu e holandês. **Revista Politics**. Publicação Núcleo de Pesquisas e Estudo de Formação/NUPEF. N° 14, fevereiro de 2013. p. 09-22.

informação. A possibilidade de o usuário barrar ou não a coleta de seus dados pessoais deve ganhar forma, mostrando-se perceptível, sob pena de não contar com o consentimento informado.

Esta é, sem dúvida, a opção do legislador consumerista ao pontuar, em seu artigo 42, §3°, do CDC, que para a "abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicado por escrito ao consumidor, quando não solicitado por ele".

A *mens legis* alcança, por certo, o ato inicial que viabiliza o banco de dados, qual seja, a coleta de dados, concluindo-se pela imprescindibilidade do consumidor em optar por sua abertura, sendo que, em seu silêncio, inviabilizado estará a coleta de dados.

Num segundo momento, após a viabilização da coleta de dados, surge a *tutela substancial* do controle de dados que se estreita pelas seguintes garantias.

Primeiro, o conhecimento sob qual contexto dar-se-á a utilização dos dados coletados. Não basta informar a respeito da coleta de dados, dever-se propiciar ao consumidor o conhecimento da finalidade para a qual eles serão utilizados, vedando-se a sua utilização para propósitos outros que aqueles informados, como estabelecem a Lei do Cadastro Positivo[72], o Marco Civil da Internet[73], e os Decretos n°s 6.135/2007,[74] 6.245/2008[75] e 6523/2008.[76]

72 Artigo 5°, inciso VII, da Lei n° 12.414/2011 (Lei do Cadastro Positivo): "ter os seus dados pessoais utilizados somente de acordo com a *finalidade* para a qual eles foram coletados". (destaque)

73 Artigo 7°, inciso VIII – *a informações claras e completas* sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para *finalidades* que: a) justificaram sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços." (destaque)

74 "Art. 8° Os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes *finalidades*:§ 1° São vedadas a cessão e a utilização dos dados do CadÚnico com o objetivo de contatar as famílias para qualquer *outro fim que não aqueles indicados neste artigo*." (destaque)

75 "Art. 6° Ficam assegurados o sigilo e a proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para *fins estranhos aos previstos na legislação educacional aplicável.*" (destaque)

76 "Art. 11. Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados *exclusivamente para os fins do atendimento*." (destaque)

Trata-se do denominado *princípio da especificação dos propósitos* pelo qual qualquer mudança de finalidade deve contar com a autorização do consumidor. Por isso, se o indivíduo fornece seus dados no comércio eletrônico para a compra e a consecutiva entrega de um produto, tais dados devem se restringir à base de dados daquele fornecedor e, tão somente, para a apontada finalidade.[77]

Logo, deve ser considerada abusiva eventual cláusula de política de privacidade e termos de uso de uma determinada aplicação na internet que estipula, genericamente, como seriam utilizados os dados pessoais dos seus usuários, colocando o consumidor em uma situação de extrema desvantagem, gerando para ele uma situação de iniquidade que restringe o seu direito à proteção de seus dados pessoais (artigo 51, inciso IV e §1°, inciso II, ambos do CDC).

Ad secundus, advoga-se pela implementação de uma interpretação extensiva do artigo 43, §2, do CDC, assim como faz Antônio Herman Benjamim,[78] pela qual o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados do indivíduo, possibilitando-lhe acompanhar de *forma dinâmica* o fluxo de seus dados.

Se há o acréscimo ou a retificação de um novo dado, a subtração, a *transferência* e/ou compartilhamentos dos dados deve-se contar sempre com a anuência do consumidor, obtendo-se, assim, uma espécie de *consentimento gradual*, espaçado no tempo, para conformar a famigerada *tutela dinâmica* de controle dos dados pessoais.

77 A proteção de dados pessoais nas relações de consumo: para além da informação creditícia/Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. p. 46.

78 BENJAMIN, Antônio Herman de Vasconcellos e Benjamin. **Código brasileiro de defesa do consumidor**: comentado pelos autores do anteprojeto. vol. 1. Direito material (arts. 1° a 80° e 105 a 108.) Rio de janeiro: Forense, 2011. p. 476: "Daí que, cada vez que o arquivo de consumo recebe dado que significa inovação, se se quer incorporá-la precisa informar o consumidor. Vale dizer, o direito à comunicação não se exaure num momento específico e inicial da vida do arquivo de consumo, mas se protrai no tempo, enquanto este permanecer."

Nesse sentido, o Marco Civil da Internet exige que a transferência dos dados pessoais para terceiros seja precedida de "consentimento livre, expresso e informado"[79], aperfeiçoando-se o conceito de autodeterminação informacional como o direito de o usuário ter controle sobre todos os *movimentos* de seus dados pessoais.

Prosseguindo, sob uma outra vertente, deve-se considerar um de prazo de validade dos dados fornecidos, à espécie do que preceitua o artigo 43, §1°, do CDC, a fim de não legitimar uma *autorização eterna* para que a pessoa seja estigmatizada.[80] Aqui, na verdade, defende-se, aliás, pela exclusão de dados tidos como negativos ou positivos, cabendo, inclusive, ao consumidor identificá-los como tais, até porque estamos a tratar de direito da personalidade, de modo que o titular, melhor do que ninguém, sabe quais informações podem afetar o livre desenvolvimento de sua personalidade.

Por isso mesmo, o consentimento será sempre passível de revogação,[81] pois não se está a tratar de direitos da propriedade, mas, ao revés, de direitos da personalidade, o que, como dito, dada a sua própria indisponibilidade (art. 12 do CC) torna inequívoca a ilegalidade de uma devassa perpétua de tal esfera do indivíduo.

79 "Artigo 7°, inciso VII – *ao não fornecimento a terceiros de seus dados pessoais*, inclusive registros de conexão, e de acesso a aplicações de Internet, *salvo mediante consentimento livre, expresso e informado* ou nas hipóteses previstas em lei;" (destaque).

80 O Marco Civil da Interne (Lei 12.965/2014) prevê a possibilidade do usuário solicitar a exclusão definitiva de seus dados junto ao provedores de aplicação: "Art. 7°, inciso X: exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;"

81 DONEDA, Danilo. Da privacidade... *Op. Cit*. p. 380: "A ideia de revogabilidade incondicional deste tipo de consentimento encontra fundamento no fato de que se está protegendo a própria personalidade, entre cujos atributos estaria a indisponibilidade. Neste ponto de vista, o consentimento será sempre revogável, e a sua caracterização como ato jurídico unilateral serve a reforçar essa revogabilidade. (...)Examinando a natureza do instituto e dos interesses em questão, deve-se reconhecer a possibilidade de revogação do ato pelo qual uma pessoa consente no tratamento de seus dados pessoais. Neste poder do sujeito, encontra-se o próprio sentido de autodeterminação em relação à construção de sua esfera privada, poder este que, ligado ao livre desenvolvimento da personalidade, merece a tutela do ordenamento."

Por último, deve-se possibilitar ao usuário o livre acesso às informações sobre ele coletadas, isto é, ao banco de dados para que ele possa, eventualmente, solicitar a sua correção, e, como dito acima, até mesmo a exclusão de alguns dados, assegurando-se a sua exatidão/qualidade como já previsto nas leis e decretos supracitados.[82]

Verifica-se, por todo o exposto, que o dever de informação funcionaliza a autodeterminação informacional/informativa, já que é necessário empregar uma *comunicação adequada*, na qual a informação prestada seja *eficiente* para tal desiderato, não só cientificando seu receptor da sua faculdade de autodeterminação informacional, mas, principalmente, como, em sede do ambiente eletrônico, fazer uso de tal *funcionalidade*.

Por isso, os prestadores de serviços na internet devem estabelecer o supracitado diálogo, e, acima de tudo, moldar a *arquitetura da internet*[83] para esse fim último. O exemplo supracitado de que os próprios navegadores não deveriam ter uma configuração padrão para permitir a coleta, mas, ao revés, serem formatados para que seu usuário consentisse, expressamente, sobre a possibilidade de se rastrear a sua navegação, é um clara amostra como o dever-direito de informação (o direito) pode ser efetivado pela própria tecnologia (arquitetura da rede).

Em outros termos, não se deve prever, apenas, o controle sobre os dados pessoais, sem, antes, pensar e compreender como a informação a respeito de tal direito será entregue[84] ao

82 Trata-se dos princípios do livre acesso e qualidade/exatidão dos dados: Artigo 43, *caput* e §3°, do CDC; Artigo 4°, *caput*, da Lei do Habeas Data; Artigo 3° do Decreto 6.425/2008; Artigo 8°, §3° e 16 ambos do Decreto 6.523/2008.

83 Faz-se uma clara alusão ao referencial teórico de Lawrence Lessig para quem o direito e a tecnologia (arquitetura da rede) podem ser combinados, não excluindo um ao outro para a regulação da internet. LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

84 Nesse sentido, Ryan Calo, pesquisador e professor do Centro de Tecnologia e Sociedade de Stanford, considera a imprescindibilidade de causar uma reação efetiva sobre o usuário da internet para que ele, efetivamente, externe a sua escolha/consentimento sobre →

consumidor/usuário para que ele, efetivamente, possa autodeterminar as suas informações pessoais, sob pena de torná-la utópica.

Políticas de privacidade e termos de uso com textos logos e poucos claros não transmitem, na maioria das vezes, uma mensagem adequada para que o consumidor seja cientificado a respeito do fluxo dos seus dados pessoais. Ao revés, acaba por desinformá-los, trazendo ainda maior opacidade e assimetria de informações, desconsiderando, pois, o resultado ótimo/esperado de transparência que tal canal de comunicação deveria propiciar.

Deve-se reconhecer, como já exposto em todo o trabalho, a vulnerabilidade (informacional) do consumidor, e, com isso, com base nas ideias de Daniel J. Solove, dispor a rede de modo tal que permita ao usuário ter acesso a todas essas funcionalidades propostas para o controle de seus dados (*arquitetura de vulnerabilidade da internet*).[85]

Percebe-se, portanto, que a informação avoca, antes de qualquer coisa, um papel que precede a autodeterminação informacional. Com efeito, trata-se de elemento que *contorna* o exercício de tal direito, circundando a própria *racionalização* da autodeterminação informacional.

Conclui-se que a autodeterminação informacional já se encontra abraçada pelo ordenamento jurídico vigente, especialmente, pelo dever de informar e o princípio da transparência que oxigenam o artigo 43 do CDC, tal como mediante a aplicação da teoria do diálogo das fontes das normas legais e infralegais que

→ o trânsito de seus dados pessoais, tendo denominado tal tipo de abordagem como "*visceral consent*": CALO, Ryan,. Against notice skepticism in privacy (and elsewhere). *In* **Notre Dame law review**, vol. 87:3, march, 2011. p. 1.046. "The goal of visceral privacy notice, then, should be to create awareness of data collection and other relevant issues and realities, rather than to stop consumers from disclosing per se. In other words, the goal of notice is not to manipulate preferences but to give consumers the information they need to act upon preferences. (...)Clever design can indeed leverage psychological predispositions to change an individual's mental model, or basic understanding, of a product or situation"

85 SOLOVE, Daniel J. *Op. cit*. p. 100.

sistematizam o direito ao controle das informações pessoais, acrescentando importantes normas que conformam o exercício de tal direito, especialmente princípios tais como: i) o da especificação dos propósitos, ii) consentimento para coleta e tráfego dos dados pessoais e iii) o acesso e qualidade dos dados.

Elaborada por Erik Jayme e trazida ao Brasil por Cláudia Marques, a teoria do diálogo das fontes[86] indica, como a própria terminologia induz, a uma intersecção e complementação das normas que não mais estanques[87] passam a convergir, afastando-se, por completo, de uma monossolução para uma lógica de *coordenação*, isto é, de um verdadeiro diálogo.[88]

E, sendo assim, tal teoria revelar-se-á muito útil como uma teoria geral de direito[89] para preencher a lacuna[90] derivada da inexistência de uma lei geral de proteção de dados pessoais,

86 A doutrina do diálogo das fontes é de autoria da Erik Jayme, tendo sido "nacionalizada" pela professora Cláudia Lima Marques. Em apertada síntese, tal doutrina, ciente do cenário pós-moderno em que há "fontes legislativas plúrimas", desvencilha-se do método tradicional do conflito aparente de leis, que, por exemplo, pelo critério da especialidade ou da anterioridade resulta na prevalência de uma sobre a outra com a sua consequente exclusão. Ao revés, tal teoria procura compatibilizar ou harmonizar tal explosão normativa, por meio de uma aplicação simultânea das leis, mediante uma influência recíproca, havendo, por isso, daí a terminologia, um diálogo porque as leis não se repelem, aproximam-se por meio de tal premissa hermeneuta. (MARQUES, Cláudia Lima. BENJAMIN, Antônio Herman V. MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2.010. p. 30-32)

87 MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo a Erik Jayme. *In* **Diálogo das Fontes**. Cláudia Lima Marques, coordenação. São Paulo: Revista dos Tribunais, 2012. p. 25.

88 Ibidem. p. 26-27: "A bela expressão do mestre Heidelberg é semiótica e autoexplicativa: direito-a-logos, duas "lógicas",duas "leis" a seguir e coordenar um só encontro no "a", um "coerência" necessariamente "a restaurar" os valores deste sistema desta "nova" ordem de fontes, em que uma não mais "revoga" a outra (o que seria um monólogo, pois só uma lei fala), e, sim, dialogam ambas as fontes, em um aplicação conjunta e harmoniosa guiada pelos valores constitucionais e, hoje, em especial, pela luz dos direitos humanos. (...) Erik Jayme alerta, porém, que os tempos pós-modernos não mais permitem este tipo de clareza e "monossolução", sequer a hierarquia dessas leis é clara, mas apenas dos valores constitucionais."

89 Ibidem. p. 21.

90 MIRAGEM, Bruno. Eppur si muove: Diálogo das fontes como método de interpretação sistemática no direito brasileiro. *In* **Diálogo das Fontes**. Cláudia Lima Marques, coordenação. São Paulo: Revista dos Tribunais, 2012. p. 70.

permitindo-se, ao menos, coordenar a supracitada tutela periférica e desorganizada.

Nesse sentido, dentre os diálogos possíveis,[91] destaca-se o diálogo de complementariedade e subsidiariedade que permitirá coordenar toda a citada *proteção fragmentada* e dispersa da proteção dos dados pessoais para que se alcance uma *resposta normativa* mais *unitária* para tal desafio da sociedade da informação.

A título de exemplo será, como visto, o diálogo das fontes entre as normas legais e infralegais que preveem o princípio da especificação dos propósitos, somado ao dever de informação e a proteção contratual do consumidor que acarretará a abusividade de políticas e termos de privacidade que nada especificam sobre a coleta, utilização e processamento dos dados pessoais, colocando o consumidor em uma situação de extrema desvantagem, esvaziando o seu direito de controlar o fluxo de seus dados pessoais.

Em caso de inexistência de uma lei específica (uma lei geral de proteção de dados pessoais) para normatizar tal fato social, tal diálogo mostra-se de suma relevância para extrair de todos os dispositivos do ordenamento jurídico vigente uma proteção mais ampla e sistematizada possível ao consumidor, protegendo, assim, tal sujeito vulnerável,[92] conforme lhe assegura o mandamento constitucional.

91 MARQUES, Claudia Lima. O "Diálogo das Fontes"...Op. Cit. p. 32: " pensei em que três são os tipos de "diálogo" entre essas: a) uma lei pode servir de base conceitual para outra (diálogo sistemático de coerência), especialmente se uma lei é geral e a outra especial, se uma é lei central do sistema e a outra um microssistema específico; b) uma lei pode complementar a aplicação de outra, a depender de seu campo de aplicação (diálogo de complementariedade e subsidiariedade), tanto suas normas, quanto seus princípios e cláusulas gerais no sentido contrário da revogação ou ab-rogação clássicas, em que uma lei era superada e "retirada" do sistema pela outra; e, por fim, c)há o diálogo das influências recíprocas sistemáticas, como a redefinição do campo de aplicação em uma lei para outra, influência do sistema especial no geral e do geral para o especial (diálogo de coordenação e adaptação sistemática)."

92 Ibidem. p. 61: "Nesse sentido, alerte-se que o método do diálogo das fontes, por respeito aos valores constitucionais e direitos humanos que lhe servem de base, não deve, por exemplo, ser usado para retirar dos direitos consumidor: o diálogo só pode ser usado em favor do sujeito vulnerável (....)Em outras palavras, o diálogos já tem a ➔

Ter-se-á, assim, uma proteção ao consumidor com relação aos seus dados pessoais mediante a aplicação do diálogo das diálogo das fontes[93] que serve como um método sistemático para organizar e coordenar as fontes[94] legais e infralegais supracitadas,[95] dispensando uma resposta normativa atual e moderna frente aos desafios propiciados pelos bancos de dados na sociedade da informação.[96]

Registre-se, por derradeiro, que mesmo havendo uma lei geral de proteção de dados pessoais, não se deve descartar o diálogo proposto, sobretudo a teorização acima delineada a respeito do dever-direito de informação e o princípio da transparência para que, efetivamente, aperfeiçoe-se a prometida esfera de controle dos dados pessoais, sob pena de torná-la utópica e, por conseguinte, (des)proteger os dados pessoais dos consumidores.

➔ lógica/racionalidade preponderante: é a promoção pelo julgador dos direitos do consumidor, como impõe o art. 5°, XXXII, da CF/1988, incluída nas cláusulas gerais pétreas brasileiras: promover os direitos do consumidor "na forma da lei" mais favorável ao sujeito de direitos vulnerável"

93 Em sentido análogo acenando para o diálogo das fontes entre CDC e a Lei do Cadastro Positivo: BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12,414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011. p. 54-59.

94 MIRAGEM, Bruno. Eppur si muove...*Op. Cit*. p. 80.

95 Percorrendo o mesmo caminho normativo legal e infralegal para a constatação de que há no ordenamento jurídico brasileiro o conceito de proteção dos dados pessoais com base em tais princípios elencados. MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. Ano 20. Vol. 79. jul-set 2011. p. 69.

96 CARVALHO, Ana Paula Gambogi. *Op. Cit*. p. 953: " Constata-se, a partir da leitura das lições do autor mencionado, que todos os princípios por ele elencados já se encontram positivados no texto do Código de Defesa do Consumidor, seja no próprio art. 43, que trata especificamente dos bancos e cadastros de dados, seja nas normas sobre a responsabilidade civil do fornecedor (em cujo conceito se subsume o gestor de um banco de dados de consumo) pela reparação de danos morais e patrimoniais sofridos pelo consumidor.

6. VERTICALIZAÇÃO DAS PREMISSAS TEÓRICAS-NORMATIVAS DIANTE DA ANÁLISE DA AÇÃO COLETIVA Nº 2013.01.1.184921-7 (MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS X FACEBOOK E O APLICATIVO "LULU"): CONVERGÊNCIAS E DIVERGÊNCIAS PARA A SISTEMATIZAÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS DOS CONSUMIDORES

Com o intuito de validar e testar todo o percurso teórico-normativo percorrido, analisar-se-á o notório caso da ação coletiva promovida pelo Ministério Público do Distrito Federal e dos Territórios em face do rede social *Facebook* e o aplicativo 'Lulu" que será dívida em duas partes: i) narrativa: mediante a descrição dos fatos que circunstanciara o caso, notadamente como se aperfeiçoou a parceria comercial entre os Réus da ação que é donde se desdobra todo suporte fático do litígio; ii) apreciação técnica: análise da petição inicial da ação coletiva e da decisão de segunda instância que concedeu o pedido de tutela antecipada para, dentre outros pedidos, cessar o compartilhamento dos dados pessoais dos consumidores.[97]

97 A divisão estabelecida entre narrativa e apreciação técnica para o estudo de um caso são as orientações metodológicas tecidas por: GHIRARDI, José Garcez. PALMA, Juliana Bonacorsi de. VIANA, Manuela Trindade. Posso fazer um trabalho inteiro sobre um caso específico? *In* **Metodologia jurídica**: um roteiro prático para trabalhos de conclusão de curso. Rafael Mafei Rabelo Queiroz e Marina Ferfebaum (Coordenadores). São Paulo: Saraiva, 2012. p. 179.

Deste modo, será possível constatar convergências e divergências das premissas teórico-normativas traçadas na primeira parte desta monografia, empregando uma abordagem mais concreta e dinâmica,[98] refletindo-se sobre a própria racional da petição inicial da ação coletiva e da decisão judicial supracitada, confrontado, em última análise, a propugnada sistematização da proteção dos dados pessoais dos consumidores que se revela e se apresenta como a grande conquista, ainda em construção, da proteção do consumidor no século XXI.

6.1 Narrativa e suporte fático do caso sob análise: o funcionamento do aplicativo "Lulu" por meio da sincronização de perfis do Facebook

O Lulu é um aplicativo para *smartphones* e para computadores que acaba por sincronizar[99] o perfil do seu usuário com aquele relativo ao da sua rede social, no caso o *Facebook*. Por isso, de forma bem esquemática, pontuar-se-ia que o aplicativo desenvolvido pela *Lulusive Incorporation* funcionaria como uma rede social paralela à do *Facebook*.[100]

O diferencial desta rede paralela é que as suas usuárias mulheres poderiam avaliar e classificar os seus amigos, o que já não

98 Ibidem. p. 177-178.

99 "o Lulu funciona a partir da sincronização com o perfil do Facebook e permite que a usuária faça uma espécie de "resenha" de algum amigo, ex-namorado, ficante, etc. que seja seu amigo na rede social, ou ainda, que veja as impressões de alguém que achou interessante, mas não conhece." (Disponível em: <http://canaltech.com.br/noticia/internet/O-polemico-Lulu-saiba-o-que-e-como-funciona-e-como-evitar-avaliacoes/>. Acesso em 23 de abril de 2014)

100 "O aplicativo Lulu, funciona como uma rede social paralela ao Face, onde é possível avaliar todos os garotos que estejam com perfis cadastrados no Facebook, ao conectar-se ao Lulu. Será feita uma varredura dos meninos existentes em seu perfil do Face, tornando possível visualizar os perfis de seus conhecidos e ler as avaliações que foram feitas por outras garotas." (Disponível em: <http://ziggi.uol.com.br/downloads/lulu>. Acesso em 23 de abril de 2014).

é factível na rede social *Facebook* em razão da ausência de tal funcionalidade.

O objetivo seria que o público feminino pudesse tomar "decisões inteligentes" para "iniciar relacionamentos", mediante a "troca de experiências"[101] propiciada pela aventada classificação e avaliação do público masculino.

Com base em frases curtas previamente formatadas e disponibilizadas pelo próprio aplicativo - *hashtags*[102] - do tipo: i) ele não é um babaca; ii) dá sono ou é mais barato que um pão na chapa; iii) prefere o videogame, permitir-se-ia às mulheres, de forma anônima e privada, classificar e avaliar os homens para viabilizar as citadas decisões inteligentes no âmbito afetivo, colocando "as garotas no controle".[103]

Veja-se, portanto, que o funcionamento do aplicativo "Lulu" somente fora aperfeiçoado pelo *compartilhamento dos dados pessoais* dos usuários do *Facebook*, mediante a transposição do perfil de uma plataforma para a outra.

Em outros termos, o público masculino da rede social não optou, a princípio, para ter um perfil no mencionado aplicativo,

101 As palavras entre aspas foram extraídas de tradução livre do próprio sítio do aplicativo Lulu. Disponível em: "<http://company.onlulu.com/en/how_lulu_works/>. Acesso em 23 de abril de 2014.

102 "A avaliação é feita por meio de questões de múltipla escolha e de hashtags que representam pontos negativos e positivos, como #filhinhodamamãe, #nãovailigarnodiaseguinte ou #sorrisoépico. No final, o conjunto gera uma nota de 1 a 10. Apesar de ser vinculada ao perfil do homem, a avaliação não é vista por ele, do mesmo jeito que as resenhas são anônimas e, consequentemente, não são vistas nem mesmo pelas participantes do Lulu." (Disponível em: <http://canaltech.com.br/noticia/internet/O-polemico-Lulu-saiba-o-que-e-como-funciona-e-como-evitar-avaliacoes/>. Acesso em 23 de abril de 2014)

103 A frase é da própria criadora do aplicativo: "O app foi criado pela britânica Alexandra Chong e lançado em fevereiro nos Estados Unidos. Contudo, chegou ao Brasil só agora. Segundo Chong, a escolha pelo Brasil está relacionada ao fato de as pessoas serem muito sociáveis aqui. Em entrevista ao Mashable em junho, a fundadora disse que o app ajuda a informar as mulheres sobre características importantes de um homem, "colocando a garota no controle". Entretanto, tal ideia trouxe à tona diversas discussões. Enquanto alguns apoiam que as mulheres "deem o troco" nas avaliações feitas pelos homens, outros já acham que a iniciativa é errada se feita de ambos os lados." (Disponível em: <http://canaltech.com.br/noticia/internet/O-polemico-Lulu-saiba-o-que-e-como-funciona-e-como-evitar-avaliacoes/>. Acesso em 23 de abril de 2014)

tendo havido, simplesmente, a *sincronização* de uma plataforma para a outra. Para que o usuário do *Facebook* não tivesse um perfil no mencionado aplicativo seria necessário que ele acessasse o site do seu desenvolvedor para solicitar a sua remoção,[104] optando *a posteriori* pelo não compartilhamento de seus dados pessoais.

Obviamente que tal modelo de negócios e parceria comercial repercutiu na esfera da privacidade dos usuários do *Facebook*, tendo havido uma repercussão social que culminou, por fim, com a proposição de uma ação coletiva ajuizada pelo Ministério Público do Distrito Federal e dos Territórios em face do *Facebook* e da sociedade empresária desenvolvedora do aplicativo, diante da coletividade de consumidores exposta a tal prática comercial (artigo 2°, p. único e 29 ambos do Código de Defesa do Consumidor).

A petição inicial tinha, dentre outros pedidos, o pleito em sede de tutela antecipada para a remoção dos perfis dos usuários por conta da inexistência de consentimento prévio e informado para tal compartilhamento, possibilitando-se que tal prática somente seja permitida em havendo consenso prévio, informado e específico dos consumidores.

O pedido de tutela antecipada foi negado em primeira instância, mas por uma fundamentação que se prende na questão de legitimidade *ad causam* do *parquet* para a tutela de interesse coletivo,[105] o que não tem pertinência para a metodologia ora traçada nessa monografia.

104 Há um botão intitulado "remover meu perfil", cuja remoção dependia da autenticação da conta pelo facebook, de modo a obstruir tal sincronização. Disponível em: <http://company.onlulu.com/en/deactivate/>. Acesso em 23 de abril de 2014.

105 "(...) manutenção de ambiente e contexto jurídico que prezem pelo respeito e salvaguarda dos direitos e garantias fundamentais, porquanto inerentes à condição humana. Porém, a proteção dos direitos insculpidos no artigo 5.º da Constituição Federal deve ser postulada por cada uma das pessoas que, concretamente, experimentaram violação a seus atributos da personalidade, inclusive, eventualmente, em razão do aplicativo de informática "sub judice", falecendo, por conseguinte, ao Ministério Público, em relação a tais demandas, legitimidade ativa "ad causam" para tanto". Acesso da decisão em 20 de abril de 2014 no sítio www.tjdft.jus.br.

Será relevante a *ratio decidendi* de segunda instância que deu provimento ao agravo de instrumento para deferir o pedido de tutela antecipada, a fim de que fossem removidos os perfis dos usuários do mencionado aplicativo.

Cumpre dizer, no entanto, que a tal decisão judicial sequer precisou ser oficiada para fins de cumprimento,[106] pois, diante da comoção social, o aplicativo não está mais em funcionamento e indisponível para *download* nas lojas de aplicativos, o que teria sido causado pela noticiada ação coletiva e as demais ações individuais de consumidores.[107]

Portanto, o agravo de instrumento não teve julgamento de mérito, tendo sido retirada da pauta de julgamento. A ação principal não teve ainda sequer a apresentação de contestação por parte dos Réus, de modo que o seu julgamento de mérito não ocorreu e tarda a acontecer.

Em suma, esse é todo o suporte fático que circunstanciou a ação coletiva supracitada, cabendo verificar a racional da petição inicial da ação coletiva e a decisão de concessão da tutela antecipada, identificando-se convergências e divergências em comparação às premissas teóricas-normativa para a sistematização da proteção dos dados pessoais como acima abordada.

106 Nesse sentido, há despacho nos autos dando conta de que teria havido o cumprimento voluntário da decisão judicial. Acesso em 20 de abril de 2014 no sítio www.tjdft.jus.br.

107 **'Lulu' completa 25 dias fora das lojas de aplicativos**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/01/lulu-completa-25-dias-fora-das-lojas-de-aplicativos.html>. Acesso em 20 de abril de 2014.

6.2 Apreciação técnica da ação coletiva

6.2.1 A racional da petição inicial e o seu contraste com as premissas teóricas-normativas delineadas para a sistematização de proteção de dados pessoais

De início, cabe destacar que a petição inicial se utilizou, expressamente, da expressão autodeterminação informacional,[108] elevando-a como sinônimo de proteção dos dados pessoais, convergindo, pois, com a premissa teórico-normativa até agora construída para a sistematização da proteção dos dados pessoais.

A racional da exordial da ação coletiva estruturou-se sob a premissa de que deveria ser assegurado aos usuários da rede social do *Facebook* o controle sobre as suas informações pessoais (autodeterminação informacional), considerando, por isso, que a ausência de consentimento prévio, informado e específico para que houvesse a sincronização dos perfis violou o direito à privacidade dos consumidores.[109]

Destaca-se, assim, a coerência argumentativa da inicial ao considerar que a autodeterminação informacional deve ser concretizada por meio de um controle do consumidor sobre o fluxo de seus dados pessoais.

108 "*A proteção de dados pessoais ou direito à autodeterminação informativa*, como prefere parcela da doutrina, decorre da tutela constitucional de proteção à dignidade da pessoa humana. Consubstancia-se *no controle que o cidadão/consumidor deve possuir sobre seus próprios dados*, principalmente em face do avanço da informática e extrema facilidade em difusão indevida dessas informações por redes." (destaque). Disponível em: <http://www.mpdft.mp.br/portal/pdf/comunicacao/dezembro_2013/ACP%20Facebook%20e%20Lulu.pdf>. Acesso em 20 de abril de 2014. p. 09.

109 "Neste ponto, demonstra-se que a legitimidade de compartilhamento com terceiros dos dados e perfil de milhões de usuários do Facebook só é possível mediante *consentimento prévio, específico e informado* do interessado em decorrência do significado e *conteúdo atual do direito à privacidade e proteção de dados*." (destaque). Disponível em: <http://www.mpdft.mp.br/portal/pdf/comunicacao/dezembro_2013/ACP%20Facebook%20e%20Lulu.pdf>. Acesso em 20 de abril de 2014. p. 15.

Mas, mais do que isso, avançou-se na questão tormentosa de como deveria ser aperfeiçoado o indigitado controle das informações pessoais, tendo havido uma clara *correlação* entre *consentimento* e *dever de informação* para solucionar essa difícil equação da autodeterminação informacional.

Como bem foi ponderado deveriam ter sido prestadas informações claras e adequadas[110] para que o consumidor racionalizasse/decidisse sobre o trânsito de seus dados pessoais, o que no caso concreto deveria ser efetivado pela possibilidade de o usuário da rede social ser cientificado (informado) sobre o compartilhamento de suas informações para daí externar uma *opção específica* e pontual sobre tal questão.

O consentimento adjetivado como informado, específico e prévio aperfeiçoa, portanto, a premissa teórico-normativa de que a tutela da privacidade é *dinâmica* na sociedade da informação, devendo o consumidor seguir todos os *movimentos* de seus dados, sendo imprescindível, em última análise, a instauração de um *processo comunicativo* para que ele possa assim consentir especificamente sobre o trânsito de seus dados.

Nesse ponto em específico, a petição inicial poderia ter recorrido a propugnada interpretação extensiva do artigo 43, §2, do CDC, pela qual o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados do indivíduo, possibilitando-lhe acompanhar de *forma dinâmica* o fluxo de seus dados.

Da mesma forma, a racional da petição inicial poderia ter invocado o princípio da especificação dos propósitos que tangencia a autodeterminação informacional funcionalizada pelo dever

110 "Todavia, é fundamental que tal manifestação de vontade seja realizada de *modo específico*, com *transparência* e *informações claras* de como seus dados serão tratados *a partir dessa transferência*. Em outros termos, num ambiente propício de *informação adequada*, o consumidor deve ter o pleno *direito de escolha de decidir* o que lhe é mais conveniente e adequado." (destaque) Disponível em: <http://www.mpdft.mp.br/portal/pdf/comunicacao/dezembro_2013/ACP%20Facebook%20e%20Lulu.pdf>. Acesso em 20 de abril de 2014. p. 20.

informacional. Ora, tal princípio aperfeiçoa-se, justamente, pela prestação de uma informação clara e específica a justificar a coleta e/ou o processamento em *sentido lato* dos dados pessoais (no caso em específico o seu compartilhamento) para que, então, sobrevenha o consentimento pontual sobre tal movimentação de seus dados pessoais.

O princípio da especificação dos propósitos é, como visto, o que orienta uma série de normas legais e infralegais relativas à proteção dos dados pessoais no ordenamento jurídico brasileiro, proibindo-se que haja a sua utilização para outra finalidade que aquele informada ao sujeito dos dados pessoais.

Até, por isso, poderia ser considerada abusiva[111] a cláusula de política de privacidade da rede social *Facebook* que, genericamente, estipula como seriam utilizados os dados pessoais dos seus usuários,[112] colocando o consumidor em uma situação de extrema

111 "Assim, trazendo tais considerações para o objeto da presente demanda coletiva, a única conclusão possível é no sentido de que eventual transferência de dados pessoais dos usuários/consumidores do Facebook para terceiros ou aplicativos, como é o caso do Lulu, só e legítima se houver consentimento prévio, informado e específico. *Não possui valor jurídico, a aceitação genérica e automática de regulamento do Facebook*." (destaque) Disponível em: <http://www.mpdft.mp.br/portal/pdf/comunicacao/dezembro_2013/ACP%20Facebook%20e%20Lulu.pdf>. Acesso em 20 de abril de 2014. p. 20.

112 Ao consultar a política de privacidade da mencionada rede social, verifica-se: " Usamos as informações que recebemos sobre você em relação aos serviços e recursos que fornecemos a você e a outros usuários, como seus amigos, nossos parceiros, os anunciantes que compram anúncios no site e os desenvolvedores que criam os jogos, aplicativos e sites que você usa. Por exemplo, além de ajudar as pessoas a ver a encontrar as coisas que você faz e compartilha, podemos usar as informações que recebemos sobre você: como parte de nossos esforços para manter os produtos, serviços e integrações do Facebook seguros e protegidos; para proteger os direitos ou propriedades do Facebook e de outros; para fornecer recursos e serviços de localização, como informar você e seus amigos quando algo está acontecendo nas redondezas; para avaliar ou entender a eficiência dos anúncios que você e outras pessoas visualizam, incluindo fornecer anúncios relevantes para você; para fazer sugestões para você e outros usuários do Facebook, como: sugerir que seu amigo use nosso importador de contatos porque você encontrou amigos usando-o, sugerir que outro usuário o adicione como amigo porque o usuário importou o mesmo endereço de e-mail que você ou sugerir que seu amigo marque você em uma foto que ele carregou e que você esteja presente; e para operações internas, que incluem correção de erros, análise de dados, testes, pesquisa, desenvolvimento e melhoria do serviço. Conceder-nos permissão para usar suas informações não só nos permite fornecer o Facebook tal como é hoje, mas também nos permite fornecer ➔

desvantagem e por restringir o seu direito à proteção de seus dados pessoais (artigo 51, inciso IV e §1°, inciso II, ambos do CDC).

A falta de alusão expressa a tal princípio, correlacionando-o à autodeterminação informacional pode ser decorrência da não percepção de que normas legais e infralegais o preveem, podendo-se recorrer à teoria do diálogo das fontes para ser estabelecida tal sistematização, como propugnado nessa monografia.

Percebe-se, então, a importância da teoria do diálogo das fontes para a sistematização da autodeterminação informacional por coordenar normas que teorizam uma compreensão completa de como deve ser aperfeiçoado o indigitado controle do consumidor sobre seus dados pessoais, consistindo, em última análise, o seu fundamento legal.

Destaca-se, em conclusão, como último ponto divergente das premissas teórico-normativas traçadas nessa monografia, a não alusão à teoria do diálogo das fontes que, dentre outros princípios, poderia ser extraído o princípio da especificação dos propósitos que reforçaria e acresceria na linha argumentativa traçada na própria petição inicial da ação coletiva.

6.2.2. A decisão do TJDFT

A decisão do Tribunal de Justiça do Distrito Federal e Territórios poderia, salvo melhor juízo, ter utilizado um outro fundamento para dar provimento ao agravo de instrumento para a concessão da antecipação da tutela, a fim de que fossem removidos os perfis dos usuários compartilhados entres *Facebook* e o aplicativo "Lulu".

Com efeito, a fundamentação da decisão judicial ateve-se, unicamente, a questão de que a Constituição Federal - artigo 5° inciso IV - garante a liberdade de expressão, vedando-se o anonimato.

> ➔ recursos e serviços inovadores que desenvolvermos no futuro que usam, de novas maneiras, as informações que recebemos sobre você." Disponível em: <https://www.facebook.com/full_data_use_policy#howweuse>. Acesso em 20 de abril de 2014.

Daí concluiu que a referida avaliação e classificação propiciada pelo aplicativo seria ilícita, vedando a avaliação de forma anônima.

Nesse sentido, vale transcrever trecho da r. decisão:

> "Verifica-se nessa norma uma dupla garantia, a primeira em favor daquele que expressa o pensamento, sendo livre sua manifestação, e a segunda em favor daquele a quem a opinião alheia é dirigida, permitindo-lhe conhecer o subscritor daquela manifestação.
> Como conteúdo da Dignidade da Pessoa Humana, tanto a liberdade de expressão quanto o direito à intimidade, constituem direitos indisponíveis, não podendo ser derrogados por vontade dos seus titulares.
> Assim, em tese, não poderia uma pessoa concordar com a manifestação de uma opinião sobre si de forma anônima, pois isso seria, na prática, a disponibilidade de um direito fundamental.
> Dessa forma, aplica-se a regra prevista na Constituição da República em relação à vedação ao anonimato. Logo entendo, não pode ser mantida, ao menos em cognição sumária, a possibilidade de avaliações de pessoas sem que essas tenham o conhecimento do seu teor e do seu subscritor."

Tal fundamentação alberga, tão somente, um dos objetos da tutela antecipada que é a determinação para que não sejam permitidas avaliações e classificações de forma anônima, deixando de enfrentar e congregar a tese argumentativa relativa ao outro objeto do pedido de efeito ativo do agravo de instrumento, qual seja, que a exclusão dos perfis do aplicativo dar-se-ia pela ausência de consentimento prévio e informado para que houvesse a sincronização dos perfis por parte dos consumidores da rede social *Facebook*.

Não obstante, a decisão de segunda instância tenha deferido ambos os objetos da tutela antecipada, acabou por apenas conclamar na sua fundamentação a tese argumentativa relativa à

vedação do anonimato para a classificação e avaliação funcionalizada pelo aplicativo.

Reconhece-se, entretanto, que a parte dispositiva fez alusão expressa ao fato de que a remoção dos perfis dar-se-ia em razão da falta de consentimento expresso, informado e específico para o compartilhamento dos dados pessoais entre as plataformas, de modo que teria, implicitamente, acolhido a tese argumentativa do *parquet*.

Por isso, tal decisão acabaria por convergir com a premissa teórica-normativa de que o controle dos dados pessoais, *in casu* o seu compartilhamento com terceiros deve ser funcionalizado pelo dever de informação, fazendo-se necessário que seja precedido de um consentimento específico para tal desiderato.

Empregar-se-ia, assim, a perspectiva de uma tutela *dinâmica* da privacidade, na medida em que o sujeito da informação pessoal deve ser cientificado (informado) dos seus movimentos, externando o seu controle por meio de um consentimento específico.

Registre-se, no entanto, que a falta de uma fundamentação substancial para o acolhimento de tal pedido pode ser decorrência da não percepção de uma interpretação extensiva do artigo 43 do CDC, tal como da propugnada teoria do diálogo das fontes que sistematizaria a autodeterminação informacional, empregando-lhe, sobretudo, uma fundamentação legal.

Com efeito, ao analisar a questão do anonimato o Juízo *ad quem* fez questão de citar o dispositivo constitucional que o vedava para, então, determinar a proibição de que futuras avaliações seguissem tal modelo de anonimato.

De qualquer forma, o caso sob análise é paradigmático, pois reconhece, ainda que timidamente, o direito do consumidor de autodeterminar as suas informações pessoais (autodeterminação informacional).

6.3. Convergências e divergências extraídas da análise do caso

Em resumo, podem ser apontadas as seguintes convergências (numeração 1) e divergências (numeração 2) extraídas do estudo do caso, mediante a comparação entre as premissas teóricas-normativa traçadas nessa monografia e a racional contida na petição inicial da ação coletiva e da decisão do TJDFT:

1.a. O reconhecimento da *autodeterminação informacional* como parâmetro normativo para a proteção dos dados pessoais, a fim de que o consumidor tenha *controle sobre seus dados pessoais*;

1.b. A *funcionalização* da autodeterminação informacional pelo dever de informação, devendo o consumidor ser cientificado (*informado*) de maneira clara e suficiente sobre o trânsito de seus dados, de modo que, no caso sob análise, deveria ser instado a respeito do compartilhamento de suas informações pessoais junto ao aplicativo "Lulu" para que, então, pudesse *consentir especificamente* sobre tal questão;

1.c. A percepção de que a tutela da privacidade na sociedade da informação é, portanto, *dinâmica*, sujeitando-se ao aventado processo comunicativo entre o detentor da base de dados e o sujeito da informação pessoal para que ele possa *autodeterminar* a *movimentação* de seus dados pessoais, como no caso de compartilhamento de suas informações pessoais entre a rede social Facebook e o aplicativo "Lulu";

2.a. A ausência da consideração de que a autodeterminação informacional já se encontra abraçada pelo ordenamento jurídico, mediante a interpretação de que o dever de informar e o princípio da transparência oxigenam o artigo 43 do Código de Defesa do Consumidor, como, por exemplo, para uma interpretação extensiva do seu §2 pela qual o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados pessoais do indivíduo, possibilitando-lhe acompanhar de *forma dinâmica* o fluxo de seus dados.

2.b. A ausência de alusão à teoria do diálogo das fontes que permitiria somar na linha argumentativa traçada na própria petição inicial da ação coletiva, como, por exemplo, o princípio da especificação dos propósitos que está previsto em normas legais e infralegais, proibindo que os dados sejam utilizados para outra finalidade que aquela previamente informada. Tal princípio aperfeiçoa-se, justamente, pela prestação de uma informação clara e específica a justificar a coleta e/ou o processamento em *sentido lato* dos dados pessoais (no caso em específico o seu compartilhamento) para que, então, sobrevenha o consentimento específico sobre tal movimentação de seus dados pessoais, o que somaria, repita-se, na linha argumentativa para a sistematização da autodeterminação informacional para a proteção dos dados pessoais.

2.b.1. A ausência de uma fundamentação explícita a respeito da autodeterminação informacional pode ter sido decorrência da não percepção dos itens 2.a e 2.b que lhe emprestam uma fundamentação legal, sistematizando-a, razão pela qual a própria decisão do TJDFT teria somente considerada a questão do consentimento para o fluxo dos dados pessoais em sua parte dispositiva e não em sua fundamentação. Tal consideração torna pertinente o quadro normativo desenhado nessa monografia, pois visa, justamente, normatizar a autodeterminação informacional por meio do dever de informação, o princípio da transparência e a teoria do diálogo das fontes, emprestando-lhe um amparo legal.

Reconhece-se, obviamente, que o Marco Civil da Internet não havia sido sancionado à época dos acontecimentos dos fatos da analisada ação coletiva. Contudo, como visto, já havia uma série de normas legais e infralegais, especialmente a Lei do Cadastro Positivo que possibilitariam extrair tal construção normativa para que fosse emprestado amparo legal à autodeterminação informacional.

À guisa de conclusão, constata-se o que cerne das premissas teóricas-normativa traçadas nessa monografia convergem com a racional que conduziram até o momento a ação coletiva sob análise

(itens 1.a à 1.c), ponderando-se, no entanto, que as "divergências" não são inconciliáveis. Ao revés, elas podem dialogar - para usar o termo que intitula esta monografia -, porque reforçam, sistematizam e emprestam fundamento legal à autodeterminação informacional que é uma das grandes conquista da defesa do consumidor em meio a sociedade da informação, mas que pode avançar, a começar por sua consolidação normativa através da tríade: dever de informação, transparência e diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores.

7. CONCLUSÃO

O mercado informacional é uma realidade sendo que um dos seus combustíveis são os dados pessoais de consumidores que transitam, à revelia de seu consentimento, por toda a rede.

As implicações de tal fenômeno são ainda incipientes, mas algumas experiências já são conhecidas como é o caso da ação coletiva promovida em face da rede social *Facebook* e o do aplicativo "Lulu", em razão da primeira prestadora de serviços ter compartilhado sem o consentimento prévio, informado e específico de seus consumidores seus dados pessoais com a segunda prestadora de serviços, gerando prejuízos para a esfera extrapatrimonial de toda uma coletividade sujeita e exposta a tal prática comercial.

A personalidade das pessoas projeta-se, assim, por meio de *bits* - dados pessoais - no ambiente eletrônico,[113] redimensionando os direitos da personalidade no estágio atual da sociedade.

113 BIONI, Bruno R. O direito ao esquecimento. *In* **Anais do II Simpósio de Iniciação Científica da USP da Faculdade de Direito de Ribeirão Preto***, 2013*. Disponível em: <http://myrtus.uspnet.usp.br/pesqfdrp/portal/arquivos/docs/II_simposio_pesquisa/bruno_ricardo_bioni.pdf>. Acesso em 20 de abril de 2014.

Nessa perspectiva, deve-se propiciar ao titular dos dados pessoais o controle de seus dados pessoais conquanto a sua cumulação, transmissão e retificação, autodeterminando as informações que lhes acomete (autodeterminação informacional). Somente, assim, salvaguardará a privacidade dos consumidores, sendo essa a sua conotação atual na sociedade da informação.

Deve-se, assim, estabelecer um imprescindível processo de comunicação entre o detentor do banco de dados e a pessoa estigmatizada, revelando-se a informação como a pedra de toque para o enredo proposto. Ora, é a informação a premissa para tal relação intersubjetiva, eis que, é ela (a informação) que empregará forma e conteúdo à troca das mensagens necessárias para tal interação.

Vale dizer, é a dita prestação da informação que cientificará seu receptor, *in casu* aquele afetado pelo fluxo informativo, a respeito da possibilidade de controlar seus dados pessoais, o que perpassa desde o ato inaugural de coleta dos dados (dimensão procedimental) até a sua destinação, transmissão, eliminação e/ou retificação (dimensão substancial).

A autodeterminação informacional surge, assim, como um parâmetro normativo para a proteção dos dados pessoais, sendo que a prometida esfera de controle dos dados pessoais deve ser funcionalizada pelo dever-direito de informação, tendo sido esta a conclusão da monografia que é convergente com a racional que conduziu o caso analisado da supracitada ação coletiva.

Atenta-se, nesse sentido, toda a teorização acima delineada sobre como tal informação deve ser entregue ao consumidor - aspectos qualitativos e quantitativos da informação - para que o usuário possa, efetivamente, controlar as suas informações pessoais, sob pena da prometida esfera de controle sobre seus dados pessoais tornar-se uma utopia. Daí porque, a própria arquitetura da rede deve ser moldada para permitir ao usuário ter acesso a todas essas funcionalidades propostas para o controle de seus dados pessoais.

Por isso, conjugando-se o papel central que a informação avoca no microssistema consumerista e o princípio da transparência ao proposto controle dos dados pessoais, conclui-se ser aplicável a autodeterminação informacional, mediante uma interpretação ampliativa do artigo 43 do Código de Defesa do Consumidor, em especial do seu do seu §2 pela qual o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados, possibilitando ao consumidor acompanhar de *forma dinâmica* o fluxo de seus dados.

Soma-se, ainda, a aplicação da teoria do diálogo das fontes das normas legais e infralegais abordadas que sistematizam o direito ao controle das informações pessoais, acrescentando importantes normas que conformam o exercício de tal direito, especialmente princípios tais como: i) o da especificação dos propósitos, ii) consentimento para coleta e tráfego dos dados pessoais; e iii) o acesso e qualidade dos dados.

Nesse diapasão, aliás, com a aprovação do Marco Civil da Internet que dedica, como visto, uma quantidade relevante de dispositivos para a proteção dos dados pessoais dos usuários da internet, torna-se imperioso, mais do que nunca, a propugnada coordenação das fontes normativas para a sistematização da proteção dos dados pessoais dos consumidores.

As "divergências" encontradas entre as premissas teóricas-normativa traçadas nessa monografia e a racional que orientou a condução da ação coletiva, em especial a petição inicial e a decisão de concessão da tutela antecipada não são inconciliáveis. Ao revés, elas podem dialogar - para usar o termo que intitula esta monografia -, porque reforçam, sistematizam e emprestam fundamento legal à autodeterminação informacional que é uma das grandes conquista da defesa do consumidor em meio a sociedade da informação, mas que pode avançar, a começar por sua consolidação normativa através da tríade: dever de informação, transparência e diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores.

A intelecção proposta é, certamente, o avanço que se faz necessário para que seja construída uma "cultura" jurídica para a proteção dos pessoais no cenário nacional.

Registre-se, por fim, que mesmo diante de uma lei geral de proteção de dados pessoais, não se deve descartar o diálogo proposto, sobretudo a teorização delineada a respeito do dever-direito de informação e o princípio da transparência para que, efetivamente, aperfeiçoe-se a prometida esfera de controle dos dados pessoais, sob pena de torná-la utópica e, por conseguinte, (des) proteger os dados pessoais dos consumidores.

8. BIBLIOGRAFIA

"**Lulu**". (Disponível em: <http://ziggi.uol.com.br/downloads/lulu>. Acesso em 23 de abril de 2014).

____, Contratos no código de defesa do consumidor: o novo regime das relações contratuais. São Paulo: Editora Revista dos Tribunais, 2011.

____, Da boa fé no direito civil. Coimbra: Almedina, 2011.

____, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo a Erik Jayme. *In* **Diálogo das Fontes**. Cláudia Lima Marques, coordenação. São Paulo: Revista dos Tribunais, 2012. p. 17-66.

A proteção de dados pessoais nas relações de consumo: para além da informação creditícia/Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

Air passenger data. <http://www.migalhas.com/mostra_noticia.aspx?op=true&cod=154037>. Acesso em 15/04/2013.

BARBOSA, Fernanda Nunes. **Informação**: direito e dever nas relações de consumo. São Paulo; Revista dos Tribunais, 2008.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BENJAMIN, Antônio Herman de Vasconcellos e Benjamin. **Código brasileiro de defesa do consumidor**: comentado pelos autores do anteprojeto. vol. 1. Direito material (arts. 1° a 80° e 105 a 108.) Rio de janeiro: Forense, 2011.

BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12,414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

BEVILAQUA, Clovis. **Direito das obrigações**. Rio de Janeiro: Livraria Francisco Alves, 1945.

BIONI, Bruno R. O direito ao esquecimento. *In* **Anais do II Simpósio de Iniciação Científica da USP da Faculdade de Direito de Ribeirão Preto**. Disponível em: < http://myrtus.uspnet.usp.br/pesqfdrp/portal/arquivos/docs/II_simposio_pesquisa/bruno_ricardo_bioni.pdf>. Acesso em 20 de abril de 2014.

BORGESIUS, Frederick Zuiderveen. Segmentação comportamental: Do not track e o desenvolvimento jurídico europeu e holandês. **Revista Politics**. Publicação Núcleo de Pesquisas e Estudo de Formação/NUPEF. N° 14, fevereiro de 2013. p. 09-22.

BRAMAN, Sandra. A economia representacional e o regime global da política da informação. *In* **Informação, conhecimento e poder**: mudança e inovação social. Org. MACIEL, Maria Lucia; ALBAGAJI, Sarita. Rio de Janeiro: Garamound, 2011. p. 41-66.

CALO, Ryan, Against notice skepticism in privacy (and elsewhere). *In* **Notre Dame law review**, vol. 87:3, march, 2011. p. 1027-1072.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *In* **Coleção doutrinas essenciais do Direito do consumidor: proteção da confiança e práticas comerciais**; v. 3 / Claudia Lima Marques, Bruno Miragem organizadores. São Paulo: Revista dos Tribunais, 2011. p. 907-956.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

COSTA, Carlos Celso Orcesi. **Cadastro positivo**: lei n. 12.414/2011. São Paulo: Saraiva, 2012.

CUSUMANO, Michael A. GOELDI, Andreas. New Businesses and new business models. *In* **The oxford handbook of internet studies**. William H. Dutton (Organizador). United Kingdom: Oxford University Press, 2012. p. 239-261.

DANTAS, Marcos. **A lógica do capital-informação**: a fragmentação dos monopólios e a monopolização dos fragmentos num mundo de comunicações globais.

DELGADO, Mário Luiz. Comentários à Parte Especial – artigos 233 a 420 do Código Civil. *In* **Código civil comentado**. Regina Beatriz Tavares da Silva. (Org.). São Paulo: Saraiva, 2012.

Dilma sanciona Marco Civil na abertura do NETMundial. Disponível em: <http://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml>. Acesso em 23 de abril de 2014.

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

GHIRARDI, José Garcez. PALMA, Juliana Bonacorsi. VIANA, Manuela Trindade. Posso fazer um trabalho inteiro sobre um caso específico? *In* **Metodologia jurídica**: um roteiro prático para trabalhos de conclusão de curso. Rafael Mafei Rabelo Queiroz e Marina Ferfebaum (Coordenadores). São Paulo: Saraiva, 2012. p. 178-192.

GONÇALVES, Maria Eduarda. **Direito da Informação**. Coimbra: Almedina, 2003.

HOUAISS, Antônio. VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa**. Rio de janeiro: Objetiva, 2009.

LASTRES, Helena Maria Martins; FERRAZ, João Carlos. Economia da Informação, do conhecimento e do aprendizado. *In* **Informação e globalização na era do conhecimento**. Org. LASTRES, Helena M. M.; ALBAGAJI, Sarita. Rio de Janeiro: Campus, 1999. p. 27-57.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. **Code and other laws of cyberspace, version 2.0.** Nova York, Basic Books, 2006.

LISBOA, Roberto Senise. **A obrigação de informar.** São Paulo: Almedina, 2012.

LÔBO. Paulo Luiz Netto. A informação como direito fundamental do consumidor. *In* **Coleção doutrinas essenciais do Direito do consumidor**: proteção da confiança e práticas comerciais; v. 3 / Claudia Lima Marques, Bruno Miragem organizadores. São Paulo: Revista dos Tribunais, 2011. p. 593-612

'Lulu' completa 25 dias fora das lojas de aplicativos. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/01/lulu-completa-25-dias-fora-das-lojas-de-aplicativos.html>. Acesso em 20 de abril de 2014.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. *In* **Coleção doutrinas essenciais de Responsabilidade civil**: direito à informação; v. 8 / Nelson Nery Júnior. Rosa Maria de Andrade Nery (organizadores). São Paulo: Revista dos Tribunais, 2010. 27-40.

MARQUES, Cláudia Lima. BENJAMIN, Antônio Herman V. MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2.010.

MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. São Paulo: Revista dos Tribunais, 2008.

MARTINS, Leonardo. **Introdução à jurisprudência do Tribunal Constitucional Federal Alemão**. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1999.

MARZAGÃO, Nelcina C. de O. Tropardi. **Da informação e dos efeitos do excesso de informação no direito do consumidor**. São Paulo: USP-SP, 2005. Tese (Doutorado), Universidade de São Paulo Faculdade de Direito.

MATTOS, Karla Cristina da Costa e Silva. **O valor econômico da informação nas relações de consumo**. São Paulo: Almedina, 2012.

MAYER-SCHONEBERGER, Viktor. CUKIER, Kenneth. **Big Data**: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. Ano 20. Vol. 79. jul-set 2011. p. 45-80.

MENEZES CORDEIRO, António Manuel da Rocha e. **Tratado de direito civil das obrigações**. 2°: Direito das obrigações, 1° t: Introdução, sistemas e direito europeu, dogmática geral. Coimbra: Almedina, 2009.

MIRAGEM, Bruno. **Direito do Consumidor**: fundamentos do direito do consumidor: direito material e processual do consumidor; proteção administrativa do consumidor; direito penal do consumidor. São Paulo: Editora Revista dos Tribunais, 2008.

MIRAGEM, Bruno. Eppur si muove: Diálogo das fontes como método de interpretação sistemática no direito brasileiro. *In* **Diálogo das Fontes**. Cláudia Lima Marques, coordenação. São Paulo: Revista dos Tribunais, 2012. p. 67-110.

MONTEIRO, Washington de Barros. MALUF, Carlos Alberto Dabus. **Curso de direito civil**, vol. 4: direito das obrigações, 1ª parte: das modalidades das obrigações da transmissão das obrigações. São Paulo: Saraiva, 2012.

MURRAY, Andrew. **Information technology law**. Oxford: Oxford University Press, 2010.

O polêmico Lulu: saiba o que é, como funciona e como evitar avaliações. Disponível em: <http://canaltech.com.br/noticia/internet/O-polemico-Lulu-saiba-o-que-e-como-funciona-e-como-evitar-avaliacoes/>. Acesso em 23 de abril de 2014).

Petição Inicial da Ação Coletiva promovida em face do Facebook e o aplicativo "Lulu". Disponível em: <http://www.mpdft.mp.br/portal/pdf/comunicacao/dezembro_2013/ACP%20Facebook%20e%20Lulu.pdf>. Acesso em 20 de abril de 2014.

Revista Veja. edição n° 2321, ano 46, n° 20. **Entenda o que é Big Data**: o megafenômeno digital que transforma em riqueza dados pessoais, posts, tuítes, e-mails e cliques. 15 de maio de 2013. p. 71-81.

RIPERT, Georges. **A regra moral nas obrigações civis**. Campinas: Bookseller, 2009.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHEREIBER, Anderson. **Os direitos da personalidade**. São Paulo: Altas, 2011.

SILVA, Clóvis do Couto e. **A obrigação como processo**. Rio de janeiro: Editora FGV, 2006

SOLOVE, Daniel J. **The digital Person: technology and privacy in the information age**. New York: New York University Press, 2004.

STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect (October 1, 2013). 2013. **NYU School of Law, Public Law Research Paper** No. 13-62; NYU Law and Economics Research Paper No. 13-34. p. 94-172.

TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions. **Rev. Online. Stanford**, n° 63. fev, 2012. p. 63-69.

TEPEDINO, Gustavo; SCHREIBER, Anderson. **Código civil comentado**: direito das obrigações: artigo 233 a 420, volume IV. São Paulo: Atlas, 2008.

TOMASETTI JÚNIOR, Alcides. O objetivo da transparência e o regime jurídico dos deveres e riscos da informação nas declarações negociais para consumo. **Revista de Direito do Consumidor**. São Paulo: Revista dos Tribunais, n.4, p. 59, 1992. p 52-90.

TOMASEVICIUS FILHO, Eduardo. **Informação assimétrica, custos de transação, princípio da boa-fé**. São Paulo: USP-SP, 2007. Tese (Doutorado), Universidade de São Paulo Faculdade de Direito.

VARELA, João de Matos Antunes. **Das obrigações em geral**: vol. 1. Coimbra: Almedina, 2012.

WORLD ECONOMIC FORUM. **Big data, big impact:** new possibilities for international development. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em 08 de março de 2014.

LEGÍTIMO INTERESSE:
a disputa travada ao longo dos trabalhos preparatórios da LGPD

Bruno Ricardo Bioni, Mariana Rielli e Marina Kitayama

FASE DO ANTEPROJETO

O processo que culminou na aprovação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) durou cerca de 8 anos, desde a publicação do primeiro texto de Anteprojeto[1] submetido à consulta pública pelo Ministério da Justiça, em dezembro de 2010. A matéria do legítimo interesse, entretanto, não esteve presente desde o início nos textos que vieram a dar corpo à lei. Ao se analisar a primeira versão do Anteprojeto, bem como as versões iniciais dos projetos de lei 4060/2012[2], do então deputado federal Milton Monti (PR-SP), e 330/2013[3], do então senador Antônio Carlos Valadares (PSB/SE), verifica-se que não havia a hipótese legal do legítimo interesse como hipótese de autorização para o tratamento de dados pessoais.[4]

Na realidade, o fio condutor dos textos iniciais, com destaque para o Anteprojeto de lei, era a figura do consentimento, considerada até então como a base legal prevalente, prioritária sobre as demais.[5] Dessa forma, no Anteprojeto, o art. 9º previa como

1 MINISTÉRIO DA JUSTIÇA. **Anteprojeto de Lei de Proteção de Dados Pessoais.** Brasília, DF, dezembro de 2010. Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf

2 CONGRESSO NACIONAL. **Projeto de Lei 4060/2012.** Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012

3 SENADO FEDERAL. **Projeto de Lei 330/013.** Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília, DF, agosto de 2013. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927883&ts=1567533189767&disposition=inline

4 No caso do PL 330/2013, havia a seguinte previsão: "Art. 12. A interconexão de dados pessoais deve atender aos seguintes requisitos: I – adequação às finalidades legais ou estatutárias e aos interesses legítimos dos proprietários e gestores de bancos de dados; [...]". Entretanto, o projeto não faz outras menções à ideia de interesses legítimos, no sentido de defini-los, nem faz referência ao conceito em sua justificação.

5 BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil**. GPoPAI-USP, 2016. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil

regra o consentimento "livre, expresso e informado ao titular" e elencava outras hipóteses[6] como exceções. Já nos projetos provenientes das Casas Legislativas, o consentimento se apresentava como a base legal para o tratamento de dados sensíveis[7] e de crianças e adolescentes[8].

As movimentações em torno da inserção da categoria legítimo interesse, ou interesses legítimos, começaram em razão das consultas públicas a que o Anteprojeto do Poder Executivo foi submetido. Na primeira rodada, realizada em parceria com o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro e que durou cerca de 5 meses, foram recebidas 794 contribuições, provenientes de empresas e organizações do terceiro setor, majoritariamente. Conforme indica estudo publicado pela Associação Brasileira de Marketing Direto - ABMED, naquele momento houve poucas contribuições ou sugestões relacionadas ao legítimo interesse.[9] Não foi, ainda, nessa ocasião que a base legal despontou.

6 Tais hipóteses eram: obrigação contratual ou legal, dados de acesso público irrestrito, exercício de funções próprias dos poderes do Estado, pesquisa histórica, científica ou estatística, proteção da vida ou incolumidade física do titular ou terceiro, quando o consentimento não for possível, exercício do direito de defesa ou casos que digam respeito ao inadimplemento de obrigações por parte do titular, nos termos do Código de Defesa do Consumidor.

7 No PL 4060/2012, a previsão era a seguinte: "Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal." Já no PLS 330/2013: "Art. 4º Ao tratamento de dados pessoais aplicam-se os seguintes princípios: [...] IV – consentimento prévio e expresso do titular de dados como requisito à coleta, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado (art. 10);"

8 A redação inicial do PL 4060/2012 quanto a esse ponto é: "Art. 17. O tratamento de dados pessoais de crianças somente será possível mediante o consentimento dos seus pais, responsáveis legais ou por imposição legal."

9 A única delas que corresponde à ideia de legítimo interesse que veio a ser incorporada posteriormente é a contribuição da NOKIA. Nos termos do relatório: "Por fim, a Nokia ressalta também ser necessário que as hipóteses de dispensa abranjam também os casos em que o tratamento for necessário para fins de interesses legítimos do responsável pelo tratamento dos dados ou de terceiro a quem os dados sejam comunicados, sendo preservados sempre os direitos e liberdades fundamentais do titular". Disponível em: https://www.abemd.org.br/interno/DadosPessoais_ContribuicoesdasEntidades.pdf

Isso veio a ocorrer apenas em julho de 2015, por ocasião do primeiro substitutivo[10] apresentado pelo então senador Aloysio Nunes ao PL 330/2013, na Comissão de Ciência e Tecnologia (CCT), do Senado. Foi a primeira vez que as bases legais para o tratamento de dados foram incluídas na forma de incisos paralelos, sem preponderância de uma sobre a outra, e com a presença da hipótese do legítimo interesse.[11] Não nos parece que isso tenha ocorrido por acaso, uma vez que à época ocorria a segunda rodada de consultas públicas ao Anteprojeto de lei de dados pessoais do Ministério da Justiça, e havia o interesse de harmonizar a proposta do Senado com aquela que eventualmente iria para a Câmara.[12] Uma pista a esse respeito foi a participação do então Senador Aloysio Nunes, relator do PLS 330/2013, no evento de lançamento da versão pós-consulta pública do Anteprojeto de Lei do Executivo, quando afirmou, inclusive, que o texto do Executivo deveria ser encaminhado, com regime de urgência constitucional, ao Legislativo.[13]

10 SENADO FEDERAL. **Parecer 2015.** Brasília, DF, Rel. Senador Aloysio Nunes Ferreira. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1567533189932&disposition=inline

11 Cada inciso é elemento discriminativo do artigo ou do parágrafo. Assim, quando há mais de um, os incisos são equidistantes do arranjo nuclear representado pelo artigo, dentro da estruturação lógica do tema regulado. Para a leitura normativa é necessário se utilizar de diretrizes de interpretação estrutural, considerando o ordenamento como totalidade orgânica em perene dinamismo. Regras do direito encerram um motivo e um sentido consubstanciadores de certa intencionalidade. Portanto, a escolha do legislador em distribuir logicamente o texto de determinada maneira não é trivial. Ver: MENDES, Gilmar Ferreira. **Hermenêutica Constitucional e Direitos Fundamentais**. Brasília: Brasília Jurídica, 2000. p. 82-84; PENNA, Sérgio; MACIEL, Eliane Cruxên. **Técnica Legislativa: orientação para a padronização de trabalhos**. Brasília: Consultoria Legislativa do Senado Federal, 2002. p. 124, 125.

12 RIELLI, Mariana. O processo de construção e aprovação da Lei Geral de Dados Pessoais: bases legais para tratamento de dados em um debate multissetorial. **Revista do Advogado**, a. XXXIX, n. 144., p. 07-14, 2019.

13 PEDUZZI, Pedro. **MJ finaliza nova versão sobre anteprojeto sobre proteção de dados na internet.** Agência Brasil, Brasília, 19 de out. de 2015. "A ideia de dar urgência à matéria já havia sido defendida pelo senador da oposição Aloysio Nunes (PSDB-SP), durante a abertura do seminário. 'Sugiro que o projeto seja apresentado pela presidente [Dilma Rousseff] com urgência constitucional ao Legislativo, para nos livrar de certos embaraços que fazem com que iniciativas interessantes se percam no Congresso Nacional', ➔

Naquele momento da segunda consulta pública, que contou com mais de 1.800 contribuições,[14] discutiam-se ambos os pontos - a não-hierarquização de bases legais, ao menos no caso de dados triviais, e a inclusão da hipótese do legítimo interesse, conforme melhores práticas internacionais. Consolidado o texto do Executivo, ele foi enviado à Câmara como PL 5276/2016 com nove distintas bases legais, dentre as quais ambos consentimento e legítimo interesse, hierarquicamente equivalentes. Assim, a partir de 2016, tanto o projeto do Senado quanto os projetos da Câmara, estes apensados ao PL 4060/2012, passaram a tramitar com a hipótese do legítimo interesse, que veio a ser lapidada a partir de então.

➔ argumentou o senador tucano." Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Acesso em: 14 de dez. de 2020.

14 Conforme estudo do InternetLab, houve uma cisão de posicionamentos em relação ao legítimo interesse, embora não tenha havido entidades que rejeitaram a proposta como um todo. De um lado, empresas como Claro, Vivo, Sky e associações empresariais como Febraban e Brasscom, dentre outras, trouxeram contribuições no sentido da inclusão da hipótese do legítimo interesse a partir de uma lógica de consentimento tácito. Parte da argumentação centrou-se na ideia de "fadiga do consumidor" em relação à hipótese do consentimento. As empresas defenderam o legítimo interesse como hipótese legal facilitadora do tratamento de dados em situações nas quais não haveria impactos indevidos sobre os direitos dos indivíduos. Entretanto, a questão dos interesses do titular não é central nessas colaborações. Outras contribuições, como a de Marcel Leonardi, ressaltou o fato de o legítimo interesse integrar a legislação europeia sobre o tema desde 1995, de forma que se criaria um descompasso e um atraso caso o Brasil optasse por não seguir esse mesmo caminho. Entidades como ITS Rio e o Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI) centraram suas contribuições na necessidade de, no caso de haver a nova hipótese dos interesses legítimos, ela vir acompanhada de um teste de razoabilidade/proporcionalidade, a fim de assegurar os direitos dos titulares de dados pessoais frente a uma situação de flexibilização do seu consentimento. Assim, sugestões como a inclusão da obrigatoriedade de anonimização dos dados como forma de proteção do titular foram feitas. Em: INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais**. São Paulo, SP, 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

Síntese 1

O legítimo interesse é fruto do debate travado aos longos dos trabalhos preparatórios da LGPD. Antes era um total desconhecido, mas quando foi introduzido tornou-se o centro das atenções, alocado em pé de igualdade com as demais hipóteses de autorização de tratamento de dados, em especial o consentimento. Ou seja, não há qualquer tipo de hierarquia entre as 10 (dez) bases legais constantes do artigo 7º da LGPD.

FASE DO PROJETO DE LEI

O substitutivo do senador Aloysio Nunes, cujo texto manteve-se o mesmo quanto ao legítimo interesse ao longo da tramitação, era relativamente econômico, sendo a única contraposição ao legítimo interesse do controlador a seguinte condicionante: "desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados".[15] Algo bastante similar à estrutura do texto do Regulamento Geral de Proteção de Dados (RGPD) e da Diretiva no 95/46-1995 do parlamento europeu, essas semelhanças e também suas diferenças em relação à lei brasileira serão sistematizadas mais adiante.

Já o texto que foi apresentado pela Presidência da República à Câmara, quase um ano depois (e após a segunda consulta pública), trazia a hipótese legitimadora de forma mais robusta, com

15 SENADO FEDERAL. **Parecer 2015.** Brasília, DF, Rel. Senador Aloysio Nunes Ferreira. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1567533189932&disposition=inline

uma série de parágrafos que contemplavam os seguintes pontos: legítima expectativa do titular (art. 10, §1º), medidas de transparência e possibilidade de oposição por parte do titular (art. 10, §2º), princípio da necessidade e anonimização, quando compatível com a finalidade do tratamento (art. 10, §3º), e, por fim, possibilidade de solicitação de relatório de impacto pelo "órgão competente".[16]

Nesse sentido, verifica-se influência de contribuições como a do Grupo de Pesquisa em Políticas Públicas Para o Acesso à Informação (GPoPAI) e Instituto Tecnologia e Sociedade (ITS-Rio),[17] que sugeriram alterações no texto do Anteprojeto de lei a fim de incluir menções à legítima expectativa, necessidade, transparência e medidas de segurança, inclusive anonimização, dentre outros. O projeto do Executivo, após a rodada de contribuições, com especial atenção às contribuições da academia, criou uma versão do legítimo interesse mais consistente, em relação ao do Senado, com a ideia de um teste de balanceamento entre o interesse do controlador e as legítimas expectativas e direitos do titular de dados pessoais.[18] Esse fio condutor continuou ao longo do restante da tramitação do projeto.

16 BRASIL. Congresso Nacional. **Projeto de Lei 5276/2016.** Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e dignidade humana. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=B847DDE7464E52A5396BD7DDB37BD7EA.proposicoesWebExterno2?codteor=1457459&filename=PL+5276/2016

17 "A grande preocupação com advento da nova exceção por interesses legítimos é que tal exceção sabote, ou mesmo, fragilize o pilar normativo do APL, qual seja, o consentimento como a regra geral para o tratamento dos dados pessoais [GPoPAI]. Por isso, os proponentes que debateram, controversamente, acerca dessa nova exceção acabam por sugerir que a lei preveja, expressamente, um teste para a ponderação dos interesses envolvidos que deve levar em conta uma série de fatores [ITS-Rio]." INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais.** São Paulo, SP, 2016. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

18 BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil**. GPoPAI-USP, 2016. p. 50-51. "Sob o ponto de vista de coerência normativa centrada na regra geral do consentimento e da autodeterminação informacional, um sistema de freios e contrapesos mais rígido acaba por não esvaziar a promessa de que o cidadão deve exercer →

O primeiro substitutivo do Relator Orlando Silva (PCdoB-SP)[19] no âmbito da Comissão Especial, foi apresentado após uma rodada de audiências públicas, dentre as quais uma especificamente sobre legítimo interesse.[20] Incorporadas as considerações dos convidados, o Relator apresentou uma versão ligeiramente alterada do texto inicial submetido à Câmara, retirando do artigo referente ao legítimo interesse a menção à anonimização e a medidas de segurança. A manutenção dos dispositivos protetores do titular dos dados, como o princípio da necessidade, da transparência, além da legítima expectativa, foi objeto de disputa até o momento final antes da apresentação do substitutivo,[21] com forte atuação

➔ controle sobre seus dados pessoais. Por exemplo: I. mecanismos de transparência quanto ao tratamento de dados pessoais via a hipótese de interesse legítimos, em conjunto com meios pelos quais o titular dos dados possa a ela se opor; II. padrões de segurança que minimizem os riscos à privacidade, como a anonimização dos dados, e, ainda; III. resguardar ao órgão fiscalizador o poder de auditar tais práticas do mercado, mediante a exigência de relatórios de impacto à privacidade.". Disponível: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil

19 BRASIL. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei NO 4060, de 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=161610896C391A39888C72EEE6DBA082.proposicoesWebExterno2?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012

20 Segundo o relatório do Relator Orlando Silva, a audiência pública foi composta por representantes da Federação Brasileira de Bancos - FEBRABAN, do Instituto Brasileiro de Direito Digital – IBDDIG, da organização não-governamental ARTIGO 19 e de especialista em privacidade e proteção de dados e professor de Direito Digital e Internacional da Universidade Presbiteriana Mackenzie.

21 DATA PRIVACY BRASIL. **Observatório da Privacidade**: Memória da LGPD. Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Transcrição do depoimento de Beatriz Barbosa, Coordenadora do Intervozes. "Tinha um artigo que tratava de uma das hipóteses de tratamento de dados pessoais e que, para sociedade civil, era uma preocupação grande, que é uma hipótese baseada no legítimo interesse das empresas de tratarem esses dados. Essa sempre foi uma preocupação para a sociedade civil, que essa hipótese não fosse um cheque em branco para as empresas tratarem os dados da maneira como elas quisessem, então a gente queria colocar algumas condicionantes nesse trecho. A gente já tinha ido para a mesa de negociação e não tinha rolado, não tinha conseguido incluir isso porque as empresas não tinham deixado a mesa de negociação, mas tinha setores da sociedade civil muito preocupados. Eu lembro que, uma meia hora antes do deputado Orlando protocolar o texto dele, a versão final do substitutivo depois da rodada de negociação que ia para o plenário, ele estava em comissão discutindo um outro tema, conversando com um consultor da câmara que ia fazer a redação final do substitutivo para ele e eu cheguei ➔

do terceiro setor para garantir que a previsão do legítimo interesse não fosse desequilibrada.[22]

Além disso, o relator reforçou em seu parecer dois aspectos: (i) que a previsão do legítimo interesse correspondia a uma tendência europeia presente desde os anos 90 e atendia a necessidades legítimas do setor privado; (ii) que o legítimo interesse não é um cheque em branco[23] e que deve ser balizado de acordo com os interesses e direitos dos titulares dos dados pessoais.

Após um parecer às emendas da Comissão Especial,[24] e o parecer proferido em Plenário,[25] o texto final referente ao legítimo interesse não foi alterado em relação ao primeiro substitutivo. Dessa forma, a versão aprovada pela Câmara (e, posteriormente, referendada pelo Senado) incluiu os seguintes elementos: (i) finalidade legítima; (ii) situação concreta; (iii) balanceamento em relação a direitos e liberdades fundamentais do titular; (iv) princípio da necessidade; (v) medidas para garantia da transparência; (vi) possibilidade de solicitação, ao responsável, de relatório de impacto à proteção de dados.

➔ e falei para ele "Orlando não vai dar, esse trecho aqui não pode passar desse jeito, se passar desse jeito a sociedade civil vai criticar o seu relatório e vai ser muito ruim ele chegar no plenário com críticas da sociedade civil.". Ele falou: "está bom, como é que vocês querem?" Aí eu arranjei uma folhinha do bloco que tinha na minha bolsa, escrevi correndo, grifei os dois trechos que precisavam incluir e entreguei o papel, quase um guardanapo assim para o Orlando. Aí ele pegou e entregou para o consultor, que fez uma cara não muito feliz, e falou assim "coloca desse jeito" e aí o relatório substitutivo foi para o plenário desse jeito. Ele fez a inclusão a nosso pedido e isso foi um dos trechos da Lei que sobreviveu a todo esse processo."

22 Mais sobre esse processo na Memória da LGPD, processo do Observatório da Privacidade e Proteção de Dados, do Data Privacy Brasil. Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/

23 Ponto que foi extensamente levantado por participantes da referida audiência pública, em especial Renato Leite Monteiro, então representante da Universidade Presbiteriana Mackenzie. Disponível em: https://www.youtube.com/watch?v=F1_NiqerjRs; 1h06min-31sec - 1h30min03sec.

24 BRASIL. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei no 4060/2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206&filename=PPP+1+PL406012+%3D%3E+PL+4060/2012

25 BRASIL. Parecer às Emendas de Plenário Apresentadas ao PL 4060/12. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664233&filename=PEP+2+PL406012+%3D%3E+PL+4060/2012

Dessa forma, verifica-se a permanência de uma visão mais detalhada do legítimo interesse, com referência a princípios da proteção de dados e medidas para concretizar os direitos dos titulares[26] e balanceá-los frente aos interesses do controlador. A versão que tramitou no Senado Federal (PLS 330/2013), por outro lado, manteve a redação mais enxuta do legítimo interesse até o final.

Síntese 2

A previsão do legítimo interesse foi objeto de uma intensa disputa. Um cabo de força foi puxado especialmente entre terceiro setor e setor privado para, respectivamente, bloquear-restringir e ampliar o espaço a ser por este ocupado. Ao final, alcançou-se um denominador comum, a partir de uma solução mediada e proposta pelo setor acadêmico, em que a sua previsão veio acompanhada de um dispositivo da lei que parametriza a sua aplicação. Com isso, a lei brasileira inovou ao prever no seu próprio texto critérios para a aplicação de um conceito jurídico determinado e, assim, trazer maior previsibilidade quanto à sua aplicação e interpretação. Desde o seu nascedouro, já havia a preocupação quanto aos efeitos colaterais, em termos de segurança jurídica, da introdução do legítimo interesse, o que foi potencialmente remediado no desenho final da LGPD.

26 DATA PRIVACY BRASIL. **Observatório da Privacidade:** Memória da LGPD. Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/. Transcrição do depoimento de Bruno Bioni, Fundador e Diretor do Data Privacy Brasil: "Em 2010/2011 não tinha legítimo interesse. Em 2015, versão pré consulta pública, não tinha legítimo interesse. Aí vem a enxurrada de contribuições públicas, vem o setor privado e fala 'eu quero o legítimo interesse', vem o terceiro setor e fala 'eu não quero o legítimo interesse' porque isso vai flexibilizar demais. No centro desse movimento pendular você tem a academia, dizendo 'olha é importante ter essa base legal, mas é importante ter essa base legal com algumas restrições ou, pelo menos, com algumas diretrizes de como isso será interpretado'. Esse é o típico exemplo em que dos dois polos, dos dois extremos, não teve a redação que desejavam, mas se teve um denominador comum, algo que ambos fizeram concessões. Acho que isso é muito simbólico do que é a Lei Geral de Proteção de Dados Pessoais."

BIBLIOGRAFIA

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil**. GPoPAI-USP, 2016.

BRASIL. **Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei no 4060/2012**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206&filename=PPP+1+PL406012+%3D%3E+PL+4060/2012

BRASIL. **Parecer às Emendas de Plenário Apresentadas ao PL 4060/12**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664233&filename=PEP+2+PL406012+%3D%3E+PL+4060/2012

CONGRESSO NACIONAL. **Projeto de Lei 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências**. Brasília, DF, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012

DATA PRIVACY BRASIL. **Observatório da Privacidade:** Memória da LGPD. Disponível em: https://observatorioprivacidade.com.br/memoria/como-a-lei-mudou-desde-2010/.

PEDUZZI, Pedro. **MJ finaliza nova versão sobre anteprojeto sobre proteção de dados na internet.** Agência Brasil, Brasília, 19 de out. de 2015.

RIELLI, Mariana. O processo de construção e aprovação da Lei Geral de Dados Pessoais: bases legais para tratamento de dados em um debate multissetorial. **Revista do Advogado**, a. XXXIX, n. 144., p. 07-14, 2019.

MINISTÉRIO DA JUSTIÇA. **Anteprojeto de Lei de Proteção de Dados Pessoais**. Brasília, DF, dezembro de 2010. Disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf

SENADO FEDERAL. **Parecer 2015**. Brasília, DF, Rel. Senador Aloysio Nunes Ferreira. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1567533189932&disposition=inline

SENADO FEDERAL. **Projeto de Lei 330/013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências**. Brasília, DF, agosto de 2013. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3927883&ts=1567533189767&disposition=inline

COLOCANDO EM MOVIMENTO O LEGÍTIMO INTERESSE

Bruno Ricardo Bioni, Mariana Rielli e Marina Kitayama

1. OS DIREITOS-DEVERES DESENGATILHADOS PELO LEGÍTIMO INTERESSE: A EQUAÇÃO DO ARTIGO 7, IX + ARTIGO 10, I + 37, *CAPUT*, DA LGPD

O legítimo interesse, conforme estruturado na legislação brasileira e na doutrina, dá origem a um conjunto de direitos e deveres para controladores, terceiros e titulares. Neste item, cada um desses elementos será desenvolvido conforme suas particularidades.

1.1 Legítimo interesse enquanto um direito: base legal para o tratamento de dados

As leis gerais de proteção de dados têm como objetivo não apenas a proteção dos direitos dos titulares, mas também a promoção de um livre fluxo de dados que dê ensejo ao desenvolvimento econômico,[1] tendo sido essa a dupla de valores que motivou o nascimento do legítimo interesse.[2] Dessa forma, a própria ideia dessa base legal autorizativa do tratamento de dados[3] dá origem a um direito para o controlador e para terceiros, uma vez que,

1 A própria lei deixa claro que com a privacidade e a proteção de dados devem conviver outros fundamentos, como o desenvolvimento econômico e tecnológico e a inovação (art. 1º, V) e a livre iniciativa, a livre concorrência e a defesa do consumidor (art. 1º, VI).

2 BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. Thomson Reuters, 2019. p. 469.

3 A construção histórica das bases legais para o tratamento de dados tem a ver com a ideia de legalidade ("lawfulness"), condição para o tratamento que aparece em normativas como a Convenção 108, do Conselho da Europa, e a Diretiva sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

cumpridas as normas que os sujeita, surge o direito de manipular dados pessoais.

1.1.1 Base legal para os "controladores"

O controlador é pessoa natural ou jurídica, de direito público ou privado, "à qual é atribuída a competência - tomada de decisões - para tratar dados pessoais (art. 5º, inciso VI, LGPD), de acordo com os parâmetros desenhados pela nova normativa".[4] Trata-se da figura, na relação jurídica estabelecida entre as partes, que decide em que sentido se dará o tratamento de dados pessoais, inclusive em relação a terceiros e operadores. Dessa forma, o controlador é o primeiro dos atores a que se referem as expressões "necessário para" e "interesses legítimos", do art. 7º, IX. Como este relatório tratará do aspecto da necessidade em item à parte, passa-se à análise do sentido e alcance do termo "interesses legítimos".

O Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*),[5] em seu parecer (*Opinion*) sobre legítimo interesse,[6] faz algumas distinções que merecem atenção. A primeira delas é entre "finalidade" e "interesse". A finalidade é o propósito específico do tratamento de dados pessoais, enquanto o interesse é o valor mais amplo que um tratamento de dados pessoais representa para o seu controlador (ou terceiros, ou a sociedade como um

4 BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. Thomson Reuters, 2019. p. 477.

5 O Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*) era, até a entrada em vigor do Regulamento Europeu de Proteção de Dados, o órgão responsável por interpretar, de forma não vinculante, os dispositivos da Diretiva 95/46/EC e outros assuntos de privacidade e proteção de dados.

6 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014.

todo). Um interesse, portanto, seria a garantia da segurança e da saúde de um determinado grupo de pessoas, enquanto uma finalidade seria determinado tratamento de dados que garante tal interesse, por exemplo a instalação de controles de acesso em um local.

Uma segunda distinção diz respeito ao termo "legítimo" (em que consiste um interesse legítimo?). Primeiramente, esse interesse deve ser *legal*, isto é, deve respeitar todas as leis e normas infralegais aplicáveis àquela situação específica. Bioni ilustra tal requisito com o exemplo da proibição à coleta, mesmo com consentimento, de dados relacionados a gravidez ou HIV em situações de trabalho.[7] Além disso, a legitimidade do interesse relaciona-se também ao seu caráter *articulado*, isto é, relacionado a uma situação concreta e, portanto, não especulativa, o que decorre do próprio princípio da finalidade ("propósitos legítimos, *específicos*"[8]).

No caso da Lei Geral de Proteção de Dados, especificamente, tanto o interesse quanto à finalidade (essa por força do art. 10, *caput*[9]), devem ser legítimos e concretos.

7 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5.

8 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 25.

9 BRASIL. **Lei 13. 709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas [...]."

Síntese 3

O adjetivo "legítimo" é um qualificador recorrente na LGPD. Aparece junto à definição do princípio da finalidade, bem como quando se enuncia a base legal contida no artigo 7º, IX, o legítimo interesse. Apesar de tal recorrência, tal terminologia exerce funções distintas. No primeiro caso, seu significado serve a uma análise mais restrita: a atividade de tratamento de dados em questão não deve ser vedada por lei ou norma infralegal. Já no segundo caso, o termo funcionaliza uma análise de aderência às condicionantes contidas no artigo 10 para que um interesse possa ser considerado legítimo. É recomendável levar em consideração tal distinção de escopo e alcance do termo.

1.1.2 Base legal para "terceiros"

O legítimo interesse, entretanto, não é aplicável apenas ao controlador, mas também à figura do "terceiro".[10] Isso significa que o controlador pode realizar um tratamento de dados que não seja no seu próprio interesse (ou exclusivamente no seu próprio interesse), mas no de terceiros ou da sociedade como um todo. Por exemplo:

(i) O exemplo mais contundente dessa conformação legal é a aplicação da hipótese do legítimo interesse para o combate a fraudes. A um só tempo, é de interesse de uma empresa evitar, por

10 BRASIL. **Lei 13. 709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD)."Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou [...]." (grifo nosso).

exemplo, que o cartão de crédito que ela oferece seja fraudado, e é interesse do sistema bancário e financeiro, bem como da sociedade, que a referida fraude não ocorra. Um eventual compartilhamento de dados entre agentes do sistema financeiro (que não a instituição financeira que presta o serviço para o titular e que seria o controlador) enquadram-se na figura de terceiros;

(ii) Outro exemplo claro de legítimo interesse de terceiros é a *due diligence* em processos de fusão e aquisição, em que terceiros que não têm nenhuma relação pré-estabelecida com os titulares de dados pessoais possuem o legítimo interesse de tratar esses dados[11] para avaliar a viabilidade da operação societária;

(iii) Hipótese em que o legítimo interesse de terceiros também é aplicável é o do tratamento de dados por equipes de respostas de emergência computacional e equipes de resposta de incidentes de segurança computacional. O recital 49 do RGPD traz de forma expressa que, para as finalidades de asseguração das redes e segurança cibernética, o legítimo interesse é base legal aplicável, citando inclusive as CERTs e CIRTs (siglas do inglês para as referidas equipes), terceiros que, portanto, poderiam se fundamentar no legítimo interesse;

(iv) Mais um exemplo seria aquele em que se publica dados para fins de transparência e *accountability*, mesmo nos casos em que não há tal obrigatoriedade por força da Lei de Acesso à Informação.[12] Nesses casos, o interesse que prevalece não é o do próprio controlador que divulga o dado em questão, mas de

11 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5. p. 240.

12 Veja o caso, por exemplo, das Defensorias Públicas, que não estão listadas na Lei de Acesso à Informação (LAI), mas que, dado a função por elas exercida de assistência judiciária, submetem-se às regras contidas na LAI para fins de controle social. A mesma lógica pode ser aplicada a algumas associações de classe, especialmente aquelas com propósito de autorregulação e certificação como base para se legitimar como órgão normatizador.

outros atores, como jornalistas, empregados e a sociedade como um todo;[13]

(v) Outro caso possível de aplicação do legítimo interesse de terceiro seria o compartilhamento de dados entre o controlador e terceiros interessados na sua utilização para fins acadêmicos. Um exemplo mais concreto é o compartilhamento de dados entre entes do sistema de justiça, como as Defensorias Públicas, Ministério Público e Poder Judiciário, e estudantes de pós-graduação, com base no legítimo interesse desses terceiros para a elaboração de investigações acadêmicas sobre o acesso à justiça no país.[14]

Ressalta-se que, em todos os casos, os testes relativos à base legal, que serão detalhados adiante, devem ser realizados, a fim de se confirmar que ela é adequada.

A aplicação do legítimo interesse de terceiros, contudo, não se limita de forma estrita às hipóteses antes levantadas. Considerando que a LGPD não traz uma definição própria sobre a figura do terceiro, não se deve restringir, a priori, a interpretação sobre quem pode ser esse sujeito. Os exemplos antes citados são casos em que a legitimidade de terceiros se manifesta de modo mais evidente, mas não têm a pretensão de fazer uma sistematização exaustiva.

Se, por um lado, a previsão do terceiro como um dos sujeitos que pode mobilizar a base legal do legítimo interesse na LGPD se aproxima do RGPD, por outro, ela se distancia, já que na

13 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 27.

14 É importante ressaltar que a LGPD não excepcionou de forma integral do seu escopo de aplicação da lei as atividades de tratamento de dados para fins acadêmicos (artigo 4, II, "b"), na medida em que tais atividades devem observar os artigos 7º e 11. Em outras palavras, tais atividades de tratamento de dados devem se amparar em uma das bases legais constantes dos referidos dispositivos da lei. Leia-se o artigo em questão: "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei."

regulamentação europeia foi definido quem é terceiro e quando ele se enquadra na figura de recipiente. O recipiente é definido pelo regulamento europeu como a pessoa física ou jurídica, autoridade pública, agência ou outro órgão, ao qual os dados pessoais são divulgados, seja um terceiro ou não.[15] Para ilustrar esta figura, o *European Data Protection Board*[16] utiliza o exemplo do pagamento de salários de funcionários das instituições da União Europeia (UE). Nesse caso, a folha de vencimento não vai apenas para o trabalhador, mas também para o Eurostat (organização estatística da UE), ente que, na hipótese, se configura como recipiente. Logo em sequência, o regulamento traz a definição do terceiro, sendo este a pessoa física ou jurídica, autoridade pública, agência ou organismo diferente do titular dos dados, controlador, processador e pessoas que, sob a autoridade direta do controlador ou operador, estão autorizados a tratar dados pessoais.[17]

15 PARLAMENTO EUROPEU e CONSELHO DA UNIÃO EUROPEIA. Regulação 2016/679. General Data Protection Regulation. "Article 4 (9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2 However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.".

16 "An illustrative example may be salary payments of officials of the EU institutions and bodies. The salary slip does not only go to the employee, but also to the institution or body where he or she works, and Eurostat receive the data" (compiled). EUROPEAN DATA PROTECTION SUPERVISOR. **Glossary**. Disponível em: https://edps.europa.eu/data-protection/data-protection/glossary/r_en

17 PARLAMENTO EUROPEU e CONSELHO DA UNIÃO EUROPEIA. Regulação 2016/679. General Data Protection Regulation., "Article 4 (10): 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;".

Síntese 4

A previsão de que o interesse legítimo pode ser de um terceiro foi introduzida na versão do Anteprojeto de lei de proteção de dados encaminhada ao Congresso, que se tornou o PL 5276/2016. Diferentemente do RGPD, a lei brasileira não traz uma definição de quem seria o terceiro, nem quando este se enquadra na figura de recipiente, de modo que é ainda mais desafiador interpretar o alcance da base legal do legítimo interesse de terceiro na LGPD. Como exemplos de quem pode ser um terceiro em uma relação de tratamento de dados pessoais, há desde pessoas naturais e jurídicas até a coletividade. É recomendável tratar distintamente tais categorias de terceiro, na medida em que implicam riscos diferentes para os titulares. Nesse sentido, cabe, aliás, ao próprio controlador avaliar se o interesse desse terceiro é, de fato, legítimo quando a base de dados estiver sob seu domínio.

1.2 Os deveres decorrentes do Legítimo Interesse

O legítimo interesse é uma base legal que depende de algumas condições para ser aplicável. Dentre estas condições, está, em primeiro lugar, a existência de um interesse que seja, de fato, legítimo. Essa qualificação só é alcançada quando são cumpridos uma série de deveres, listados abaixo.

1.2.1 O alcance do artigo 10 da LGPD

O art. 10[18] da Lei Geral de Proteção de Dados é o dispositivo que explicita todas as condições para a aplicação do legítimo interesse. Conforme mencionado anteriormente, ele surgiu nos anteprojetos de lei que deram origem à LGPD, especialmente a versão da segunda rodada de consulta pública promovida pelo Ministério da Justiça, em 2015. Assim, quando o projeto 5276/2016 foi enviado à Câmara dos Deputados, ele contava com uma versão do art. 10 semelhante à que veio a ser finalmente aprovada.

O conteúdo do artigo em questão revela uma preocupação, externada por organizações como GPoPAI e ITS-Rio à época, com a alta carga de discricionariedade dos atores que viriam a fazer uso da base legal: a ideia de um "cheque em branco" para controladores tratarem dados pessoais como bem entendessem. Fazendo frente a tal preocupação, vieram as sugestões de incorporação de elementos das normativas europeias, já consolidados pela interpretação do Grupo de Trabalho do Artigo 29[19] e reforçados nos Considerandos 47 e 48[20] do Regulamento Geral de Proteção de Dados (RGPD).

18 BRASIL. **Lei 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - 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, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

19 Ainda sob a égide da Diretiva 95/46/EC.

20 No Considerando 48 do RGPD, diz-se: "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect ➔

Assim, surge a ideia de um balanceamento dos direitos em jogo, entre o titular e as entidades que fazem uso dos seus dados.[21] Tão importante quanto compreender que há uma diretriz normativa geral de ponderação de interesses, é entender a função e o alcance do artigo 10 da LGPD, sob pena de cair em uma *armadilha hermenêutica*. Pelo menos duas dúvidas interpretativas merecem ser endereçadas:

1.2.1.1 Os pressupostos da aplicação do Legítimo Interesse traçados no art. 10 alcançam apenas o controlador? Ou também terceiros?

Um primeiro modo de compreender as hipóteses de aplicação do art. 10 é por meio de uma interpretação restritiva, segundo a qual os pressupostos do dispositivo referem-se exclusivamente ao legítimo interesse do controlador, não incluindo aqueles advindos de terceiros. Essa interpretação restritiva poderia ser extraída a partir da escolha de um método interpretativo *literal gramatical*, que parte do pressuposto de que as palavras que compõem o comando normativo representam aquilo que estritamente descrevem. Esta conclusão restritiva, contudo, está longe de ser a única interpretação possível do dispositivo.

→ at the time and in the context of the collection of the personal data that processing for that purpose may take place.". PARLAMENTO EUROPEU e CONSELHO DA UNIÃO EUROPEIA. Regulação 2016/679. General Data Protection Regulation.

21 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5, p. 235.

Uma interpretação[22] sistemática e teleológica[23] do artigo 10, que alcançaria também a figura do terceiro, mostra-se possível.[24] A partir dela, evita-se uma valoração distinta entre os destinatários da norma e, com isso, obtém-se uma aplicação mais uniforme da base legal do legítimo interesse, independentemente de quem seja o seu favorecido. Um resultado hermenêutico preferível para não afetar a própria substância do direito,[25] ainda mais quando o próprio arranjo normativo não justifica por que deveria haver a imposição de deveres em proporções distintas para o controlador e terceiros.

Nesse sentido, é importante lembrar que o artigo 10 da LGPD foi criado para governar todo e qualquer tipo de aplicação do legítimo interesse, a fim de impedir que esse conceito jurídico indeterminado se transformasse em um "cheque em branco". O ponto de atenção é a base legal em si e os possíveis abusos que dela podem se desdobrar, pouco importando quem a mobilize. Essa interpretação ampliativa do alcance do artigo 10 está alinhada com o próprio espírito de uma lei geral de proteção de dados, que é ser um estatuto da informação[26] que estabelece, via de regra, deveres e

22 Sobre as diversas técnicas hermenêuticas atuais e o seu repúdio ao método escolástico de prevalência de um método sobre o outro, especialmente o literal-gramatical: GRAU, Eros Roberto. **Ensaio e Discurso sobre a Interpretação/Aplicação do Direito**. 5ª ed. Malheiros Editores. p. 43

23 Por interpretação teleológica quer dizer ter-se em vista a globalidade dos fins a que serve a lei, que, com base na coerência, apoia-se na localização de um preceito no teto da normativa e na sua conexão com outros preceitos. Em:LARENZ, Karl. **Metodologia da Ciência do Direito**. Trad. José Lamego, Fundação Calouste Gulbenkian, Lisboa, 3ª ed. p. 464.

24 LARENZ, Karl. **Metodologia da Ciência do Direito**. Trad. José Lamego, Fundação Calouste Gulbenkian, Lisboa, 3ª ed. p. 450.

25 ENGISCH, Karl. **Introdução ao pensamento Jurídico**. Trad. J. Baptista Machado. Fundação Calouste Gulbenkian, Lisboa, 8ª ed. 2001. p. 313.

26 A LGPD inaugurou uma nova lógica, que busca regular uma ordem informacional, algo que não havia antes de forma tão sistematizada e harmônica. Ver: SCHERTEL, Laura Mendes. Palestra "Seminário Internacional – Lei Geral de Proteção de Dados: a caminho da efetividade". Superior Tribunal de Justiça, 2019. Disponível em: <https://www.youtube.com/watch?v=0E0USaGQ6h8>

direitos de forma *horizontal* e *simétrica* entre os diferentes atores que compõem esse ecossistema informacional. Ao mesmo tempo, decorre de uma leitura do todo da LGPD e não apenas das suas "tiras"[27] - nesse caso, o texto isolado do artigo 10.[28]

1.2.1.2 As condições distribuídas ao longo dos incisos e parágrafos do artigo 10 são cumulativas ou alternativas?

Uma segunda questão interpretativa a ser endereçada sobre o art. 10 diz respeito às condições distribuídas ao longo de seus incisos e parágrafos: seriam elas condições cumulativas ou alternativas? O espaço para interpretação surge do fato de que o *caput* do artigo em questão determina que as finalidades legítimas serão "consideradas a partir de situações concretas, que incluem, mas não se limitam a: [...]".

A leitura do *caput* assim redigido, sem um exercício hermenêutico mais aprofundado, abre margem tanto para o entendimento de que (i) os pontos listados na sequência, bem como outros não descritos, poderiam cada um ensejar a aplicação do legítimo interesse separadamente, quanto de que (ii) ambos os pontos em sequência devem ser observados enquanto requisitos de aplicação da base legal e, ainda, poderiam se considerar outras condições necessárias, a depender do contexto.

Novamente, tendo em vista as possibilidades abertas pela literalidade do texto, exige-se o recurso a critérios interpretativos, a fim de se chegar à sua *mens legis*. No caso, um critério, o da teleologia objetiva, merece análise mais pormenorizada.

Esse critério se funda na coerência entre o dispositivo específico e a lei em que ele se inscreve, tendo em vista que grande

27 A expressão é de GRAU, Eros Roberto. **Ensaio e Discurso sobre a Interpretação/Aplicação do Direito**. 5ª ed. Malheiros Editores. p. 17.

28 GRAU, Eros Roberto. **Ensaio e Discurso sobre a Interpretação/Aplicação do Direito**. 5ª ed. Malheiros Editores. p. 44.

parte das regras jurídicas têm função de preencher certos fins em combinação com outras normas, completar finalisticamente outras disposições.[29] No caso, o objetivo central do artigo 10 é o de criar parâmetros que norteiem a aplicação do legítimo interesse como um todo.

Tomando este ponto como premissa, a interpretação de que as condicionantes são alternativas leva a um resultado criticável, o de que bastaria a promoção das atividades do controlador para que se configure legítima a hipótese legal. Com isso, a própria função do artigo 10, que é o balanceamento dos interesses do controlador ou de terceiros frente ao do titular, ficaria esvaziada.

Síntese 5

Colocando em prática as técnicas de hermenêutica jurídica sobre a interpretação do art. 10 da LGPD, entende-se que o dispositivo (i) refere-se tanto ao legítimo interesse do controlador, quanto de terceiros e que (ii) a relação de incisos e parágrafos do artigo impõe condicionantes cumulativas e não alternativas. Com isso, garante-se uma aplicação uniforme da base legal do legítimo interesse, independentemente de quem a mobilize, bem como para que não se esvazia a função do artigo 10 como um todo, que é a de promover o balanceamento dos interesses do controlador ou de terceiros frente aos do titular. Uma interpretação sistemática e teleológica do artigo 10 está alinhada com o próprio espírito de uma lei geral de proteção de dados, que é o de estabelecer, via de regra, deveres e direitos de forma horizontal e simétrica.

29 ENGISCH, Karl. **Introdução ao pensamento Jurídico**. Trad. J. Baptista Machado. Fundação Calouste Gulbenkian, Lisboa, 8ª ed. 2001. p. 141.

1.2.2 Os deveres exigidos para a utilização da base legal do legítimo interesse também se aplicam a microempresas e a empresas de pequeno porte?

Uma vez que este documento tem como objetivo propor interpretações que possam balizar atividades de tratamento de dados de empresas e entidades de diferentes dimensões, é importante partir de um pressuposto ditado pela própria LGPD: o tratamento potencialmente diferenciado para microempresas, empresas de pequeno porte e negócios inovadores e disruptivos, como startups. Com isso, abre-se espaço para uma regulação assimétrica quando o porte e o volume, sem deixar de lado os riscos da atividade de tratamento de dados, justificam um regime normativo mais brando para não prejudicar a livre concorrência (artigo 2°, VI, da LGPD)

Conforme disposto pelo art. 55-J, XVIII, é competência da Autoridade Nacional de Proteção de Dados editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que esses modelos de negócios possam se adequar à lei. Trata-se de disposição que está em consonância com um dos objetivos centrais da LGPD, que é harmonizar a proteção de dados pessoais dos titulares ao desenvolvimento econômico e à inovação.

Nesse sentido, ficará a critério da Autoridade Nacional delimitar um regime normativo específico para esse grupo de empreendimentos, podendo incluir questões procedimentais mais brandas também no que toca ao legítimo interesse. Um exemplo do que poderia acontecer, na prática, é uma interpretação menos rígida da exigência da documentação ou o relaxamento dos componentes do LIA.

Entretanto, é importante ressaltar que, em que pese a previsão de tratamentos especiais para empresas de menor porte, os deveres documentais e procedimentais referentes à utilização da base legal do legítimo interesse, a princípio, direcionam-se a todos os

modelos de negócio, isto é, são horizontais. Tendo em vista que a Autoridade acaba de ser criada e que sua estrutura é enxuta, considerada a quantidade de atribuições, é incerto quando essas normativas serão criadas, e mesmo quando forem, não é possível prever qual será o seu conteúdo exato.

Síntese 6

A LGPD foi construída tendo como base a necessidade de equilíbrio entre a proteção de dados pessoais e o desenvolvimento econômico e inovação. Dessa dupla decorre a própria figura do legítimo interesse, conforme discutido anteriormente. Nesse sentido, a lei também consagrou a previsão de um possível regime diferenciado para pequenos negócios, inclusive quanto a procedimentos como prazos, a ser definido pela Autoridade Nacional de Proteção de Dados. Essa procedimentalização diferenciada pode ser aplicada ao legítimo interesse, como, por exemplo, pela não exigência da documentação ou pelo relaxamento dos componentes do LIA. Entretanto, é importante pontuar que se trata de uma possibilidade em aberto, de forma que, em princípio, aplicam-se horizontalmente, a todos os agentes de tratamento, as previsões da lei.

2. ÔNUS ARGUMENTATIVO REFORÇADO COM RELAÇÃO A ALGUNS DOS PRINCÍPIOS

Quando se olha para as condições que devem ser preenchidas para garantir a aplicabilidade do legítimo interesse, fica claro que

o que elas criam, para o controlador e terceiros, é um ônus argumentativo reforçado em relação a alguns dos princípios da legislação, como finalidade, necessidade e transparência.[30] Os princípios da LGPD, descritos no art. 6º, têm incidência horizontal, irradiando-se sobre todos os seus dispositivos e independentemente de qual seja a base legal, mas, no caso do legítimo interesse, optou-se por empregar maior vigor em relação a alguns deles.[31] Se não se chegasse a essa conclusão, grande parte do artigo 10 seria *meramente decorativa* e se esvaziariam parâmetros de ponderação entre os diferentes interesses em jogo.

Os princípios também servem como uma *barreira de modulação* ao voto de confiança dado ao agente de tratamento de dados, que é quem terá discricionariedade para avaliar se o seu interesse é legítimo. É ele que primeiro levanta a voz para aferir se um interesse é legítimo ou não, de modo que a racionalidade da LGPD foi articular parâmetros para uma prestação de contas a respeito desse juízo de valor que lhe cabe, em linha com o princípio da responsabilidade e prestação de contas (artigo 6º, X). Tal diferenciação tem implicações normativas, exploradas no presente documento.

2.1 Finalidade e adequação

Os primeiros dois princípios que permitem derivar as condições de aplicabilidade do legítimo interesse são a finalidade e a adequação, pelos quais a finalidade deve ser específica para cada tratamento de dados pessoais, que, por sua vez, deve se limitar a essa finalidade e ser plenamente adequado para o seu preenchimento.

30 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Reino Unido, 2017. Disponível em: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

31 BUCAR, Daniel; VIOLA, Mario. **Tratamento de Dados Pessoais por "legítimo interesse do controlador":** primeiras questões e apontamentos. *In* Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Thomson Reuters, 2019. p. 476.

2.2 Situação concreta

Como mencionado anteriormente, o interesse (e a finalidade, no caso brasileiro) além de legítimo, deve ser concreto. Diferente da Diretiva 95 e do Regulamento Geral de Proteção de Dados, em que este elemento foi acoplado à disciplina do legítimo interesse por orientações/interpretações não vinculantes,[32] no caso da norma brasileira a concretude vem estampada no próprio art. 10, segundo o qual "o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de *situações concretas* [...]" (grifo nosso).

A inserção do termo não se deu por acaso, mas foi fruto de colaborações à época das discussões do Anteprojeto.[33] Assim, a situação concreta representa mais um requisito para que o legítimo interesse não seja concebido como um "cheque em branco". Por tal razão, a existência de um contexto real em que se dará o tratamento de dados é imposta àqueles que desejam se utilizar da base legal, não sendo aceitas situações que podem vir a existir no futuro, ou que sejam abstratas e genéricas.

32 A exemplo dos pareceres do antigo Grupo de Trabalho do Artigo 29. Cf. ARTICLE 29, Data protection working group. Opinion 06/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 55 ("be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete); [...]").

33 "[...] Quando o tratamento se der com base no legítimo interesse é necessário um teste específico de balanceamento, em que serão colocados na balança os interesses legítimos, esses interesses legítimos de quem está se valendo desta hipótese eles tem que ser reais, eles não podem ser especulativos, eu não posso achar que no futuro eu vou tratar esses dados pessoais para essa finalidade hipotética que possa ser útil para a sociedade, eles têm que ser baseados em casos concretos. Essa situação concreta e específica tem que ser colocada na balança em contraponto com direitos fundamentais [...]". Fala de Renato Leite Monteiro na Reunião Deliberativa do PL 4060/12 sobre o tratamento e proteção de dados pessoais, realizada em 05/04/2017, que relembra esse como sendo um dos pontos de tensão à época da segunda consulta pública em 2015 do anteprojeto de lei. Disponível em: https://www.youtube.com/watch?v=F1_NiqerjRs; 1h20min05sec - 1h20min40sec.

Esse requisito se relaciona diretamente com o princípio da finalidade, já que, se é verdade que o legítimo interesse não vem atrelado a uma finalidade *a priori*,[34] como é o caso de outras bases legais,[35] isso não significa que ele não requeira uma finalidade específica para *cada situação* de tratamento de dados pessoais, observada em sua concretude. A própria LGPD já previu, no art. 10 duas hipóteses de finalidades para a aplicação do legítimo interesse: "I - apoio e promoção de atividades do controlador; e II - 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, nos termos desta Lei". Trata-se de rol exemplificativo, e não taxativo, justamente pela lógica de maior flexibilidade e análise casuística do legítimo interesse.[36]

Assim, o tratamento de dados levado a cabo com base na hipótese do legítimo interesse deve ser realizado de forma adequada à finalidade concreta pretendida.

Síntese 7

O legítimo interesse desengatilha um ônus argumentativo maior quanto ao princípio da finalidade, já que, para evitar seu uso de forma especulativa, o legislador optou por frisar que sua aplicação é derivável apenas de uma situação concreta. Tal reforço cumpre uma função que serve ao próprio agente de tratamento de dados, já que, quanto mais bem delineado for o seu interesse, mais fácil será a sua

34 LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado AASP.** Nº 144. 2019. p. 69.

35 No caso brasileiro, pode-se citar a proteção ao crédito, que foi inserida na reta final de tramitação do PL 4060/2012 na Câmara dos Deputados.

36 LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado AASP.** Nº 144. 2019. p. 70.

ponderação, especialmente para se analisar se a quantidade de dados processados é realmente necessária, bem como quais são as medidas de mitigação de impacto aos direitos e liberdades do titular. Em sentido contrário, quanto mais genérico for o seu interesse, mais desarticulado será o exercício de ponderação e mais difícil será a demonstração de que o agente de tratamento de dados não está abusando da sua posição.

2.3 Boa-fé

Além das condicionantes do *caput* do art. 10 (finalidade legítima e concreta), o inciso II traz novos elementos, que devem ser observados quando a finalidade for de "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem". A essa finalidade é acoplado um novo fator: o respeito às "legítimas expectativas dele [o titular] e os direitos e liberdades fundamentais, nos termos desta Lei".

Imediatamente, a proposição gera um questionamento: seria o respeito à legítima expectativa do titular exigível, por parte do controlador, apenas no caso dessa finalidade específica? Entendemos que não. Para justificar tal posição, em primeiro lugar, é importante entender do que se trata a legítima expectativa e qual é a sua relação com um princípio muito caro ao direito brasileiro e que norteia toda a LGPD: o princípio da boa-fé.[37]

37 Para ver mais sobre a correlação entre "legítima expectativa", o princípio da confiança e da boa-fé no direito brasileiro: MARQUES, Cláudia Lima. **Contratos dos Código de Defesa do Consumidor:** o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011, p. 282; MENEZES CORDEIRO, António. **Da boa-fé no direito civil**. Coimbra: Almedina, 2011, p. 1238; e LISBOA, Roberto Senise. **Confiança Contratual**. São Paulo: Atlas, 2012, p.143.

Destaca-se que, na redação do inciso II, o interesse do titular é diretamente promovido pela letra da lei e é a primeira fase em que efetivamente há um sopesamento dos interesses do controlador e do titular dos dados.[38] De acordo com a *Opinion* do Working Party 29 sobre legítimo interesse, requer-se, nesse caso, uma análise de *compatibilidade*, isto é, uma verificação sobre a *proximidade contextual* entre o uso feito dos dados do titular e aquilo que ele espera. Ele espera ou deveria esperar aquele uso específico? Em termos mais coloquiais, ele não se sentirá "traído" ou "assustado" com tal uso do seu dado pessoal? Caso a expectativa já exista, o impacto do tratamento provavelmente já foi dimensionado. Mas, caso essa expectativa não exista, o impacto (positivo ou negativo) será inesperado para o titular, o que deve ser levado em consideração no processo de balanceamento.[39] Nisso consiste a legítima expectativa.

Importante destacar, também, que a análise de compatibilidade está diretamente relacionada com o princípio da finalidade, já que sua própria definição é a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma *incompatível* com essas finalidades". Dessa forma, deve-se analisar se o tratamento posterior é próximo do uso original dos dados pessoais e se o titular dos dados tem a expectativa de que o uso secundário seja realizado.

Tal conformação está relacionada à boa-fé, presente no *caput* do art. 6º da Lei Geral de Proteção de Dados como um norte para

38 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5, p. 237.

39 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Reino Unido, 2017. p. 17. Disponível em: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

todos os outros princípios previstos neste dispositivo.[40] Ao incluir esse dispositivo, o legislador brasileiro amarrou duplamente os conceitos jurídico-indeterminados da legítima expectativa e do legítimo interesse a um elemento bastante tradicional da cultura jurídica brasileira.[41]

O princípio da boa-fé irradia a existência de um dever de conduta por parte do agente de tratamento de dados, com destaque para: (i) lealdade junto ao titular dos dados, de sorte que não frustre a *confiança* nele depositada, o que somente é aferível caso a caso - com isso, abre-se espaço para que haja novos usos (secundários) dos dados, mas que não contrariem o contexto do fluxo informacional;[42] e (ii) cuidado, que está ligado à noção de abuso de direito, isto é, que o direito em processar dados pessoais não "exceda manifestamente os limites impostos pelo seu fim econômico ou social, [...] pelos bons costumes".[43] Nesse sentido, o instituto do abuso de direito seria o portal de entrada para os "os limites éticos e sociais impostos a uma atividade", justamente em um momento em que se verifica uma guinada da ética em meios aos debates regulatórios sobre as novas tecnologias.

Dessa forma, o legislador brasileiro procurou evitar um "transplante legal"[44] inadequado do legítimo interesse do direito comunitário europeu, sem que houvesse a devida correspondência e encaixe no ordenamento jurídico brasileiro. A boa-fé cumpre,

40 A boa fé seria um "princípio dos princípios": "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa fé e os seguintes princípios: [...]".

41 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5. p. 225.

42 Ibidem, p. 228.

43 BRASIL. Código Civil. "Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes."

44 A ideia de um "legal transplant" foi cunhada por Alan Watson nos anos 70 para indicar a transposição de uma norma ou mesmo um sistema jurídico de um país para outro. Em: A. Watson, **Legal Transplants:** An Approach to Comparative Law, Edinburgh, 1974.

portanto, essa função de modulação em torno da introdução de um conceito jurídico indeterminado e até então estranho no Brasil.

A partir dessas considerações, parte-se para uma análise sistemática dos dispositivos da LGPD referentes ao legítimo interesse, especificamente a previsão de respeito às legítimas expectativas, e à boa fé. Tal análise leva em consideração tanto a coerência interna (semântica) dos dispositivos, quanto a própria estrutura e topografia da lei.

A inclusão da boa-fé no *caput* do art. 6º, que é o cerne do dispositivo e exprime a sua norma geral,[45] é indicativa da centralidade do princípio, inclusive em relação aos demais, que são desdobramentos do *caput* expressos em incisos. Como princípio, a boa-fé está inserida na seção de disposições preliminares da lei, que também conta com fundamentos (art. 2º), escopo de aplicação (art. 3º e art. 4º) e definições (art. 5º). Representa, nesse sentido, parte do núcleo de premissas que orientam a normativa e recaem sobre todos os seus artigos.

A previsão relativa ao legítimo interesse, por sua vez, é desdobrada em dois artigos, ambos pertencentes à primeira seção do Capítulo "Do Tratamento de Dados Pessoais", intitulada "Dos Requisitos para o Tratamento de Dados Pessoais". O art. 10, sobre o qual se discorre longamente nesse documento, completa a previsão do art. 7º, o qual meramente enumera as bases legais possíveis para o tratamento de dados pessoais. Assim, o art. 10 tem como objetivo disciplinar, de forma mais detalhada, o legítimo interesse enquanto hipótese autorizativa específica.

O art. 10 possui a estrutura tradicional de um artigo de lei, já que conta com o *caput*, incisos, que o desdobram e, nesse caso, exemplificam a norma geral nele enunciada, e parágrafos, que explicam ou

45 ALVARENGA, Marcos de Castro; LESSA, Beatriz Helena Mendes Ribeiro. **Técnica Legislativa**. Belo Horizonte, 2013. Disponível em: http://camaramuriae.mg.gov.br/portal/wp-content/uploads/2018/08/apostila-tec-legislativa-unificada.pdf

modificam a disposição principal.[46] A previsão referente à exigência de respeito à legítima expectativa, objeto desse item do documento, é um desdobramento que exemplifica finalidades possíveis para o tratamento de dados pessoais baseado no legítimo interesse.

O ponto de inflexão, entretanto, é que o artigo determina que o legítimo interesse somente poderá fundamentar o tratamento de dados considerando circunstâncias que incluam o apoio e promoção de atividades do controlador (inciso I) ***e*** 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 (inciso II).

Destaca-se aqui a utilização da conjunção aditiva "e" e não alternativa "ou", escolha legislativa não trivial, que traz consequências diretas para a correta interpretação do texto, pois o legítimo interesse somente poderá ser aplicado quando ambas as condicionantes dos incisos forem observadas. Nesse sentido, por mais que a situação concreta do tratamento promova atividades legítimas do controlador, ainda é dever deste atender às previsões do inciso II, sendo o respeito às legítimas expectativas do titular um de seus requisitos.

Trata-se de leitura coerente com a ideia, aqui reafirmada, de que é pelo princípio da boa-fé que a interpretação das bases legais, e das outras normas contidas na LGPD, deve se orientar. A consideração da legítima expectativa do titular de dados pessoais na aplicação do legítimo interesse nada mais é do que o equilíbrio, buscado a todo momento pela lei, entre interesses eventualmente conflitantes, mas que devem ser harmonizados e promovidos conjuntamente: a proteção dos dados pessoais do titular e a promoção das atividades econômicas dos agentes de tratamento. Sem tal garantia, a proteção conferida pela boa fé é desnaturada e cria-se uma situação de flagrante desproporcionalidade.

46 MARINHO, Arthur de Sousa. **Sentença de 29 de setembro de 1944**. Revista de Direito Administrativo, vol I. p. 227. Cf. também PINHEIRO, Hesio Fernandes. **Técnica Legislativa**. 1962. p. 100.

Como ressalva, destaca-se que tal entendimento não garante que a legítima expectativa do titular *prevalecerá* em todos os casos (e.g., prevenção à fraude), mas sim que ela será considerada e analisada junto aos elementos que demonstram o interesse do controlador para que, a partir do equacionamento entre ambos, chegue-se a uma decisão final sobre o tratamento de dados.

Síntese 8

A ideia de legítima expectativa, que integra a previsão do legítimo interesse, está diretamente relacionada ao princípio da boa-fé, na medida em que ele está calcado em um dever de lealdade e não frustração da confiança do titular de dados. Além disso, uma outra figura parcelar da boa-fé é a vedação do abuso de direito, isto é, uma limitação ao tratamento de dados pessoais que não passe no "teste" do legítimo interesse. Na interpretação dessa base legal, deve-se levar em consideração a forte influência do princípio da boa-fé no direito privado brasileiro, de forma a se evitar um transplante legal inadequado da figura do legítimo interesse para o ordenamento jurídico nacional. Nesse sentido, a boa-fé é o "princípio dos princípios" por estar posicionada no *caput* do artigo 6º, o que revela a sua centralidade frente aos demais listados ao longo dos seus incisos. Como resultado, a melhor interpretação do dispositivo é aquela que considera que a legítima expectativa do titular deve ser considerada em todo caso de aplicação do legítimo interesse, ainda que ela não venha a prevalecer no resultado final do balanceamento de interesses em jogo por não ser um valor absoluto (e.g., prevenção a fraudes).

2.4 Necessidade

Junto à finalidade e adequação, também o princípio da necessidade é uma das condições de aplicabilidade do legítimo interesse. Os princípios, vale lembrar, espraiam-se para todas as situações de tratamento, logo para todas as aplicações de bases legais, inclusive a do legítimo interesse. No caso dessa hipótese, entretanto, a remissão ao princípio da necessidade é explícita.

2.4.1 Minimização em sentido estrito

Diz o art. 10, §1º da LGPD que: "§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados." Trata-se de reflexão do histórico[47] princípio da necessidade, ou minimização, segundo o qual deverá ser considerada a menor quantidade possível de dados pessoais que seja suficiente para atender à finalidade pretendida, e não mais do que isso.[48]

Além da análise sobre a mínima quantidade de dados, dever-se-á observar também se outra base legal, que não o legítimo interesse, poderia ser aplicada no caso concreto.[49] Isso não significa que haja uma hierarquia estabelecida entre as bases legais, mas sim que se trata de um exercício de reflexão que serve ao próprio agente de tratamento de dados, na medida em que as demais

47 Presente, por exemplo, na Convenção 108 do Conselho da Europa, primeiro documento vinculante sobre proteção de dados pessoais.

48 Mais acima, no art. 6º, que define os princípios norteadores da lei, diz: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;".

49 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5, p. 236.

bases legais não demandam, via de regra, um ônus argumentativo reforçado, tal como o exigido pelo legítimo interesse.

A necessária observância da existência de outra base legal aplicável não torna o legítimo interesse hierarquicamente inferior, pois em qualquer espécie de tratamento o controlador deverá se voltar às hipóteses previstas nos incisos do art. 7°, buscando compreender qual é a mais adequada para sua atividade. A necessidade de verificação de outras bases legais aplicáveis ao tratamento em todos os casos é, justamente, consequência da inexistência de hierarquia entre elas, na medida em que todas são potencialmente cabíveis. Isso torna a adequação entre a previsão normativa e o caso concreto o critério de determinação da base aplicável.

É importante ressaltar que o adjetivo "necessário" não se confunde com "indispensável", mas também não é sinônimo de "útil" ou "desejável". Dessa forma, a maneira mais fácil de se identificar a necessidade, para fins de aplicação do legítimo interesse, é questionar se existe outra forma de atingir a finalidade ou interesse identificado.[50] Tal teste pode chegar a algumas respostas: se não houver outra forma de atingir a finalidade ou se a outra forma exigir esforço desproporcional, então o tratamento pode ser considerado necessário. Se houver diferentes formas de se atingir a mesma finalidade ou interesse, entretanto, é **possível (embora não obrigatória)** a realização de um Relatório de Impacto à Proteção de Dados[51] para ajudar a identificar a hipótese menos intrusiva.

50 DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Reino Unido, 2017. p. 17. Disponível em: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

51 Lembrando que a própria LGPD estabelece a prerrogativa da Autoridade Nacional de Proteção de Dados de requerer o relatório de impacto à proteção de dados pessoais do controlador na hipótese de tratamento baseado no legítimo interesse.

2.4.2 Minimização em sentido lato

Se existe uma minimização em sentido estrito, isto é, pensada para mitigar o caráter intrusivo do tratamento de dados, também se deve abordar um outro tipo de minimização, em sentido lato, que não diz respeito à *quantidade* de dados coletados e tratados, mas ao *impacto* que o tratamento tem sobre os direitos e liberdades fundamentais do titular de dados.

Sendo assim, não importa se poucos ou muitos dados estão sendo manejados em um determinado tratamento para determinada finalidade; mas se parte do pressuposto de que qualquer tratamento apresenta potencial lesivo para o titular de dados, de forma que, independentemente da quantidade de dados, o controlador deve incorporar medidas de mitigação de riscos.

Essa faceta da minimização é extraída do próprio art. 10, inciso II, na medida em que ele condiciona a fundamentação do tratamento no legítimo interesse à, dentre outros elementos, "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas [...] os direitos e liberdades fundamentais, nos termos desta Lei". Medidas de promoção e proteção dos direitos e liberdades dos titulares, que se enquadram nessa categoria são, por exemplo, a anonimização ou pseudonimização, já que são aptas a mitigar os potenciais impactos negativos de um tratamento de dados pessoais. Isso também explica porque o teste multifatorial da LGPD está dividido em quatro passos, o que será abordado mais à frente.

Síntese 9

Diferente de outras bases legais, no caso do legítimo interesse há referência explícita ao princípio da necessidade como condição de aplicabilidade. A necessidade, ou minimização, divide-se em sentido estrito, que diz respeito ao tratamento da menor quantidade de dados possível para uma determinada finalidade, e sentido lato, que se refere à articulação de medidas de salvaguardas mitigatórias aos riscos para os direitos e liberdades fundamentais dos titulares. Trata-se, portanto, de um dever de cuidado duplo, que deflagra dois juízos distintos, um em torno da menor intrusividade do tratamento de dados, outro acerca da menor lesividade.

2.5 Transparência

O quarto princípio evocado pela caracterização legal do legítimo interesse é o princípio da transparência, que na LGPD está positivado no art. 6º, VI. Além de um princípio geral da lei, aplicável a todas as hipóteses de tratamento de dados pessoais, no caso do legítimo interesse ele é reforçado pelo art. 10, §2º, segundo o qual "o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse".

A medida de transparência é parte do teste de balanceamento do legítimo interesse, que inclui, após a ponderação dos interesses do controlador ou terceiro e do titular, a inclusão de salvaguardas que possam mitigar quaisquer resquícios de desequilíbrio nessa relação. Quanto maiores os impactos do tratamento sobre o titular, mais atenção deve ser dada às salvaguardas, inclusive com o aumento da transparência e práticas de transparência ativa, isto

é, a abertura espontânea de informações, sem a necessidade de requisição por parte do titular.[52]

No caso específico dessa salvaguarda, é esperado que o controlador comunique ao titular, de forma clara e transparente (de fácil compreensão), sobre os diversos aspectos do tratamento, desde a sua realização até qual a base legal empregada e por quais motivos, ou seja, porque os interesses do controlador ou de terceiros se sobrepõem, no caso concreto, aos do titular. Tais informações devem ser explícitas, claras e fornecidas separadamente. Essa deve ser a regra, mas é importante pontuar que há espaço para relativização quando a medida de transparência exigir além do que pode ser considerado um "esforço razoável"[53] por parte do controlador.

Além disso, parte do dever de transparência diz respeito à comunicação clara, ao titular, sobre seus direitos, como prevê o art. 9º, §3º, segundo o qual:

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Não é apenas ao titular dos dados que interessa, entretanto, que haja ampla transparência sobre o tratamento com base no legítimo interesse. Isso é importante também para permitir o *escrutínio público* por parte de grupos de interesse (*stakeholders*) relevantes,[54] inclusive autoridades nacionais de proteção de dados.

52 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 42.

53 Esse é um conceito que deriva do RGPD (reasonable efforts); veja, por exemplo, o artigo 8(2).

54 MATTIUZZO, Marcela; PONCE, Paula. **O Legítimo Interesse e o teste da proporcionalidade:** uma proposta interpretativa. Internet e Sociedade, V. 2, n. 2, Dezembro de 2020. p. 70 "As medidas de accountability associadas ao legítimo interesse, neste ➔

Dito de outra forma, não é porque a base legal não é o consentimento que ela fica esvaziada de qualquer perspectiva de controle e, sobretudo, de contenção de abusos. Nesse caso, a autodeterminação é diferida, uma vez que o titular e a coletividade podem levantar a sua voz durante - e não apenas previamente a - uma operação de dados. Uma das possíveis consequências dessa lógica é que o LIA (*Legitimate Interest Assessment* - Teste do Legítimo Interesse) deveria ser objeto de publicidade.

Nesse sentido é que práticas de transparência ativa possuem fundamental relevância, pois servem como forma de *controle social e não apenas individual*. Adotando a perspectiva de que a proteção de dados tutela bens jurídicos de interesse da coletividade, como a não discriminação e a dignidade humana, a publicidade sobre as práticas de tratamento é de extrema importância. Há casos em que o tratamento abusivo de dados leva a violações de direitos afetos a todo um segmento populacional, sendo conhecidas as situações de discriminação por raça, gênero e perfil socioeconômico em virtude de usos abusivos de dados pessoais. A transparência ativa das empresas desempenha também um papel de responsabilidade social, sujeitando suas próprias práticas à apreciação pública, de um lado; e criando uma cultura que padroniza essa atitude nos mercados, de outro.

Por fim, destaca-se que a transparência ativa representa, mais do que o respeito a uma obrigação legal e um compromisso social do controlador, também uma simplificação de seus futuros e prováveis trabalhos. Primeiramente, porque, em alguns casos, a exigência de abertura total não poderá ser cumprida, a depender dos esforços técnicos razoáveis que isso demandar, conforme mencionado anteriormente. Em segundo lugar, porque se, nesses casos, o controlador for claro a respeito do tratamento de forma

→ sentido, representam exatamente formas de garantir a possibilidade de escrutínio posterior do emprego da base legal por parte de titulares e outros stakeholders, como o próprio regulador."

ativa, isso pode antecipar eventuais requisições individuais que seriam realizadas em caso contrário.

Síntese 10

O princípio da transparência é uma das normas que revelam que a autodeterminação informativa vai muito além do consentimento. Ao reforçá-lo como sendo uma das medidas de salvaguarda para a aplicação do legítimo interesse, há uma engenharia normativa que franqueia não só o controle individual, mas também social sobre as atividades de tratamento de dados ao longo do seu curso. Isso porque, embora a noção de esforços razoáveis possa, eventualmente, afastar a exigência de transparência no nível individual, medidas de transparência ativa devem ser estimuladas a fim de se garantir prestação de contas e responsabilidade. Recomenda-se, portanto, que o alcance de tais deveres de transparência seja explicitado pela ANPD e, por parte dos agentes de tratamento de dados, que seja encarado como uma medida de accountability.

2.5.1 Direito de oposição (opt-out)

O Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*) ressalta, em vários pontos[55] de seu parecer (Opinion) sobre legítimo interesse, "um direito incondicional de opt-out" como exemplo de salvaguarda que o controlador deve fornecer ao titular na aplicação da hipótese autorizativa do legítimo interesse. Inclusive,

55 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 3.

trata-se de um dentre quatro itens sobre os quais o parecer se debruça de forma mais aprofundada, junto à relação entre transparência, responsabilidade e prestação de contas (*accountability*) e o empoderamento dos titulares dos dados por meio do direito à portabilidade.

Mas e no caso da normativa brasileira? A Lei Geral de Proteção de Dados dispõe no art. 18, §2º, que "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". Trata-se de uma "maneira de o titular obstruir o tratamento dos seus dados"[56] e, com isso, ter mais controle sobre os dados, independente da base legal adotada. Isso porque a possibilidade de oposição vale para todas as bases legais ofertadas na lei, à exceção do consentimento, já que essa hipótese conta com a sua própria válvula de escape (a retirada do consentimento).

Resta, para fins de interpretação, um olhar detido sobre a condição que a lei impõe para o exercício do direito: "em caso de descumprimento da lei". Isto é, o direito de oposição poderá ser exercido pelo titular se houver desrespeito à lei por parte do controlador. Um cálculo possível, sugerido por Bioni[57], é considerar que, a partir do momento em que medidas de transparência (obrigatórias por força tanto do princípio da transparência, quanto da necessidade de informar ao titular a finalidade do tratamento) são aplicadas, ao titular é concedida a possibilidade de se manifestar sobre o tratamento. Caso ele manifeste sua discordância, por considerar que é contrário às suas legítimas expectativas, e caso o controlador não respeite essa decisão, haveria, então, um desrespeito à lei.[58]

56 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5, p. 247.

57 Ibidem. p. 248.

58 Trata-se, segundo o autor, de uma interpretação sistemática entre o art. 18, §2º, referente ao direito de oposição, e o art. 10, §2º, que fala da obrigatoriedade de medidas de transparência.

Cabe, contudo, a ressalva de que o direito à oposição, apesar de peça-chave a ser considerada em um processo de avaliação do legítimo interesse, *não é um direito absoluto*,[59] que deverá ser atendido em qualquer circunstância. Primeiramente, a própria condicionante do "descumprimento de lei" já indica que a prerrogativa não se aplica injustificadamente. Além disso, mesmo quando o titular manifesta discordância em relação a algum aspecto do tratamento, isso não deflagra, automaticamente, a exigibilidade do encerramento do tratamento dos seus dados. Isso porque, embora o titular possa decidir se opor ao tratamento, demanda-se uma análise contextual que leve em consideração todos os interesses em jogo.

Nesse sentido, trataremos de uma situação concreta que exemplifica o direito de oposição na prática e demonstra que nem sempre que o titular acusa o controlador de violar, por exemplo, sua legítima expectativa (subjetiva), isso de fato prevalece. Pode-se levantar a hipótese de uma empregadora que armazenou informações de comportamento impróprio de um colaborador. Não seria apenas a alegação de quebra de expectativas subjetivas por parte do colaborador que ensejaria o direito de oposição, uma vez que há margem para sustentação de um interesse do controlador que supera o do titular. Nesse caso, a violação do tratamento não é presumível, nem, portanto, surge de pronto o direito de oposição.

A situação mencionada, contudo, não afasta a conclusão de que o direito de oposição é a regra. Seria um equívoco pressupormos que o caráter contingencial inerente às ciências jurídicas implica na inexistência de direitos. Sem dúvida, há situações específicas e contextos não generalizáveis em que determinados direitos não são aplicáveis. Essa asserção, contudo, não pode levar à conclusão de que previsões legais deixaram de estar garantidas

59 Anota-se que a RGPD traçou um regime mais detalhado sobre o direito de oposição, enunciando, inclusive, uma hipótese aonde este seria absoluto - para fins de marketing (artigo 24 (2) (3).

em sua generalidade. A hipótese antes descrita apenas traça a ressalva de que, assim como todo e qualquer direito, a oposição do titular não é absoluta, existindo casos de conflitos em que sua aplicabilidade não ocorre automaticamente. Porém, a regra continua a ser a existência da prerrogativa.

Por fim, destaca-se que, conforme aquilo defendido pelo Grupo de Trabalho do Artigo 29, o *opt-out* pode ser encarado não apenas como um direito, mas também como uma das possíveis salvaguardas a serem aplicadas por iniciativa do controlador. Uma forma de, ao final do processo de balanceamento de interesses, mitigar os possíveis impactos negativos sobre o titular dos dados e "deslocar a balança" em favor da legalidade definitiva do tratamento.[60]

Síntese 11

A LGPD condiciona o direito de oposição à existência de um "desrespeito à lei". Sendo a legítima expectativa um dos parâmetros de legalidade do legítimo interesse, somado ao reforço do princípio da transparência, uma possível interpretação é que o direito de oposição poderia ser desengatilhado sob o argumento, por parte do titular, de que sua confiança foi frustrada, o que será analisado contextualmente tendo como baliza os outros interesses em jogo. Caso contrário, tais parâmetros teriam o seu alcance demasiadamente limitado. Essa é uma recomendação normativa que evita um regime assimétrico entre as bases legais, mais especificamente frente ao consentimento, já que

60 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 45.

nesse caso o titular dos dados detém o direito potestativo de revogá-lo a qualquer momento. Uma interpretação que coloque consentimento e legítimo interesse em pé de igualdade, tal como foram articulados no artigo 7º, é também uma questão de coerência normativa interna da LGPD. Apesar disso, reitera-se que o direito não é absoluto, podendo ser flexibilizado se a análise do caso concreto revelar que o interesse do controlador ou de terceiros supera a legítima expectativa do titular (e.g., prevenção a fraudes). Relevante, ainda, pontuar uma boa prática que pode ser objeto de orientação: a oposição, ou "opt-out", não apenas como algo que o controlador é obrigado a respeitar, mas sim como uma salvaguarda oferecida por ele, por iniciativa própria.

2.5.2 Prestação de contas e responsabilidade

Um quinto princípio que pode ser observado no legítimo interesse é o da responsabilidade e prestação de contas (*accountability*), disposto no art. 6º, X, LGPD. Ele fica evidente na primeira fase do teste dessa base legal - a verificação da legitimidade do interesse do controlador. Trata-se de análise que cabe a este agente, e somente a ele em um momento inicial, realizar. O controlador deve realizar um teste cuidadoso e apriorístico, levando em consideração os elementos concretos e também as expectativas do titular dos dados.[61]

Ademais, uma vez que a legislação brasileira é explícita no requisito da transparência, isto é, que o controlador evidencie para o titular tanto o tratamento em si, quanto as razões que o permeiam,

61 Ibidem. p. 43.

fica clara a obrigatoriedade de documentação do processo como um todo. Tal obrigatoriedade é reforçada pelo texto do art. 37, que, ao dispor sobre os agentes de tratamento de dados pessoais, prevê que "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

Tal previsão explícita, aliada aos elementos presentes no art. 10 (concretude da finalidade, legítima expectativa do titular, exigência de transparência), distanciam a LGPD do RGPD, já que, no caso da legislação brasileira, os requisitos dos testes de legitimidade e de balanceamento, bem como a questão do registro do tratamento, estão inscritos na letra da lei.[62] Isto vai desaguar em um exercício de documentação especial quando uma atividade de tratamento de dados estiver lastreada no legítimo interesse.

2.5.3 O teste do legítimo interesse enquanto um registro especial da atividade de tratamento de dados em quatro passos

Desde os trabalhos preparatórios da LGPD, já havia sido identificado que o legítimo interesse era uma base legal que atribuiria uma alta margem de discricionariedade aos agentes de tratamento de dados - o que deveria ser devidamente modulado. A saída brasileira foi: (i) prever parâmetros de aplicação no próprio texto da lei, dedicando, diferentemente das demais bases legais, um dispositivo inteiro que detalha qual deve ser o exame de qualificação para que um interesse seja legítimo; e (ii) reforçar a aplicação de alguns dos princípios e, ao cruzar o legítimo interesse à legítima expectativa e a um dever de proteção quanto ao impacto a direitos e liberdades fundamentais do titular, fez uma costura direta com o princípio da boa-fé e noção de abuso de direito.

62 Enquanto no direito europeu estes elementos vêm da interpretação e dos Considerandos do RGPD.

Tudo isso, somado ao realce de que o agente de tratamento de dados deve guardar os registros das suas atividades "especialmente quando baseado no legítimo interesse", conduz à implicação normativa de que o teste do legítimo interesse (*Legitimate Interest Assessment* - LIA) deve ser obrigatório. Como já adiantado, a LGPD, se comparada a outras leis de proteção de dados, tem um desenho normativo detalhado de tal base legal. Essa interpretação é, ainda, reforçada, com base em todo o processo de construção e aprovação da lei. Do ponto de vista hermenêutico histórico e teleológico, o legítimo interesse é uma espécie de bônus aos agentes de tratamento de dados, mas que vem acompanhado desse ônus de registro especial.[63]

O LIA aplicado no contexto do RGPD possui variações quanto a sua estruturação, de modo que há versões como a do *Information Commissioner Office*, que subdivide o teste em três fases, e versões como a do antigo Grupo de Trabalho do Artigo 29, que determina existirem quatro fases.[64] Em que pese a divergência interpretativa no cenário europeu, *a estruturação da normativa brasileira* se deu de tal forma que a subdivisão de um teste em *quatro fases* se mostra como a mais adequada. São estas: (i) legitimidade; (ii) necessidade; (iii) balanceamento; e (iv) salvaguardas.

Essas quatro etapas estão segmentadas em duas partes. A primeira parte, que compreende as três primeiras fases, atribui o juízo de valor da legitimidade do interesse ao controlador e/ou ao terceiro. A segunda parte, em que está condensada na quarta fase, consiste em uma espécie de por parte do próprio titular e entidades representativas do seu interesse. Esse último momento do teste cumpre uma função de extrema importância, que é assegurar voz à outra parte cujo interesse deve ser sopesado ao do

63 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2ª edição): capítulo 5, p. 247.

64 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. p. 33. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217en.pdf

agente de tratamento de dados, em linha com um dos fundamentos da LGPD: a autodeterminação informacional.

***Quadro Comparativo do Legítimo* Interesse na Europa e no Brasil**
Elaboração própria

Fase/Teste	Europa (ICO)	Europa (WP 29)	Brasil
Fase 1 - Legitimidade Juízo de valor do controlador ou terceiro	Art. 6(4), b, do RGPD; Recital 47 e 50, da Diretiva 95 • Situação concreta • Finalidade lícita	Art. 6(4), b, do RGPD; Recital 47 e 50, da Diretiva 95 • Situação concreta • Finalidade lícita	Art. 10°, *caput*, da LGPD • Situação concreta • Finalidade lícita
Fase 2 - Necessidade Requisitos constitutivos do legítimo interesse pelo controlador ou terceiro.	Art. 6(4), a, do RGPD; Recital 47, 49, 50, da Diretiva 95 • Adequação • Minimização • Outras bases legais	Art. 6(4), e, do RGPD; Recital 47 e 50, da Diretiva 95 • Avaliação de impacto • Natureza dos dados • Tipo de tratamento • Legítimas expectativas	Art. 10°, § 1°, da LGPD • Adequação • Minimização • Outras bases legais
Fase 3 - Balanceamento Requisitos constitutivos do legítimo interesse pelo controlador ou terceiro.	Art. 6°, (4), c, d, e; 6(1), f, do RGPD Legítima expectativa Direitos e liberdades fundamentais Salvaguardas: medidas de transparência, direito de oposição, pseudonimização[65]	Art. 6(4), c, d; 6(1), f, do RGPD; Recital 47, da Diretiva 95 Direitos e liberdades fundamentais Transparência Proporcionalidade	Art. 6°, I, 7°, IX, e art. 10°, II, da LGPD • Legítima expectativa • Direitos e liberdades fundamentais

65 Na interpretação do antigo Grupo de Trabalho do Artigo 29, as salvaguardas postas, enquanto requisitos a serem considerados na fase de balanceamento, constituem uma ➔

Fase 4 - Salvaguardas Garantias necessárias quando da aplicação da hipótese e contraditório pelo titular ou entidades representativas dos seus interesses	-	Salvaguardas: art. 6(4), e, do RGPD; Recital 50, da Diretiva 95 Medidas de transparência Direito de oposição Pseudonimização Portabilidade	Salvaguardas: art. 10°, § 2° e § 3°, da LGPD • Medidas de transparência • Direito de oposição • Pseudonimização

Assim, o Brasil optou por um teste do legítimo interesse de quatro fases. O mérito dessa divisão é arquitetar um circuito decisório que considera não apenas o juízo de valor a ser realizado pelo agente de tratamento de dados, mas, também, pelo próprio titular ou representantes de seu direito. Daí a importância em ter uma fase dedicada a destacar e reforçar os princípios que dariam voz a quem deve ter seus interesses sopesados. Por fim, destaca-se, ainda, que esses 4 passos refletem exatamente a estrutura do artigo 10 e a escolha do legislador brasileiro em não fazer um transplante legal inadequado daquilo que vinha sendo desenvolvido no contexto europeu.

2.5.4 Relatório de impacto à proteção de dados pessoais

O último parágrafo do art. 10 da LGPD trata dos relatórios de impacto à proteção de dados: "A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial".

➔ fase própria - e não parte da fase de balanceamento. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

A partir disso, surge o questionamento: seria o relatório de impacto à proteção de dados *exigível* em toda situação de aplicação do legítimo interesse? Nos parece que não, justamente pelo fato de que, a despeito dessa previsão, não é uma ou outra base legal que deflagra a exigibilidade do relatório de impacto, mas sim o alto risco da atividade em questão, conforme definição trazida pela Lei em seu inc. XVII, art. 5°.[66] Tal risco independe da base legal, até porque, vale lembrar, as hipóteses legitimadoras do tratamento de dados são equivalentes em hierarquia. Dessa forma, o relatório de impacto pode ser encarado como uma boa prática, mas não como uma obrigatoriedade, já que os deveres de responsabilidade e prestação de contas (*accountability*) e de registro das atividades já são integralmente supridos pelo próprio teste do legítimo interesse.

A diferença essencial entre essas duas avaliações é que o teste do legítimo interesse é deflagrado pelo próprio texto da lei e tem como objetivo avaliar a adequação da base legal do legítimo interesse. O relatório de impacto à proteção de dados, por outro lado, tem como gatilho o alto nível de risco de qualquer atividade de tratamento de dados pessoais. O alto risco pode, inclusive, ser identificado no teste do legítimo interesse e engatilhar um relatório de impacto. Assim, o relatório de impacto à proteção de dados pode operar tanto como um facilitador das várias fases de análise que a base legal exige para ser aplicável (como a verificação da necessidade) quanto como um instrumento para governança de dados e demonstração de conformidade com as obrigações legais previstas pela LGPD.[67]

66 Esse artigo deve ser combinado com o artigo 55-J, XIII, que é o dispositivo que qualifica o risco como sendo alto.

67 GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados pessoais. Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado AASP.** Nº 144. 2019. p. 176.

Síntese 12

Deve restar claro quais são os deveres desengatilhados pelo uso da base legal do legítimo interesse, mais especificamente acerca da não necessidade da elaboração de um relatório de impacto à proteção de dados pessoais, mas sim de um teste de proporcionalidade de 4 (quatro) etapas. É o ônus na medida certa do bônus que é o legítimo interesse, já que se trata de um tipo de documentação exigida justamente para modular a discricionariedade conferida aos agentes de tratamento de dados ao se valerem de tal base legal. Com isso, evita-se uma vulgarização dos relatórios de impacto, até porque não é a base legal que define se uma atividade de tratamento de dados apresenta alto risco.

BIBLIOGRAFIA

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

ALVARENGA, Marcos de Castro; LESSA, Beatriz Helena Mendes Ribeiro. **Técnica Legislativa**. Belo Horizonte, 2013. Disponível em: http://camaramuriae.mg.gov.br/portal/wp-content/uploads/2018/08/apostila-tec-legislativa-unificada.pdf

A. Watson, **Legal Transplants:** An Approach to Comparative Law, Edinburgh, 1974.

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

BRASIL. **Lei 13. 709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).

BUCAR, Daniel; VIOLA, Mario. **Tratamento de Dados Pessoais por "legítimo interesse do controlador":** primeiras questões e apontamentos. *In* Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Thomson Reuters, 2019

DATA PROTECTION NETWORK. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Reino Unido, 2017. p. 17. Disponível em: https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

ENGISCH, Karl. **Introdução ao pensamento Jurídico**. Trad. J. Baptista Machado. Fundação Calouste Gulbenkian, Lisboa, 8ª ed. 2001

GRAU, Eros Roberto. **Ensaio e Discurso sobre a Interpretação/Aplicação do Direito**. 5ª ed. Malheiros Editores

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados pessoais. Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado AASP.** Nº 144. 2019. p. 176.

LARENZ, Karl. **Metodologia da Ciência do Direito**. Trad. José Lamego, Fundação Calouste Gulbenkian, Lisboa, 3ª ed

LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado AASP.** Nº 144. 2019

LISBOA, Roberto Senise. **Confiança Contratual**. São Paulo: Atlas, 2012, p.143

MATTIUZZO, Marcela; PONCE, Paula. **O Legítimo Interesse e o teste da proporcionalidade:** uma proposta interpretativa. Internet e Sociedade, V. 2, n. 2, Dezembro de 2020

MARINHO, Arthur de Sousa. **Sentença de 29 de setembro de 1944**. Revista de Direito Administrativo, vol I. p. 227. Cf. também PINHEIRO, Hesio Fernandes. **Técnica Legislativa**. 1962. p. 100.

MARQUES, Cláudia Lima. **Contratos dos Código de Defesa do Consumidor:** o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011

MENEZES CORDEIRO, António. **Da boa-fé no direito civil**. Coimbra: Almedina, 2011

PARLAMENTO EUROPEU e CONSELHO DA UNIÃO EUROPEIA. Regulação 2016/679. General Data Protection Regulation

COMPREENDENDO O CONCEITO DE ANONIMIZAÇÃO E DADO ANONIMIZADO[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **Compreendendo o conceito de anonimização e dado anonimizado**, Portal Jota, 2020.

1. DADOS ANONIMIZADOS COMO A ANTÍTESE DE DADOS PESSOAIS: O FILTRO DA RAZOABILIDADE

A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto (HOUAISS e VILLAR, 2009, p. 140).

Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização (DONEDA, 2006, p. 44). Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados (COUNCIL OF EUROPE, 2014), variando entre: **a)** supressão; **b)** generalização; **c)** randomização e; **d)** pseudoanonimização[2].

Com maior ou menor grau de intensidade – *e.g.*, supressão ou generalização – nota-se um método cujo mote é gerenciar circunstancialmente a *identificabilidade* de uma base de dados. As características de cada dado e a percepção de eles estarem inseridos em uma gama de informações devem orientar tal análise.

Por isso, não há um único método ou uma combinação perfeita *ex ante* para parametrizar o processo de anonimização, devendo-se analisar contextualmente como este deve ser empreendido para que os titulares dos dados anonimizados não sejam reidentificados, nem mesmo por quem procedeu à sua anonimização.

Amarrar o conceito teórico de dados anônimos a uma *análise contextual*, com os olhos voltados para a irreversibilidade do

2 Para muitos, a pseudoanonimização não é considerada uma técnica de anonimização. Isso porque se substituem, apenas, os identificadores diretos – *e.g.*, nome, CPF etc. – por pseudônimos – *e.g.*, números aleatórios, de modo que a pessoa permanece sendo identificável em razão de tais pseudônimos serem um retrato detalhado indireto delas (WP 29, 2014, p. 20).

processo de anonimização, joga luz diretamente sobre o fator problemático dessa proposição: o seu caráter elusivo ou mesmo a sua impossibilidade teórica (TEIXEIRA, 2015).

Torna-se cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível. A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito (NARAYANAN e SHMATIKOV, 2010, p. 24).

Por essa lógica, qualquer dado pessoal anonimizado detém o *risco inerente* de se transmudar em um dado pessoal (TENE, 2013, p. 1.242). A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico.

Por isso, leis que adotam o conceito expansionista[3] de dados pessoais e, ao mesmo tempo, estabelecem uma dicotomia deste com dados anônimos correriam o risco de serem tautológicas. Isso porque haveria uma *redundância normativa*, já que dados anônimos seriam, em última análise, potencial e provavelmente, dados relacionados a uma pessoa identificável.

Para não gerar tal incoerência, a única saída foi a adoção de um "filtro" que delimitasse a *elasticidade* desse conceito expansionista – neste caso o termo identificável –, sob pena de a fronteira entre dados pessoais e dados anônimos ser sempre transponível.

E, nesse sentido, o direito comunitário europeu[4] e a LGPD[5] valeram-se do critério da razoabilidade para delimitar o espectro

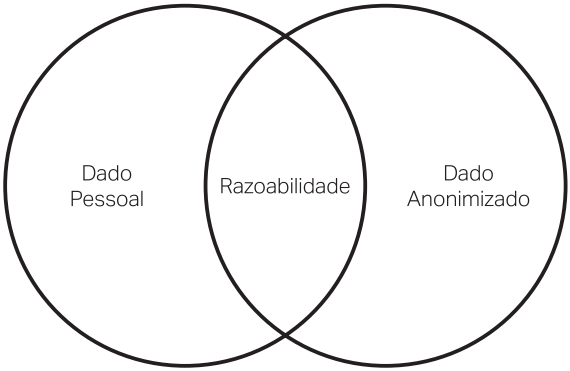
3 A definição do conceito de dados pessoais pode seguir uma orientação expansionista (a partir da delimitação de "pessoa identificável") ou reducionista ("pessoa identificada"), respectivamente alargando ou restringindo o escopo de aplicação da lei (BIONI, 2019).

4 A Diretiva 95/46 e a sua proposta de regulamentação adotam os conceitos de razoabilidade, respectivamente, nas Considerandas 26 (vinte e seis) e 23 (vinte e três).

5 Na definição de dados anônimos, de anonimização, bem como no dispositivo que prevê em quais hipóteses um dado anonimizado pode ser considerado como dado pessoal, a LGPD faz alusão ao termo razoável(is) – respectivamente, arts. 5º, II e III, e 18.

do conceito expansionista de dados pessoais. Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável (WP, 2007, p. 1.749). Essa vinculação deve ser objeto de um "esforço razoável"[6], sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável.

A contrario sensu, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável[7].



Com isso, há coerência em se estabelecer conceitos diferentes para tais espécies de dados, sobretudo sob o ponto de vista de uma dicotomia mutualmente excludente entre eles, que é

6 Essa é exatamente a terminologia utilizada pelo art. 12, *caput*, da LGPD: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

7 Ibidem, p. 21.

delimitada pelo fator da razoabilidade[8]. Do contrário, repita-se, haveria uma redundância normativa, na medida em que dados anônimos – sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, como aquele relacionado a uma pessoa identificável.

2. CALIBRANDO O FILTRO DA RAZOABILIDADE: CRITÉRIOS OBJETIVOS E SUBJETIVOS COMO FATORES DE UMA ANÁLISE DE RISCO E OS INCENTIVOS IMPLÍCITOS À PSEUDOANONIMIZAÇÃO

O legislador brasileiro procurou talhar uma norma neutra tecnológica[9]. Ao contrário de apontar para uma tecnologia em específico que poderia se tornar obsoleta ao longo do tempo, utilizou-se de um conceito indeterminado – razoabilidade – a ser significado e atualizado pelo próprio desenvolvimento científico. Simultaneamente, contudo, prescreveu balizas para reduzir a

8 Sobre as disputas interpretativas em torno do conceito jurídico indeterminado de razoabilidade, ver: BIONI, Bruno Ricardo. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. GPoPAI-USP, 2016, p. 34-35.

9 O conceito de "technology-neutral regulation" tem sido evocado para se discutir o desenho de modelos regulatórios capazes de estimular e acompanhar o desenvolvimento tecnológico, sem engessá-lo nem ser permissivo a riscos. Sobre isso: KOOPS, Bert-Jaap. Should ICT Regulation Be Technology-Neutral? *In*: Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds.). **Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners**, IT & Law Series, v. 9, The Hague: T.M.C. Asser Press 2006, ISBN 90-6704-216-1, pp. 77-108; REED, Chris. Taking Sides on Technology Neutrality. *SCRIPT-ed*, v. 4, issue 3, September, 2007; MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with 'technology' as a regulatory target. **Law, Innovation and Technology**, v. 5, p. 1-20, 2013. Para a discussão no cenário nacional, ver: BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo**, n. 273, p. 123-163, set./dez. 2016.

discricionariedade de tal exercício interpretativo e, com isso, alcançar um mínimo de previsibilidade quando tal norma viesse a ser colocada em movimento.

O primeiro eixo de análise é objetivo, sendo composto por uma matriz e dois elementos fatoriais respectivamente[10]: a) estado da arte da tecnologia; a.1) custo e; a.2) tempo[11]. Deve-se analisar o quão custoso e moroso seria reverter um processo de anonimização, de acordo com as tecnologias disponíveis para tanto. Trata-se, portanto, de uma análise dinâmica[12], a ser demarcada pelo próprio progresso tecnológico, que aponta qual deve ser o grau de investimento financeiro e temporal para se reidentificar uma base de dados anonimizada.

Por exemplo, há muito tempo se fala e se espera a chegada da computação quântica[13]. Quando isso acontecer, testemunhar-se-á um verdadeiro progresso acerca da capacidade, em termos quantitativos e qualitativos, de processamento de dados. Consequentemente, atualizar-se-á, por completo, o custo e o tempo quanto ao emprego das técnicas de anonimização, mas, também, por outro lado, das suas respectivas contra-tecnologias.

10 A GDPR, em sua Consideranda 26, também utiliza esses três fatores objetivos como delimitação à razoabilidade.

11 Artigo 12 da LGPD. Art. 12. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

12 A LGPD, em seu art. 5º, III e XI, define dado anonimizado a partir do emprego dos meios técnicos razoáveis disponíveis na ocasião (III) e no momento (XI) de seu tratamento. Esse tipo de avaliação torna-se, assim, contextual. Se, por um lado, essa análise contextual incentiva estudos sobre o tema, por outro, traz complicações à avaliação de seu cumprimento tendo em vista, por exemplo, diferenças quanto ao acesso à informação e recursos econômicos disponíveis entre os diferentes atores.

13 Em 08.01.2019 foi lançado o primeiro computador quântico de uso comercial do mundo. Contudo, estima-se um período entre cinco e dez anos para que a computação quântica passe a ser adotada nos negócios. Assim, apesar de existente, essa tecnologia não compreenderia o estado da arte da tecnologia (ou meio técnico razoável disponível, nos termos da LGPD), tornando um encargo demasiado excessivo a expectativa de sua adoção. Disponível em <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/como-computacao-quantica-vai-abalar-os-negocios-para-sempre.html>.

Em síntese, o primeiro eixo de análise propõe uma análise acerca do grau de *resiliência* de um processo de anonimização frente aos *padrões sociais*. Uma investigação de ordem objetiva cujo marcador é verificar como o estado da técnica calibra a escala de recursos (custo e tempo) para transmudar um dado anonimizado em dado pessoal.

O segundo eixo de análise é subjetivo. Deve-se levar em consideração quem é o agente de tratamento de dados e se ele dispõe de "meios próprios"[14] para reverter o processo de anonimização. Ao invés de considerar quais são os padrões sociais acerca da reversibilidade de um dado anonimizado, foca-se em analisar qual é a capacidade individual de engenharia reversa de quem processa tais dados. Abre-se, com isso, dois vetores importantes de análise.

Em primeiro lugar, sob o ponto de vista do fluxo de dados dentro de uma organização. É cada vez mais comum que organizações segmentem as suas bases de dados de acordo com suas respectivas áreas de negócio e, até mesmo em alguns casos, empreguem práticas de anonimização para a geração de *business intelligence/BIA*.

Por exemplo, é o caso de uma grande rede de loja varejistas que decide utilizar a sua base de dados de programa de fidelidade para melhorar o seu sistema de distribuição logística. Uma nova finalidade foi atribuída a um conjunto de dados, não sendo necessário saber quem são seus respectivos consumidores de forma individualizada, mas, tão somente, quais produtos têm mais ou menos entrada e saída de acordo com o perfil de vendas de cada um dos seus estabelecimentos geograficamente espalhados. Dessa forma, é factível a estruturação de uma nova base de dados sem que haja a associação direta ou indireta a indivíduos,

14 Artigo 12 da LGPD. Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente **meios próprios**, ou quando, com esforços razoáveis, puder ser revertido.

podendo ser mantida, inclusive, em separado da outra base de dados (programa de fidelidade) que lhe deu origem.

Nesse cenário, o próprio agente tem informações adicionais, ainda que mantidas separadamente, para reverter o processo de anonimização. Ou seja, ele possui meios próprios para transmudar um dado aparentemente anonimizado em um dado pessoal, o que é revelado com base em uma análise subjetiva focada na sua própria capacidade de entropia de informação[15].

O cenário acima descrito é o que se convencionou a chamar de pseudoanonimização, ou seja, uma falsa, superficial, técnica de anonimização que é quebrável em especial pela própria organização que a empregou.

A primeira reflexão que pode seguir a esse respeito é: por que a organização deveria empregar todo o esforço acima mencionado, se toda a carga regulatória da legislação de proteção de dados ainda assim recairá sobre ela (o dado não deixará de ser pessoal)?

Diferentemente da GDPR, a legislação de proteção de dados pessoais brasileira não sistematizou adequadamente a figura da pseudoanonimização, muito menos desenhou normativamente incentivos expressos para a sua adoção por parte dos agentes de tratamento de dados. Enquanto o regulamento europeu previu até mesmo o relaxamento de algumas obrigações legais[16], a lei geral brasileira de proteção de dados pessoais apenas citou pseudoanonimização de forma assistemática[17].

15 Entropia da informação é o uso de uma informação auxiliar para a reversão do processo de anonimização. No caso em análise, as informações adicionais em posse do agente de tratamento.

16 O artigo 11 da GDPR estabelece que, se o propósito do tratamento dos dados pessoais não exige (ou não exige mais) que o agente seja capaz de identificar o titular, o agente não será obrigado a manter informações adicionais para identificá-lo. E, por não o ser, estará escusado de garantir os direitos de acesso, retificação, exclusão e portabilidade do titular - a menos que o próprio titular, buscando exercer esses direitos, forneça as informações adicionais para sua identificação. Disponível em <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>.

17 Artigo 13 da LGPD. Art. 13. "Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados ➔

No entanto, ainda assim, é possível chegar à conclusão de que há sim incentivos, mesmo que indiretos, a serem burilados na lei geral de proteção de dados pessoais. Na medida em que pseudoanonimização é o "meio do caminho"[18] entre um dado pessoal e um dado anonimizado, seria possível correlacioná-la às diversas menções que a LGPD faz para que os agentes de tratamento "sempre que possível" anonimizem os dados[19]. Isto porque a lógica normativa em questão é encarar o processo de retirada dos identificadores de uma base de dados como algo que *minimiza os riscos* de uma atividade de tratamento de dados. Esse é exatamente o mote de técnicas de pseudoanonimização, ainda que não retire por completo o caráter pessoal de um dado.

Soma-se, ainda, o fato de que técnicas de pseudoanonimização podem compor o espectro de medidas, políticas e processos de um programa de governança que é referenciado pela LGPD[20].

➔ exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. (...) § 4º Para os efeitos deste artigo, a pseudoanonimização é o 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". O tema foi uma das últimas inclusões na Lei, tendo sido inserido pela primeira vez em 24.05.2018, pelo relator, deputado Orlando Silva, no substitutivo 1 ao PL 4060/2012 apresentado à Câmara dos Deputados.

18 Na pseudoanonimização, as informações adicionais que permitiriam a identificação do titular são mantidas em separado pelos agentes de tratamento, que podem, assim, reidentificar os dados se fizerem uso dessa informação. Contudo, caso excluam essas informações adicionais, os agentes não mais poderão efetuar a reidentificação "por meios próprios", caracterizando, assim, uma técnica de anonimização. É nesse sentido que a pseudoanonimização seria "o meio do caminho" para a anonimização.

19 A LGPD estabelece a necessidade de que, sempre que possível, haja a anonimização dos dados utilizados em pesquisas (arts. 7º, IV, 11, II, "c", 13 e 16, II), assim como determina que, embora uma das exceções à eliminação dos dados após o término do tratamento seja o uso exclusivo do controlador, ela está condicionada à vedação do acesso aos dados por terceiro e à anonimização dos dados (art. 16, IV).

20 Artigo 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 ➔

E, ainda, por ser uma medida tradicional de segurança da informação que pode reduzir significativamente os impactos de um incidente de segurança, a partir da simples constatação de que: **a)** uma base de dados pseudoanonimizada pode não ser reversível por terceiros-atacantes[21] e; **b)** certamente, gera menos riscos em relação a uma base de dados comprometida que não tenha havido o emprego de tais medidas.

Por fim, ainda quanto ao eixo de análise subjetiva, deve-se considerar o fluxo de dados para fora da organização. Nesse caso, como terceiros deteriam "meios próprios" para reverter o processo de anonimização dos dados. Trata-se de uma questão particularmente importante no que diz respeito a eventuais parcerias que envolvam o uso compartilhado de dados[22], mesmo que não sejam dados pessoais *a priori*.

Por exemplo, é muito comum que organizações se associem, mediante o compartilhamento e cruzamento de dados, para pesquisas científicas e outras atividades econômicas. Imagine o seguinte cenário:

➔ 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. (...) § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

21 Como as informações adicionais que permitiriam a identificação do titular são mantidas separadamente e em posse dos agentes de tratamento, terceiros terão maior dificuldade em reverter a anonimização.

22 Artigo 5º da LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) 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; (...)

a) uma pesquisa cujo objetivo é mensurar a eficácia de um determinado tratamento médico;
b) de antemão, reconhece-se ser necessário que a amostra de pessoas deve ser a mais ampla com objetivo de capturar pacientes com características distintas;
c) então, se faz necessário uma análise que envolva um conjunto de hospitais e clínicas médicas que trataram grupos de pacientes com diferentes perfis;
d) também se nota, desde logo, ser desnecessário o compartilhamento das bases de dados brutas (*raw data*), as quais identificariam diretamente cada um dos pacientes;
e) seria necessário apenas a indicação do perfil dos pacientes, os quais seriam agrupados de acordo com características semelhantes sem os tornar identificáveis *a priori*;
f) diversos testes de reidentificação foram executados, a fim de se assegurar e ser certificada a razoabilidade das técnicas de anonimização empregadas que correspondem ao estado atual da arte.

Apesar da situação hipotética descrever um cenário no qual a pesquisa rodaria em cima de uma base de dados anonimizada (critério objetivo – item "e"), isso por si só não encerraria a discussão acerca dos riscos de reidentificação. Deve-se verificar, ainda, se algum hospital ou clínica participante poderia lançar mão de "meios próprios" capazes de reverter o processo de anonimização da base como um todo. Mais uma vez, entra em cena uma análise subjetiva que é focada na capacidade de um agente em específico. Pense, por exemplo, que um dos hospitais deteria uma alta capacidade de entropia de informação, em razão de: **a)** deter uma série de informações adicionais por conta da sua capilaridade no setor com atendimento à grande parte da população representada no estudo; **b)** possuir tecnologias de processamento de dados disruptivas, que superam os padrões praticados até então no setor;

Dessa forma, também é relevante observar a capacidade subjetiva de terceiros que ingressem no fluxo informacional de uma organização. Especialmente, quando se tem em vista atividades de enriquecimento de dados que envolvam agentes externos para viabilizar uma atividade de tratamento de dados.

Em síntese, o legislador brasileiro adotou uma estratégia normativa alinhada à premissa de que os dados anonimizados seriam sempre passíveis de reversão. Os dois eixos de análise acima descritos – objetivo e subjetivo – compõem uma matriz de risco[23] em torno de possíveis engenharias reversas de um processo de anonimização. A *resiliência* de tal processo é o que determinará se haverá algum tipo de intersecção entre dados anonimizados e dados pessoais, cujos elementos de análise são de ordem objetiva (razoabilidade) e subjetiva (meios próprios).

3. EXEMPLIFICANDO ALGUNS FATORES DE RISCO: OS ENIGMÁTICOS TERMOS "NO MOMENTO" E "OCASIÃO" DO TRATAMENTO

Ao invés de considerar anonimização como algo cujo resultado (*output*) é infalível, foca-se em uma abordagem que considera a aplicação sistemática de técnicas de anonimização com o objetivo de agregar consistência ao processo como um todo[24].

23 Sobre a estratégia regulatória baseada no risco e, em particular, relacionada ao conceito de dado pessoal e dado anonimizado, veja-se: RUBINSTEIN, Ira; HARTZOG, Woodrow. Anonymization and Risk (August 17, 2015). **91 Washington Law Review**, 703, 2016; **NYU School of Law, Public Law Research Paper** n. 15-36. Disponível em: <https://ssrn.com/abstract=2646185>.

24 Ao se considerar todo o ciclo de vida dos dados em sua divulgação, a análise (e preocupação) se desloca *do dado* - i.e. seus atributos, qualidades e riscos em determinado momento - para *o processo* - i.e. a realização de um conjunto de ações voltado à proteção da informação durante toda o seu processamento. RUBINSTEIN, Ira S. e HARTZOG, ➔

Por essa razão, a análise acerca de se um dado deve ser, de fato, considerado como anonimizado é eminentemente *circunstancial*. Os dois critérios de análise – objetivo e subjetivo – acima mencionados ganharão vida somente a partir do contexto no qual está inserida uma atividade de tratamento de dados, sobre a qual se busca retirar, ao máximo, seus respectivos identificadores.

Aliás, não é por outra razão, que a LGPD amarra o conceito de dado anonimizado e anonimização, respectivamente, à "ocasião" e ao "momento" no qual se dá uma atividade de tratamento de dados pessoais. Na medida em que a definição de atividade de tratamento de dados engloba nada mais do que 20 (vinte) ações,[25] tudo o que é feito com um dado, o processo de anonimização deve representar um conjunto de ações contínuo e logicamente ordenado que abrace toda a extensão do ciclo de vida de um dado – da coleta ao descarte.

A título de exemplo, lista-se ao menos 06 (seis) fatores de risco (RUBINSTEIN e HARTZOG, 2015) e algumas medidas de mitigação:

a) **Volume dos dados**: quanto maior for a quantidade de dados, maiores são as chances de alguém fazer o caminho inverso de um processo de anonimização. Desta forma, modelos de negócios, produtos ou serviços e, até mesmo, políticas públicas (incluindo de dados abertos) que envolvam grandes massas de

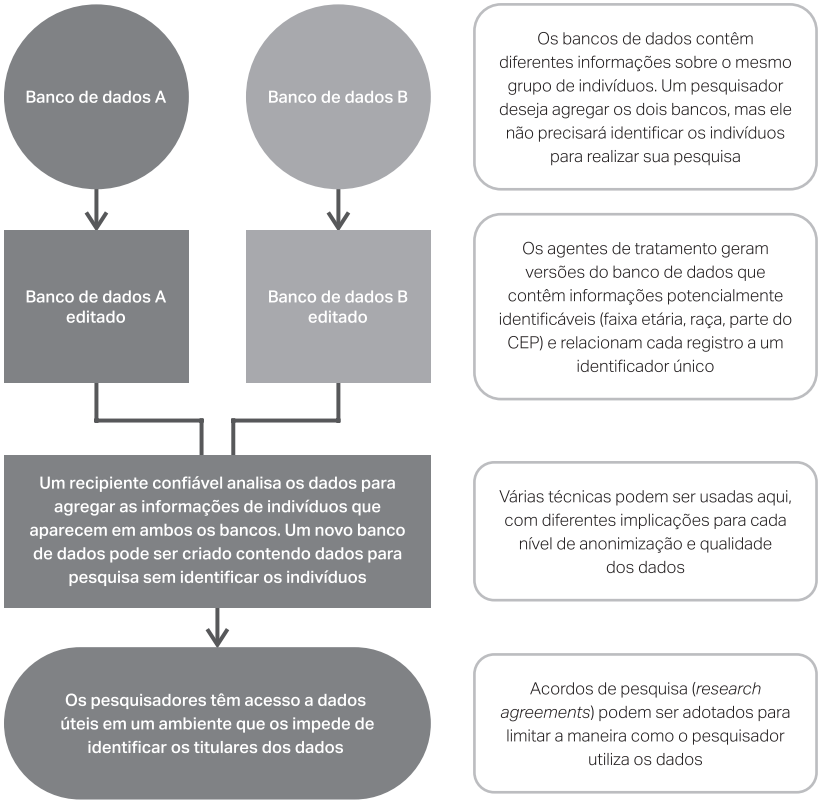
→ Woodrow. Anonymization and Risk. **New York University Public Law and Legal Theory Working Papers 530**, 2015.

25 Artigo 5º da LGPD: "Art. 5º Para os fins desta Lei, considera-se: (...) X - tratamento: 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; (...)".

dados devem proporcionalmente apresentar técnicas de anonimização correspondentes aos altos riscos de reidentificação em jogo;

b) **Natureza dos dados**: a natureza do dado (e.g., saúde, financeiro, geolocalização, etc) é determinante sobre o quão valiosas são eventuais informações que dele podem ser extraídas. Com isso, o apetite de terceiros e o quão recompensador seria reverter um processo de anonimização impulsiona os seus respectivos riscos de reidentificação;

c) **Cadeia da atividade de tratamento de dados (recipientes, compartilhamento e uso compartilhado)**: em muitas situações há uma complexa cadeia de atores para viabilizar um modelo de negócio ou mesmo uma política pública. Em regra, quanto maior for o ingresso de entidades para a geração ou mesmo o uso de uma base de dados anonimizada, mais elevado será o risco de sua reidentificação. Isto porque, não se aumenta apenas o volume do fluxo informacional (item "a"), como, também, a população que dele participa. Por exemplo, no caso acima mencionado relacionado à pesquisa científica, é comum se utilizar dos chamados "recipientes confiáveis". Esses são terceiros no qual organizações, que desejam gerar uma nova base de dados (anonimizado) a partir dos seus bancos de informações, confiam a sua execução. Uma espécie de filtro com relação a quem deteria poder informacional para reverter o processo de anonimização. Nesse caso, o ingresso do terceiro no fluxo informacional se dá justamente para tornar mais resiliente o processo de anonimização.



d) **Gerenciamento de identidades e segmentação**: tão importante quanto se colocar em prática processos de pseudoanonimização, é, também, controlar quem acessa as informações adicionais capazes de revertê-los. Por isso, é o caso de não só segregar fisicamente, mas, também, logicamente as bases de dados de uma organização (vide: exemplo supramencionado sobre uma rede varejista). Dessa forma, os riscos (internos) de reidentificação também passam a ser menores, na medida em que se reduz o número de atores que teria capacidade de juntar as peças do quebra-cabeça para formar a imagem dos titulares da informação. Nesse sentido, é importante destacar

que o Decreto do Marco Civil da Internet (Decreto 8.771/2016) já determina a adoção de mecanismos de gerenciamento de identidade a uma base de dados, inclusive com a previsão de sistemas de autenticação dupla e a individualização do respectivo usuário[26].

e) **Cláusulas contratuais**[27]: na medida em que fluxo informacional envolva cada vez mais agentes, em particular quando há o compartilhamento de dados para extração de informações, com ou sem os chamados "recipientes confiáveis", é cada vez mais comum cláusulas que: **a)** proíbam as partes de reverterem o processo de anonimização; **b)** delimitem o papel de cada um dos agentes de tratamento de dados de acordo com o objeto da atividade de tratamento de dados e, adicionalmente, vedando ou condicionando o repasse a terceiros que executariam tal atividade em nome de uma das partes; **c)** a destruição dos dados tão logo seja concluída a atividade de tratamento de dados ou caso haja a resolução de alguma condição pactuada;

f) **Atualização contínua**: anonimização é algo inacabado e fluído tal como é a própria definição da atividade de tratamento de dados, a qual procura capturar os dados em todos os seus

26 Artigo 13 do Decreto 8.771/2016. Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

27 FTC. Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers, 2012; ROSENFELD, Dana B.; HUTNIK, Alysa Zeltzer. Data security contract clauses for service provider arrangements (pro-customer). **Practical Law Company**, 2011.

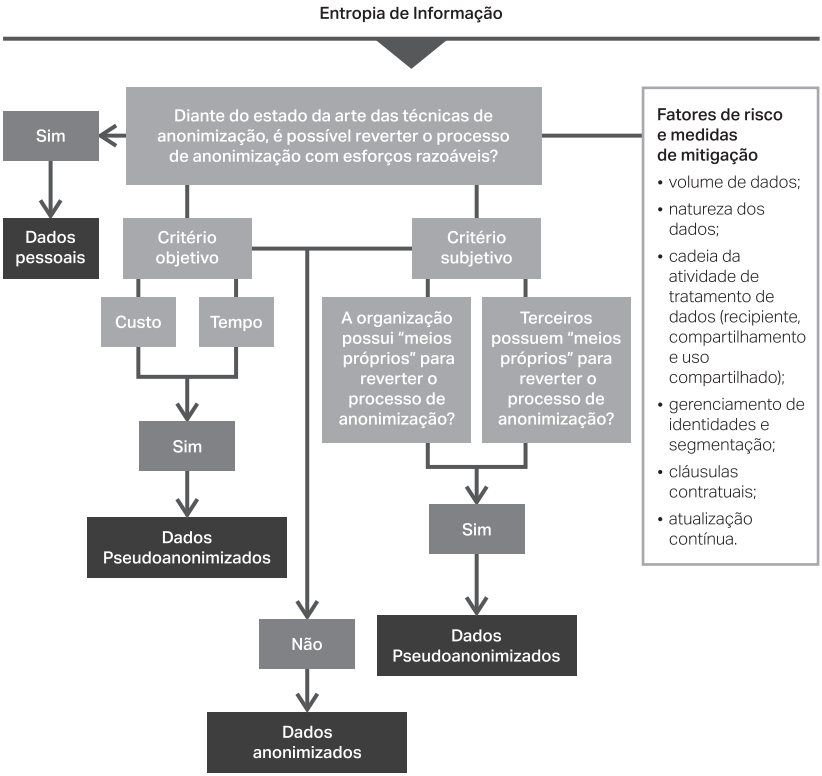
movimentos. Ao expressamente correlacionar o conceito de dado anonimizado e anonimização ao "momento" e de acordo com a "ocasião" na qual um dado está sendo processado, a LGPD procurou deixar claro que as técnicas de anonimização devem considerar toda a jornada de um dado e, sobretudo, ser constantemente atualizadas. Por exemplo, não adiantará um contrato de processamento de dados, que especificou todas as técnicas de anonimização e inclusive a forma pela qual os "recipientes confiáveis" as colocariam em prática, se esse contrato foi firmado há bastante tempo e tais medidas já se encontram defasadas. O *continuum* de uma atividade de tratamento de dados, espelhado por nada mais do que 20 (vinte) ações diferentes, também deve nortear a *dinamicidade* com a qual se emprega técnicas de anonimização[28].

Com isso, o legislador convida os agentes de tratamento de dados a conceberem e aplicarem as melhores técnicas de anonimização de acordo com as particularidades das suas respectivas atividades. É uma empreitada multifacetada, de ordem técnica, organizacional e, inclusive, contratual com o objetivo de controlar os riscos associados à reidentificação de uma determinada atividade de tratamento de dados.

28 Nesse sentido, uma das práticas previstas para se avaliar condutas pelo Modelo de Maturidade de Privacidade (*Privacy Maturity Model*), criado pelo Instituto Americano dos Contadores Públicos Certificados e pelo Instituto Canadense de Contadores (AICPA/CICA), é a otimização, i.e., "a revisão e a avaliação periódicas são utilizadas para garantir a melhoria contínua de determinado processo". Disponível em <https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf>. A aplicação desse modelo de análise (e a conformidade especificamente a essa prática) foi observada no tratamento de dados pessoais efetuado pela municipalidade de Seattle. Ver: Future of Privacy. City of Seattle: Open data risk assessment, 2018. Disponível em <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>.

4. CONCLUSÃO: MODELO ANALÍTICO ACERCA DO PROCESSO DE ANONIMIZAÇÃO DE UM DADO

A análise acerca de se a natureza de um dado pessoal, submetido a um processo de anonimização, pode ser transmudada envolve uma série de elementos. O teste abaixo agrupa logicamente os 07 (sete) critérios normativos prescritos pela própria LGPD e, ainda, lista, paralelamente, uma série de fatores, com base na literatura revisada, que ajudam na identificação do quão tolerável (razoável) são riscos de reversão das técnicas de anonimização aplicadas.



5. BIBLIOGRAFIA

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

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

COUNCIL OF EUROPE. **Handbook on European Data Protection Law**. Luxembourg: Publications Office of the Europe Union, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>.

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

HOUAISS, Antônio; VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa**. Rio de Janeiro: Objetiva, 2009.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". **Communications of the ACM**, v. 53, n. 06, June 2010. Disponível em: <www.cs.utexas.edu/~shmat/shmat_cacm10.pdf>.

RUBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and Risk. **New York University Public Law and Legal Theory Working Papers 530**, 2015.

TEIXEIRA, Lucas. **Teoricamente impossível**: problemas com a anonimização de dados pessoais. Disponível em: <https://antivigilancia.org/pt/2015/05/anonimizacao-dados-pessoais/>.

TENE, Omer. **Privacy law's midlife crisis**: a critical assessment of the second wave of global privacy laws. *Ohio State Journal*, v. 74, 2013.

A TRANSPOSIÇÃO DA DICOTOMIA ENTRE O PÚBLICO E O PRIVADO:
uma questão fundamental para a proteção dos dados pessoais[1]

Bruno Ricardo Bioni e Márcio Moretto Ribeiro

1 Originalmente publicado em: BIONI, Bruno R.; RIBEIRO, Márcio Moretto. **A Transposição da Dicotomia entre o Público e o Privado:** uma questão fundamental para a proteção dos dados pessoais. Portal Jota, 2015.

Os sites "Nomes Brasil" e "Tudo sobre Todos" tensionaram a questão da proteção de dados pessoais no cenário nacional. O "Nomes Brasil" permitia que o usuário pesquisasse, a partir do nome de uma pessoa, o seu número perante o cadastro nacional de pessoas físicas/CPF e, inclusive, o *status* de regularidade do contribuinte. Enquanto o "Tudo sobre todos" alcançava uma gama maior de informações, viabilizando, por exemplo, o acesso à data de nascimento, local de trabalho, endereços e nomes de parentes e vizinhos, cujo critério de pesquisa poderia ser o nome ou o número do CPF de uma pessoa.

Em ambas situações, a discussão foi orientada pelo fato de que tais dados seriam públicos. O CPF é o número identificador do cidadão brasileiro para a realização de operações financeiras. Ele deteria, assim, essa funcionalidade pública para individualizar alguém no trato dessas relações sociais em específico. Ao passo que a justificativa do responsável pelo site "Tudo sobre Todos" centrou-se na argumentação de que todas as informações disponíveis seriam, igualmente, públicas, tendo sido coletadas de cartórios, processos judiciais, diários oficiais, redes sociais, consultas em sites públicos e etc. Nesse sentido, tal plataforma "apenas" reuniria tais dados públicos dispersos, sendo esse o argumento em favor da sua legalidade.

A condução do discurso e do próprio debate em torno desses casos revela a importância de uma lei geral de proteção de dados pessoais. Ao contrário do direito à privacidade construído em torno da *liberdade negativa* do direito de "estar só", a salvo de interferências alheias e, enfim, da faculdade da pessoa retrair aspectos de sua vida ao domínio público; o direito à proteção de dados pessoais baliza-se por uma *liberdade positiva* de exercer sobre eles controle, pouco importando se eles são informações públicas ou privadas. Veja-se, portanto, a importância da proteção de dados pessoais angariar autonomia em relação ao direito de privacidade, já que ele não é calibrado por essa *dicotomia* entre público e privado.

No caso dos "Nome Brasil" a disponibilização dos números de CPF deu-se em um outro contexto que o de identificação do cidadão para operações financeiras. De forma similar, o site "Tudo sobre Todos", valeu-se de dados que foram utilizados para finalidades específicas de um determinado ato notarial, ato judicial, de uma rede social e assim por diante com relação às demais fontes de coleta dos dados pessoais. Em outros termos, tais plataformas trataram os dados pessoais dos cidadãos à revelia do seu consentimento e fora do contexto donde eles foram extraídos, o que determinaria a ilegalidade de tais aplicações.

Poderia se discutir que nos casos citados os dados tratados são públicos, porém não de acesso irrestrito. Esse seria o caso, por exemplo, das redes sociais, já que, somente, seus usuários podem acessá-las e não o público em geral. Além do mais, existem configurações de privacidade para limitar tal acesso apenas aos usuários que são seus "amigos". Estabelecer-se-ia, assim, uma linha tênue entre as definições de dados públicos e dados públicos de acesso irrestrito, demandando-se um certo esforço interpretativo.

De qualquer forma, não seria difícil imaginar um caso de compilação de dados pessoais sensíveis, apesar de serem de acesso público irrestrito – indexados na rede por exemplo - como a orientação política, sexual e religiosa. Por conseguinte, tais compilações de dados estariam fora do escopo de controle dos cidadãos, abrindo-se uma porta perigosa para a desproteção de dados pessoais. Isto porque, no final das contas, pode haver um volume de informações detalhado sobre uma pessoa a compor um perfil muito preciso sobre a sua personalidade.

Esse cenário torna-se, ainda mais, preocupante se for levado em consideração que vivemos em tempos de *Big Data* e *data aggregation*. Diferentemente da técnica "tradicional" de mineração de dados, o *Big Data* é uma tecnologia que descarta a etapa prévia de estruturação de dados, o que possibilita o processamento de dados em um volume, velocidade e variedade maior (os seus três famosos "Vs"). Com base em tal progresso qualitativo

e quantitativo permite-se uma agregação descomunal de dados, inferindo-se padrões de comportamentos e preferência dos seus titulares que são revelados após tal tratamento de dados. Dito de outra forma, outras informações pessoais podem ser extraídas de uma massa de dados, sendo este, aliás, o desiderato último da mineração de dados. O conjunto agregado dessas informações pode estruturar um perfil bem detalhado a orientar decisões, sejam elas automatizadas ou não, sobre a pessoa de carne e osso, ora intermediado por seus dados pessoais. Sendo essas bases de dados compostas por "dados de acesso público irrestrito", os cidadãos estariam sujeitos a tais processos de decisões à sua revelia.

Possibilitar-se-ia a formação de verdadeiras "caixas-pretas" sobre os cidadãos que retirariam a prometida esfera de controle sobre seus dados pessoais. Essa falta de transparência é o que norteia, aliás, a chamada indústria dos *data brokers*. Resumidamente, os data brokers são organizações que processam dados pessoais de diversas fontes para vender e revender tais informações com diferentes propósitos, o que perpassa desde a prevenção de fraudes até marketing e publicidade direcionada. Essas fontes são as mais variadas possíveis, incluindo-se dados de acesso público, como, por exemplo, aqueles extraídos de base de dados governamentais. No final das contas, muitos cidadãos têm sido "catalogados", sujeitando-se a um processo de tomada de decisões que nem sequer têm conhecimento a respeito. A lógica dos "dados de acesso público irrestrito" permitiria aos data brokers valerem-se de base de dados de acesso público irrestrito para continuar operando às escuras, sem que haja qualquer intervenção (entenda-se controle) do cidadão sobre seus dados pessoais.

Veja-se, pois, o risco de se operar na dicotomia reducionista entre o público e privado, ainda que sob a nova dimensão do "acesso público irrestrito". Corre-se o risco de se esvaziar, significativamente, a esfera de controle do cidadão sobre seus dados pessoais. Em tempos de *Big Data* e de agregação de dados, faz-se menos sentido, ainda, trabalhar dentro desse pensamento

binário. A premissa de que os dados pessoais – sejam ele públicos ou privados – devem gozar da mesma proteção legal permanece sendo uma questão fundamental e da ordem do dia, seja para a projeção de novas plataformas e modelos de negócio, seja para um olhar crítico em torno do horizonte normativo que se aproxima no cenário nacional.

MATERIAIS RECOMENDADOS

Boyd, Danah. **Privacy and Publicity in the Context of Big Data**. Disponível em: http://www.danah.org/papers/talks/2010/WWW2010.html

O'Neil, Cathy. **Weapons of Math Destruction**

Peppet e Ohm.**Big Data is not a Monolith**

A OBRIGAÇÃO DE REGISTRO DAS ATIVIDADES DE TRATAMENTO DE DADOS[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **A obrigação de registro das atividades de tratamento de dados**, Portal Jota, 2020.

Antes de mais nada, é importante apontar que a previsão da criação de um inventário dos dados não é em si nova no Brasil. O decreto de regulamentação do Marco Civil da Internet (Decreto No 8.711/2016)[2] já obrigava provedores de conexão e aplicações a manterem certos registros das suas bases de dados, ainda que o objetivo fosse voltado à segurança da informação. Visava-se, sobretudo, a criação de uma estrutura de controle para gerenciar e auditar quem, quando e como era feito o acesso e a manipulação das bases de dados, a fim de se garantir a sua integridade.

A lei geral de proteção de dados extrapola essa obrigação para muito além da perspectiva da segurança da informação.[3] Os agentes de tratamento de dados devem guardar registros de todas as suas operações de tratamento de dados pessoais. Levando-se em consideração que a definição do que é tratamento de dados engloba nada mais do que 20 (vinte) ações (*processing activities*)[4], ou seja, tudo o que é feito com dado: da coleta ao descarte. Definitivamente, é inédita a amplitude de tal obrigação de inventariança dos dados.

Por isso mesmo, poderia se pensar, em um primeiro momento, que organizações deveriam criar uma espécie de diário dos dados onde se anotaria literalmente tudo a seu respeito. No entanto, não nos parece ser esse o sentido normativo da obrigação em

2 Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: (...) III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; (...)

3 Artigo 37 da LGPD: "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

4 Artigo 5º da LGPD: "Art. 5º Para os fins desta Lei, considera-se: (...) X - tratamento: 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; (...)".

questão. Levando-se em consideração que a lógica por trás dessa obrigação legal é incultar nos agentes de tratamento de dados reflexão sobre um uso responsável dos dados, tal documentação deveria conter somente as informações pertinentes para tal juízo de valor. Caso contrário, quem faria tal catalogação e quem teria o poder-dever (órgãos reguladores) de requisitá-la despenderia uma energia desnecessária em meio a uma papelada infindável.

Por essa razão, o Regulamento Europeu de Proteção de Dados Pessoais (artigo 30) não só previu a obrigação de manter os registros das atividades de tratamento de dados, como, também, a calibrou. Há uma listagem das informações que deveriam compor um inventário de dados, a qual é, aliás, distinta para as figuras do controlador e processador. Destacamos o seguinte:

a) a finalidade do tratamento;
b) descrição das categorias dos dados e dos titulares;
c) o fluxo dos dados para fora da organização;
d) as medidas de segurança;
e) informações de identificação e contato do controlador;
f) os períodos para a exclusão das diferentes categorias de dados.

Portanto, ao invés de um diário dos dados onde se registraria todos os seus movimentos, tal instrumento deveria ser mais uma espécie de "ficha corrida" com os eventos mais importantes. Abusando do didatismo e da analogia, faria as vezes de um livro contábil com a descrição do fluxo e a gestão dos dados. Como dito, o objetivo é que agentes econômicos reflitam sobre os aspectos mais importantes das suas atividades de tratamento de dados, gerando uma documentação que, ao final, permita aos órgãos reguladores "puxar a capivara"[5] dos dados.

Diante disso, repita-se, tão importante quanto a previsão da obrigação do registro das atividades de tratamento de dados é a

5 "Puxar a capivara" é sinônimo da consulta aos antecedentes criminais de uma pessoa.

definição de quais deveriam ser seus componentes. Na medida em que a LGPD não chegou a tal nível de detalhes, do ponto de vista prático resta:

a) aguardar futura regulamentação da Autoridade Nacional de Proteção de Dados/ANPD, a qual deveria:
   1. precisar quais são os componentes de um inventário de dados, levando-se em consideração as particularidades entre controladores e processadores que podem resultar numa documentação igualmente distinta[6];
   2. considerar eventual exceção a tal obrigação legal, considerando-se o porte da organização e se a sua atividade de tratamento de dados seria de alto risco de acordo com as suas competências e de forma similar ao que fez o Regulamento Europeu[7];
b) na ausência de regulamentação da ANPD, socorrer-se de boas práticas e exemplos de outras jurisdições, como, por exemplo, da própria GDPR enquanto um patamar mínimo do que deve conter um inventário de dados.

6 Artigo 55-J da LGPD: "Art. 55-J da LGPD: "Art. 55-J. Compete à ANPD: (...) XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (...) XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (...)".

7 De acordo com o art. 30 (5) do Regulamento Europeu, estarão desobrigadas de realizar esses registros as instituições que (i) empregam menos de 250 pessoas, (ii) não realizam processamento de alto risco (iii) nem de categorias especiais de dados e antecedentes criminais, e (iv) realizam processamento ocasional. Os critérios são, portanto, cumulativos: "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

1. isso caso a organização não esteja sujeita à aplicação de ambas legislações, caso em que, por consequência, considerar a GDPR seria uma questão de *compliance* em sentido *strictu sensu*;

c) considerar tal obrigação enquanto um dos pilares de qualquer programa de conformidade, atentando-se para:
   a. o auxílio preferencialmente de uma consultoria técnica, a qual pode combinar métodos e soluções tecnológicas parcialmente automatizadas para a catalogação de bases estruturadas e não estruturadas;
   b. no cenário de organizações de médio ou pequeno porte, no qual o orçamento é enxuto e tal inventariança tende a ser feita internamente, considerar que o exercício de inventariança é muito próximo ao chamado mapeamento de dados. Diante disso, deve-se pensar em uma metodologia pela qual se evite a duplicação de esforços.
   c. Considerar que será um exercício contínuo, uma vez que o inventário deve retratar o organismo vivo que é uma organização em termos de tratamento de dados.

A obrigação de registro das atividades de tratamento de dados é a base de qualquer programa de governança de dados. Sem essa fotografia em série é impossível compreender o fluxo da informação, esboçar o que precisa ser modificado e o que pode ser mantido para estar em conformidade com a legislação de proteção de dados. Ao mesmo tempo, contudo, a amplitude dessa obrigação legal pode e deve ser melhor calibrada pela futura Autoridade Nacional de Proteção de Dados/ANPD para fins de segurança jurídica e equilíbrio econômico-regulatório, disciplinando especialmente o que deve compor um inventário de dados e, eventualmente, quais situações não atrairiam tal ônus. Até isso acontecer, resta seguir boas práticas e lembrar do exemplo corriqueiro no campo tributário: por mais que todos os tributos estejam devidamente recolhidos, ainda assim uma organização pode ser atuada caso não tenha sua escrituração contábil. É o mesmo racional com a LGPD.

ENTRE LINHAS DE CÓDIGO E DE FÁBRICA:
o que a GDPR tem a ver com o ex-presidente americano John F. Kennedy?[1]

Bruno Ricardo Bioni

1 Originalmente publicado em: BIONI, Bruno R. **Entre linhas de Código e de Fábrica:** o que a GDPR tem a ver com o ex-presidente americano Jonh F. Kennedy? Portal Uol, 2018.

Se você não se lembra, provavelmente seu pai ou avô, sua mãe ou avó devem se recordar o quão inseguros e perigoso já foram os bens de consumo um dia. Numa época em que as grandes indústrias estavam a pleno vapor, produzindo automóveis, medicamentos, alimentos, entre outras coisas; foi quando justamente se notou uma explosão de acidentes devido à utilização desses produtos mal fabricados. Foi com esse pano de fundo que nasceu a proteção do consumidor.

Em sua mensagem ao Congresso Americano em 1962, o ex-presidente John F. Kennedy alertou que "a marcha tecnológica" daquele período de industrialização havia gerado grandes desafios. Em particular à segurança dos consumidores, na medida em que esses bens de consumo se revelaram "perigosos" à saúde da população. Usando como exemplo a indústria de transportes, o discurso *kennedyano* apontava que o caminho seria apostar em como o "*design*" desses produtos poderia e deveria salvar vidas.

Alguns anos depois, no Brasil, em 1977, a Comissão de Inquérito Parlamentar/CPI do Consumidor também atentou para a necessidade de atuar no próprio processo de produção desses produtos, ou seja, antes que eles fossem lançados no mercado. Ao analisarem a indústria de veículos, os parlamentares consideraram que os automóveis deveriam "sair de fábrica" equipados com mecanismos que os tornassem mais seguros.

Passados mais de 40 (quarenta) anos, atualmente nós testemunhamos um movimento similar ao ocorrido nos anos 70. Justamente, em um período de reformatação da economia, o que por alguns já foi chamado de quarta revolução industrial. Nesse sentido, tem sido muito comum escutar que agora vivemos em uma sociedade e economia movida por dados.

Na análise de crédito, na precificação do plano de saúde, em um processo seletivo de emprego e, em um futuro bem próximo, com carros autônomos são os dados do nosso perfil socioeconômico, do nosso de estado de saúde, da nossa carreira profissional e do tipo ideal de um motorista prudente que calibram(rão) os

respectivos circuitos decisórios de todas essas situações. A concessão do empréstimo e a sua respectiva taxa de juros; o valor da mensalidade do plano de saúde; a aprovação para a segunda entrevista de trabalho; e, em caso de uma inevitável colisão, se o veículo desviará dos pedestres para se chocar com um poste e, com isso, também salvar a vida motorista. Tudo isso é e será calculado por um algoritmo com base nos dados nele imputados.

O Regulamento Europeu de Proteção de Dados Pessoais, a tão falada *General Data Protection Regulation/GDPR*, foi a primeira lei de proteção de dados pessoais no mundo a positivar (prever de forma expressa em lei) o conceito de *privacy by design*. Essa é uma metodologia pela qual desde a concepção de um produto ou de um serviço deve se levar em consideração a proteção dos dados pessoais dos cidadãos. Isso implica necessariamente na adoção de "medidas organizacionais e técnicas" para a "minimização" de todos os riscos em jogo, como faz referência expressa o próprio texto da lei europeia.

Nos exemplos acima, fica claro que esses riscos afetam uma série de liberdades fundamentais. Da nossa capacidade de consumo, do nosso acesso ao mercado de trabalho e à assistência médica e, até mesmo, a nossa integridade física. Nessas situações em que há uma avaliação sistemática das características de uma pessoa e na qual ela é submetida a um processo de decisão automatizada, a GDPR obriga a elaboração dos chamados "relatórios de impacto à proteção de dados pessoais".

Através desse instrumento, espera-se que os agentes econômicos possam identificar, avaliar e mitigar os riscos das suas próprias atividades. Se devidamente articulado e somado ao outro instrumento da privacidade por concepção – *privacy by design*", essa caixa de ferramentas da regulação europeia, formatada também pela Lei Geral de Proteção de Dados/LGPD (Lei 13.709/2018) pode induzir à concepção de produtos e serviços que têm o seu *design* – o código do seu algoritmo – projetado para prevenir a ocorrência de danos.

É uma racionalidade bastante próxima do que se testemunhou quando do nascimento da proteção do consumidor. Uma estratégia precaucionaria de danos e que visa a proteção de toda uma coletividade exposta e vulnerável a tais atividades econômicas. E, principalmente, que enxerga ser o design um dos principais elementos para se atingir tal resultado.

Progressivamente, nós assistimos como carros foram equipados com ferragens, cintos de segurança, sistemas de freios de diferentes gerações, *airbags*, entre outros mecanismos, que os tornaram mais seguros ao longo do tempo. Se hoje trafegamos em uma economia da informação, resta saber quais podem ser os seus equivalentes. A regulamentação europeia de proteção de dados e a LGPD podem ter a mesma importância que o discurso de *Kennedy* teve para a proteção do consumidor. Não estamos recalibrando e ressignificando uma tensão que já foi enfrentada antes por uma outra marcha tecnológica?

MATERIAIS RECOMENDADOS

Cavoukian, Ann. **Privacy by Design**: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. Disponível em: https://www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf

Langheinrich, Marc. **Privacy by Design – Principles of Privacy – Aware Ubiquitous Systems**. Disponível em: https://link.springer.com/chapter/10.1007/3-540-45427-6_23

Schaar, Peter. **Privacy by Design**. Disponível em: https://philpapers.org/rec/SCHPBD

PROTEÇÃO DE DADOS PESSOAIS E ELEIÇÕES:
um debate urgente[1]

Bruno Ricardo Bioni e Mariana Rielli

1 Originalmente publicado em: BIONI, Bruno R.; RIELLI, Mariana. **Proteção de dados pessoais e eleições:** um debate urgente. Observatório da Privacidade, 2020.

A Data Protection Commission, autoridade de proteção de dados irlandesa, deu início no final de janeiro de 2020 a um blog sobre proteção de dados pessoais e campanhas eleitorais. Trata-se de um tema "quente", que atinge boa parte dos países do mundo e mobiliza questões como manipulação de eleitores, propaganda direcionada e os impactos dessas práticas sobre a democracia.

A premissa do primeiro texto do blog da Comissão é que, quando dados pessoais forem utilizados para fins eleitorais, quem coleta e utiliza estes dados deve respeitar a privacidade dos cidadãos e adequar-se a normas de proteção de dados pessoais. Trata-se da mesma ideia que dá início ao paper "Privacy, Voter Surveillance and Democratic Engagement - Challenges for Data Protection Authorities", de Colin Bennett e Smith Oduro-Marfo, segundo o qual o tratamento de dados pessoais para fins eleitorais está no cerne dos esforços para o combate à manipulação eleitoral.

O artigo da Comissão passa, então, a descrever os direitos dos titulares de dados nesse contexto - da informação transparente, clara e concisa aos direitos de acesso, retificação e esquecimento (a GDPR, diferentemente da LGPD, garante o "right to erasure"). Quanto às obrigações dos candidatos, para os quais a Comissão também elaborou um guia rápido, a Comissão foca nos princípios de proteção de dados pessoais. A este respeito, dois princípios são pontos nevrálgicos do debate regulatório:

a) **necessidade-adequação**: há uma difícil equação, que ainda está longe de ser resolvida, em torno de quais são os limites de informações que partidos políticos e candidatos devem ter para performar o seu interesse legítimo em estabelecer uma comunicação efetiva com o eleitorado. A questão se complexifica, ainda mais, quando em determinados países, como é o caso do Brasil, o voto é obrigatório, de sorte que tal diálogo deve facilitar o exercício da cidadania;

b) **transparência**: no painel "Micro-direcionamento político sob investigação: lições das campanhas de 2019", na tradicional conferência "CPDP" em janeiro deste ano e que contou com

a participação de Colin Benett, uma das conclusões extraídas é que toda a tensão gira em torno de assimetria de informação: b.1) ainda são muito obscuras quais são as técnicas de perfilhamento (profiling), sobretudo como o perfil de um(a) eleitor(a) pode ser formado a partir da combinação de diversas fontes que nem sequer passam pela sua cabeça; b.2) é necessário ir além de iniciativas do porquê se vê um anúncio, porque elas revelam muito pouco. A abertura de toda a "biblioteca" de estereótipos seria um primeiro passo de um policy-making devidamente informado.

A relevância do posicionamento da Comissão irlandesa, e da iniciativa de produzir materiais específicos sobre o tema, está alinhada com a percepção de Bennett e Oduro-Marfo de que muito se produziu sobre a importância da privacidade para a democracia, mas pouco sobre como a democracia pode comprometer a privacidade (e, por consequência, é necessário que normas específicas regulem esta dinâmica). Esse comprometimento se dá, principalmente, pelo emprego de táticas de segmentação e *microtargeting* às escuras, sem transparência.

O *paper* trata, especificamente, do Brasil, país em que o extenso corpo legislativo que regula a relação entre campanhas e cidadãos não foi capaz de evitar o *microtargeting* e a manipulação. Duas coisas ocorreram, segundo os autores: a prevalência da coleta, compartilhamento e uso de dados sem consentimento e a centralidade de plataformas de mensageria como o WhatsApp. Segundo Rafael Evangelista e Fernanda Bruno, autores de outro *paper* sobre o assunto, essa combinação não é randômica e o seu link com um contexto mais amplo de desinformação dá conta do processo de radicalização ocorrido no país.

Como ponto positivo, Bennett e Oduro-Marfo identificam a aprovação e futura entrada em vigor da Lei Geral de Proteção de Dados brasileira, que traz um *framework* de princípios, direitos e deveres, e atinge os partidos políticos e seus candidatos. Além disso, destaca o fato das posições políticas serem consideradas dados sensíveis, revestidos de maior proteção. Especialmente, pelo

fato do rol de bases legais ser menor do que para dados triviais - artigo 11 da LGPD - e, no caso da lei brasileira, ter o consentimento como regra - de hierarquia normativa às outras 05 (cinco) bases legais - para destravar o fluxo informacional. Embora não o único, a legislação de proteção de dados representa um dos mais importantes pilares de sustentação, do ponto de vista jurídico, do combate a este cenário.

Como consequência, o papel das autoridades nacionais de proteção de dados (as chamadas "DPAs") é de centralidade. A título de conclusão, o *paper* elenca algumas das lições e desafios para as autoridades: a importância de entender a rede de campanhas políticas, a importância de entender todo o arranjo regulatório relativo às eleições, a importância da cooperação com reguladores nacionais, a importância da relação entre legislação de proteção de dados e financiamento de campanhas, a importância de proatividade na construção de orientações de boas práticas e, por fim, a importância de colaboração internacional.

A autoridade irlandesa, bem como a italiana, a francesa e a britânica, dentre outras, parece ter iniciado um movimento de adequada apropriação da pauta. No caso do Brasil, a Resolução do Tribunal Superior Eleitoral/TSE, afora a questão de doação de base de dados, limita-se a referenciar a Lei Geral de Proteção de Dados pessoais e não aprofunda os desafios acima citados. Muitas questões abertas e que precisam de arquiteturas normativas.

MATERIAIS RECOMENDADOS

Data Protection Commision Blogs. Disponível em: https://www.data protection.ie/en/dpc-guidance/blogs

Bennett, Colin; Marfo, Smith. **Privacy, Voter Surveillance and Democratic Engagement**: Challenges for Data Protection Authorities. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517889

O PRINCÍPIO DA PRECAUÇÃO NA REGULAÇÃO DE INTELIGÊNCIA ARTIFICIAL: seriam as leis de proteção de dados o seu portal de entrada?[1]

Bruno Ricardo Bioni[2] e Maria Luciano[3]

1 Este ensaio esteve presente na obra BIONI, Bruno Ricardo; LUCIANO, Maria, O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o seu Portal de Entrada?, *in*: **Inteligência Artificial e Direito - Ética, Regulação e Responsabilidade**, São Paulo: Thomson Reuters, 2019, p. 207–228.

2 Doutorando em Direito Comercial e Mestre em Direito Civil pela Universidade de São Paulo. Professor e Fundador do Data Privacy Brasil.

3 Mestra e Bacharela em Direito pela Universidade de São Paulo.

SUMÁRIO.

PALAVRAS-CHAVE

princípio da precaução; dano; incerteza; risco; responsabilidade; decisões automatizadas

SUMMARY.

KEY WORDS

precautionary principle; damage; uncertainty; risk; responsibility; automated decisions

I. INTRODUÇÃO E APONTAMENTOS METODOLÓGICOS

Concessões de crédito, apólices de seguro, direcionamento de anúncios em redes sociais, autocorretor em aplicativos de mensagem, reconhecimento facial e etc. Decisões automatizadas estão cada vez mais presentes no dia-a-dia das pessoas. Elas compreendem uma das técnicas de Inteligência Artificial (IA), que, em geral, procuram identificar padrões a partir da análise de dados por meio de uma lógica matemática (algoritmo) e aprendizado de máquina (*machine learning*).

Contudo, acreditar que algoritmos sejam isentos de subjetividade, erro ou manipulação é uma "ficção cuidadosamente construída" (GILLESPIE, 2014). A escolha de quais dados importam e porquê importam nesse processamento depende de suposições prescritas a esses sistemas. Problemas decorrentes de algoritmos enviesados têm sido frequentes.[4] Eles parecem indicar o abismo entre os desenvolvedores desse tipo de tecnologia e aqueles que são impactados por ela. Dentre as razões para isso têm sido apontadas a falta de regulação, monopólios no setor de IA, estruturas de governança insuficientes dentro de empresas de tecnologia, assimetrias de poder entre empresas e usuários, a distância cultural entre os responsáveis por pesquisas em tecnologia e a diversidade das populações nas quais essa tecnologia é utilizada (AI Now, 2018). Esse diagnóstico tem suscitado demandas sociais por maior transparência no uso de IA.

4 "Bias in criminal risk scores is mathematically inevitable, researchers say". Disponível em <https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say>. Facebook has been charged with housing discrimination by the US government". Disponível em <https://www.theverge.com/2019/3/28/18285178/facebook-hud-lawsuit-fair-housing-discrimination>. "Self-driving cars may be more likely to hit you if you have dark skin". Disponível em <https://www.technologyreview.com/the-download/613064/self-driving-cars-are-coming-but-accidents-may-not-be-evenly-distributed/>.

Como o emprego dessa tecnologia, em geral, demanda o processamento de dados pessoais, essas questões têm sido endereçadas em leis de proteção de dados. A Lei Geral de Proteção de Dados no Brasil (Lei no. 13.709/2018 - LGPD), por exemplo, prevê o fornecimento de informações sobre o tratamento desses dados, incluindo os critérios utilizados e a possibilidade de solicitar revisão de decisões automatizadas. Nesse sentido também a Regulação Geral de Proteção de Dados da União Europeia (RGPD) prevê o fornecimento de informações sobre a lógica do processamento automatizado, seu significado e consequências para o titular.

A discussão de transparência nesse caso, contudo, não parece tão simples. A transparência pura e simples dos sistemas automatizados empregados parece gerar outros problemas: perpetuação dos problemas caso as informações apreendidas não sejam utilizadas para mudança, podendo aprofundar assimetrias de poder já existentes; danos à privacidade e exposição de grupos já marginalizados; fornecimento de informações pouco úteis que podem se sobrepor a informações realmente úteis; criação do falso binário segredo/transparência; a invocação de modelos liberais que pressupõem plena capacidade de todos os indivíduos entenderem e processarem as informações fornecidas; a crença na causalidade, ainda pouco comprovada empiricamente, de que a transparência, sozinha, aumenta a confiança nas instituições; a impossibilidade de se disponibilizar *toda* a informação, sem considerá-las em seus contextos e histórias específicas; a preferência por *ver* uma informação ao invés de *entendê-la*; a desconsideração de que, por vezes, existem limitações técnicas à transparência (Ananny e Crawford, 2018). A *accountability* desses sistemas parece demandar, assim, um tipo de transparência *qualificada*. E, nesse cenário, o princípio da precaução, há muito invocado no campo da proteção ambiental, parece um *framework* útil para se pensar essa questão.

Nesse sentido, o presente artigo pretende investigar se leis gerais de proteção de dados são possíveis vetores de entrada para

a aplicação do princípio da precaução como parte da empreitada regulatória de Inteligência Artificial. Para tanto, analisa-se se o princípio da *accountability*, relatórios de impacto à proteção de dados pessoais e o direito à revisão de decisões automatizadas carregam consigo expressões normativas do princípio da precaução. Em particular, qual é o grau de abertura nos processos de tomada de decisão quanto ao emprego dessa tecnologia, bem como na ação ou inação em lançar mão de IA frente aos riscos que lhes são subjacentes. Analisa-se, ainda, a regulação efervescente de tecnologias de reconhecimento facial como um caso de fronteira que atrai diversos graus de aplicação do princípio da precaução.

O artigo está dividido em duas seções. A primeira delas mapeia o debate normativo em torno do princípio da precaução, buscando compreender sua racionalidade e verificar a procedência, ou não, das críticas feitas a ele. E a segunda seção pretende averiguar de que forma o princípio da accountability, relatórios de impacto à proteção de dados pessoais e o direito à revisão de decisões automatizadas poderiam servir como ferramentas à aplicação concreta desse princípio e, por fim, de que forma a regulação de tecnologias de reconhecimento facial também internaliza conotações normativas do referido princípio.

II. APLICAÇÃO DO PRINCÍPIO DA PRECAUÇÃO EM DISCUSSÕES REGULATÓRIAS: DEFININDO OS TERMOS DO DEBATE

Durante a década de 1970, desenvolveu-se na Europa um movimento em defesa de políticas públicas baseadas em evidência ("*evidence-based policy*"). Buscava-se com isso a promoção de análises rigorosas de políticas, com vistas a fornecer informação e conhecimento aos reguladores para sua implementação. Contudo, o reconhecimento de que essas discussões ocorrem em uma arena

política, permeada por valores, persuasão e negociação entre diversos atores, em que evidências e conhecimento científico são inevitavelmente valorados e ressignificados, requalificou o debate. Mais recentemente, muitos autores e instituições internacionais passaram a adotar a expressão "política públicas informadas por evidências" (evidence-informed policy") (Head, 2016).

Ademais, as incertezas e limitações do conhecimento científico acabam dificultando esse tipo de abordagem, impondo novos desafios a práticas regulatórias. O conceito de "incerteza" é mais complexo do que aparenta. Para além da falta de dados ou inadequação de modelos de avaliação de risco, ele também abarca a "indeterminação" (quando não se conhece todas as relações causais), a "ambiguidade" e a "ignorância" (*unknow unkowns*) (Science for Environment Policy, 2017). Os métodos tradicionais de regulação de risco (*risk assessment, risk management* e análises de custo-benefício), que pressupõem algum conhecimento e estimativas de probabilidade na antecipação de riscos, parecem não dar conta do desconhecido.

É nesse cenário que surge o princípio da precaução. Originado na década de 1970 a partir de iniciativas de proteção ambiental, o princípio passa a fazer parte, na década de 1980, do direito alemão () (Majone, 2002; Stirling, 2016). Seu significado, contudo, permanece em disputa até os dias atuais. Tem-se notícia de 11 (onze) significados diferentes atribuídos a ele nos debates sobre políticas públicas (Resnik, 2003). Destacamos os três mais importantes.

Uma das primeiras formulações, e a mais aceita por diferentes jurisdições (Stirling, 2016), é a da Declaração do Rio sobre Meio Ambiente e Desenvolvimento de 1992 (Rio 92), segundo a qual uma abordagem precaucionária deveria ser amplamente aplicada pelos Estados, de acordo com suas capacidades, para a proteção do meio ambiente.[5] A falta de "completa" certeza científica quanto

5 "Art. 15: In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be ➔

a ameaças de dano "sério" ou "irreversível" não poderia, assim, ser usada como desculpa para não se empregar medidas para evitar danos ambientais.

Em 1998, em uma conferência de cientistas, filósofos, advogados e ativistas ambientais em Wisconsin nos EUA, a Declaração de Wingspread (Wingspread Statement, 1998) determinou que medidas precaucionárias deverão ser tomadas em casos de ameaça de dano à saúde humana ou ao meio ambiente, ainda que relações causais entre a atividade e os possíveis danos não sejam estabelecidas cientificamente. Nesses casos, haveria ainda uma inversão do ônus da prova, cabendo então ao proponente da atividade demonstrar a segurança do seu exercício.[6]

Finalmente, em 2000, um Comunicado da Comissão Europeia (CE) buscou esclarecer pontos a respeito da aplicação do princípio que vinham sendo disputados em tribunais ao redor da União Europeia. Segundo o documento, o recurso à aplicação do princípio pressupõe efeitos potencialmente perigosos ocasionados por um fenômeno, produto ou processo, e cuja avaliação científica não fornece grau suficiente de certeza. Nesse caso, diversas seriam as medidas possíveis a serem adotadas, de contratos e acordos legalmente definidos a projetos de pesquisa e recomendações. Em alguns casos, inclusive, a medida correta seria não fazer nada.[7]

Nenhuma das formulações conceitua o que seja o princípio da precaução. Elas apenas indicam situações em que a abordagem e

→ used as a reason for postponing cost-effective measures to prevent environmental degradation."

6 "When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not established scientifically. In this context the proponent of the activity, rather than the public, should bear the burden of proof."

7 "Recourse to the precautionary principle presupposes that potentially dangerous effects deriving from a phenomenon, product or process have been identified, and that scientific evaluation does not allow the risk to be determined with sufficient certainty. In some cases, the right answer may be not to act or at least not to introduce a binding legal measure. A wide range of initiatives is available in the case of action, going from a legally binding measure to a research project or a recommendation."

lógica da precaução deve ser adotada. Essas situações podem ser mais ou menos restritivas, o que tem levado alguns autores a diferenciar graus de aplicação desse princípio de acordo com essas formulações históricas. Nesse sentido, Garnett e Parsons (2017), por exemplo, ao analisarem a jurisprudência europeia sobre o tema, observaram "ambiguidades inerentes" à determinação do nível de incerteza e o tipo de dano que justifiquem a invocação do princípio. Para esses autores, a Declaração Rio 92 representaria uma aplicação fraca do princípio da precaução, enquanto o Comunicado da CE e a Declaração de Wingspread teriam, respectivamente, uma aplicação moderada e forte.

Grau de força da aplicação do Princípio da precaução	**Fraca:** incerteza não justifica inação	**Moderada:** incerteza na avaliação do risco justifica ação	**Forte:** quando houver ameaça de dano, medidas de precaução devem ser tomadas; diante da incerteza, inverte-se o ônus da prova
Gravidade dos danos potenciais que demandariam ações de precaução	A **Declaração do Rio de 92** sugere que medidas podem ser tomadas para evitar "*danos sérios e irreversíveis*"	A **Comunicação da Comissão Europeia** sugere o uso de regulação proporcional ao nível de risco dos "*efeitos perigosos potenciais*", com avaliação científica objetiva preliminar	A **Declaração de Wingspread** determina que a responsabilidade de provar que uma atividade é segura recai sobre o proponente dessa atividade, mesmo que a relação causa e efeito não possa ser cientificamente determinada para evitar "*a ameaça de dano*"

Grau de incerteza ou qualidade das evidências que demandariam ações de precaução	É **permitida regulação na ausência de certeza científica**; medidas de precaução podem ser invocadas diante da incerteza	Pesquisas serão necessárias para reduzir incertezas; até lá, **ações de precaução incluem o estabelecimento de padrões regulatórios** com grandes margens de segurança	A **incerteza demanda a proibição da atividade potencialmente arriscada** até que o seu proponente demonstre que ela não oferece risco ou oferece risco aceitável
Natureza das ações de precaução	Pressuposto de **gerenciamento de risco**	Pressuposto de gerenciamento de risco implícito; **medidas sujeitas a revisão quando novas informações ou evidências científicas surgirem**	Pressuposto de se **evitar o risco**
Indicação dos atores envolvidos na avaliação dos riscos ou na definição das medidas a serem adotadas	A melhor maneira de tratar as questões ambientais é **assegurar a participação de todos os cidadãos interessados**; cada indivíduo terá **acesso adequado às informações** relativas ao meio ambiente, **inclusive informações acerca de materiais e atividades perigosas em suas comunidades**, bem como a oportunidade de participar dos processos decisórios	Julgar quais níveis de risco são "aceitáveis" é tarefa eminentemente *política*; os **processos de tomada de decisão devem ser transparentes e envolver o máximo de atores possíveis**	Corporações, entidades governamentais, organizações, comunidades, cientistas e outros indivíduos devem adotar uma abordagem de precaução para todos os empreendimentos humanos; o processo de **aplicação do princípio da precaução deve ser aberto, informado e democrático** e deve **incluir as partes potencialmente afetadas**

Tabela 1: Quadro comparativo das definições e aplicações do Princípio da Precaução

Fonte: Elaborada pelos autores com base em Garnett & Parsons D. J. (2017)

Entretanto, alguns pontos parecem comuns às formulações apresentadas. Primeiramente, não se trata de um recurso a ser invocado de maneira indiscriminada, havendo exigências de potencial dano.

Outro ponto importante é que, ao não definir expressões como "dano", "irreversível", "risco", "sério", as formulações parecem deixar a tarefa de fazê-lo às experiências participativas e deliberativas que procuram promover (Tabela 1). Essas expressões parecem conter uma presunção normativa em favor de certos valores ou qualidades que, em um regime democrático, caberia à toda a sociedade definir. Ademais, os valores a serem protegidos com a aplicação do princípio, como saúde, meio-ambiente e privacidade, quando confrontados com outros valores, demandam algum tipo de *trade-off* (Persson, 2016). Nesse sentido, o princípio da precaução reconheceria as assimetrias de poder e de informação dos processos de avaliação regulatória e ajudaria a remodelar os diferentes conhecimentos dos diversos atores envolvidos e afetados por esses processos (Stirling, 2016, p. 649). Trata-se, assim, de assumir compromissos com a deliberação e a *accountability*, assegurando justificações explícitas e cuidadosas sobre as escolhas regulatórias feitas diante de um "conhecimento incompleto" - algo que, inclusive, fomentaria e criaria obrigações para com a pesquisa e o conhecimento científico, com vistas a obtenção de informações sobre os riscos desconhecidos (Hartmann, 2012).

Compreender o princípio da precaução como um tipo de racionalidade a ser empregada durante a escolha das medidas regulatórias endereça as principais críticas feitas à sua aplicação. A primeira delas aponta a indeterminação de alguns dos conceitos utilizados nas formulações (*ill-defined*) (Majone, 2012; Sunstein, 2005). Essa crítica pressupõe tratar-se de uma regra procedimental e autossuficiente, o que o distanciaria da própria ideia de princípio. O Comunicado da CE endereça esse questionamento ao indicar o princípio da precaução como um *framework* para se

pensar medidas regulatórias, dentre as quais contratos, sanções, acordos legalmente definidos, financiamento a projetos de pesquisa e recomendações. É justamente essa tarefa de determinação que abre espaços para a discussão de valores a serem protegidos ou preteridos, convidando diferentes stakeholders a discutir padrões de segurança. Schomberg (2012) aponta essa abertura de padrões de atuação como uma característica positiva de regimes regulatórios em sociedades democráticas.

A segunda crítica caracteriza o princípio como "irracional" e "não científico" (Sunstein, 2005; Resnik, 2003) por seu suposto caráter normativo. Esses autores parecem atribuir uma confiança demasiada à crença do conhecimento *científico neutro*, presumindo que procedimentos regulatórios convencionais cientificamente orientados (e menos aberto à participação de diversos stakeholders, vale dizer) seriam capazes de transpor essa normatividade e indeterminação. Apenas os "experts" teriam competência para, "ao menos tentar", estimar e valorar os custos em uma análise de custo-benefício, enquanto "cidadãos comuns" imprimiriam seus medos irracionais às decisões regulatórias (Sunstein, 2005, p. 86). Além disso, essa crítica ignora que os métodos tradicionais de avaliação e gestão de riscos também demandam julgamentos avaliativos. Nesse sentido, o princípio da precaução seria tão "intrinsicamente imune" a manipulações como qualquer outro método (Stirling, 2016).

Finalmente, a terceira crítica à aplicação do princípio seria sua rejeição a novas tecnologias por seu caráter "paralisante", priorizando medidas que ponham fim ou dificultem o desenvolvimento tecnológico com determinações de "não-fazer" (Sunstein, 2005). Como já apontamos, a decisão por não tomar qualquer medida é apenas uma das possibilidades dentro do *framework* da precaução. O princípio tem por foco as razões para se tomar determinadas decisões regulatórias, e não as decisões em si (Stirling, 2016), bem como verificar qual é o nível de engajamento e participação pública nesses processos de tomada de decisão.

III. LEIS DE PROTEÇÃO DE DADOS PESSOAIS: O PORTAL DE ENTRADA PARA A APLICAÇÃO DO PRINCÍPIO DA PRECAUÇÃO EM DECISÕES AUTOMATIZADAS E REGULAÇÃO DE IA?

Uma vez realizada a radiografia do princípio da precaução, pretende-se verificar qual é o seu nível de aproximação frente aos objetivos regulatórios e o formato atual das leis de proteção de dados pessoais/LDPD. O princípio da *accountability* e os relatórios de impacto à proteção de dados pessoais, elementos centrais das LPDPs, revelam-se como possíveis feixes de entrada para a aplicação do princípio da precaução à IA, ainda mais quando se tem em vista que boa parte do emprego dessa tecnologia envolverá o processamento de dados pessoais.

III. A. Regulação da proteção de dados enquanto regulação de risco e o princípio da accountability: primeiro possível feixe de entrada do princípio da precaução[8]

Houve e está havendo uma virada "Copernicana" (Kuner, 2012) no campo da proteção de dados, representada por um "ponto de virada" em sua "moldura teórica". Se antes o sistema girava todo em torno da perspectiva da autodeterminação informacional, a sua rotação se dá cada vez mais ao redor de processos de gerenciamento dos riscos das atividades de tratamento de dados.[9]

8 Parte dos achados dessa subsecção derivam de outro trabalho: BIONI, 2019.

9 Veja os debates e os desafios teóricas dessa "risquificação" do campo de proteção de dados pessoais por: Quelle, 2017.

Como bem alerta Rafael Zanatta (2018), não se trata de "um processo de colisão jurídica ou de substituição normativa", mas de uma nova tipologia a respeito da emergência de mecanismos mais centrados na identificação e mitigação das incertezas e das probabilidades dos malefícios decorrentes da manipulação das informações pessoais dos indivíduos. Nadezhda Purtova resume bem: há uma guinada de "*informational self-determination*" na direção de "*information-induced-harms*" (Purtova, 2018). Em poucas palavras, o *saldo normativo* das novas leis de proteção de dados pessoais é resultado cada vez mais de uma *arquitetura precaucionária* de danos.

O fio condutor de todo esse processo é o acirramento da assimetria de informação[10], o qual, apesar de ser um elemento histórico da própria formação de leis de proteção de dados[11], atingiu um patamar ainda mais elevado diante dos avanços da tecnologia e pela consolidação de uma economia movida e orientada por dados. A nova onda de tecnologias de informação e comunicação (TICs) tornou ainda mais exponencial os possíveis efeitos adversos de uma atividade de tratamento de dados pessoais. Juntas, Internet das Coisas, *Big Data* e Inteligência Artificial permitem a coleta massiva de informações pessoais e, principalmente, inferências mais intrusivas a respeito dos cidadãos (Spina, 2014). Com isso, torna-se mais complexo o processo de cognição, avaliação e gerenciamento dos riscos de uma economia de dados. Os agentes de tratamento de dados – controladores e operadores – passaram a deter uma superioridade informacional ainda maior frente

10 Com maior ou menor intensidade o debate regulatório de proteção de dados pessoais sempre envolveu o gerenciamento de risco, mas o que nos parece mais sintomático é a complexificação no processo de reunião de informação para tomadas de ações ou inações para a modificação de comportamentos, o que impacta o próprio conceito e empreitada de regulatória desse campo. Veja, nesse sentido: Gellert, 2016.

11 Veja, por exemplo, a própria decisão da Corte Constitucional Alemã que, ao cunhar o termo autodeterminação informacional, traz ínsita a ideia de reduzir a assimetria de informação perante o cidadão para que o cidadão tenha controle sobre seus dados. Schwabe, Martins e Woischnik, 2005.

aos demais atores – cidadãos e órgãos fiscalizadores – desse ecossistema.

Esse é o pano de fundo que está por trás de uma estratégia que desloca mais "competências decisórias" (Quelle, 2017, p. 96) para quem está com a "mão na massa" dos dados. A introjeção ou o reforço[12] de ferramentas como relatórios de impacto à proteção de dados indicam o tamanho da fé que está sendo depositada em tais agentes da cadeia de tratamento de dados. A partir dessa e outras ferramentas (Bennett e Raab, 2006), espera-se que a empreitada regulatória seja cada vez mais colaborativa com quem está no "chão da fábrica" e, sobretudo, que contas sejam prestadas - princípio da *accountability* - acerca das ações tomadas para avaliar e gerir os riscos em jogo.

Nesse cenário, o princípio da *accountability* apresenta-se como um vetor determinante para a *abertura* dos processos de tomada de decisão acerca do que será considerado como um *risco tolerável* nas atividades de tratamento de dados. Isto porque a participação e o engajamento público em tais circuitos decisórios serão diretamente proporcionais ao quão elástico será o conteúdo de tal obrigação de prestação de contas por parte dos agentes econômicos. Com isso, permite-se, ao mesmo tempo, que a discussão seja porosa a valores eventualmente preteridos, uma vez experimentada a participação de atores com um outro olhar e motivados por interesses até mesmo antagônicos por parte de quem tem o dever de reportar.

Esse é o ponto de chegada proposto pelo jurista italiano Alessandro Mantelero, ao defender um arranjo institucional multissetorial em tais processos de tomada de decisão (Mantelero, 2016). Tal olhar plural seria o gatilho inclusive para considerações de ordem ética, social e de direitos humanos, muitas vezes

12 Com exceção de *privacy by design*, todo os outros mecanismos já estavam positivados leis de proteção de dados ainda que com um grau mais normativo apagado. Por isso, fala-se em reforço e não apenas introjeção.

negligenciados por análises tecnocráticas, com o objetivo de conter riscos sistêmicos e de ordem coletiva (Mantelero, 2018).

Na medida em que boa parte dos processos de decisões automatizadas com o emprego de IA envolverá o processamento de dados pessoais, leis gerais de proteção de dados, talhadas com base em uma mentalidade de regulação de risco e no princípio da *accountability*, são vetores de democratização do próprio processo de regulação de tal tecnologia. Tais leis apresentam-se como um feixe de entrada para a aplicação do princípio da precaução, em sua conotação de deliberação pública, acerca da adoção ou não de IA em vista da definição do tipo de riscos que lhes são subjacentes.

III.B. Relatórios de Impacto: o grau de força de aplicação do princípio da precaução

Os relatórios de impacto à proteção de dados pessoais (RIPDP) têm ganhado um protagonismo cada vez maior nas leis de proteção de dados pessoais (Wright e De Hert, 2012). Em linhas gerais, tais relatórios seriam a documentação pela qual o controlador - quem tem poder de tomada decisão na cadeia de tratamento de dados – registraria seus processos de tratamento de dados e as respectivas medidas adotadas para mitigar riscos gerados aos direitos dos titulares dos dados.

No cenário europeu, o controlador é obrigado a executar um RIPDP sempre que houver um *alto risco em jogo*. Há uma lista exemplificativa das hipóteses em que o tratamento de dados seria de alto risco, destacando-se a situação de perfilhamento[13] como

13 De acordo com a definição adotada no RGPD: "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"

ponto de apoio para tomada de decisões. Através dessa definição, o emprego de IA para automatização de processos de concessão de crédito, precificação de planos e seguro de saúde, seleção ou recrutamento de candidatos, elegibilidade a programas de assistências social, dentre uma outra série de situações do nosso cotidiano, deveriam ser antecedidos pela elaboração de um RIPDP. Além disso, quando o controlador não encontrar meios para mitigar os prováveis malefícios da sua respectiva atividade, deve, nesse caso, aguardar "luz verde" do regulador para seguir em frente.

No cenário brasileiro, a lei geral de proteção de dados pessoais não procedimentalizou minimamente o RIPDP. Muito embora haja algumas menções a tal instrumento, não há um capítulo próprio para tratar da matéria. Dessa forma, o RIPDP estaria condicionado à regulação posterior por parte de órgãos reguladores que precisariam quando seria obrigatório, bem como quais elementos e o tipo de análise que se espera encontrar em tal documentação.

No cenário americano, há, igualmente, um projeto de lei,[14] de autoria dos Senadores Cory Booker e Ron Wyden, que obriga a elaboração de relatórios de impacto à proteção de dados, bem como de um relatório de impacto mais genérico, nas hipóteses em que não há o tratamento de dados pessoais, toda vez que houver o emprego de IA para automatização de processos de tomada decisão. Intitulado como , diferentemente da racionalidade regulatória europeia, não há a previsão da necessidade de iniciar uma conversa com o regulador quando se deparar com uma situação de alto risco e na qual não se encontrou medidas para controlá-lo.

Do norte ao sul global e dos dois lados do Atlântico, nota-se a emergência de uma racionalidade regulatória bastante próxima ao conteúdo normativo do princípio da precaução. Cabe ao proponente da atividade demonstrar a segurança da sua atividade,

14 Disponível em: <https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf>

especialmente as medidas adotadas para gerenciar os seus respectivos riscos. Diferem, no entanto, com relação ao grau de força do princípio da precaução:

Grau de força da aplicação do Princípio da precaução	**Fraca:** incerteza não justifica inação	**Moderada:** incerteza na avaliação do risco justifica ação	**Forte:** quando houver ameaça de dano, medidas de precaução devem ser tomadas; diante da incerteza, inverte-se o ônus da prova
RGPD (EU)	**Forte:** ao se deparar com uma situação de alto risco que não pode ser mitigado por meio de medidas adequadas em acordo com a tecnologia disponível e os custos de implementação, o controlador não deve seguir em frente com o tratamento de dados e, ainda, deve consultar antes a autoridade de proteção de dados (*prior notification*).		
Accountability Algorithm (USA)	**Moderado:** apesar de obrigar a elaboração de RIPDP em situações de alto risco, é silente quanto à eventual paralisação de uma atividade quando houver ameaça de dano e medidas de prevenção. Dessa forma, a incerteza quanto aos malefícios de uma atividade pode justificar ação, sendo uma discricionariedade do próprio proponente da atividade		
LGPD (BR)	**Fraca:** ao não procedimentalizar minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser os elementos a compor tal documentação, a incerteza quanto aos malefícios de uma atividade não justifica inação. No entanto, regulação posterior, por parte dos órgãos reguladores (e.g., ANPD), podem alterar o *status* de força de aplicação do princípio da precaução em questão.		

Tabela 2: Quadro comparativo da aplicação do princípio da precaução quanto ao desdobramento e exigências de relatórios de impacto à proteção de dados pessoais
Fonte: elaboração pelos autores

Em conclusão, um outro possível vetor de entrada para a aplicação do princípio da precaução na regulação IA são os RIPDPs previstos em leis de proteção de dados pessoais. No entanto, varia o grau de força com que ele é cristalizado a partir de tal ferramenta, especialmente se a avaliação do risco resultará em

ação ou inação por proponente da tecnologia em lançá-la ao meio ambiente.

III. C. Direito à revisão de decisões automatizadas: princípio da precaução como racionalidade para o direito à explicação

O direito à explicação decorre do princípio da transparência[15], previsto na maioria das leis de proteção de dados do mundo (Monteiro, 2018). A RGPD, por exemplo, prevê o direito à informação *qualificada* (*meaningful*) sobre a lógica dos processos de decisões automatizadas (Selbst e Powles, 2017). Já a LGPD, em seu art. 20, garante o direito de revisão de decisões tomadas unicamente por tratamento automatizado. A lógica do direito à explicação e do direito à revisão de decisões automatizadas que impacta o titular dos dados, contudo, já havia sido inaugurada, no Brasil, no artigo 5º da Lei de Cadastro Positivo (Lei 12.414/2011).[16] Ao não dispor de uma proibição geral à perfilização, o dispositivo parece objetivar a garantia do direito à não discriminação[17] e fornecer instrumento

15 LGPD, art. 6º, "VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;". RGPD, art. 5. "Personal data shall be: 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".

16 Art. 5º São direitos do cadastrado: IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados.

17 Art. 8º São obrigações das fontes: VI - fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados.

para a identificação de potenciais violações de direitos (Zanatta, 2019).[18]

A explicação surge, assim, como uma ferramenta à *accountability* de IA ao expor a lógica da decisão, devendo permitir ao observador determinar a extensão em que um *input* particular foi determinante ou influenciou um resultado (Doshi-Velez e Kortz, 2017). Entretanto, os segredos comercial e industrial constituem objeções à transparência.

A abordagem da precaução parece ser útil na definição dos contornos desse debate. De um lado, ela colabora na construção de espaços de deliberação para se discutir o que seria "informação qualificada" ou como mitigar os problemas em decisões futuras. De outro, ela possibilita endereçar questionamentos a respeito dos segredos comercial e industrial. Ao exigir informações sobre a racionalidade de uma decisão específica, o direito à explicação não se confunde com a transparência pura e simples. Variações nos dados de raça, por exemplo, já poderiam fornecer o impacto e a maneira como esse tipo de dado impacta uma decisão, sem, contudo, demandar a revelação de todo o sistema automatizado envolvido naquela decisão (Doshi-Velez e Kortz, 2017). Ademais, espaços deliberativos com a participação de diversos atores podem ajudar a mitigar os custos envolvidos em sistemas de explicação - que, de outra forma, poderia afetar desproporcionalmente empresas menores - bem como os desafios tecnológicos de se pensar esse tipo de sistema.

18 Lógica semelhante à do Código de Defesa do Consumidor (Lei No. 8.078/90), que prevê a transparência e a boa-fé como princípios norteadores (artigos 4º, 6º e 43).

III. D. Tecnologias de reconhecimento: um caso de fronteira à aplicação do princípio da precaução

Reconhecimento facial parece ser o estopim de uma demanda regulatória represada em torno de inteligência artificial[19] de uma maneira geral (AI Now, 2016).[20] Evidências sobre os altos índices de falso positivos[21] e, principalmente, revelações em torno do reforço de práticas discriminatórias (Garvie, 2016) a partir do seu emprego para fins de policiamento preditivo, fizeram com que vários atores do campo de políticas públicas se movimentassem recentemente.

No setor privado, ao clamar por uma regulação estatal, o presidente da Microsoft, Brand Smith, mostrou ceticismo caso se apostasse em uma autorregulação do setor que forçaria as empresas a escolherem entre responsabilidade social e sucesso no mercado.[22] Por parte do terceiro setor, a American Civil Liberties Union (ACLU) ganhou adesão dos próprios funcionários da *Amazon* ao peticionar que a empresa suspendesse a venda de tecnologias de reconhecimento facial para autoridades de repressão penal.

As incertezas quanto aos benefícios e os riscos do emprego de tecnologias de reconhecimento facial formaram uma arena

19 É a partir do emprego de algoritmos supervisionados ou de autoaprendizagem que se torna possível treinar uma máquina (machine-learning) a reconhecer padrões em imagens e, com isso, identificar não só os donos de seus rostos, mas, até mesmo, o seu respectivo estado emocional. Essa última técnica ficou conhecida como *affect recognition*.

20 Veja, a título de ilustração, as primeiras discussões do AI Now 2017: https://ainowinstitute.org/AI_Now_2016_Report.pdf

21 Em maio de 2018, a BBC divulgou estudo do grupo Big Brother Watch, que, baseado em pedidos de informação encaminhados a todas as forças de segurança do Reino Unido, identificou números desproporcionalmente elevados de falsos positivos em Londres e no País de Gales. Matéria disponível em: https://www.bbc.com/news/technology-44089161

22 O posicionamento completo pode ser acessado em: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

regulatória efervescente, a qual está formatada em três eixos. O que lhes permite comparar é justamente a carga de atribuição de obrigações precaucionárias diante das incertezas quantos aos benefícios e riscos em jogo decorrentes do emprego de tecnologias de reconhecimento facial:

a) de um lado, ainda há parte do setor privado que acredita na suficiência de diretrizes éticas e autorregulação enquanto uma estratégia regulatória que não colocaria entraves ao desenvolvimento da tecnologia em questão;

b) no outro extremo, há vozes que clamam pelo banimento da tecnologia por vislumbrar no seu *design* riscos exacerbados para fins de opressão (Hartzog, 2019);

c) ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos, de modo que o emprego de tecnologias de reconhecimento facial deveria ser antecedido de ações por parte do seu próprio proponente que mitigassem seus eventuais malefícios. A produção de possíveis evidências científicas (AI Now, 2018) acerca da segurança de tais tecnologias (Calo, 2017), sobretudo de ordem dos próprios agentes econômicos poderia desencadear um sistema de corregulação que evitaria a *ossificação* de uma regulação baseada em comando e controle somente por parte do Estado (Wright, 2019).

Como será detalhado na tabela a seguir, diante da experiência estrangeira e do que foi mapeado em termos de modelos regulatórios de tecnologias de reconhecimento facial, LGPD apresenta um *modelo fraco* e janelas muito incipientes para a estruturação de um modelo de governança:

a) há baixa atribuição de deveres para os desenvolvedores de tais tecnologias, bem como por parte de quem será seu consumidor final e dele fará uso seja o setor público ou privado; **a.1)** ao não procedimentalizar minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser

os elementos a compor tal documentação, a LGPD abre espaço para a adoção de tais tecnologias sem que haja correspondentes ações para mitigar seus possíveis malefícios; **a.2)** em especial não há a previsão do controlador iniciar conversas regulatórias quando se deparar em uma situação de um risco não controlável, hipótese na qual notificaria os órgãos reguladores antes de lançar uso da tecnologia a exemplo do que se encontra no RGPD;

b) não há um processo de tomada de decisão que extrapole as figuras do controlador e do órgão regulador, diferentemente de outras propostas aonde se busca um debate público informado com a inclusão de representantes dos interesses dos cidadãos nos circuitos decisórios (e.g., *Code - Acquisition of Surveillance Technology, San Francisco, EUA*);

c) ainda assim, futura regulamentação *a posteriori* da Autoridade Nacional de Proteção de Dados Pessoais/ANPD concernente a relatórios de impacto à proteção de dados pessoais, bem como na validação de códigos de boa conduta ou mesmo de entidades certificadoras podem formatar uma regulação mais catalisadora dos benefícios em contraposição aos riscos do emprego da IA para fins de reconhecimento facial no âmbito do setor privado. Há, portanto, espaço para uma regulação experimental que é, no entanto, condicionada pela efetiva operação da ANPD e da definição do seu próprio perfil institucional ainda indefinido (Bioni, 2019);

d) no âmbito do setor público, o emprego de tecnologias de reconhecimento facial para fins de segurança pública, segurança nacional, defesa do Estado e investigações de natureza penal estão parcialmente excepcionados do escopo de aplicação da LGPD. Ainda que sejam aplicáveis os princípios de proteção de dados pessoais e do devido processo legal, bem como a observação do interesse público, a nova redação dada ao artigo 4º, § 3º, retira da ANPD o poder de emitir opiniões técnicas, recomendações e de solicitar RIPDPs (Bioni & Rielli, 2019);

Princípio da precaução e estratégias regulatórias para tecnologias de reconhecimento facial

Legenda:

Baixo: o fato de haver incerteza quanto ao risco gerado pela atividade de tratamento de dados não pode justificar inércia por parte do controlador;

Moderado: incerteza na avaliação do risco justifica ação, mas há algum grau de discricionariedade;

Forte: quando houver ameaça de dano, medidas de precaução devem obrigatoriamente ser tomadas; diante da incerteza, inverte-se o ônus da prova, que passa a ser do controlador para o emprego da tecnologia em questão e com arranjos de deliberação pública.

Estratégias de Regulação

Regulação específica para dados biométricos-reconhecimento facial

Lei-norma	Descrição	Grau de força da aplicação do Princípio da Precaução
1. Biometric Information Privacy Act, Illinois[23], EUA	A Lei, que foi a primeira a regular a coleta e tratamento de dados biométricos nos Estados Unidos, requer que empresas que operem no estado de Illinois cumpram alguns requisitos: **1.** informem o titular dos dados sobre a coleta e armazenamento do dado, bem como a finalidade do tratamento e o tempo de armazenamento; **2.** obtenham consentimento expresso e escrito para tal; Os mesmos requisitos se aplicam para a disseminação de dados biométricos. Além disso, a Lei também proíbe que as empresas efetuem transações com dados biométricos de indivíduos e exige que as empresas elaborem e publicizem uma política com cronograma de retenção de dados e princípios para destruição de identificadores de biometria (cujo prazo máximo é de 3 anos, contando da última interação entre empresa e indivíduo). Por fim, a Lei exige que as empresas armazenem e protejam os dados biométricos, mantendo um padrão que seja no mínimo o mesmo adotado pela empresa para outras informações sensíveis e que seja razoável dentro da indústria em que se encontra.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e, por fim, quanto ao período de armazenamento. O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.

23 A lei pode ser consultada na íntegra, em inglês, no seguinte link: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

2. HB 1493, Washington[24], EUA	A Lei, aprovada em 2018, aplica-se à utilização de dados biométricos para fins comerciais, excluindo expressamente seu uso com finalidade de segurança. Veda a inclusão de dados biométricos em bases de dados para fins comerciais caso não haja uma de três opções: (i) um aviso, que é definido como "uma notificação dada por meio de um procedimento desenhado para estar prontamente disponível para indivíduos afetados"; (ii) consentimento expresso (que deve ser renovado a cada novo uso comercial) ou (iii) provisão de um mecanismo para prevenir o uso posterior de identificadores biométricos para fins comerciais. A não ser que tenha sido obtido o consentimento expresso, a lei veda a venda, arrendamento ou outro uso comercial, a não ser que o objetivo seja o cumprimento de obrigações legais, o perfazimento de transações comerciais ou financeiras autorizadas pelo titular ou a transferência a um terceiro contratualmente obrigado a não repassar novamente os dados ou dar a eles finalidade inconsistente com a Lei. Aquele que detém dados biométricos utilizados para fins comerciais deve manter cuidados razoáveis contra acessos não autorizados e armazenar os referidos dados por não mais do que o razoavelmente necessário para cumprir obrigações legais, proteger os dados de possíveis fraudes e outros ilícitos ou preencher o objetivo para o qual os dados foram coletados.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e sem que haja um controle social em torno da decisão do emprego da tecnologia e, por fim, quanto ao período de armazenamento. O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.

24 A lei pode ser consultada na íntegra, em inglês, no seguinte link: http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Passed%20Legislature/1493-S.PL.pdf

3. Texas Business and Commerce Code - BUS & COM § 503.001. Capture or Use of Biometric Identifier, Texas[25], EUA	A Lei exige a informação prévia sobre a coleta de dados biométricos para fins comerciais, seguida do consentimento do indivíduo. A venda, arrendamento ou divulgação de dados biométricos que foram capturados para fins comerciais é vedada, exceto nas hipóteses de autorização por lei federal, cumprimento de obrigações legais, perfazimento de transações financeiras autorizadas pelo titular ou autorização pelo titular de divulgação para fins de investigação em caso de desaparecimento ou morte. Os controladores dos dados biométricos devem armazená-los e protegê-los, mantendo um padrão que seja no mínimo o mesmo adotado pela empresa para outras informações sensíveis e que seja razoável dentro da indústria em que se encontra. Por fim, devem destruir estes dados dentro de um tempo razoável, que, em regra, não pode passar de 1 ano da data em que a finalidade para a coleta original expirar.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e, por fim, quanto ao período de armazenamento. O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.

25 A lei pode ser consultada na íntegra, em inglês, no seguinte link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

Regulação específica para reconhecimento facial		
Lei-norma	**Descrição**	**Grau de força da aplicação do Princípio da Precaução**
4. Ordinance amending the Administrative Code - Acquisition of Surveillance Technology, San Francisco, EUA[26]	O projeto, de autoria do conselheiro Aaron Peskin, condiciona o uso de tecnologia de vigilância à aprovação, pelo Conselho de Supervisores da cidade, de uma Política de Tecnologia para Vigilância. Além da política, a proposta também determina que o solicitante de aprovação para emprego destas tecnologias publique, no site do órgão e com ao menos 30 dias de antecedência em relação à reunião em que o pedido será avaliado, um Relatório de Impacto à Vigilância. O critério para aprovação de um pedido é a avaliação de que os impactos positivos da implantação da tecnologia de vigilância superam os efeitos negativos. Em caso de aprovação, os órgãos ficam obrigados a submeter relatórios anuais de vigilância.	**Alto grau de força do princípio da precaução:** a proposta em tramitação na cidade de São Francisco parte do pressuposto de que os riscos apresentados por tecnologias de vigilância, que incluem reconhecimento facial, superam seus eventuais benefícios. Assim, em regra, veda sua aplicação, relegando ao proponente do emprego da tecnologia demonstrar que, no caso concreto, sua proposta não se encaixa nesta regra. Antes de administração pública empregar tal tecnologia, é necessário a execução de RIV que deve ser revisar pelo procurador do município e, em seguida, ser enviado ao Conselho Supervisor para sua aprovação. Tal relatório deve identificar os riscos para direitos liberdades fundamentais dos cidadãos e os benefícios para a sociedade

26 O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://cdn.vox-cdn.com/uploads/chorus_asset/file/13723917/ORD__Acquisition_of_Surveillance_Technology.pdf

5. Bill S.1385, Massachusetts, EUA[27]	O projeto, de autoria da Senadora estadual Cynthia Creem, pretende condicionar a "aquisição, posse, acesso ou uso" de qualquer sistema de vigilância com biometria ou qualquer informação obtida por meio do uso desse tipo de tecnologia a uma autorização estatutária. A autorização, conforme o projeto, deve conter, dentre outras informações: **1.** quais entidades podem usar os sistemas de vigilância com biometria, as finalidades para estes usos e usos proibidos; **2.** padrões para o uso e manejo de informação obtida por estes meios, inclusive quanto à retenção de dados, compartilhamento, acesso e trilhas de auditoria; **3.** proteções rigorosas ao devido processo legal, à privacidade, liberdade de expressão e associação e equidade racial, religiosa e de gênero; **4.** mecanismos para garantia de *compliance*.	**Moderado grau de força do princípio da precaução:** ao reconhecer os riscos em jogo com o emprego de tecnologias de reconhecimento facial, proíbe-se a sdua adoção até que seja estabelecidos padrões de segurança e regras de auditoria sobre tais sistemas.
6. Bill H.287, Massachusetts, EUA[28]	Essa proposta, do Senador Ronald Mariano, inclui dados biométricos nas categorias protegidas da lei estadual de segurança de dados. Dessa forma, entidades que tratam esse tipo de dado deverão revelar aos titulares caso as informações sejam hackeadas, perdidas ou roubadas.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização do dever de informação.

27 O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/SD671

28 O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/H287

7. Commercial Facial Recognition Privacy Act of 2019, EUA[29]	O projeto de lei, introduzido pelos Senadores Brian Schatz e Roy Blunt, pretende regular os usos comerciais de tecnologias de reconhecimento facial. O projeto condiciona o uso de tecnologia de reconhecimento facial a: **1.** consentimento expresso do titular; **2.** quando possível, a apresentação de um aviso sobre o uso da tecnologia e onde encontrar mais informações e informações gerais e acessíveis sobre as características da tecnologia. O projeto também veda o uso dessa tecnologia com fins discriminatórios e com fins distintos àqueles apresentados ao titular. Por fim, proíbe o compartilhamento destes dados com terceiros, a não ser que haja consentimento específico para isso.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento).

Tabela 3: Quadro comparativo da aplicação do princípio da precaução nas estratégias regulatórias para tecnologias de reconhecimento facial

Fonte: Bioni & Rielli (2019)

No campo da regulação de tecnologia de reconhecimento facial experimenta-se um grau de maturidade peculiar, havendo variações fraca, moderada e forte do princípio da precaução. O apetite dessa regulação setorial deságua não só no reforço de deveres de cuidado e segurança por quem pretende lançar mão da tecnologia em específico, mas, também e principalmente, na constituição de arranjos de deliberação pública a seu respeito (e.g., *Code - Acquisition of Surveillance Technology, San Francisco, EUA*).

29 O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://pt.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act

IV. CONSIDERAÇÕES FINAIS

O princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia. A automatização de processos de tomada de decisão, a partir do emprego de IA, não deve se constituir como um argumento ingênuo em defesa de sua objetividade e neutralidade. Tais circuitos decisórios carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômicos, de forma implícita ou explícita, que lhes são subjacentes (Data & Society, 2018).

Diante disso, o princípio da precaução apresenta dois vetores de regulação que merecem atenção: **a)** a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; **b)** a atribuição de obrigações que reduzam as incertezas quanto aos benefícios e riscos em questão, de sorte a determinar a adoção ou não de IA.

Nesse sentido, leis gerais de proteção de dados pessoais, leis setoriais de dados biométricos e de reconhecimento facial apresentam um ferramental precaucionário a ser analisado. A sua calibração variará a escala em baixa, moderada e alta quanto ao nível de prudência acerca do emprego de IA. Ao contrário de paralisia ou inação, a execução de relatórios de impacto à proteção de dados pessoais, de mecanismos de auditoria e conversas com os órgãos reguladores e outros atores afetados são ações que podem servir de força motriz consciente e responsável para o lançamento dessa tecnologia no meio ambiente (Abramovay, 2016).

V. REFERÊNCIAS BIBLIOGRÁFICAS

AI Now, AI Now Report 2018, dec.2018. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf

AI Now, AI Now Report 2016, dec.2016. Disponível em: https://ainowinstitute.org/AI_Now_2016_Report.pdf

ABRAMOVAY, Ricardo. A A heurística do medo, muito além da precaução. *In* **Revista de Estudos Avançados da Universidade de São Paulo.** São Paulo: USP, p. 167-179.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to . **New media & society**, Vol. 20 (3), 2018, pp. 973-989.

BENNETT, Colin J.; RAAB, Charles D., **The governance of privacy:** policy instruments in global perspective, 2nd and updated ed. Cambridge, Mass: MIT Press, 2006.

BIONI, Bruno Ricardo. **Agenda da privacidade de proteção de dados em 2019.** Portal Jota, março de 2019. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2019-28012019>.

_____, Bruno Ricardo. Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito de privacy by design (no prelo). *In* **Direito & Internet IV:** Lei Geral de Proteção de Dados Pessoais (Organizadores Newton de Lucca et al.,) Quartier Latin, 2019.

_____, Bruno; LEITE MONTEIRO, Renato; OLIVEIRA, Maria Cecília. **GDPR Matchup:** Brazil's General Data Protection LAW, IAPP, 2018.

_____, Bruno Ricardo. RIELLI, Mariana. **Contribuição do Data Privacy Brasil a MPV 869/2018:** tratamento de dados no âmbito do setor público. São Paulo: abril, 2019.

_____, Bruno Ricardo. RIELLI, Mariana. **Contribuição do Data Privacy Brasil à audiência publica de tecnologias de reconhecimento facial** (Organizador Ministério Público do Distrito Federal e Territórios/MPDFT). Brasília: abril, 2019

CALO, Ryan, **Artificial Intelligence Policy:** A Primer and Roadmap (August 8, 2017). Disponível em SSRN: https://ssrn.com/abstract=3015350 ou http://dx.doi.org/10.2139/ssrn.3015350

Comissão Europeia. Comunicação da Comissão relativa ao Princípio da Precaução, 2000.

Conferência das Nações Unidas sobre o Meio Ambiente. Declaração do Rio sobre Meio Ambiente e Desenvolvimento, 1992.

Data & Society. : A Primer, 2018.

Declaração de Wingspread sobre o Princípio da Precaução. Eugene, OR: Science & Environmental Health, 1998.

DOSHI-VELEZ, Finale; KORTZ, Mason. **Accountability of AI Under the Law:** The Role of Explanation, 2017.

GARNETT, Kenisha; PARSONS, David J. **Multi-Case Review of the Application of the Precautionary Principle in European Union Law and Case Law.** Risk Analysis, Vol. 37, No. 3, 2017.

GARVIE, Clary et al . **The Perpetual Line-up Unregulated Police Face Recognition in America:** Georgetwon Univerisity, 2016.

GILLESPIE, Tarleton. "The relevance of algorithms". *In* (Ed.), **Media Technologies: Essays on Communication, Materiality, and Society.** Cambridge: The MIT Press, 2014.

HARTMANN, Ivar Alberto Martins. **O princípio da precaução e sua aplicação no direito do consumidor:** dever de informação. Direito & Justiça, v. 38, n. 2, jul./dez., 2012, pp. 156-182.

HARTZOG, Woodrow. SELINGER, Evan. **Facial recognition is the perfect tool for oppression.** Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

HEAD, Brian W. Toward More “Evidence-Informed” Policy Making? **Public Administration Review**, Vol. 76, no. 3, 2015, pp. 472-484.

KUNER, Christopher. The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. **Bloomberg BNA Privacy and Security Law Report**, v. 6, n. 11, p. 1–15, 2012.

MAJONE, Giandomenico. **What Price Safety? The Precautionary Principle and its Policy Implications.** Journal of Common Market Studies, 40. 2002, pp. 89-110.

MANTELERO, Alessandro, **AI and Big Data:** A blueprint for a human rights, social and ethical impact assessment, Computer Law & Security Review, v. 34, n. 4, p. 754–772, 2018

MANTELERO, Alessandro, **Personal data for decisional purposes in the age of analytics:** From an individual to a collective dimension of data protection, Computer Law & Security Review, v. 32, n. 2, p. 238–255, 2016.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Artigo Estratégico 39, Instituto Igarapé, 2018.

PERSSON, Erik. **What are the core ideas behind the Precautionary Principle?** Science of the Total Environment, 557–558, 2016, pp. 134–141.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, v. 10, n. 1, pp. 40–81, 2018.

QUELLE, Claudia, Privacy, Proceduralism and Self-Regulation in Data Protection Law, Rochester, NY: **Social Science Research Network**, 2017. p. 96.

RESNIK, David B. **Is the Precautionary Principle Unscientific?** Studies in the History and Philosophy of Biological and Biomedical Sciences, 34(2), 2003, pp. 329-344.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data privacy Law**, 2017, Vol. 7, No. 4, pp. 233-242.

SCHOMBERG, René von. The Precautionary Principle: Its Use Within Hard and Soft Law. **European Journal of Risk Regulation**, No. 2, 2012, pp. 147-156.

Science for Environment Policy, **The Precautionary Principle:** decision making under uncertainty. Future Brief 18. Produced for the European Commission DG Environment by the Science Communication Unit, UWE, Bristol, 2017. Disponível em < http://ec.europa.eu/science-environment-policy >.

SPINA, Alessandro, Risk regulation of big data: has the time arrived for a paradigm shift in EU data protection, **European Journal of Risk Regulation**, v. 2, p. 248–252, 2014.

STIRLING, Andrew. Precaution in the Governance of Technology. Working Paper. **SPRU - Science Policy Research Unit**, Brighton, 2016.

SUNSTEIN, Cass R. **Laws of Fear:** beyond the Precautionary Principle. Cambridge: Cambridge University Press, 2005.

WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

WRIGHT, Elias. **The Future of Facial Recognition Is Not Fully Known:** Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector. In Fordham Intell. Prop. Media & Ent. L.J. 611 (2019). Disponível em: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? *in*: **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, pp. 175–193.

ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos:** do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, 2019.

ECOLOGIA:
uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes?[1]

Bruno Ricardo Bioni

1 Publicado originalmente em: BIONI, Bruno R. **Ecologia:** uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes? *In*: Chiara de Teffé, Sérgio Branco e Victor Vicente (Org.). Cidades inteligentes em perspectivas. Obliq: São Paulo, 2019.

I. INTRODUÇÃO[2]

Esse artigo é antes de mais nada uma tentativa de encontrar referenciais teóricos que conectam pessoas de formação e *expertise* distintas para se investigar os desafios e as oportunidades do uso intensivo de tecnologias da informação e comunicação (TICs) nos espaços urbanos. Ao retomar o termo "cidades ecológicas", procura-se identificar quais são os aportes teóricos e normativos que a ecologia fornece para que urbanistas, arquitetos, engenheiros, gestores públicos, advogados, dentre outros profissionais, possam desenvolver uma visão holística de como o ambiente urbano está sob reconfiguração, analisando-se em particular as questões relacionadas à privacidade e a proteção dos dados pessoais dos cidadãos.

II. CIDADES INTELIGENTES, INFOESFERA E ECOLOGIA

Os espaços urbanos nunca estiveram tão populosos e as suas respectivas infraestruturas nunca foram tão deficitárias para prover os mais diversos tipos de serviços públicos. É nesse contexto que o termo cidades inteligentes aparece para descrever o uso intensivo de TICs como uma das possíveis soluções para os problemas urbanos e, consequentemente, para a melhoria da qualidade de vida dos cidadãos.[3]

2 Esse texto foi publicado originalmente em: **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**. Alexandre Barbosa. (Org.). 1ed.São Paulo: Comitê Gestor da Internet, 2018, v. 3, p. 191-200.

3 Macaya, Javiera. **Smart Cities**: tecnologias de informação e comunicação e o desenvolvimento de cidades mais sustentáveis e resilientes. Panoram Setorial da Internet, 2(9) (2017), p. 4.

Em si o uso de TICs como uma ferramenta da gestão urbana não é nenhuma novidade[4]. Toda a ideia de planejamento ordenado sempre esteve apoiada no uso em especial de tecnologias de coleta e processamento de dados para a formulação de políticas públicas. Até hoje essa é a dinâmica, por exemplo, dos censos sociodemográficos em que a coleta dos dados pessoais dos cidadãos permite a geração de estatísticas que podem orientar a expansão e a administração de um território nacional e local.[5]

O que muda é que com os recentes avanços computacionais (*big data*, internet das coisas, inteligência artificial, etc) torna-se possível um uso mais intensivo das TICs. Há, sobretudo, uma transformação do próprio espaço urbano que passa a ser arquitetado com artefatos para a coleta e processamento massivo de dados. A figura ostensiva e única do censor é agregada a de sensores dispersos e distribuídos[6] por todo o território e uma boa parcela das ações do gestor público passa a ser automatizada.

Nesse cenário, tão importante quanto a infraestrutura física é a infraestrutura informacional para o desenvolvimento urbano. No caso da mobilidade, por exemplo, os dados de tráfego – infraestrutura informacional – podem tornar mais eficiente toda a malha viária – infraestrutura física, a partir da sincronização dos semáforos e até do redirecionamento das rotas de acordo com os pontos de congestionamento. O mesmo pode ocorrer com relação aos sistemas de saúde e educação, de distribuição de energia e água, dentre outros. Há uma interdependência entre tais infraestruturas

4 Nam, Taewoo. Pardo, Theresa. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. *In* J. Bertot & Association for Computing Machinery (Orgs.), **Proceedings of the 12th Annual International Digital Government Research Conference Digital Government Innovation in Challenging Times**. New York, NY: ACM, (2011), p. 283.

5 Miller, Arthur. **The assault on Privacy**: computers, data banks, and dossiers. Ann Arbor: University of Michigan Press, 1971, p. 223.

6 Bruno, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Rio de Janeiro: Sulinas, 2013, p. 24-26)

que desencadeia uma nova dimensão para o (auto)monitoramento e a (auto)gestão da própria cidade.[7]

É em razão dessa imbricação que se fala na existência de uma infoesfera[8] em que todas as entidades de um ecossistema – incluindo os cidadãos com seus *smartphones* e sensores a sua volta – são organismos que mutualmente se relacionam e interagem entre si através da troca de dados.[9] Um ambiente cujo funcionamento é organizado prioritariamente por fluxos informacionais que podem influir ou definir os mais variados aspectos da vida de um cidadão.

Vive-se, portanto, em um meio não só constituído por elementos naturais, físicos e biológicos, mas, também, por todas as tecnologias que mediam nossas relações.[10] Essa acepção mais ampla do que é meio-ambiente[11] é um convite para refletir sobre como se dá interação dos organismos que o habitam e se a forma como ela está sendo modelada – pelos fatores naturais, físicos, biológicos e tecnológicos – é desejável e sustentável.

A ecologia é justamente o campo de estudo das relações dos seres (vivos e não vivos) com o meio ambiente, partindo da premissa de que há uma interdependência e uma interconexão entre todos eles.[12] O seu mote de análise é compreender o "todo", fornecendo uma visão holística da estrutura e funcionamento de um ecossistema, isto é, da interrelação entre os organismos e o

7 Nam, Taewoo. Pardo, Theresa. Conceptualizing Smart City. Op. Cit., p. 285.

8 Floridi, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. Oxford: Oxford Univ. Press, 2014, p. 25.

9 Ibidem., p. 45.

10 Spina, Alessandro. **Laudato Si' and Augmented Reality**: in Search of an Integral Ecology for the Digital Age. Rochester, NY: Social Science Research Network. Disponível em: https://papers.ssrn.com/abstract=3088487 (2017). Acesso em 08 de março de 2018, p. 03.

11 Fiorillo, Celso Antônio. **Curso de direito ambiental brasileiro**. São Paulo: Saraiva, 2011, p. 45.

12 MacIntosh, Robert. **The background of ecology**: concept and theory. Cambridge: Cambridge University Press, 2000, p. 08.

conjunto de fatores a sua volta que formam o ambiente no qual estão inseridos.[13]

Uma visão ecológica do uso intensivo das TICs nos espaços urbanos é útil por colocar em perspectiva outras variáveis que não só a do discurso da eficiência dos serviços públicos e da solução dos problemas urbanos, mas incluir tudo a sua "volta" o desenvolvimento sustentável (Nusdeo, 1995).[14] É, sobretudo, uma narrativa a ser explorada para identificar como essa nova arquitetura dos espaços urbanos desencadeia uma série de reações no seu "entorno" e, em especial, no que diz respeito à privacidade e a capacidade de autodeterminação dos cidadãos.

III. ECOLOGIA DA PRIVACIDADE: (RE)VISITANDO A INTERDEPENDÊNCIA ENTRE TECNOLOGIA E PRIVACIDADE

A criação e a consolidação do direito à privacidade sempre estiveram associadas à existência de uma infraestrutura tecnológica que as abraçasse e lhes desse vazão. Ou seja, de condições materiais[15] que capacitassem os indivíduos para o controle de informações a seu respeito e, com isso, o livre desenvolvimento de sua personalidade. Não é por acaso que uma dentre várias definições e metáforas possíveis ao direito à privacidade seria a faculdade do indivíduo se privar do convívio social, recolhendo-se ao seu castelo.

Nesse sentido, direitos corolários ao da privacidade têm sido igualmente articulados com forte preocupação com a arquitetura

13 Boff, Leonardo. **Ecologia, Mundialização, Espiritualidade**. São Paulo: Record, 2008, p. 27.

14 Nusdeo, Fabio. **Desenvolvimento e ecologia**. São Paulo: Saraiva, 1995, p. 13.

15 Doneda, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 10-12.

(física) que lhe dá apoio. Por exemplo, algumas constituições falam expressamente em "casa" e em "correspondência" ao dispor sobre a inviolabilidade do domicílio e da comunicação.[16] Mais do que prescrever a proteção do espaço em que uma pessoa se estabelece de forma definitiva (domicílio) e a transmissão de mensagens (comunicação), os textos legais enunciam qual é o tipo de tecnologia em que tais direitos estão apoiados.

Portanto, a existência de zonas de privacidade[17] em que os indivíduos retraem e controlam informações a seu respeito são condicionadas por fatores ambientais. Tão ou talvez mais importante que a arquitetura jurídica para o exercício do direito à privacidade é a arquitetura tecnológica,[18] havendo uma interdependência que pode enfraquecê-lo ou fortalecê-lo.[19] É a chamada "ecologia da privacidade"[20] que denota justamente essa interrelação entre privacidade e tecnologia.[21]

É óbvio que o uso intensivo de TICs nos espaços urbanos altera drasticamente a dinâmica de captura, coleta e processamento dos dados pessoais dos cidadãos, tornando-os uma das engrenagens principais para o próprio funcionamento da cidade. Isso

16 Esse é o caso da Constituição Federal do Brasil: Artigo 5, XI, - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; Artigo 5, 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.

17 Kaye, David. **Promotion and protection of the right to freedom of opinion and expression**. Nova York: Organização das Nações Unidas, 2015, p, 10.

18 Cohen, Julie E. **Examined Lives**: Informational Privacy and the Subject as Object. Stanford Law Review, 52(5), 1373 (2000). Disponível em: https://doi.org/10.2307/1229517, p. 1.377.

19 Bioni, Bruno Ricardo. **Autodeterminação informacional**: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. São Paulo: Faculdade de Direito da Universidade de São Paulo, 2016, p. 211.

20 Sommer, R. **The Ecology of Privacy**. The Library Quarterly, 36(3) (1996), p. 234–248.

21 Hildebrandt, Mireille. **Smart technologies and the end(s) of law**: novel entanglements of law and technology. Cheltenham: EE Edward Elgar Publishing, 2016, p. 217.

tende a se tornar pouco visível para os indivíduos e a reforçar a assimetria hoje já existente na sua relação com o Estado e, em última análise, a desafiar a sua capacidade de autodeterminação nesse ecossistema.

IV. PROTEÇÃO DE DADOS PESSOAIS E ASSIMETRIA DE INFORMAÇÃO: (META)TECNOLOGIAS E TRANSPARÊNCIA

Historicamente, a proteção de dados pessoais foi calibrada por deveres de transparência por parte dos responsáveis pelo processamento, exigindo-se, dentre outras coisas, que a coleta se dê para uma finalidade específica previamente conhecida por seu titular.[22] Essa foi, por exemplo, a tensão do paradigmático caso em que a Corte Federal Alemã considerou ser parcialmente inconstitucional uma lei do censo que não especificava de forma precisa o uso e a finalidade do compartilhamento dos dados coletados pela Administração Pública.[23]

Ao cunhar o termo "autodeterminação informacional", a racionalidade dessa decisão histórica leva em consideração que o cidadão deve ter uma esfera mínima de controle sobre como tal fluxo informacional impacta as suas vidas, até porque eram seus dados o ativo para formulação de políticas públicas das quais seriam beneficiários. Já havia a percepção de que a proteção dos dados pessoais era uma condicionante da própria capacidade de

22 Doneda, Danilo. Princípios e proteção de dados pessoais. *In*: Newton de Lucca, Cíntia Rosa Pereira de Lima & Adalberto Simão Filho (Orgs.), **Direito & Internet III**: Marco Civil de Internet (p. 369–384). São Paulo: Saraiva, 2015, p. 378.

23 Schwabe, Jurgen. Martins, Leonardo. Woischnik, Jan. **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Fundación Konrad-Adenauer, 2005, p. 233-238.

autodeterminação do indivíduo e da coletividade que tinham a sua personalidade e características projetadas nesses dados,[24] os quais subsidiavam decisões por parte do gestor público que impactavam as suas vidas.

Essa problemática persiste no cenário das cidades inteligentes: por um lado, questiona-se se o processamento massivo de dados pessoais a partir do uso intensivo de TICs acarretará de fato em uma melhor qualidade de vida urbana; e, por outro e principalmente, até que ponto ele pode minar a capacidade de autodeterminação do cidadão, cada vez mais mediada por processos de decisões automatizadas. Tal como anteriormente no paradigmático caso da Corte Federal Alemã, um dos elementos chave dessa equação parece ser a redução de assimetria de informação.

Voltando ao conceito de infoesfera, é essencial que a infraestrutura informacional das cidades inteligentes esteja submetida ao escrutínio público dos seus habitantes. Isso implica em pensar tecnologias *sobre* as tecnologias de (auto)monitoramento e (auto) gestão da cidade. Ou seja, metatecnologias[25] que garantam uma visualização nítida da sua infoesfera e, principalmente, que permita aos cidadãos o controle sobre suas informações e do que delas é extraído para a gestão da cidade.

Toda essa jornada teórica percorrida até aqui tem reverberação direta no ordenamento jurídico vigente no Brasil. A Lei de Acesso à Informação (Lei nº 12.527/2011)[26] associa diretamente a proteção de dados pessoais a uma gestão transparente da informação. Uma leitura ecológica da Lei de Acesso à Informação coloca justamente em perspectiva como o dever de transparência ativa e passiva do gestor público perpassa pelo desenvolvimento de metatecnologias para tanto.

24 BIONI, Bruno Ricardo. Autodeterminação informacional...Op. Cit., p. 70.

25 FLORIDI, Luciano. The fourth...Op. Cit., p. 224.

26 Essa é uma interpretação sistemática que combina os artigos 4º, IV, 6º, inciso III e 31, *caput*.

Em poucas palavras, pensar ecologicamente o uso intensivo de TICs nos centros urbanos demanda necessariamente o desenvolvimento de artefatos que permitam a leitura desse ambiente informacional, especialmente de como os organismos desse ecossistema estão interligados e sua capacidade é interdependente. Do gestor público, passando pelos fatores ambientais (incluindo os tecnológicos) até o cidadão.

V. DIMENSÃO COLETIVA DA PROTEÇÃO DE DADOS PESSOAIS: O "TODO" DA CIDADE INTELIGENTE

Não se trata, portanto, de um indivíduo isolado e específico nesse ambiente informacional, mas de como todos os seus organismos formam uma unidade que faz pulsar um conjunto de informações para o funcionamento da cidade. Com o uso intensivo de TICs nos espaços urbanos não só se mapeia todo o seu território, como, também, se prevê e modula o comportamento coletivo (de grupos) da população para a otimização dos recursos da cidade.

Do policiamento preditivo até soluções para o sistema de saúde, a dinâmica é necessariamente a de agregação dos dados dos cidadãos para segmentá-los em grupos. Não é o indivíduo em si, mas o grupo do qual ele faz parte, se de potenciais criminosos ou dos propensos a certos tipos de doenças, que vai determinar a investida policial ou a assistência médica-farmacêutica, respectivamente (Lyon, 2003).[27] Há a formação de entidades coletivas que

27 Lyon, David. Surveillance as social sorting: computer codes and mobile bodies. *In*: David Lyon (Org.), **Surveillance as social sorting**: privacy, risk, and digital discrimination (p. 13–31). New York: Routledge, 2003, p. 12.

projetam e impactam a autodeterminação dos indivíduos que nela foram categorizados.[28]

Por isso, a proteção de dados pessoais assume sobretudo uma dimensão coletiva, isto é, de uma tutela focada nas externalidades negativas difusas em jogo.[29] Nesse sentido, são cada vez mais recorrentes pesquisas que apontam que a vulnerabilidade e a marginalização de certos grupos nos espaços urbanos tende a ser reforçada pelo uso de TICs na gestão urbana, como é o caso de tecnologias de reconhecimento facial e policiamento preditivo com relação à população afrodescendente.[30]

Esse é um passo importante a ser dado para se pensar proteção de dados pessoais não somente como um direito individual, mas, também, transindividual. Isto é, de um grupo de pessoas, ou toda uma população, que têm a sua vida impactada pela infraestrutura informacional do ambiente no qual estão inseridos. Essa compreensão ampliada do que é meio ambiente é um aporte teórico relevante no campo da proteção de dados pessoais que rompe com uma abordagem histórica focada no indivíduo na direção de uma tutela coletiva.[31]

V. DA TEORIA À PRÁTICA: DECODE E A CIDADE DE BARCELONA

A partir do projeto *Decentralised Citizen-owned Data Ecosystem/ DECODE*, a cidade de Barcelona, liderada por Francesca Bria que é

28 Mantelero, Alessandro. Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. **Computer Law & Security Review**, 32(2) (2016), 238–255, p. 12.

29 Ibidem. p.14.

30 Garvie, C., Bedoya, A. M., & Frankle, J. **The Perpetual Line-Up**: unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technlogy: Washington, 2016, p. 03.

31 Mantelero, Alessandro. Personal data...Op. Cit., p. 08.

a sua secretária de inovação e tecnologia, coloca em prática todo o aporte teórico de uma visão ecológica do uso intensivo de TICs para gestão urbana. A própria referência ao termo "ecossistema de dados" transparece tal fundação teórica, levando em consideração como os cidadãos – organismos que integram esse ecossistema – devem fazer parte de um processo de "tomada de decisão coletiva" para o funcionamento da cidade (DECODE, 2017, p. 79).[32]

Parte-se da premissa de que aos cidadãos deve ser assegurada "soberania" sobre seus dados (Rohaidi, 2017), focando-se prioritariamente na criação de uma "infraestrutura técnica" que os capacite para tanto. De forma bastante esquemática, essa infraestrutura, que é chamada de "smart rules"[33], está subdividida em dois grandes eixos:

i) empoderar os cidadãos com um controle mais significativo sobre seus dados, tornando escaláveis e granulares suas escolhas (consentimento) quanto ao uso de seus dados;

ii) garantir que tais escolhas sejam efetivas, a partir de uma trilha auditável de quem acessa e quais usos são feitos com os dados dos cidadãos;

Blockchain seria uma das bases de toda essa infraestrutura técnica por meio da qual uma rede de computadores descentralizada automatizaria as permissões dos cidadãos sobre o uso de seus dados, bem como registraria todo o seu acesso e utilização por terceiros. Ao invés de centenas de políticas de privacidade cujo leque de opções é binário (aceitar ou recusar) e depende da intervenção manual dos cidadãos e que, na prática, garante pouca transparência sobre o seu processamento, haveria uma "arquitetura

32 DECODE. **Me, my data and I**: the future of the personal data economy, p. 79. (Disponível em: https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy. Acesso em 15 de março de 2018).

33 Ibidem, p. 61.

distribuída de gerenciamento dos dados" controlada de forma granular pelos cidadãos e sob escrutínio público constante.

É justamente uma abordagem que articula a tecnologia como um elemento de capacitação e de transparência para que o cidadão controle seus dados e sobre o que deles são extraídos para a gestão da cidade. O resultado esperado é que haja um arranjo de "governança coletivo" em que cada um dos cidadãos contribua para um "controle democrático" da arquitetura informacional da cidade.

Não é o objetivo desse ensaio analisar criticamente os aspectos técnicos e conceituais de toda a iniciativa catalã, mas, a partir dela, identificar como todo o aporte teórico da ecologia detêm desdobramentos bastante práticos em termos do que se idealiza com o uso intensivo de TICs nos centros urbanos. Em especial, como o seu lançamento nos espaços urbanos pode contribuir para que haja:

i) um controle mais significativo dos cidadãos sobre seus dados, a partir da premissa de que a tecnologia é um elemento desencadeador dessa habilidade (ecologia da privacidade);

ii) o desenvolvimento de tecnologia de transparência sobre o uso que se faz de tais dados e de toda a infraestrutura informacional da cidade (metatecnologias e redução da assimetria de informação);

iii) o reconhecimento de uma dimensão coletiva da proteção dos dados pessoais, levando-se em consideração que o comportamento de grupos da população ou dela como um todo é modulado pela agregação e processamento massivo dos dados dos indivíduos (caráter transindividual da proteção dos dados pessoais).

Tudo isso é fruto de um olhar holístico de como a introjeção de TICs no espaço urbano afeta todo o seu entorno, especialmente os cidadãos enquanto organismos integrantes desse ecossistema. Essa visão alargada leva em consideração até mesmo como a

proteção dos dados pessoais dos cidadãos pode ser um vetor de arranjos de governança coletiva para a gestão da cidade e, talvez o mais importante, como parte do escrutínio público sobre se a gestão das infraestruturas física e informacional da cidade está acarretando de fato melhoria na qualidade de vida. Em última análise, trata-se de dar publicidade à própria atuação do Estado para aferir a eficiência da sua gestão, ainda mais quando um dos seus principais ativos são bens da personalidade dos cidadãos – seus dados pessoais.

VI – CONCLUSÃO: CIDADES ECOLÓGICAS

Por ser o campo de estudo das relações dos seres (vivos e não vivos) com o meio ambiente, a ecologia é útil para entender como o uso intensivo de TICs nos espaços urbanos impacta os organismos deles integrantes, em especial os cidadãos. Nesse sentido, o termo "cidades ecológicas" coloca em perspectiva o "todo" de um ecossistema sob reconfiguração, cujos novos artefatos podem alavancar a proteção dos dados pessoais dos cidadãos e, ao mesmo tempo, gerar transparência a respeito da administração da infraestrutura informacional e física da cidade e se ela está acarretando de fato uma melhoria na qualidade de vida. Essa parece ser uma narrativa inteligente para compreender o fenômeno das cidades inteligentes, especialmente as suas virtudes e vicissitudes no que diz respeito à proteção da privacidade e aos dados pessoais dos cidadãos.

BIBLIOGRAFIA

Bioni, Bruno Ricardo. **Autodeterminação informacional**: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. São Paulo: Faculdade de Direito da Universidade de São Paulo, 2016.

Boff, Leonardo. **Ecologia, Mundialização, Espiritualidade**. São Paulo: Record, 2008.

Bria, Francesca. **Decentralised Citizens Owned Data Ecosystem**. Palestra Apresentada em My Data, Helsinki (2017). Disponível em: https://www.youtube.com/watch?v=VURibCURnkY

Bruno, Fernanda. **Máquinas de ver**, *modos de ser*: vigilância, tecnologia e subjetividade. Rio de Janeiro: Sulinas, 2013.

Cohen, J. E. **Examined Lives**: Informational Privacy and the Subject as Object. Stanford Law Review, 52(5), 1373 (2000). Disponível em: https://doi.org/10.2307/1229517

DECODE. **Me, my data and I**: the future of the personal data economy. Disponível em: https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy. Acesso em 15 de março de 2018.

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

Doneda, Doneda. Princípios e proteção de dados pessoais. *In* Newton de Lucca, Cíntia Rosa Pereira de Lima & Adalberto Simão Filho (Orgs.), **Direito & Internet III**: Marco Civil de Internet (p. 369–384). São Paulo: Saraiva, 2015.

Fiorillo, Celso Antônio. **Curso de direito ambiental brasileiro**. São Paulo: Saraiva, 2011.

Floridi, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. Oxford: Oxford Univ. Press, 2014.

Garvie, C., Bedoya, A. M., & Frankle, J. **The Perpetual Line-Up**: unregulated Police Face Recognition in America. GeorgeTown Law Center on Privacy &Technlogy: Washington, 2016. Disponivel em: https://www.perpetuallineup.org/Hildebrandt, Mireille. **Smart technologies and the end(s) of law: novel entanglements of law and technology**. Cheltenham: EE Edward Elgar Publishing, 2016.

Kaye, David. **Promotion and protection of the right to freedom of opinion and expression**. New York: Organização das Nações Unidas, 2015.

Lyon, David. Surveillance as social sorting: computer codes and mobile bodies. In David Lyon (Org.), **Surveillance as social sorting**: privacy, risk, and digital discrimination (p. 13–31). New York: Routledge, 2003.

Macaya, Javiera. **Smart Cities**: tecnologias de informação e comunicação e o desenvolvimento de cidades mais sustentáveis e resilientes. Panoram Setorial da Internet, 2(9) (2017), 1–8.

MacIntosh, Robert. **The background of ecology**: concept and theory. Cambridge: Cambridge University Press, 2000.

Mantelero, Alessandro. Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. **Computer Law & Security Review**, 32(2) (2016), 238–255. Disponível em: https://doi.org/10.1016/j.clsr.2016.01.014

Miller, Arthur. **The assault on Privacy**: computers, data banks, and dossiers. Ann Arbor: University of Michigan Press, 1971

Nam, Taewoo. Pardo, Theresa. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. In J. Bertot & Association for Computing Machinery (Orgs.), **Proceedings of the 12th Annual International Digital Government Research Conference Digital Government Innovation in Challenging Times**. New York, NY: ACM, (2011). p. 282–291

Nusdeo, Fabio. **Desenvolvimento e ecologia**. São Paulo: Saraiva, (1995)

Rohaidi, Nurfilzah. How Barcelona's citizens will control the use of their data. Disponível em: https://govinsider.asia/inclusive-gov/

barcelona-city-council-citizen-data-sharing-francesca-bria/. Acesso em 15 de março de 2018.

Schwabe, Jurgen. Martins, Leonardo. Woischnik, Jan. Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevideo: Fundación Konrad-Adenauer, 2005.

Sommer, R. **The Ecology of Privacy**. The Library Quarterly, 36(3) (1996), 234–248.

Spina, Alessandro. **Laudato Si' and Augmented Reality**: in Search of an Integral Ecology for the Digital Age. Rochester, NY: Social Science Research Network. Disponível em: https://papers.ssrn.com/abstract=3088487 (2017). Acesso em 08 de março de 2018.

DEVIDO PROCESSO INFORMACIONAL:
um salto teórico-dogmático necessário?[1]

Bruno Ricardo Bioni e Pedro Martins

1 Originalmente publicado em: BIONI, Bruno R.; MARTINS, Pedro. **Devido processo informacional: um salto teórico-dogmático necessário?** Portal Jota, 2020.

O julgamento da Ação Direta de Inconstitucionalidade 6.389, também conhecida como caso IBGE, pelo Supremo Tribunal Federal já se tornou um marco para a tutela da proteção de dados no Brasil. Para além do reconhecimento da proteção de dados enquanto um direito fundamental autônomo, a fundamentação de parte dos votos abre espaço para uma outra discussão de talvez ainda maior importância: a releitura da cláusula do devido processo em meio a um cenário crescente de automatização de processos de tomada de decisão que afetam as liberdades dos indivíduos, que já tem sido chamado de devido processo informacional. O Ministro Gilmar Mendes, em seu voto afirma:

> "É possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, **a preservação de verdadeiro "devido processo informacional" (informational due process privacy right)**, voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios."

Nesse texto, iremos apresentar algumas discussões ligadas à regulação e imposição de salvaguardas em processos de tomada de decisão automatizados. O tópico de discriminação e vieses em algoritmos não é novo. Contudo, queremos chamar atenção para a (falta) de aderência da cláusula do devido processo, especialmente quando se trata de uma situação em que o poder público está avaliando seus cidadãos para a tomada de uma decisão a seu respeito.

Em primeiro lugar, é importante deixar claro sobre o que estamos falando. Diversas atividades de tratamento de dados buscam classificar-perfilhar (*profiling*) um indivíduo ou um grupo de indivíduos (*grouping*) de acordo com alguma finalidade. Um conhecido exemplo é a elaboração de scores de crédito, indicando o grau de risco de determinada pessoa quitar ou não uma dívida.

Contudo, diversos outros exemplos podem ser encontrados. Recentemente, o sistema de avaliação de entregadores e motoristas de aplicativos de entrega, que pode levar aos trabalhadores serem bloqueados no aplicativo, vem sendo questionado.

Outro exemplo conhecido é o emprego de algoritmos de análise de risco em processos criminais, avaliando a chance de reincidência de um réu, servindo de base para juízes concederem ou não a liberdade condicional. Em um dos casos mais famosos, o COMPAS, investigações encontraram evidências que réus negros eram sistematicamente discriminados, recebendo avaliações que indicavam um risco maior de reincidência.

Além dos danos individuais advindos de processos discriminatórios, há de se ter também uma preocupação a respeito de como o uso de soluções guiadas pelo tratamento de dados, quando não abertas ao escrutínio público, podem intensificar a exclusão de grupos vulneráveis. A cidade de Boston decidiu lançar, em 2012, um aplicativo de celular que cidadãos utilizariam enquanto dirigem seus carros para detectar buracos e falhas no asfaltamento das ruas. A partir dessas informações, a prefeitura da cidade iria determinar os pontos prioritários para recapeamento das ruas. Contudo, a produção desses dados só era feita por cidadãos que possuíam algum smartphone, áreas mais pobres se tornaram invisíveis pela métrica adotada.

Como argumenta a autora Julie Cohen, a garantia do direito à privacidade (e porque não, também a proteção de dados), tem como propósito não a reclusão do indivíduo perante à sociedade, mas justamente o oposto, propiciando a capacidade de navegar por múltiplos ambientes sociais e culturais com liberdade para experimentar diferentes vivências sem que seja estigmatizado por isso.

> Além disso, a privacidade não protege apenas os indivíduos. A privacidade promove objetivos fundamentais de políticas públicas relacionadas à cidadania liberal democrática, à inovação e ao florescimento humano, e esses propósitos também devem ser levados em consideração na elaboração de políticas de privacidade.[2]

Por consequência, com uma privacidade diminuída ou ameaçada a possibilidade de exercício de uma subjetividade crítica também é afetada. Isso também implica diretamente na possibilidade de concretização e manutenção de um sistema de democracia liberal, visto que nesse cenário os cidadãos terão cada vez menos a capacidade ou disposição de contestar práticas que consideram abusiva e buscar agendas de mudança[3].

Uma das alternativas à aplicação de sistemas totalmente automatizados é a inserção de humanos no processo de tomada de decisão (também conhecido como Human-in-the-loop). Contudo, essa solução, embora possa mitigar alguns dos problemas, também deve ser analisada com cuidado.

Alguns autores argumentam que, mesmo quando uma decisão automatizada serve apenas como recomendação para a decisão final (a ser tomada por um humano), ela poderá ser o elemento decisivo, transformando a própria noção do que entendemos como processo de tomada de decisão. Isso porque, para desconsiderar uma recomendação o operador humano terá que usar argumentos que seriam aferíveis quantitativamente tanto quanto as previsões algorítmicas. Nesse caso, todo espaço para alguma concepção pessoal de justiça ou mesmo de incerteza é eliminado em favor de uma mensuração preditiva avessa a riscos[4].

2 COHEN, Julie. What is Privacy For. **Harvard Law Review**, vol. 126, 2013, p. 19-20.

3 COHEN, Julie. What is Privacy For. **Harvard Law Review**, vol. 126, 2013.

4 ROUVROY, Antoinette. The end(s) of critique: data behaviourism versus due process. *In*: HILDEBRANDT, Mireille; DE VRIES, Katja (eds.). **Privacy, Due Process and the →**

Portanto, alguns dos principais problemas encontrados com sistemas de tomada de decisão automatizada incluem: falta de transparência, dificuldade de identificação e correção de erros, dificuldade de contestar decisões e reforço de desigualdades já existentes[5].

No sistema democrático de direito (rule of law), decisões que afetam o interesse de uma pessoa (por exemplo, a revogação de uma assistência social) devem ser informadas previamente para que ela possa contestar a decisão, se defender, ou apresentar informações adicionais que podem resultar na reversão da decisão. Como colocam os autores Danielle Citron e Frank Pasquale:

> "Novos tomadores de decisão algorítmicos são soberanos sobre aspectos importantes da vida individual. Se a lei e o devido processo estão ausentes nesse campo, estamos essencialmente abrindo caminho para uma nova ordem feudal de intermediários reputacionais que não são chamados a prestar contas".

É exatamente para evitar o crescimento da assimetria informacional e colocar em xeque relações de poder que o devido processo informacional se mostra como uma garantia cada vez mais necessária. Aliás, a própria autonomia do direito à proteção de dados pessoais frente ao direito à privacidade está enraizada nessa racionalidade de devido processo. Essa foi afirmação pioneira do advogado Arthur Miller durante o processo de elaboração das chamadas fair information practice principles no Departamento de Estado e bem estar social dos Estados Unidos da América:

➔ **Computational Turn**: the philosophy of law meets the philosophy of technology. New York: Routledge, pp. 143-167, 2013.

5 CITRON, Danielle, PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. **Washington Law Review**, Vol. 89, 2014, p. 19.

> **Existe uma certa combinação entre temas de privacidade e os demais temas constitucionais. Minha visão pessoal é que provavelmente um dos maiores bastiões constitucionais da privacidade ainda não explorado pelas cortes ou pelos defensores ativistas é o conceito de devido processo legal, a noção de que governos não podem privá-lo de sua vida, liberdade, propriedade, sem o devido processo legal, uma restrição que recai tanto sobre o governo nacional quanto, claro, sobre os estados e governos locais. Me parece que está por ser escrito o capítulo sobre devido processo informacional**. E certos tipos de levantamentos, usos e disseminação de informação governamental podem ser desafiados quando violarem o devido processo (...) E é também interessante notar que o direito original à privacidade, concebido por Warren e Brandeis, em seu doutrinário e significante artigo em 1890, era simplesmente o direito que um indivíduo teria contra a mídia de massa. Não foi concebido para ser um direito geral. Não foi concebido para ser um direito individual contra o Estado. Era simplesmente, como colocou Brandeis, o direito de ser deixado a sós pela grande mídia.[6]

Assim, o devido processo legal, para além de sua dimensão de ser um instrumento de garantias processuais em sede judicial (servindo de base para princípios como do juiz natural, inafastabilidade da jurisdição e todas demais garantias previstas pelo sistema processual), deve também ser entendido como uma ferramenta de assegurar a simetria e proporcionalidade de uma forma mais ampla. Tanto as relações indivíduo-estado, quanto as relações privadas em que há uma assimetria de poder devem ser permeadas pela garantia do devido processo, evitando que ações arbitrárias

6 MILLER, Arthur. Transcription of the 1st Meeting Part I of the Secretary's Advisory Committee on Automated Personal Data Systems of the U.S. Department of Health, Education and Welfare, p. 267. [Destaques não constam no original].

e intrusivas sejam tomadas sem que o sujeito tenha a capacidade de se defender.

Essa capacidade vem sendo ameaçada com a adoção de sistemas de tomada de decisão automatizada, que, seja por razões técnicas (dificuldade de auditar uma decisão algorítmica que emprega técnicas de machine-learning, por exemplo), seja por razões jurídicas (proteção do segredo comercial ou industrial), levam a decisões que são determinantes para a vida do sujeito, sem que este possa ao menos saber os fatores que levaram àquela decisão, sendo mais difícil ainda uma eventual contestação do resultado.

A Lei Geral de Proteção de Dados (Lei 13.709/2018) inaugura esse regime com o direito de revisão de decisões automatizadas, previsto em seu art. 20, *caput*. Além disso, o art. 20 §1º vem sendo entendido por alguns autores como uma garantia de direito à explicação[7]. Ambas são importantes salvaguardas que permitem uma permeabilidade do Direito nos processos algoritmos. Contudo, mais mecanismos de transparência, auditoria e especialmente quando se tratar de decisões tomadas pelo Estado, devem continuar a ser elaborados.

Para além da imposição de obrigações legais sob atividades de tratamento de dados, a participação pública e popular na elaboração de soluções digitais e tecnológicas pode também ser um caminho ainda mais proveitoso. Um dos melhores exemplos a serem citados é o da cidade de Barcelona, que sob a coordenação da pesquisadora Francesca Bria iniciou o "Programa de digitalização aberto e ágil da Prefeitura de Barcelona [Barcelona City Council's Open and Agile Digitalisation Programme]."

A partir de software livre, código, padrões e formatos abertos os cidadãos poderão colaborar na elaboração de políticas públicas e o uso de blockchain para registro do que o Estado faz com os

7 MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais? **Instituto Igarapé, Artigo Estratégico nº 39**, dezembro de 2018.

dados pessoais dos cidadãos. Há uma espécie de contravigilância cujo objetivo é a redução da assimetria de informação e, sobretudo, de co-deliberação na formatação desses circuitos decisórios automatizados.

Iniciativas como essa demonstram que é possível conjugar avanços tecnológicos e digitalização de serviços à observância de direitos fundamentais, sem recair nas armadilhas dos exemplos citados no texto. A garantia do devido processo lhes dá densidade jurídica, garantindo uma espécie de contraditório e ampla defesa a ser exercido de forma coletiva em contraponto à ação em tempo real e opaca dos algoritmos.

BIBLIOGRAFIA

CITRON, Danielle, PASQUALE, **Frank. The Scored Society**: Due Process for Automated Predictions. *Washington Law Review*, Vol. 89, 2014, p. 19

COHEN, Julie. What is Privacy For. **Harvard Law Review**, vol. 126, 2013.

MILLER, Arthur. **Transcription of the 1st Meeting Part I of the Secretary's Advisory Committee on Automated Personal Data Systems of the U.S.** Department of Health, Education and Welfare, p. 267

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais? **Instituto Igarapé, Artigo *Estratégico nº 39***, dezembro de 2018

ROUVROY, Antoinette. The end(s) of critique: data behaviourism versus due process. *In*: HILDEBRANDT, Mireille; DE VRIES, Katja (eds.). **Privacy, Due Process and the Computational Turn**: the philosophy of law meets the philosophy of technology. New York: Routledge, pp. 143-167, 2013.

PROTEÇÃO DE DADOS PESSOAIS COMO ELEMENTO DE INOVAÇÃO E FOMENTO À ECONOMIA:
o impacto econômico de uma Lei Geral de Dados Pessoais[1]

Bruno Ricardo Bioni e Renato Leite Monteiro

1 Publicado originalmente em: BIONI, Bruno R.; MONTEIRO, Renato Leite. **Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia:** O impacto econômico de uma lei geral de dados pessoais. *In*: REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. Horizonte presente tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito; FGV, p. 232-248, 2019.

INTRODUÇÃO: BREVES NOTAS SOBRE A AGENDA "ECONÔMICA" DA PROTEÇÃO DE DADOS PESSOAIS

Uma Lei Geral de Proteção de Dados Pessoais tem por objetivo não só garantir a privacidade e outros direitos fundamentais dos cidadãos, mas, também, fomentar a economia. Ao mesmo tempo em que se reduz a assimetria de informação entre entidades privadas, públicas e indivíduos, franqueando aos últimos controles sobre suas informações pessoais,[2] estabelecem-se alicerces claros para a utilização e monetização dessas informações. Com isso, garante-se, em última análise, segurança jurídica para tais relações.

Ao invés de um custo operacional, os setores regulados, principalmente a iniciativa privada, podem e devem enxergar a proteção dos dados pessoais como um elemento de inovação e fomento à economia. Essa é, aliás, uma perspectiva que tem acompanhado historicamente a criação e a consolidação das normativas a esse respeito.

Nesse sentido, já na década de 80, a Organização para o Desenvolvimento e Cooperação Econômica/OCDE emitiu diretrizes a respeito do tema,[3] as quais foram atualizadas e ampliadas 04 (quatro) décadas depois (2013).[4] Em ambos os momentos, a

2 A proteção de dados pessoais tem sido historicamente associada ao direito de os cidadãos autodeterminar as suas informações pessoais (autodeterminação informacional). Nesse sentido, veja-se as obras de: DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006; Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

3 **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. elaboração: André-Pascal França: OECD Publications Service, 2011. p. 32.

4 **The OECD Privacy Framework 2013**, Disponível em:<http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em 25 de julho de 2015.

narrativa em torno de tal documento se pautou pelo papel estratégico dos dados pessoais para o progresso socioeconômico.[5]

É sintomático, da mesma forma, verificar a recorrência desse movimento em outros organismos internacionais para fins de cooperação econômica, como aconteceu, por exemplo, no âmbito dos países asiáticos e do pacífico. Em 2005, a Cooperação Econômica Ásia-Pacífico (APEC)[6] criou um conjunto de definições e princípios (*Privacy Framework*)[7] que também tinha como seu fio condutor tal aspecto econômico, notadamente o de expandir o comércio eletrônico.[8]

Com a aprovação da Lei Geral de Proteção de Dados Pessoais/LGPD (Lei no. 13.709/2018) mostra-se pertinente mais do que retomar essa narrativa histórica em torno da sua função de fomento à economia, identificar como isso se reverbera dentre alguns dos princípios e direitos desse corpo normativo.

SEGURANÇA JURÍDICA: A NECESSIDADE DE UMA REGULAÇÃO GERAL NO CONTEXTO DE UMA SOCIEDADE MOVIDA POR DADOS (DATA-DRIVEN SOCIETY)

A ideia de uma lei geral de proteção de dados pessoais é justamente a concepção de um corpo normativo, cujo conjunto de regras e princípios, organizados e projetados de forma unitária, forneça uma regulamentação uniforme. Afinal, uma regulação setorial e,

5 Ibidem. p. 3-5 (Prefácio).

6 Sobre a APEC, veja-se: http://www.apec.org/About-Us/About-APEC

7 **APEC Privacy Framework**. Disponível em: <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>

8 Ibidem (Prefácio).

portanto, fragmentada é, desde o seu nascedouro, viciada para tal objetivo.

Em uma sociedade cada vez mais movida por dados (data-driven society),[9] essa infraestrutura jurídica se faz ainda mais necessária. Ela é capaz de fornecer respostas a esse fenômeno totalmente multifacetado.

Antes da LGPD não existia sequer uma definição clara do conceito de dados pessoais. Diferentes leis[10] e decretos[11] traziam conceitos díspares e de aplicação setorial. Além disso, as poucas normas infraconstitucionais que conceituavam dado pessoal não definiam, ao mesmo tempo, o que seria um dado anonimizado e, *via-a-vis*, qual o conjunto de direitos e obrigações, mais ou menos rígido, a que tais atividades deveriam seguir.

Assim, uma lei geral de proteção de dados pessoais é capaz de trazer um horizonte de segurança jurídica para todos os setores da economia que têm as suas atividades permeadas, de alguma forma, pelo processamento de dados pessoais. Do setor securitário ao da publicidade comportamental, do financeiro ao de serviços de Internet, haveria um "manual de instruções" sobre como processar tais dados, mitigando, em última análise, os riscos de todas essas atividades empresariais.

9 A terminologia tem se tornando um *buzzword* atualmente. No entanto, já havia sido utilizado em 2013 pela OECD: Privacy framework...Op. Cit. p.04.

10 Veja-se, por exemplo, a definição contida no artigo 4º, inciso IV, da Lei de Acesso à Informação (Lei nº 12.527/2011: IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

11 Veja-se, por exemplo, o artigo 14, inciso I, do Decreto de Regulamentação do Marco Civil da Internet (Decreto nº 8711/2016): "dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;"

PRINCÍPIO DA QUALIDADE DOS DADOS: MAIOR EFICIÊNCIA DE UMA CADEIA PRODUTIVA BASEADA EM DADOS E EM PROCESSOS DE DECISÃO AUTOMATIZADOS

Apesar da quantidade de dados em circulação hoje em dia, pessoais ou não, a grande maioria deles pode ser considerado lixo, ou, no termo técnico, ruído - "*noise*". Uma consequência direta é que muito tempo e dinheiro são gastos visando transformar esse ruído em dados de qualidade, que sejam "interoperáveis", para que possam ser cruzados para, ao final, ser extraída uma informação útil.

Com a positivação de regras e fundamentos gerais, transversais e multissetoriais de proteção de dados pessoais, todos os agentes estarão obrigados a manter dados que sejam exatos, atualizados e corretos. A tendência será, então, que eles, com o passar o tempo, se tornem mais "limpos", e, por consequência, mais úteis.

Em uma economia cada vez mais orientada pela inteligência de grande base de dados (big data) e de automatização de decisões (algoritmos), trata-se de um elemento crítico a alocar maior eficiência em toda a economia. Da publicidade comportamental à precificação de contratos securitários e financeiros, zelar pela qualidade de dados significa a adoção de estratégias comerciais mais eficazes, lastreadas em informações mais precisas.

Esse é o caso, por exemplo, do setor de crédito. Hoje a análise não se faz mais apenas com base no histórico negativo, isto é, das obrigações não pagas pelo consumidor. Aos postulantes de crédito é atribuída uma nota (*credit score*) que congrega também o seu histórico positivo, isto é, das obrigações por ele adimplidas.[12]

12 Para uma análise do conceito de credit score, bem como da Lei do Cadastro Positivo, veja-se: BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12,414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

Com isso, forma-se um perfil da capacidade econômico-financeira do potencial consumidor que determina o valor e a taxa de juros de tais contratos. Se essa *personalização do crédito* é precisa e não discriminatória,[13] trata-se de uma ferramenta útil para prevenir o fenômeno do superenvidamento da população e, última análise, a saúde de uma economia de consumo altamente dependente da "democratização do crédito".

Todavia, se esta contiver, também, dados imprecisos, desatualizados e em excesso, o cálculo do "score" do consumidor poderá estar errado, o que por sua vez pode prejudicar e trazer danos econômicos tanto para o cidadão quanto para a instituição privada.

Ao final, essas e outras transações comerciais, seja da economia *online* e/ou *offline*, serão otimizadas em razão do cidadão-consumidor estar representado fidedignamente por seus dados. Essa sinergia implica em um mercado mais confiável e que internaliza a proteção dos dados pessoais como um elemento de fomento à economia.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: A (IN) EVITABILIDADE DO VAZAMENTO DE DADOS PESSOAIS

Após o vazamento de dados do sistema SWIFT – responsável por transferências internacionais de valores - na Ásia, as autoridades de vários países se reuniram para rever as regras de proteção de

13 ZANATTA, Rafael. DONEDA, Danilo. **O que há de novo no debate "credit score" no Brasil?** Portal JOTA, 2017. Disponível em: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017>.

dados da APEC Privacy Framework.[14] A conclusão foi de que seriam necessárias normas mais rígidas por duas razões.

Primeiro, as fraudes bancárias diminuiriam, uma vez que o acesso indevido aos dados pessoais dos consumidores, o que se convencionou chamar de roubo de identidade,[15] propicia transações financeiras por terceiros que não são seus reais beneficiários, causando danos econômicos para o correntista e para a própria instituição financeira.

Segundo, porque a recorrência de tais incidentes gera desconfiança[16] entre todos os agentes do ecossistema financeiro, principalmente nos próprios consumidores. Isso os inibiria não só de utilizar o serviço específico em questão, como todo o sistema bancário (tradicional). Em um cenário em que emergem novos rivais nesse mercado, as chamadas *fintechs*, esse risco seria ainda mais significativo.

O mesmo raciocínio seria aplicável a todos os demais setores da economia. Vale mais a pena investir em padrões de segurança da informação para prevenir tais incidentes de segurança do que arcar com os custos de transações fraudulentas e a perda da audiência dos seus consumidores.

Esse é o "cálculo" que orienta as leis gerais de proteção de dados pessoais, especialmente o princípio da segurança lógica e física. A economia gerada com a prevenção de fraudes e o reforço da criação de um ambiente de confiança, associado ao ganho reputacional despertado no consumidor, supera as perdas econômicas causadas por incidentes de segurança da informação.

14 http://www.wsj.com/articles/regulators-to-tighten-cyberdefenses-as-attacks-in-asia-increase-1465899792

15 SOLOVE, Daniel. **The Digital Person: Technology and Privacy in the Information Age**. New York: New York University Press, 2006.

16 MARQUES, Cláudia Lima. **Confiança no Comércio Eletrônico e a Proteção do Consumidor**. São Paulo: Revista dos Tribunais, 2004.

No Brasil, estima-se que tais incidentes de segurança atingiriam R$ 33,00 (trinta e três reais) dos R$ 225,00 (duzentos e vinte e cinco reais) da renda per capita dos brasileiros. [17] Tais incidentes podem causar não somente danos monetários e reputacionais, mas até mesmo ocasionar incidentes sistêmicos que podem atingir todo o sistema e atividades baseadas nesse fluxo informacional que é transfronteiriço.

Uma lei geral de proteção de dados pessoais, bem como um sistema de fiscalização dessas leis por meio de um agente regulador central com expertise adequada, atuando em conjunto com outros agentes reguladores, pode ter como efeito a diminuição considerável desses riscos locais e sistêmicos, ao não só estabelecer padrões mínimos de segurança da informação, mas, também, fomentar a adoção de códigos de conduta discutidos e pensados pelos próprios players do mercado.

Ademais, a LGPD positivará a obrigação de informar ao regulador, e eventualmente aos titulares atingidos, casos de incidentes de vazamentos de dados, principalmente nas situações em que os responsáveis pelo tratamento não se adequaram aos *standards* definidos pelo mercado em conjunto com a autoridade de proteção de dados pessoais. Esta pode, em moldes similares a *recall* de carros ou medicamentos, não só aplicar penalidades, mas, também, obrigar que os indivíduos atingidos sejam diretamente informados e de alguma forma os seus riscos de exposição indevida a práticas abusivas mitigados.

O estabelecimento da obrigação de notificar incidentes de vazamentos de dados pessoais deve ser encarado não como um custo operacional maior ou um risco à imagem do responsável pelo tratamento, mas sim como incentivo a mais para que todos as entidades, públicas e privadas, adotem os mais altos níveis de

17 Telesintese. **Fraude on line cresce quase 200% no ano passado, diz Febraban**. Disponível em: <http://www.telesintese.com.br/fraude-on-line-cresce-quase-200-no-ano-passado-diz-febraban/>.

segurança e de procedimentos, o que, por consequência, pode, justamente, melhorar a reputação da entidade perante o mercado e a sociedade.

Desta forma, sob diferentes prismas, os retornos econômicos, reputacionais e de eficiência superam os custos de implementação, adequação e supervisão que tanto assustam parte da iniciativa privada nacional e internacional.

AS HIPÓTESES DE TRATAMENTO DE DADOS COM BASE NO CONSENTIMENTO E NOS LEGÍTIMOS INTERESSES: BASE ADEQUADA PARA CONFERIR SEGURANÇA JURÍDICA AOS MAIS DIFERENTES MODELOS DE NEGÓCIO DA SOCIEDADE DA INFORMAÇÃO

A pedra angular para o tratamento de dados pessoais é o consentimento do titular, que deve ser, pelo menos, livre, informado e para finalidades determinadas. Todavia, a adjetivação do consentimento varia entre diferentes regulações, o que pode ocasionar um grande impacto nos mais diferentes modelos de negócio.

Por exemplo, o Marco Civil da Internet determina que o consentimento seja livre, expresso, informado e para finalidades específicas. Entretanto, a obrigatoriedade de um consentimento tão rígido pode, na verdade, ter efeitos contrários, seja para que o usuário simplesmente aceite tudo o que aparece na sua frente (o famoso aceite dos termos de uso sem ter conhecimento do conteúdo, na clássica teoria do *overload* informacional[18]) ou para

18 MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. *In* **Coleção doutrinas essenciais de Responsabilidade civil:** direito à informação; v. 8 / Nelson Nery Júnior. Rosa Maria de Andrade Nery (organizadores). São Paulo: Revista dos Tribunais, 2010. ➔

que haja um engessamento na forma de obtenção deste, o que, na prática, pode levar a um desrespeito das normas, prevendo autorizações genéricas como "compartilhamento com parceiros comerciais", conceito amplo e vago comum em muitas políticas de privacidade aceitas por usuários de serviços de Internet.

Diferentemente do Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) traz em seu texto dez hipóteses autorizativas para o tratamento de dados pessoais, sendo o consentimento apenas uma delas.[19] Ainda, a adjetivação do consentimento é mais fluída, aceitando que este seja inequívoco e para finalidades determinadas,[20] a exceção é o caso de tratamento de dados pessoais sensíveis ou para fins de transferência internacional. Isso pode evitar com que tratamento de dados seja realizado fora do escopo legal da norma, ou em afronta direta a esta.

Uma outra importante hipótese autorizativa para o tratamento de dados pessoais é a dos legítimos interesses, conceito já presente em diversas legislações, mas ainda não positivado no nosso. Os legítimos interesses é a hipótese que deve ser utilizada em situações onde: (i) o consentimento do usuário é muito difícil de obter ou desnecessário para as finalidades almejadas; ou (ii) ela se mostrar o embasamento legal mais adequado para a situação concreta, uma vez que a sua aplicação depende de um prévio teste de

➔ p. 27: "Estudos sobre o conceito de racionalidade limitada (bounded rationality) e sobrecarga de informação (overloaded information), têm evidenciado que a equação: maior informação = maior capacidade de decisão consciente (e, portanto, livre) frequentemente não corresponde à realidade".

19 As bases legais para o tratamento de dados pessoais estão distribuídas nos dez incisos do artigo 13 da LGPD.

20 Veja-se, nesse sentido, a análise comparativa das diferentes adjetivações empregadas ao consentimento, quando, ainda não tinha havido a consolidação dos diversos projetos de lei em discussão no Congresso Nacional: BIONI, Bruno. Xeque-mate...Op. Cit., p. 47-52.

proporcionalidade[21] entre os interesses em jogo e os direitos e liberdades individuais dos titulares.

Os legítimos interesses devem ser encarados, antes de tudo, como uma base adequada para o tratamento que pode conferir segurança jurídica para diferentes modelos de negócio que hoje provavelmente processam dados pessoais de forma indevida ou se aproveitando de hiatos regulatórios. Este é o caso, por exemplo, de novos modelos baseados em Internet das Coisas e em metodologias de processamento de dados agrupadas no conceito de *Big Data*,[22] que, devido às características já detalhadas neste artigo, podem encontrar dificuldades em buscar o consentimento dos titulares dos dados pessoais envolvidos. Justamente por estas razões que a iniciativa privada se manifestou fortemente durante a segunda consulta pública do então anteprojeto para que esta possibilidade fosse incluída no rol de bases legais para o processamento de dados[23].

Desta forma, o legítimo interesse pode ser encarado como uma real oportunidade para os modelos de negócios baseados no uso de dados oferecerem seus serviços com segurança jurídica.

21 Ibidem., p. 50-51: "Freios e contrapesos entre a hipótese do legítimo interesse e a regra geral do consentimento".

22 BIONI, Bruno Ricardo. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação (Mestrado). Faculdade de Direito da Universidade de São Paulo. São Paulo: USP-SP, 2016. p. 265.

23 Reporta do InternetLab, disponível em <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>: "Em 2015, durante o debate público feito na Internet, o Poder Executivo incluiu no projeto de lei uma hipótese adicional que autoriza o tratamento de dados pessoais, o "legítimo interesse" do responsável (art. 7, IX): [o tratamento de dados pessoais poderá ser realizado] quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais, em especial se o titular for menor de idade". "O conceito foi incluído no texto para autorizar determinadas situações nas quais o consentimento não precisaria ser emitido. São situações nas quais não é necessário perguntar ao cidadão ou cidadã se aquele tratamento pode ser realizado, pois, segundo o artigo 10 do projeto, ele deve contemplar as suas "legítimas expectativas". Conceito presente nas regras europeias de proteção de dados, tal hipótese concentrou preocupações de diferentes setores".

Todavia, tal instrumento não pode ser encarado como uma bala de prata, um cheque em branco para autorizar o tratamento de dados pessoais, ou muitos menos ser um substitutivo ao consentimento.

Primeiramente, legítimos interesses não devem ser encarados como qualquer interesse, muito menos interesses amplos, vagos ou hipotéticos, que podem dar margem a mais diferentes práticas de tratamento de dados pessoais. Interesses legítimos devem ser baseados em situações concretas, em interesses reais, mesmo que estes sejam puramente comerciais, baseados em garantir novos usos a um determinado conjunto de dados[24], em benefício ao responsável pelo tratamento, desde que levem em consideração as legítimas expectativas do titular, seus interesses razoáveis, mesmo que os novos usos são sejam em seu benefício. Ou seja, deve tratar-se de uma situação concreta que poderia ser eventualmente aceita por este, assegurados seus direitos fundamentais e liberdades individuais.

Para garantir o cenário acima descrito, o tratamento de dados pessoais com base nos legítimos interesses do responsável pelo processamento dos dados deve sempre estar acompanhado de uma análise contextual[25] em que um teste específico verificará se os interesses apontados são reais, e não meramente especulativos, e os direitos de transparência, acesso, correção, oposição e liberdades individuais não serão mitigados. Trata-se, portanto, de um teste de proporcionalidade e necessidade em que se corroborará se o uso desta hipótese autorizativa é realmente necessário para se atingir as finalidades almejadas

24 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC from Working Party 29. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>

25 Veja-se, nesse sentido, o capítulo intitulado como: "Interesses legítimos e o tratamento dos dados pessoais para usos secundários: concreção da privacidade contextual no direito comunitário europeu e o APLPDP e a sua aplicação a casos hipotéticos". BIONI, Bruno Ricardo. Autodeterminação informacional...Op. Cit., 260.

O Working Party 29[26], por meio da sua opinião sobre o uso dos legítimos interesses[27], lista uma série de questões que ajudariam a balancear os interesses do responsável pelo tratamento e as legítimas expectativas do titular pender para o lado daquele com base: (i) na natureza dos dados; (ii) na impacto do tratamento nos indivíduos; e se (iii) há salvaguardas técnicas e jurídicas que possam mitigar eventual impacto.

Um outro importante fator que pode favorecer o uso de legítimos interesses como base legal é assegurar ao titular o direito à portabilidade dos seus dados para um outro serviço ou base de dados, caso seja do seu interesse. Esta seria, inclusive, uma forma de fomentar a concorrência entre diferentes modelos de negócio baseados no uso massivo de dados, uma maneira de "compartilhar a riqueza"[28] quase que natural no uso de dados pessoais como moeda corrente da sociedade da informação.

Um clássico exemplo de tratamento de dados permitido com base em legítimos interesses seria o uso de dados para verificação de situações de fraudes, mesmo que estes não tenham sido originalmente coletados para tal propósito[29]. Nesta situação, não faria

26 O Article 29 Working Party (WP 29) é um órgão consultivo formado por representantes de todas as autoridades de proteção de dados dos membros da União Europeia, por um membro do European Data Protection Supervisor e um membro da Comissão Europeia. Sua principal função é emitir opiniões sobre determinados assuntos envolvendo práticas de tratamento de dados pessoais. Mais informações: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

27 Idem: (i) na natureza dos dados: os dados são necessários para exercício de um direito? Há um interesse público subjacente no tratamento? Quais os benefícios sociais e culturais?
(ii) no impacto do tratamento nos indivíduos: O processamento envolve dados sensíveis? Os dados são combinados com outros? Quais as expectativas razoáveis do titular? O titular é parte vulnerável na sociedade? Qual o poder econômico do processador?
(iii) há salvaguardas técnicas e jurídicas que possam mitigar eventual impacto: Princípio da minimização foi aplicado? Há medidas técnicas para impedir decisões automatizadas? Há uso de técnicas de anonimização? Há uso de medidas adicionais?

28 Idem.

29 United Kingdom Information Commissioner's Office. The conditions for processing. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>

muito sentido tentar obter o consentimento de um indivíduo se o responsável pelo tratamento quer justamente verificar se este foi o sujeito ativo de uma fraude. Neste caso, haveria um interesse legítimo do responsável pelo tratamento, pois ser alvo de uma fraude poderia ocasionar um prejuízo econômico, e também o novo uso estaria dentro da esfera de legítimas expectativas do titular dos dados, pois mesmo que os interesses não lhe beneficiassem, seria razoável esperar que no caso de uma fraude seus dados poderiam ser utilizados para investigá-lo.

Todavia, um exemplo que provavelmente não passaria no teste de proporcionalidade dos legítimos interesses seria a situação em que um grupo de eleitores fornecessem seu dados para um determinado partido na espera que estes sejam utilizados para efetivar a comunicação das plataformas políticas dos seus candidatos, ou até mesmo conclamar para assembleias e encontros. Todavia, se o partido, no afã de angariar fundos, resolve vender sua base de dados para um *data broker* ou agência de marketing, que utilizará os dados para fins de oferecimento comercial de produtos e serviços, sem que haja o consentimento dos titulares para tanto, tal prática pode ser considerada desproporcional, fora das expectativas dos titulares do que eventualmente poderia ser feito com seus dados, além destes serem compartilhados sem que direitos como transparência, acesso, retificação, oposição, cancelamento e portabilidade sejam garantidos. Portanto, numa situação como esta, o interesse puramente comercial do partido provavelmente seria considerado ilegítimo, caracterizando-se como um tratamento de dados pessoais ilegal e não autorizado.

Levando em consideração tais premissas, após as sugestões e interesses amplamente discutidos na segunda consulta pública, os legítimos interesses foram incluídos no rol de bases legais para o tratamento de dados pessoais previstos na LGPDP:

> **Art. 13, IX**: "[o tratamento de dados pessoais poderá ser realizado] quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais".

Ainda, o art. 16 implementa um efetivo teste de proporcionalidade, nos moldes não só do já previsto em legislações estrangeiras, mas, também, acatando as sugestões dadas pelo Working Party 29 na opinião acima mencionada. Desta feita, quanto aos legítimos interesses, na forma como desenhados na legislação projetada:

- A hipótese dos legítimos interesses permite usos secundários dos dados pessoais, mas não pode ser um cheque em branco que autorize qualquer novo tipo de tratamento;
- O legítimo interesse do responsável pelo tratamento deve respeitar os direitos e liberdades fundamentais do titular;
- O tratamento com base nos legítimos interesses deve ser necessário e baseado em uma situação concreta. Não pode ser uma excusa genérica;
- O legítimo interesse deverá contemplar as legítimas expectativas do titular, e não mitigar seus direitos, inclusive os garantidos pela própria lei geral;
- Transparência deve ser garantida, visando o possível direito de oposição do titular, que deve obedecer aos preceitos da norma;
- Os dados pessoais objeto do tratamento devem ser anonimizados sempre que compatível com a finalidade do tratamento;
- O órgão competente pode requisitar e auditar práticas do mercado, exigindo relatórios de impacto à privacidade (Privacy Impact Assessment)[30];

30 Art. 16, §3º, da LPGPD.

Todavia, o pesquisador Rafael Zanatta, em apresentação privada feita em março de 2017 para o Ministério das Comunicações e Tecnologia – MCTIC, levantou algumas questões polêmicas que devem ler levadas em consideração: (i) apesar da prevalência dos Direitos Fundamentais no teste de proporcionalidade, como verificar essa posição na prática? (ii) como evitar a fuga do consentimento como pedra basilar do tratamento de dados pessoais para os legítimos interesses? (iii) seriam as balizas previstas na lei suficientes para garantir um balanceamento adequado no caso concreto? (iv) como garantir que a Autoridade de Proteção de Dados terá expertise e capacidade para verificar os casos baseados em legítimos interesses? e (v) como evitar que os argumentos baseados nos usos benéficos do Big Data se sobreponham às medidas para garantir direitos fundamentais?

Importante enaltecer que a maleabilidade dada ao consentimento e à possibilidade de tratamento com base nos legítimos interesses do responsável não deve retirar o controle por parte do titular, uma vez que o ônus para provar a obtenção deste continuará com o responsável pelo processamento dos dados, mas permitirá uma melhor experiência do usuário (apesar deste ser um argumento clássico para justificar coletas massivas de dados pessoais), a criação de diferentes modelos de negócio, sem que necessariamente haja uma limitação de direitos, conferindo uma maior segurança jurídica.

FLUXO INTERNACIONAL DE DADOS: COMO ASSEGURAR DIREITOS E SEGURANÇA JURÍDICA EM UM MEIO QUE NÃO RESPEITA LIMITES GEOGRÁFICOS?

É necessário ver o livre fluxo internacional de dados como um diferencial competitivo entre diferentes mercados. Um dos princípios

basilares no tratamento de dados pessoais na sociedade em que o fluxo destes não respeita fronteiras geográficas é a necessidade dos diferentes países onde os dados serão tratados oferecerem níveis adequados de proteção dos dados pessoais, para que os direitos garantidos aos cidadãos em uma jurisdição não sejam mitigados em outra com um sistema protetivo inferior.

Neste contexto, o Brasil, ainda não oferece um nível de proteção adequado, principalmente quando comparado com o arcabouço legal europeu. Países vizinhos como Argentina e Uruguai[31], que há anos dispõem de leis gerais, já receberam a chancela da autoridade central europeia, o que na prática autoriza que estes recebem dados pessoais de cidadãos europeus ou originalmente tratados na União Europeia. Os impactos econômicos e comerciais dessas decisões de adequação são enormes.

Por exemplo, uma empresa europeia que oferece serviços através da Internet pode escolher utilizar datacenters instalados em Montevideo por estes terem um custo operacional bem inferior aos praticados no velho continente. Todavia, esta mesma empresa não poderia alugar servidores no Brasil para receber dados pessoais de seus clientes, mesmo que o serviço nas terras tupiniquins fosse mais barato, pois ainda não estamos liberados para receber, armazenar e tratar tais dados. Referido cenário poderá ser revertido com a LGPD.

Importante salientar que mesmo com a possibilidade de transferência internacional por meio de consentimento específico, hipótese prevista na LGPD,[32] isso só significa que podemos enviar dados do Brasil para outro país, mas não constitui uma garantia que dados de cidadãos de países terceiros poderão ser enviados para o nosso. Existem outros instrumentos jurídicos, como

31 Decisão que conferiu o nível de adequação à Argentina e ao Uruguai: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

32 Art. 33, VIII, da LGPD.

cláusulas contratuais padrão e *binding corporate rules* (BCRs), que podem ser utilizados, mas estas são específicas, caso a caso, por muitas vezes burocráticas, o que por sua vez pode não acarretar a mesma eficiência e segurança de uma lei geral, transversal e multissetorial.

Portanto, no contexto do fluxo internacional de dados, o Brasil só tem a ganhar recente promulgação da LGPD. Importante salientar que mesmo com a possibilidade de transferência internacional por meio de consentimento específico, isso só significa que podemos enviar dados do Brasil para outro país, mas não constitui uma garantia que dados de países terceiros poderão ser enviados para o nosso.

PRIVACY BY DESIGN E DATA PROTECTION BY DESIGN: PROTEÇÃO AOS DADOS PESSOAIS DESDE O MOMENTO DA CONCEPÇÃO DOS SERVIÇOS E PRODUTOS

Na esteira de garantir a segurança dos dados como diferencial competitivo, cada vez mais as empresas se voltam para metodologias conhecidas como *Privacy by Design* e *Data Protection by Design*, que em suma pregam a necessidade de se ter por norte a proteção à privacidade e aos dados pessoais desde o momento da concepção do serviço/produto, durante o seu desenvolvimento, oferecimento ao mercado e futura supervisão para tentar identificar falhas ou práticas que não puderam ser antevistas no momento adequado. A adoção de tais metodologias se torna de supra importância no cenário da Internet das Coisas, em que até mesmo os equipamentos mais simples e banais presentes no nosso dia contarão com sensores que coletarão dados pessoais de forma quase que ininterrupta, que por ventura serão compartilhadas

com outros equipamentos inteligentes, uma vez que a eficiência destes está diretamente ligada à possibilidade de conversarem entre si para permitir maior automação da vida pessoal do indivíduo.

A escolha por não empregar padrões, princípios e regras que visem garantir a proteção dos dados pessoais desde o momento da concepção do produto e do serviço pode ter consequências nefastas, como o incidente que permitiu que quase metade da Internet dos EUA fosse derrubada por horas devido a uma falha de segurança presente em roteadores de webcams conectadas diretamente a Internet, que por sua vez foram capturadas para realizar ataques de DDoS[33]. Em um outro cenário possível, o que impedia que estas mesmas webcams não fossem massivamente atacadas para permitir o controle sobre as suas capturas de vídeo, desta forma filmando e monitorando milhares de pessoais, em abismal violação ao direito à privacidade destas.

O emprego massivo de diferentes formas de criptografia é um exemplo claro desse movimento de adotar tais métodos. Mas este não é o único. Cada vez mais as empresas se valem dessas orientações para escrever os algoritmos que serão responsáveis por decisões automatizadas, visando evitar que estes, ao se valerem das diferentes variáveis disponíveis no seu ambiente, cheguem a resultados que possam ser considerados discriminatórios ao ponto de mitigar ou violar direitos e garantias fundamentais dos indivíduos atingidos, o que pode ensejar a responsabilização das entidades que processam os dados pessoais. Tal prática é conhecida como *Algorithmic Accountability*.

Ainda, a prática conhecida como *Privacy by Default* determina que os serviços já venham com configurações de privacidade mais restritivas de fábrica, cabendo aos usuários flexibilizá-las se assim desejarem. As diferentes abordagens do Facebook com relação à

33 Time. How Web Cams Helped Bring Down the Internet, Briefly. Disponível em: < http://time.com/4542600/internet-outage-web-cams-hackers/>

privacidade são bons exemplos dessa técnica, uma vez que a rede social começou permitindo que qualquer pessoa tivesse acesso aos perfis e aos conteúdos compartilhados pelos seus usuários, para depois restringir apenas aos amigos ou círculos de pessoas pré-estabelecidos, podendo estes serem estendidos a terceiros, caso fosse do interesse.

As três situações acima descritas (*Privacy by Design*, *Data Protection by Design* e *Privacy by Default*) estão presentes na LGPD, algumas consideradas mandatórias, outras melhores práticas.[34]

DIREITO DE PORTABILIDADE: SERIA ESTE A MAIS EFETIVA FORMA DE GARANTIR A COMPETIÇÃO ENTRE DIFERENTES *PLAYERS* DO MERCADO E CONFERIR EFETIVO CONTROLE AOS TITULARES DOS DADOS PESSOAIS?

Como já tivemos a oportunidade de destacar anteriormente[35], dentre outras inovações trazidas pela LGPD,[36] assegura-se o chamado direito de "portabilidade". Os usuários poderão "levar" consigo seus dados pessoais ao trocar uma aplicação na Internet por outra (ou qualquer outro tipo de serviço que se valha do tratamento de dados pessoais), devendo, inclusive, a antiga aplicação fornecer os meios adequados para operacionalizar tal transmissão de dados, preferencialmente através de protocolos interoperáveis.

34 Veja, por exemplo, o capítulo VII da LGPD – Segurança e boas práticas.

35 MONTEIRO, Renato. BIONI, Bruno. **Que tal uma pizza de tofu com rabanetes? Você vai adorar! Huffington Post**. Disponível em: <http://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar_a_21682549/>.

36 Art. 7, V, da LGPD.

A privacidade poderá se tornar, literalmente, um elemento de competitividade. Afinal, quem trocaria de plataforma caso não pudesse levar consigo todo a sua "vida digital"? Os usuários poderiam, por exemplo, não só migrar para serviços que lhes sejam mais atraentes, inovadores, mas também para àqueles que lhes forneçam maiores garantias à proteção de seus dados pessoais.

Em um cenário pós-Snowden, no qual a confiança nos gigantes da Internet mostra-se fragilizada, não só já existem redes sociais[37] implementando criptografia e servidores descentralizados como ferramentas antiespionagem, mas várias empresas utilizam o incremento na robustez da segurança dos dados dos clientes como bandeiras de marketing, inclusive defendendo judicialmente esse elemento dos seus modelos de negócio. Casos emblemáticos como a batalha entra a Apple e o FBI[38] e os bloqueios do WhatsApp no Brasil[39] por este serviço implementar criptografia ponta-a-ponta são exemplos de até onde estas empresas estão dispostas a ir para defender a privacidade dos dados de seus clientes.

Diversas empresas já consideram a proteção à privacidade um elemento essencial dos seus modelos de negócio, considerando-o um elemento competitivo que os destaca no gigantesco universo de soluções baseadas no uso de dados pessoais. A adoção de serviços como Snapchat no lugar do Instagram; Signal no lugar do WhatsApp, antes desse último ter adotado também criptografia ponta-a-ponta; práticas como dupla autenticação e senhas mais robustas são pequenos exemplos de como as pessoas ainda se preocupam com a sua privacidade e proteção dos seus dados, diferentemente do cenário verbalizado por muitos.

37 Diáspora: https://diasporabr.com.br/

38 Carta da empresa Apple explicando o seu ponto de vista do caso: http://www.apple.com/customer-letter/answers/

39 Bloqueios.info, iniciativa do InternetLab que lista e analisa os casos de bloqueio de aplicativos e serviços de Internet no Brasil: www.bloqueios.info

CONCLUSÃO

Nesse sentido, uma LGPD visa garantir a autodeterminação informativa e, ao mesmo tempo, fomentar o desenvolvimento econômico e tecnológico por meio de regras balanceadas para assegurar os interesses de todos os atores do ecossistema de uma economia e sociedade cada vez mais movida por dados. Em particular, a iniciativa privada poderá se valer da proteção de dados pessoais como diferencial competitivo nesse novo arranjo econômico, altamente baseado no uso, quase que irrestrito, de dados.

BIBLIOGRAFIA

APEC Privacy Framework. Disponível em: <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>.

BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12,414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

BIONI, Bruno Ricardo. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação (Mestrado). Faculdade de Direito da Universidade de São Paulo. São Paulo: USP-SP, 2016.

BIONI, _____. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o *Facebook* e o aplicativo 'Lulu'. **Revista de Direito do Consumidor**, v. 94, p. 283-326, 2014.

BIONI, _____. **Xeque-mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Disponível em: < http://

www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>

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

InternetLab. O que está em jogo no debate sobre dados pessoais no Brasil? 2016. Disponível em http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/

MARQUES, Cláudia Lima. **Confiança no Comércio Eletrônico e a Proteção do Consumidor**. São Paulo: Revista dos Tribunais, 2004.

MONTEIRO, Renato. BIONI, Bruno. **Que tal uma pizza de tofu com rabanetes? Você vai adorar! Huffington Post**. Disponível em: <http://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar_a_21682549/>.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Elaboração: André-Pascal. França: OECD Publications Service, 2011.

Working Party 29. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Time. How Web Cams Helped Bring Down the Internet, Briefly. Disponível em: < http://time.com/4542600/internet-outage-web-cams-hackers/>

The OECD Privacy Framework 2013, Disponível em:<http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

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

SOLOVE, Daniel. **The Digital Person:** Technology and Privacy in the Information Age. New York: New York University Press, 2006.

United Kingdom Information Commissioner's Office. The conditions for processing. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

ZANATTA, Rafael. DONEDA, Danilo. **O que há de novo no debate "credit score" no Brasil?** Portal JOTA, 2017. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017

O REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA: mapeando convergências na direção de um nível de equivalência[1]

Bruno R. Bioni[2] e Laura Schertel Mendes[3]

1 Este ensaio esteve presente na obra BIONI, Bruno Ricardo; MENDES, Laura Schertel, O Regulamento Europeu de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência, *in*: TEPEDINO, Gustavo *et al* (Orgs.), **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**, São Paulo, SP, Brasil: Thomson Reuters, Revista dos Tribunais, 2019, p. 791–813.

2 Doutorando em Direito Comercial e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (USP). Professor e Fundador do Data Privacy Brasil e consultor jurídico em regulação e tecnologia, com ênfase em privacidade e proteção de dados pessoais.

3 Professora Adjunta de Direito Civil da Universidade de Brasília (UnB) e professora do mestrado acadêmico em Direito Constitucional do Instituto Brasiliense de Direito Público (IDP). Doutora em Direito Privado pela Universidade Humboldt de Berlim, pelo DAAD (Serviço Alemão de Intercâmbio Acadêmico). Mestre em Direito, Estado e Constituição pela Universidade de Brasília (UnB). Vice presidente da Comissão de Proteção de Dados da OAB Federal.

ÁREA DO DIREITO:
Direito Civil, Direito do Consumidor e Direito Constitucional.

RESUMO:
Em meio à ascensão da necessidade global de se regular de maneira efetiva o tratamento de informações e dados pessoais, o presente estudo faz uma comparação entre a recém aprovada Lei Geral de Proteção de Dados Brasileira e o Regulamento Europeu de Proteção de Dados Pessoais. A análise tem como objetivo mapear convergências entre a lei brasileira e a norma europeia, de modo a fornecer critérios de análise para uma futura decisão de adequação por ambos os lados. Alerta-se, por isso, que o texto não se presta a uma mera entabulação da LGPD e RGPD, mas, pelo contrário, em alçar diretrizes capazes de fazer uma radiografia estrutural a seu respeito.

PALAVRAS-CHAVE
Lei Geral de Proteção de Dados, Regulamento Geral de Proteção de Dados, Proteção de dados, Privacidade, Dados pessoais.

ABSTRACT
With rise of the global need to effectively regulate the processing of personal data, the present paper compares the Brazilian General Data Protection Act and the European General Data Protection Regulation (GDPR). The analysis aims to find convergences between Brazilian law and the European Regulation, in order to provide criteria for a future adequacy decision by both sides. It is therefore pointed out that the paper seeks to make a structural radiography of both norms.

KEYWORDS
Brazilian General Data Protection Act, General Data Protection Regulation, Data protection, Privacy, Personal Data

SUMÁRIO

titulares como pilares. 3.2.2. Racionalidade ex-ante. 3.2.3. Entre controle individual e social: a função da *accountability*. 3.2.4. Arranjo institucional: do texto frio da lei ao sistema de *enforcement*. 4. Conclusão: qual é o sentido de equivalência?

1. INTRODUÇÃO

Historicamente, a agenda de padronização de normas é um elemento que se confunde com a própria gênese das leis gerais de proteção de dados pessoais. A Organização para Cooperação e Desenvolvimento Socioeconômico/OCDE e o Conselho da Europa/CoE ao formularem, respectivamente, diretrizes e uma convenção internacional pautaram toda a produção normativa que lhe é posterior. É por isso que se experimentou um alto de grau de convergência das leis de proteção de dados pessoais ao redor do mundo, na medida em que estão estruturadas sobre fundações comuns e fincadas desde o início da década de 80.

Hoje, no entanto, vive-se um momento singular de uma nova ebulição regulatória. Organismos internacionais como a própria OCDE e CoE, blocos regionais como União Europeia/UE e diversos países estão modernizando ou editando, pela primeira vez, suas leis de proteção de dados pessoais. Tais variações normativas abrem necessariamente uma nova rodada de discussão sobre o nível de convergência dessas normas recentemente promulgadas.

Esse é exatamente o caso brasileiro e europeu. Ambos passaram há pouco tempo por um (re)ajuste de suas infraestruturas regulatórias, o que aconteceu no curto espaço de tempo dos últimos 02 (dois) anos. Em 2016, a UE aprovou o Regulamento de Proteção de Dados/RGDP em substituição à antiga diretiva de meados da década de 90. Por sua vez, o Brasil editou, em agosto de 2018, a sua primeira lei geral de proteção de dados pessoais.

Nesse contexto, o presente artigo se presta a mapear convergências entre a lei brasileira e europeia com o objetivo de fornecer

critérios de análise para uma futura decisão de adequação por ambos os lados. Alerta-se, por isso, que o texto não se presta a uma mera entabulação da LGPD e RGPD, mas, pelo contrário, em alçar diretrizes capazes de fazer uma radiografia estrutural a seu respeito.

Em vista de que tais normas foram talhadas com técnicas legislativas completamente distintas, tal exercício mostra-se ainda mais pertinente. Eventual nível de equivalência deve ser calibrado por uma análise qualitativa e não quantitativa. Ao partir desse racional, o artigo conclui que: **i)** a investigação em torno da convergência de regimes regulatórios passa a ser cada vez mais orientada por qual é a racionalidade regulatória que estrutura o seu corpo normativo e; **ii)** em vista da proeminência do princípio da *accountability*, acoplado a ferramentas de corregulação, o arranjo institucional, a atuação das autoridades de proteção de dados, torna-se ainda mais relevante para verificar a aproximação do nível de proteção de dados entre diferentes países e/ou blocos econômicos.

2. INSTRUMENTOS DE DIREITO INTERNACIONAL E CONVERGÊNCIA REGULATÓRIA: UMA TENSÃO PERMANENTE NO CAMPO DA PROTEÇÃO DE DADOS

Ao fazer uma radiografia sobre a convergência regulatória no campo da proteção de dados pessoais, o cientista político Colin Bennett não só fornece um quadro analítico composto por quatro possíveis forças motoras, mas, também e principalmente, pistas de que, historicamente, a agenda de padronização normativa é um elemento que se confunde com a própria gênese da arena regulatória em si.[4] Nesse sentido, o jurista Viktor-Mayer Schönberger, em

4 Os quatro elementos de análise são: **a) determinismo tecnológico**: ainda que países tivessem aspectos culturais socioeconômicos e jurídicos distintos, acabaram por ➔

outro texto, também com perfil analítico-histórico, dá grande ênfase à atuação de organismos internacionais, como a Organização para Cooperação e Desenvolvimento Socioeconômico/OCDE e a Convenção Internacional de Proteção de Dados Pessoais, ao longo do progresso geracional das leis de proteção de dados pessoais.[5]

Por essa razão, chama a atenção o curto espaço de tempo entre a elaboração das *Fair Information Practice Principles/FIPPs* pelo Departamento da Saúde e Bem-Estar do governo estadunidense em 1973 (capítulo infra 3.2.1),[6] a elaboração das diretrizes sobre privacidade da OCDE em 1980[7] e a abertura para adesões à Convenção Internacional de Proteção de Dados do Conselho da Europa em 1981.[8] Tão importante quanto notar esse desdobramento histórico, é o diagnóstico de que tais instrumentos internacionais mencionados foram impulsionados enquanto vetores para integração econômica entre seus países aderentes.

////////////////////

→ enfrentar problemas e desafios comuns que os aproximaram a adotar soluções regulatórias similares; **b) emulação**: a criação de normas sobre a matéria que acabaram por serem adaptadas ou copiadas por regulações posteriores. Nesse sentido, as *Fair Information Practice Principles* foram gestadas no contexto estadunidense, mas acabaram cruzando o Atlântico e influenciando toda a jornada europeia; **c) harmonização**: por questões de interesse econômico e de relações exteriores, percebeu-se a necessidade da articulação de padrões normativos para não inviabilizar a integração entre diferentes países e blocos econômicos sob o argumento de normas conflitantes; **d) penetração**: a ação de atores políticos no processo de construção de regimes jurídicos que forçaram essa agenda de padronização. BENNETT, Colin J.; RAAB, Charles D., Revisiting the governance of privacy: Contemporary policy instruments in global perspective: Revisiting the governance of privacy, **Regulation & Governance**, 2018.

5 MAYER-SCHONEBERGER, Viktor, Generational development of data protection in Europe, *in*: AGRE, Philip; ROTENBERG, Marc (Orgs.), **Technology and privacy: the new landscape**, 1st paperback ed. Cambridge, Mass.: MIT Press, 1998, p. 219–242.

6 Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

7 É importante destacar que a OCDE já vinha atuando fortemente na agenda de padrões normativos pelo menos desde o final dos anos 60: "The OECD established its first expert group, the Data Bank Panel, as early as 1969. In 1978, a new Group of Experts on Transborder Data Barriers and Privacy Protection was established and instructed to draft a set of recommendations. The resulting "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (Guidelines) were adopted by the OECD in 1980". BING, Jon. The Council of Europe Convention and OECD Guidelines on Data Protection. **Michigan Legal Studies**, v. 5, p. 271, 1984.

8 Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

No que diz respeito à OCDE, as *guidelines* são intituladas para a "proteção da privacidade e do fluxo transfronteiriço de dados pessoais". Nota-se, portanto, que as normas em questão são nomeadas com vistas a atingir dois objetivos de forma concomitante. Em linha similar, para potencializar o livre[9] fluxo informacional, a Convenção Internacional 108 estabelece, como regra, a *proibição* de que os países signatários imponham restrições uns aos outros, sob o argumento puro e abstrato da proteção da privacidade, no que diz respeito à transferência internacional de dados.[10] Portanto, a penetração de padrões internacionais é, em grande medida, resultado da pressão pela criação de regimes jurídicos interoperáveis, como deixa transparecer o texto da Convenção Internacional e a própria nomenclatura das diretrizes da OCDE.

O país ou bloco econômico que não incorporasse tais padrões internacionais poderia ser penalizado com a sua não inclusão no mapa global de livre fluxo de dados. Nesse sentido, a emergência de leis nacionais e regionais vieram, em sua grande maioria,[11] acompanhados de regras duras sobre transferência internacional, o que, em princípio, somente seria possível se o país destinatário tivesse um nível equivalente de proteção. É o que até hoje se costuma se referenciar se um país possui ou não um nível adequado de proteção de dados, cuja análise se equaciona com base nos

9 Esse é um adjetivo que se desdobra constantemente ao longo das guidelines da OCDE e que até hoje é repetido em seus documentos, como a **Privacy Framework** de 2013: https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

10 Trata-se do artigo 12 do Convenção cuja proibição foi mantida na versão revisada de 2018: "A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation."

11 Uma das exceções é o modelo canadense pelo qual a transferências internacional de dados é permitida, pouco importante uma análise do regime jurídico do país destinatário. Veja-se, nesse sentido, seção 4.1.3 do Personal Information Protectionand Electronic Documents Act/PIPEDA.

referidos padrões internacionais. Em vista de que tais instrumentos internacionais antecederam muitas das leis nacionais de proteção de dados pessoais, reforça-se, mais uma vez, o indicativo que o fenômeno de convergência regulatória se confunde em si com a própria disseminação e produção normativa sobre proteção de dados pessoais.[12]

Décadas depois, principalmente a partir dos anos 2000, após a emergência e consolidação de tais padrões internacionais, atestado por um alto nível de convergência entre leis de proteção de dados pessoais ao redor do mundo,[13] depara-se com uma nova movimentação em busca de facilitar o livre fluxo de dados.

Em 2005, o fórum para Cooperação Econômica Ásia-Pacífico/APEC estabeleceu um sistema de certificação para transferência internacional - Regras Transfronteiriças de Privacidade/CBPR, pelo qual organizações poderiam aderir voluntariamente a tais regras, sendo certificado os seus respectivos programas de conformidade para viabilizar transferência internacional de dados dentre os países que fazem parte do programa. Em 2015, a APEC editou um conjunto de diretrizes sobre proteção de dados buscando a criação de padrões normativos "interoperáveis" com o objetivo de reforçar o fluxo transfronteiriço de dados.

Em 2013 e em 2018, respectivamente, OCDE e CoE revisitaram suas normas de proteção de dados, passando a prever ou reforçar a importância de compromissos voluntários por parte das organizações para fins de transferência internacional. Como uma válvula de escape ao sistema de análise que averiguava se o país destinatário teria um nível equivalente de proteção de dados, selos e

12 BIONI, Bruno Ricardo, A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço, *in*: **Direitos e novas tecnologias: XXIII Encontro Nacional do Conpedi**, Florianópolis: Conpedi, 2014, v. 1, p. 59–82.

13 Exemplo disso é a quantidades de países signatários da Convenção 108 de Proteção de Dados Pessoais, os quais estão localizados em continentes e com perfis socioeconômicos bastantes distintos uns dos outros. A lista pode ser encontrada aqui: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=5jUUyWW2

códigos de boas condutas passaram a compor um cardápio mais amplo de opções para destravar o livre fluxo de dados. Nota-se, inclusive, um movimento semelhante no cenário brasileiro e da união europeia acerca do alargamento da caixa de ferramentas para fins de transferência internacional[14]:

OCDE 2013	**CoE 2018**	**EU 2016**	**Brasil 2018**
Ao destacar a importância dos programas corporativos de privacidade, acaba por interligá-los ao movimento da APEC, CBPRs, que respalda a transferência internacional de dados em compromissos voluntários firmados pelas organizações e certificados por terceiros.	Ao prever que a transferência internacional de dados poderá se dar de forma *ad hoc* ou mediante salvaguardas padronizadas através de instrumento vinculante por parte?, o novo texto da Convenção abre espaço para que códigos de boas condutas e selos sejam veículos para transferência internacional de dados.	Enquanto a diretiva reconhecia apenas expressamente cláusulas contratuais-padrão enquanto um compromisso voluntário para respaldar transferência internacional, o Regulamento previu também códigos de boas condutas e selos.	Selos e códigos de boas condutas não constavam na versão do então anteprojeto de lei, tendo sido incorporados somente no desenho final da lei aprovada no Congresso Nacional.

Em síntese, desde a década de 80, há uma tensão permanente em se arquitetar arranjos normativos a nível regional e

14 Esse quadro foi elaborado em um trabalho anterior: BIONI, Bruno Ricardo. ZANATTA, Rafael A. F. Direito e Economia Política dos Dados: um guia introdutório (no prelo). *In* **Economia de Dados** (Organizados Ladislau Dowbor).

transnacional convergentes que não restrinjam o fluxo de informações transfronteiriço. As últimas gerações de leis de proteção de dados pessoais reforçaram essa tônica ao ampliar os mecanismos pelos quais se pode ativar a transferência internacional de dados, criando ou reforçando válvulas de escape com base em compromissos privados de organizações que dependem desse livre trânsito de dados para suas operações. Cabe investigar se, diante desse novo cenário, abre-se uma nova agenda de investigação em torno de uma nova rodada de convergência regulatória. Principalmente, quando se nota um movimento que vai além das FIPPs e, no contexto brasileiro e europeu, se tem em perspectiva normas talhadas com técnicas legislativas bastante distintas.

3.0. LGPD VS RGPD: DESAFIOS E PERSPECTIVAS PARA UMA ANÁLISE DE EQUIVALÊNCIA

3.1. Divergência na técnica legislativa

Ainda que seja inegável a influência do Regulamento Europeu de Proteção de Dados Pessoais/ RGPD sobre a Lei Geral brasileira de Proteção de Dados/LGPD,[15] há diferenças substanciais entre tais regimes jurídicos. Uma das mais significativas delas se dá com relação à técnica legislativa utilizada para talhar ambas as leis.

O RGPD é o ponto de chegada de uma longa jornada europeia no campo da proteção de dados pessoais. Após ter sido incluído o direito à proteção de dados como um direito fundamental na

15 BIONI, Bruno Ricardo. GOMES, Maria Cecilia Oliveira. MONTEIRO, Renato Leite. **GDPR matchup:** Brazil's General Data Protection Law. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Cf também MENDES, Laura Schertel e DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *In*: **Revista de Direito do Consumidor**, Vol. 120, nov/dez 2018, p. 469-483.

Carta de Direitos Fundamentais da UE[16] e anos de vigência da Diretiva 95/46, houve o diagnóstico[17] em torno da necessidade de uma abordagem mais consistente e uniforme da proteção de dados por todo o bloco econômico europeu. A diretiva consistia em orientações de como os países membros da UE deveriam formular suas respectivas leis nacionais, havendo, por conseguinte, bastante espaço para *variação jurídica* por cada um dos países membros. Já o regulamento é um mecanismo do direito comunitário europeu com eficácia imediata, sem a necessidade de internalização dos seus países membros e muito mais prescritivo.[18] Como apontam os considerandos do RGPD, o objetivo principal mira na criação de um regime jurídico harmônico e uniforme sobre proteção de dados por toda a UE:

> "(8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de protecção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objectivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam actualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras?

16 RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 175.

17 EUROPEAN COMMISSION, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, **"A comprehensive approach on personal data protection in the European Union"**, Brussels, 2010,

18 Sobre tais técnicas normativas, veja-se: POLIDO, Frabricio *et al*. **GDPR e suas repercussões no direito brasileiro:** primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade/IRIS: Belo Horizonte, 2018. p. 05-11. E, também, as definições constantes no site da própria União Europeia em: < https://europa.eu/european-union/eu-law/legal-acts_en>.

de dados pessoais seja regulada de forma coerente e em conformidade com o objectivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma acção comunitária com vista à aproximação das legislações;

(9) Considerando que, devido à protecção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estados-membros uma margem de manobra que, no contexto da aplicação da directiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a protecção actualmente assegurada na respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verficar-se disparidades na aplicação da directiva, o que poderá reflectir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade";

Por essa razão, em termos quantitativos, o RGPD é um corpo normativo mais extenso em comparação à LGPD. Enquanto o primeiro é composto por 173 (cento e setenta e três) "considerandos" e 99 (noventa e nove) artigos; a segunda possui 65 (sessenta e cinco) artigos e não conta com orientações interpretativas. Fazendo uma interseção entre o direito comunitário europeu e o brasileiro, o RGPD seria um código de proteção de dados que conta com uma quantidade maior de dispositivos e com uma espécie de exposição de motivos, ao passo que a LGPD seria uma lei mais enxuta e sem pistas interpretativas deixadas por parte do legislador.

Nesse cenário, verificar qual é o nível de convergência entre o RGPD e a LGPD não é um exercício trivial. É necessário ir além do mero entabulamento das leis em questão, fazendo-se necessário um olhar *qualitativo* sobre a racionalidade regulatória que orienta cada uma das normas. A partir desse referencial analítico, pavimenta-se a via para ensaiar a constatação de eventual nível de equivalência entre a lei brasileira e a europeia.

3.2. LGPD vs GDPR: racionalidades regulatórias convergentes

Na análise comparativa ora realizada sobressai a convergência em três aspectos importantes, quais sejam, nos princípios enunciados por ambas as regulamentações, no modelo *ex-ante* de proteção, bem como no papel central da *accountability* em ambos os modelos regulatórios. No que diz respeito ao *enforcement*, o foi positivado pela Medida Provisória 869, posteriormente convertida na Lei 13.853/2019. Todos esses aspectos serão analisados a seguir.

3.2.1. FIPPs: práticas justas e direitos dos titulares como pilares

Apesar das diferentes técnicas legislativas, há uma convergência perceptível entre os princípios previstos no RGPD e na LGPD. Essa convergência pode ser atribuída menos a uma influência direta do processo legislativo europeu na lei brasileira do que a um longo processo de construção de um consenso transnacional acerca dos princípios básicos que regem essa matéria.

Ao longo do desenvolvimento da temática da proteção de dados pessoais, estabeleceu-se, por meio de instrumentos internacionais e transnacionais, um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados. Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder de controle ao indivíduo sobre o fluxo de seus dados.

A convergência internacional estabelecida acerca dos princípios é marcante: mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. Esse quadro comum de princípios é conhecido por "*Fair Information Practice Principles*" e teve a sua origem na década de 70 de forma quase simultânea nos EUA, Inglaterra e Alemanha.[19]

Em 1972, no âmbito do Departamento de Saúde, Educação e Bem-Estar (*Department of Health, Education, and Welfare*),[20] deu-se a primeira ação do Poder Executivo americano em relação ao tratamento dos dados pessoais.[21] Neste ano, foi designado pelo então Secretário desse departamento um comitê consultivo de sistemas automatizados de dados pessoais ("*Advisory Committee on Automated Personal Data Systems*"), para o estudo da questão. Em 1973, o comitê emitiu um relatório sobre "Registros, Computadores e Direitos do Cidadão", que propunha a redefinição do conceito de privacidade, além de cinco princípios fundamentais que todo o processamento de dados deveria seguir:

> "1. Não deve existir nenhum banco de dados pessoais, cuja existência seja secreta;
> 2. Deve haver um meio para o indivíduo conhecer quais informações a seu respeito estão armazenadas e de que forma elas são usadas;
> 3. Deve existir um meio pelo qual o indivíduo possa impedir que uma informação obtida para uma finalidade seja utilizada para outros fins, sem o seu consentimento;

19 BENNETT, Colin. **Regulating Privacy:** data protection and public policy in Europe and the United States. Op. Cit., p. 96 a 99.

20 U.S. DEPARTMENT OF HEALTH, EDUCATION AND WELFARE. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: < https://www.justice.gov/opcl/docs/rec-com-rights.pdf >

21 Idem, p. 70 e 71.

4. Deve existir um meio pelo qual o indivíduo possa corrigir ou emendar uma informação pessoal armazenada a seu respeito;
5. Qualquer organização que crie, mantenha, use ou dissemine dados de pessoas identificadas deve assegurar que a informação somente será usada da forma pretendida e deverá tomar as precauções razoáveis para prevenir o abuso do dado."[22]

No mesmo período, já estava em andamento na Grã-Bretanha a análise pelo Comitê de Privacidade, coordenado por Kenneth Younger, a respeito dos riscos do tratamento automatizado de dados realizado por organizações privadas. O comitê emitiu um relatório que sugeria dez princípios para a proteção da privacidade:

"1. A informação deve ser armazenada para uma finalidade específica e não deve ser utilizada para outras finalidades, sem a devida autorização.
2. O acesso à informação deve ser conferido àqueles que têm a autorização de mantê-la com os fins pelos quais elas foram coletadas.
3. A quantidade de informações coletadas e armazenadas deve ser o mínimo necessário para se atingir um objetivo específico.
4. Em sistemas computadorizados que processam dados pessoais com fins estatísticos, medidas adequadas devem ser tomadas em seu *design* e programas para separar a identidade do restante dos dados.
5. Deve haver mecanismos pelos quais o sujeito possa ser comunicado sobre a informação armazenada a seu respeito.

22 EUA, HEW, "Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems." Julho, 1973, tradução livre. O relatório pode ser acessado na seguinte página: http://epic.org/privacy/hew1973report/c3.htm (Data de acesso: 24.02.2012, 18:04).

6. O nível de segurança a ser atingido por um sistema deve ser especificado previamente pelo usuário e deve incluir precauções contra abusos deliberados ou mau uso da informação.
7. Um sistema de monitoramento deve ser provido para facilitar a detecção de qualquer violação da segurança do sistema.
8. No design de sistemas de informação, devem ser especificados períodos para além dos quais a informação não pode mais ser armazenada.
9. Os data? armazenados devem ser corretos. Deve haver instrumentos para a retificação de incorreções e para a atualização da informação.
10. Deve ser tomado cuidado na codificação de julgamentos válidos. (tradução livre)."[23]

Em 1975 é publicada a primeira lei de proteção de dados do mundo, a lei do Estado de Hesse, na Alemanha, na qual constam princípios muito semelhantes àqueles previstos no relatório da comissão Young.[24] Desde então, esse quadro comum de princípios foi positivado em diversos tratados, convenções e legislações nacionais.

A Diretiva 95/46/CE e, posteriormente, o Regulamento geral de proteção de dados europeu (RGPD) acabou incorporando também esse consenso em torno dos FIPPs. O RGPD é essencialmente mais abrangente do que a Diretiva: ele contém 99 artigos enquanto a Diretiva possui 34. No que tange à análise da legalidade, a proposta não difere fundamentalmente da Diretiva. As exigências feitas pela Diretiva à qualidade dos dados foram conservadas, só que sob outro título no RGPD: princípios do tratamento de dados.

23 BENNETT, Colin. **Regulating Privacy:** data protection and public policy in Europe and the United States. Op. Cit., p. 98 e 99.

24 Idem, p. 99.

Continuam sendo previstos os princípios da necessidade, lealdade, finalidade e proporcionalidade, bem como exatidão e atualidade dos dados. Estes podem ser encontrados no art. 5 do RGPD, que passou a abranger três novos princípios: a transparência (art. 5, n. 1, alínea "a"), a minimização dos dados (art. 5, n. 1, alínea "c") e a responsabilidade (art. 5, n. 2).

Também o legislador brasileiro optou por estabelecer uma série de princípios no texto da lei, que na sua topografia, constam do art. 6 Este recurso se deve, entre outros fatores, à necessidade de estabelecer as principais balizas para as suas normas, que são em essência normas abertas e cuja interpretação deverá ser concretizada no ato de aplicação da Lei.

A LGPD prevê todos os princípios presentes no Regulamento europeu e estabelece ainda outros três: segurança, prevenção e não discriminação. O princípio da boa-fé mereceu destaque no texto legal ao constar do próprio *caput* do art. 6°. E, embora dialogue com o princípio da lealdade do RGPD, tem o diferencial de remeter a toda uma tradição do direito civil germânico, que permite o controle de situações subjetivas a partir de parâmetros legais objetivos.

Esses novos princípios previstos na LGPD evidenciam a preocupação da Lei com aspectos contemporâneos da proteção de dados e com novas demandas sociais, como o princípio da não-discriminação pelo tratamento de dados, abordando o potencial discriminatório do uso de dados gerado por mecanismos de decisão automatizada, ou mesmo o princípio da prevenção - que pode ser utilizado para o desenvolvimento de medidas relacionadas à privacidade na concepção, como os conceitos de *Privacy by Design* e o *Security by Design*.

No que diz respeito aos direitos dos titulares, é possível se observar uma convergência entre RGPD e LGPD, especialmente no que tange aos direitos consolidados nessa temática desde a sua origem, como os direitos de acesso, notificação, retificação e cancelamento de seus dados. Semelhante também é a previsão

do direito à portabilidade, que constitui uma inovação em ambos os ordenamentos. No RGPD esses direitos estão previstos no capítulo 3, a partir do art. 12. Na LGPD, os direitos constam curiosamente também do capítulo 3 da Lei e são regulados entre os art. 18 e 22.

Apesar da semelhança da previsão de grande parte dos direitos do titular, há divergências importantes que merecem destaque. Em primeiro lugar, o direito à oposição parece ter uma abrangência maior no direito europeu do que no direito brasileiro, vez que o RGPD trata da possibilidade de oposição à comercialização direta de dados pessoais (art. 21, n. 2 e 3).

Outra questão digna de nota é a regulação de decisões automatizadas. Apesar das diferentes técnicas de redação empregadas,[25] em ambos os sistemas devem ser resguardados os direitos de explicação e a possibilidade de auditoria caso haja um potencial discriminatório. A maior controvérsia reside, contudo, no direito de "obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão", previsto no art. 22, n. 3, do RGPD. Isso porque a LGPD em sua versão original previa a revisão por pessoa natural, o que foi alterado com a MP 869 e está no momento sob discussão no Congresso. Mesmo com a nova redação da MP, poder-se-ia inferir a partir da principiologia da Lei que a intervenção humana continua a ser uma exigência em alguma fase do processo de contestação da decisão automatizada, ainda que não no primeiro pedido de revisão. A prevalecer essa interpretação no direito brasileiro, as normas se aproximariam bastante. É cedo, contudo, para o deslinde dessa questão. Destaca-se ainda uma outra diferença entre os dois

25 O direito europeu trata de um "direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar" (art. 22, n. 1, RGPD), enquanto a norma brasileira trata de um direito de "solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses" (art. 20).

sistemas jurídicos na regulação das decisões automatizadas que é o art. 21 da LGPD. Este estabelece que "os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo". Um exemplo de aplicação desse artigo seria o caso em que o exercício do direito de acesso pelo titular ao seu histórico de crédito é utilizado em seu prejuízo, reduzindo, por exemplo, o seu credit score. O RGPD não prevê tal norma de forma expressa.

Por fim, vale mencionar que o RGPD se diferencia da LGPD ao estabelecer expressamente o direito ao esquecimento (art. 17), previsão que não está clara no texto brasileiro. Nesse ponto, a norma europeia inovou em relação à Diretiva, que não trazia de forma expressa o direito ao esquecimento, mas que foi utilizada como base para o desenvolvimento desse direito pelo Tribunal de Justiça da União Europeia no caso Google Spain vs Costeja. Uma questão interessante e que certamente suscitará amplo debate é se o direito previsto no art. 18, IV, da LGPD poderia levar ao desenvolvimento de um direito ao esquecimento, da forma como ocorreu no direito europeu durante a vigência da Diretiva 95/46.

Como se viu, há, de forma geral, grande convergência quanto aos princípios e aos direitos previstos no sistema europeu e brasileiro, ainda que diferenças normativas possam ser encontradas em temas específicos, como no direito ao esquecimento e nas decisões automatizadas.

3.2.2. Racionalidade *ex-ante* de proteção

Característica marcante do modelo europeu de proteção de dados é a exigência de que o controlador só possa tratar dados se estiver amparado em uma base legal, o que pode ser compreendido como uma racionalidade *ex-ante* de proteção de dados. Essa concepção do direito europeu está presente desde a edição da Diretiva 95/46 e não é uma racionalidade oriunda invariavelmente dos instrumentos transnacionais de proteção de dados acima mencionados.

Esse modelo *ex-ante* de proteção foi consolidado com o RGPD, que prevê em seu art. 6º,os requisitos de licitude para o tratamento de dados, elencando ao todo 6 (seis) bases legais: consentimento, execução de um contrato, obrigação jurídica, defesa de interesses vitais, exercício de funções de interesse público ou ao exercício da autoridade pública, e legitimo interesse.

Há grande semelhança quando se compara os direitos europeu e brasileiro sob esse ponto de vista. Afinal, a grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida exatamente na instituição de um modelo *ex-ante* de proteção de dados.

Fundamenta-se esse conceito no fato de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação[26]. Considerando que os dados pessoais são projeções diretas da personalidade[27], qualquer tratamento de dados acaba por influenciar a representação da pessoa na sociedade, podendo afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais.

Esse modelo está amparado em três características centrais: i) um conceito amplo de dado pessoal[28], ii) necessidade de que qualquer tratamento de dados tenha uma base legal e iii) legítimo interesse como hipótese autorizativa e a necessidade de realização de um teste de balanceamento de interesses.

Ao se comparar as bases legais presentes no direito europeu e no direito brasileiro, percebe-se grande semelhança entre elas,

26 A constatação foi feita pelo Tribunal Constitucional alemão na decisão que consagrou a autodeterminação informativa (ver nota de rodapé 2). A respeito cf: MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor.** Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

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

28 É o que se convencionou chamar de conceito expansionista de dado pessoal: BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Gen-Forense, 2019.

com a diferença de que a lei brasileira possui quatro bases legais adicionais, totalizando dez bases para o tratamento de dados. Essas estão também previstas no art. 7° da LGPD e são a realização de estudos por órgão de pesquisa (IV), o exercício regular de direitos em processo judicial (VI), tutela da saúde (VIII) e proteção do crédito (X).

Vale ressaltar que a base legal relacionada à proteção do crédito tem como finalidade harmonizar as diferentes normas que tratam do tema, ao fazer referência expressa a outras normas que regulam o tratamento de dados no contexto do crédito, como a Lei do Cadastro Positivo (Lei n. 12.414/2011) e o Código de Defesa do Consumidor (Lei n. 8.078/1990). O termo "inclusive" busca explicitar que nessa hipótese não haveria exclusão da aplicação da LGPD, mas sim que as leis específicas serão aplicadas em diálogo com a lei geral.

No que diz respeito à base legal do serviço público, percebe-se uma diferença entre a LGPD e o RGPD, visto que a base da lei brasileira tem uma finalidade mais restrita ao tratar apenas de execução de políticas públicas. Tal base não abrange toda a gama de serviços executados pelo Estado em que se faz necessário o tratamento de dados, o que poderia gerar à primeira vista problemas para fundamentar legalmente diversas outras atividades estatais que exigem o processamento de informações pessoais. Um olhar atento à lei, todavia, permite corrigir tal déficit, na medida em que o art. 23 da LGPD acaba por enunciar uma base legal mais ampla para o tratamento de dados pelo setor público, podendo, portanto, também ser considerada uma base legal para o tratamento de dados pelos controladores públicos.

Do exposto, percebe-se que também no que se refere à racionalidade *ex-ante* de proteção de dados há grande convergência entre os sistemas europeu e brasileiro. Algumas diferenças aqui analisadas são pontuais e se referem a bases legais específicas.

3.2.3. A guinada da "accountability"[29]

Ao se estabelecer metas[30] como de *privacy by design* aos agentes da cadeia de tratamento de dados, as novas leis de proteção de dados pessoais apostam, cada vez mais, na colaboração de quem está prototipando produtos e serviços para mitigar os riscos das suas próprias atividades. Ao contrário de toda e qualquer atividade de tratamento de dados ser notificado às autoridades fiscalizadoras,[31] hoje a regulação europeia só exige algum tipo de comunicação quando tal atividade atrai um risco elevado para os titulares dos dados. Todo o sistema é calibrado por esse voto de confiança e por uma série de ferramentas pelas quais os agentes de tratamento de dados demonstrem a eficácia das medidas tomadas para estarem em conformidade com as regras de proteção de dados pessoais.

Uma das principais ferramentas são os chamados relatórios de impacto à proteção de dados pessoais,[32] pelos quais o controlador - quem tem poder de tomada decisão na cadeia de tratamento de dados - deve obrigatoriamente executá-los quando houver um *alto risco em jogo*. A regulação europeia, além de trazer uma lista exemplificativa dessas situações, exige que os órgãos fiscalizadores sejam comunicados apenas quando o próprio agente econômico não encontrar meios de mitigar os prováveis malefícios da

29 Parte das conclusões derivam de um trabalho anterior: BIONI, Bruno Ricardo. ZANATTA, Rafael A. F. Direito e Economia Política dos Dados: um guia introdutório (no prelo). *In* **Economia de Dados** (Organizados Ladislau Dowbor).

30 GELLERT, Raphaël, **Understanding the risk-based approach to data protection:** An analysis of the links between law, regulation, and risk, Vrije University Brussel, Bruxelas, 2017.

31 Veja, por exemplo, a obrigação de notificação de qualquer atividade de tratamento de dados pessoais às autoridades europeias na antiga diretiva de proteção de dados pessoais, a qual deixou de existir no novo regulamento europeu (artigo 18 da Diretiva 95/46/EC).

32 WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

sua respectiva atividade, devendo nesse caso aguardar "luz verde" da autoridade para seguir em frente. Portanto, diferentemente da diretiva, em que qualquer atividade deveria ser comunicada, a GDPR estabelece um regime totalmente novo de reunião de informação cujo gargalo é torneado por quem está tratando os dados. Os "considerandos" do Regulamento deixam claro essa mudança da mentalidade regulatória:

> "(89) Diretiva 95/46/EC estipulava a obrigação geral de notificar o tratamento de dados para as autoridades supervisoras (...) essas notificações gerais indiscriminadas devem ser abolidas, sendo substituídas por procedimentos e mecanismos efetivos com foco em quais tipos de operações são de alto risco para os direitos e liberdades fundamentais (...) ao envolver o uso de novas tecnologias".
> "(84) (...) quando um relatório de impacto à proteção de dados pessoais indicar que o tratamento envolve um alto risco, o qual não pode ser mitigado por meio de medidas adequadas em acordo com a tecnologia disponível e os custos de implementação, uma consulta à autoridade de proteção de dados deve ser realizada antes de processamento de dados."

Nessa mesma linha, a LGPD também adotou o instrumento de avaliação de impacto. O chamado "relatório de impacto à proteção de dados" é definido como "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" (art. 5º, XVII). No entanto, ele não é obrigatório para atividades de alto risco, como definido na legislação europeia, sendo apenas mencionado como algo exigível *a posteriori* por parte da Autoridade Nacional de Proteção de Dados Pessoais.

Portanto, enquanto o Regulamento sistematiza os relatórios de impacto em um capítulo próprio, apontando em quais casos

são obrigatórios e em que momento se deveria estabelecer "conversas regulatórias"[33] com o órgão fiscalizador, a LGPD não lista, por exemplo, quais seriam os casos de obrigatoriedade, nem define quais atividades de tratamento de dados seriam de alto risco.

Além dos relatórios de impacto, a previsão de códigos de boas condutas e certificações seriam outras ferramentas pelas quais os agentes de tratamento de dados demonstrariam ser responsivos às regras de proteção de dados pessoais. Respectivamente, pares de um mesmo setor verticalizaram normas transversais às realidades e desafios dos seus respectivos setores[34] e, ainda, haveriam terceiros imparciais que certificariam[35] os programas corporativos de privacidade das demais diversas organizações. Todos esses mecanismos seriam um cardápio de opções à disposição dos agentes de tratamento para demonstrar a sua aderência às normas de proteção de dados pessoais, o que deveria ser obrigatoriamente contabilizado na imposição de qualquer penalidade como resultado das ações de fiscalização.[36]

Na linha da GDPR, a lei brasileira também previu o princípio específico da accountability,[37] ao lado dos relatórios de impacto à

33 BLACK, Julia, What is regulatory innovation?, *in*: BLACK, Julia; LODGE, Martin; THATCHER, Mark (Orgs.), **Regulatory innovation: a comparative analysis**, Cheltenham, UK ; Northampton, MA: Edward Elgar, 2005, p. 1–16.

34 Consideranda 98 da GDPR.

35 Consideranda 77 da GDPR.

36 Regulamento Europeu de Proteção de Dados ressalta que a fixação das penalidades deve levar em consideração as medidas técnicas e organizacionais implementadas para se evitar o dano, especificamente privacy by design e padrões de segurança da informação, bem como a aderência a códigos de boas condutas e selos (Artigo 83, "d" e "j", da GDPR).

37 Artigo 6°, X- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

proteção de dados pessoais,[38] selos[39] e códigos de boas condutas.[40] Tudo isso pode dar roupagem à "boa-fé" dos agentes de tratamento de dados pessoais, o que deve calibrar a imposição de eventuais penalidades.[41] Há, no entanto, uma diferença significativa entre tais legislações e que decorre do próprio tipo de técnica legislativa de uma lei, mais geral, em relação a um regulamento, mais prescritivo. A legislação brasileira *não procedimentaliza minimamente* como tais mecanismos deveriam ganhar vida, deixando para posterior regulação por parte da Autoridade Nacional de Proteção de Dados Pessoais.

Apesar, portanto, de um sistema de corregulação, através do princípio da *accountability*, ser uma tendência que aproxima o modelo brasileiro do europeu, deve-se ter em mente a diferença em torno não só da estrutura normativa em questão, mas, também, do contexto socioeconômico em que serão aplicados. Dessa forma, eventual equivalência entre o quadro regulatório brasileiro e europeu tende a ser calibrada pela atuação da futura Autoridade brasileira de Proteção de Dados Pessoais, já que regulamentações posteriores sinalizarão de forma mais precisa qual será o espaço ocupado por tais ferramentas de corregulação e, em última análise, como ganhará vida o princípio da *accountability*.

38 Artigo 5º, 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.

39 Artigo 33, I, "d".

40 Artigo 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.

41 Artigo 52, § 1º, II e e IX, da LGPD.

3.2.4. Arranjo institucional: do texto frio da lei ao sistema de enforcement

O sistema europeu tem como um de seus pilares centrais a autoridade de proteção de dados. Isto é, entende-se que a regulação de proteção de dados não pode ser efetiva sem uma autoridade técnica e independente para aplicá-la. Essa ideia que estava expressa na Convenção 108 do Conselho da Europa, é reforçada na Carta de Direitos Fundamentais da União Europeia, que prevê a exigência de uma autoridade no âmbito de proteção do próprio direito fundamental à proteção de dados, conforme se extrai do seu art. 8.:

> "Proteção de dados pessoais: 1. Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." (grifo nosso)

A referida concepção de independência acabou por se consolidar também no RGPD, especialmente, nos seus considerandos:

> (121) "a fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão exercer as suas funções com integridade, abster-se de qualquer ato incompatível com as mesmas e, durante o seu mandato, não deverão exercer nenhuma atividade, seja ou não remunerada, que com elas seja incompatível. A autoridade de controlo deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente criado nos termos do direito do Estado-Membro, que deverá estar

exclusivamente sujeito à orientação do membro ou membros da autoridade de controlo."

(123) "As autoridades de controlo deverão controlar a aplicação das disposições do presente regulamento e contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados a nível do mercado interno. Para esse efeito, as autoridades de controlo deverão cooperar entre si e com a Comissão, sem necessidade de qualquer acordo entre os Estados-Membros quer sobre a prestação de assistência mútua quer sobre tal cooperação.

(125)"A autoridade principal deverá ser competente para adotar decisões vinculativas relativamente a medidas que deem execução às competências que lhe tenham sido atribuídas nos termos do presente regulamento. Na sua qualidade de autoridade principal, a autoridade de controlo deverá implicar no processo decisório e coordenar as autoridades de controlo interessadas. Nos casos em que a decisão consista em rejeitar no todo ou em parte a reclamação apresentada pelo titular dos dados, esta deverá ser adotada pela autoridade de controlo à qual a reclamação tenha sido apresentada."

(129) "A fim de assegurar o controlo e a aplicação coerentes do presente regulamento em toda a União, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso de reclamação apresentada por pessoas singulares, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e intervir em processos judiciais. Essas competências deverão incluir o poder de impor uma limitação temporária ou definitiva ao tratamento, ou mesmo a sua proibição."

A análise do caso brasileiro referente ao modelo de autoridade que irá aplicar a LGPD é bastante intrigante. Não obstante a previsão legal da ANPD, os dispositivos referentes à sua criação foram vetados no ato da sanção da Lei. Como se lê da motivação do veto, os artigos 55 a 59, que tratavam da criação de uma Autoridade Nacional de Proteção de Dados e de um Conselho de Proteção de Dados, foram vetados em razão de vício de iniciativa.

A Lei 13.853/2019, que recriou a autoridade, não restabeleceu o modelo original que havia sido vetado; ao contrário, em vez de estabelecer uma autoridade na administração indireta, acabou o fazendo debaixo da Presidência da República. A constituição desta autoridade é fundamental, mas, também e principalmente, qual será o seu modelo jurídico, de modo a lhe assegurar independência, poder sancionatório e expertise.

Primeiramente, a autoridade é uma estrutura fundamental para garantir a efetividade dos direitos dos cidadãos sobre os dados pessoais. Também sob o ponto de vista do setor privado, a existência de uma autoridade é um fator importante para facilitar a adequação ao marco normativo, pois ela poderá auxiliar na construção de padrões de aplicação da lei. Tal papel dificilmente pode ser exercido pelos tribunais, que acabam se manifestando em situações específicas de conflito.

Para que a autoridade possa ser caracterizada como independente, faz-se necessário a inexistência de hierarquia das suas atividades de fiscalização, aplicação de sanção e de decisão. Fundamental para a sua independência é que os membros com poder decisório na autoridade tenham mandato, de modo que possam executar suas funções de forma imparcial, técnica e sem risco de interferências políticas. Essa é a razão pela qual a LGPD, na sua versão original aprovada pelo Congresso, estabeleceu a natureza de autarquia especial à Autoridade Nacional de Proteção de Dados.

Como se percebe, uma autoridade independente, com real autonomia e dotada dos recursos necessários para a realização de

suas funções é condição *sine qua non* para tornar efetivas as garantias presentes na LGPD. Além disso, é um fator fundamental para que o país possa obter os benefícios econômicos e políticos decorrentes da LGPD, seja por meio da facilitação do ingresso do Brasil na OCDE, seja por meio da obtenção da adequação europeia - o que garantiria o livre fluxo de dados entre o Brasil e a Europa, abrindo um mercado de 500 milhões de consumidores para as empresas brasileiras.

Dessa forma, embora na aprovação da LGPD os modelos de *enforcement* europeu e brasileiro convergissem bastante, com o veto à autoridade e a construção de um outro modelo via Lei 13.853/2019, vinculado à Administração Direta, rompe-se com tal movimento de aproximação. Tão importante quanto um arranjo normativo equivalente, é a existência de um arranjo institucional que faça uma fiscalização e aplicação uniforme e eficiente da lei. Ainda mais, quando se nota um modelo de regulação que delega uma série de atividades aos próprios atores regulados, os quais, por sua vez, devem prestar contas – princípio da *accountability* – acerca da eficiência das suas ações para estarem em conformidade com as normas de proteção de dados.

3.2.5. Conclusão: voltando ao básico, qual é o sentido de equivalência?

O sistema normativo de proteção de dados pessoais emerge no âmbito da sociedade de informação, como forma de proteger a personalidade do indivíduo contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. Esse sistema exerce uma dupla função, ao buscar proteger a pessoa que é titular desses dados, ao mesmo tempo em que fomenta o livre fluxo de informações entre países com nível de proteção equivalente.

Em um contexto tecnológico em que os dados podem fluir sem qualquer obstáculo de um país para outro ou mesmo em que bases de dados podem ser utilizadas de forma compartilhada por

controladores e operadores residentes em países diferentes, sujeitos a regulações com níveis de proteção completamente diferentes, fundamenta-se que sem tal exigência de equivalência qualquer regulação nacional sobre regulação da informação pessoal seria completamente inócua.

Nesse sentido, vê-se que não só os instrumentos transnacionais aqui abordados, mas também a exigência da equivalência no âmbito nacional, e em especial do Regulamento europeu, acabou por criar incentivos para que os regimes nacionais de proteção de dados fossem sendo criados ou modificados de modo a permitir algum grau de interoperabilidade entre eles. Sem essa interoperabilidade, não se poderia falar nem em proteção de dados em âmbito nacional ou transnacional, menos ainda em um livre fluxo de dados entre países.

Considerando a recente aprovação da LGPD e o seu sistema de *enforcement* ainda em formação, a discussão sobre o grau de equivalência entre ela e o RGPD adquire importância por dois motivos centrais e, ao mesmo tempo, bastante diversos. Em primeiro lugar para se saber a probabilidade de o Brasil ser considerado um país "adequado" sob o ponto de vista do sistema europeu de proteção de dados e obter uma decisão da Comissão Europeia favorável a um eventual pleito nesse sentido, o que constituiria uma importante vantagem para as entidades públicas e privadas no Brasil que tratam e transferem dados.

Em segundo lugar, porque em razão do teor do art. 33, I, da LGPD, o Brasil também terá que desenvolver os seus próprios critérios para examinar o grau de adequação de normas estrangeiras à LGPD. Essa norma deve ser interpretada com a do art. 34, que estabelece que o nível de proteção de dados do país estrangeiro será avaliado pela autoridade nacional, que levará em consideração diversos critérios, entre eles, as normas gerais e setoriais da legislação em vigor no país de destino; a natureza dos dados; a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares; a existência de garantias judiciais

e institucionais para o respeito aos direitos de proteção de dados pessoais, entre outros.

Se por um lado a limitação da transferência de dados a países com proteção equivalente é uma regra do regime europeu desde pelo menos a Diretiva Europeia 95/46 de1995, tendo sida confirmada pelo Regulamento europeu de proteção de dados pessoais, para o ordenamento brasileiro esse conceito constitui uma grande novidade e trará certamente um desafio em sua implementação. Tendo em vista a tendência natural da proteção de dados na busca pela interoperabilidade entre os diversos ordenamentos jurídicos nacionais, o estabelecimento das variáveis para tal análise comparativa no Brasil deverá usar como parâmetro, além da própria norma brasileira, também o contexto transnacional e internacional da proteção de dados, conforme exposto no presente artigo.

Por fim, em vista de que tais normas foram talhadas com técnicas legislativas completamente distintas, eventual nível de equivalência deve ser calibrado por uma análise qualitativa e não meramente quantitativa. A investigação em torno da convergência de tais regimes regulatórios deve ser orientada: i) pela racionalidade regulatória que estrutura os seus respectivos corpos normativos (*regulação ex-ante*) e; ii) em vista da proeminência do princípio da *accountability*, acoplado a ferramentas de corregulação, ao arranjo institucional, à atuação das autoridades de proteção de dados, que dará *normatividade* a instrumentos como relatórios de impacto à proteção de dados pessoais, códigos de boa conduta, selos e etc.

BIBLIOGRAFIA

BENNETT, Colin, **Regulating Privacy: data protection and public policy in Europe and the United States**. Ithaca, New York: Cornell University, 1992.

BENNETT, Colin e RAAB, Charles, **The Governance of Privacy: policy instruments in global perspective**. Cambridge: MIT, 2006.

BENNETT, Colin e RAAB, Charles, **Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective**, 2018 (https://ssrn.com/abstract=2972086).

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

BIONI, Bruno Ricardo. ZANATTA, Rafael A. F. Direito e Economia Política dos Dados: um guia introdutório (no prelo). *In* **Economia de Dados** (Organizador Ladislau Dowbor).

BIONI, Bruno Ricardo. GOMES, Maria Cecilia Oliveira. MONTEIRO, Renato Leite. **GDPR matchup:** Brazil's General Data Protection Law. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>.

BIONI, Bruno Ricardo, A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço, *in*: **Direitos e novas tecnologias:** XXIII Encontro Nacional do Conpedi, Florianópolis: Conpedi, 2014, v. 1, p. 59–82.

BLACK, Julia, What is regulatory innovation?, *in*: BLACK, Julia; LODGE, Martin; THATCHER, Mark (Orgs.), **Regulatory innovation:** a comparative analysis, Cheltenham, UK ; Northampton, MA: Edward Elgar, 2005, p. 1–16.

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

GELLERT, Raphaël, **Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk**, Vrije University Brussel, Bruxelas, 2017.

MAYER-SCHONEBERGER, Viktor, Generational development of data protection in europe, *in*: AGRE, Philip; ROTENBERG, Marc (Orgs.), **Technology and privacy:** the new landscape, 1st paperback ed. Cambridge, Mass.: MIT Press, 1998, p. 219–242.

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

MENDES, Laura Schertel e DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *In*: **Revista de Direito do Consumidor**, Vol. 120, nov/dez 2018, p. 469-483.

POLIDO, Fabricio Pasquot. **GDPR e suas repercussões no direito brasileiro:** primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade/IRIS: Belo Horizonte, 2018. p. 05-11.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Tradução Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

WRIGHT, David; DE HERT, Paul (Orgs.), **Privacy Impact Assessment**, Dordrecht: Springer Netherlands, 2012.

RESPONSABILIDADE CIVIL NA LGPD:
construção do regime por meio de interações com o CDC

Bruno Bioni[1] e Daniel Dias[2]

1 Doutorando em Direito Comercial e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (USP). Foi pesquisador visitante do European Data Protection Board e do Departamento de Proteção de Dados do Conselho da Europa Professor e Fundador do Data Privacy Brasil.

2 Professor da FGV Direito Rio. Doutor em Direito Civil pela USP (2013-2016), com períodos de pesquisa na Universidade *Ludwig-Maximilians* de Munique e no Instituto Max-Planck de Direito Comparado e Internacional Privado, na Alemanha (2014-2015). Estágio pós-doutoral na *Harvard Law School*, nos EUA (2016-2017).

ÍNDICE:

1. Introdução e apontamentos metodológicos; 2. A (in)evolução do texto da LGPD: a disputa travada em torno do papel da culpa na definição do regime de responsabilidade civil com um olhar para o todo da LGPD; 3. Responsabilidade em caso de "violação à legislação de proteção de dados pessoais" e de "violação da segurança dos dados"; 3.1. Tratamento irregular; 3.1.1. Dubiedade de critérios quanto à violação à segurança dos dados: medidas aptas (art. 44. parágrafo único) *versus* a segurança que dele se pode esperar (art. 44, II); 3.1.2. Conectando inobservância da legislação e o não fornecimento de segurança esperada, a partir do conceito de "legítimas expectativas de segurança"; 3.1.3. Circunstâncias relevantes: conectando o artigo 43 ao 50 da LGPD para um juízo de culpa caso a caso; 3.1.4 Circunstâncias relevantes: as técnicas de tratamento de dados disponíveis à época (inciso III do artigo 43); 3.2. Presunção de alguns dos pressupostos de responsabilidade e inversão do ônus da prova quanto aos demais; 3.3. Obrigação de meio *versus* de resultado: a significação dos termos aptas, eficazes e eficientes; 4. Conclusão.

1. INTRODUÇÃO E APONTAMENTOS METODOLÓGICOS

A Lei n. 13.709/2018, chamada de Lei Geral de Proteção de Dados (LGPD) inaugurou uma espécie de "estatuto da informação",[3] prescrevendo, pela primeira vez no ordenamento jurídico brasileiro, um conjunto de normas – regras e princípios – vocacionados[4] para governar o tratamento de dados pessoais em todos os

3 A LGPD inaugurou uma nova lógica, que busca regular uma ordem informacional, algo que não havia antes de forma tão sistematizada e harmônica. Ver: SCHERTEL, Laura Mendes. Palestra: "Seminário Internacional – Lei Geral de Proteção de Dados: a caminho da efetividade. Superior Tribunal de Justiça, 2019. Disponível em: <https://www.youtube.com/watch?v=0E0USaGQ6h8>. Acesso em: 01 maio 2020.

4 BIONI, Bruno Ricardo. **País precisa ser competitivo em uma economia de dados. Valor Econômico**, 19 jul. 2018. Disponível em: <https://valor.globo.com/opiniao/coluna/como-o-brasil-pode-inovar-na-protecao-de-dados-pessoais.ghtml>. Acesso em: 01 maio 2020.

setores da economia e em todas as demais atividades do cotidiano do cidadão.

Tamanha é a importância desse novo ingrediente na cultura jurídica que é comparado a uma repactuação do próprio contrato social,[5] uma vez que hoje, a todo momento, as pessoas são julgadas e avaliadas com base no que seus dados pessoais dizem a seu respeito. Do acesso a programa de transferência de renda ao de linha de crédito, essas oportunidades sociais são filtradas pelo processamento de seus dados.

Um dos eixos da lei foi justamente delimitar quais são as obrigações dos agentes de tratamento de dados e, com isso, fixar regime jurídico para sua responsabilização.[6] É inevitável que nesse "admirável novo mundo", cheio de riscos,[7] experimentar-se-á efeitos colaterais que deverão ser compensados e, preferencialmente, prevenidos.[8] A esse respeito, a seção sobre responsabilidade e ressarcimento de danos (seção III, do capítulo VI, da LGPD) desafia um exercício difícil de dogmática jurídica.

A doutrina brasileira tem, nesse primeiro momento, focado a sua atenção para responder essencialmente uma pergunta: se o regime da responsabilidade é objetivo ou subjetivo.[9] Entendemos

5 BIONI, Bruno Ricardo. Nota do coordenador. **Revista do Advogado**, n. 144, nov., 2019.

6 SCHERTEL, Laura Mendes; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**, vol. 120, p. 469–483. São Paulo: Ed. RT, nov.-dez. 2018. Os autores afirmam ser possível identificar outros quatro eixos: (i) unidade e generalidade da aplicação da lei, (ii) legitimação para o tratamento de dados, (iii) princípios e direitos do titular e (iv) obrigações dos agentes de tratamento de dados.

7 MIRAGEM, Bruno. **A internet das coisas e os riscos do admirável mundo novo.** Consultor Jurídico, 29 mar. 2017. Disponível em: <https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo>. Acesso em: 01 maio 2020.

8 COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, vol. 28, 2012, 14-24.

9 Ver, em especial: GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. **Caderno especial LGPD**, p. 167-182. São Paulo: RT, nov. 2019, um dos mais extensos sobre a matéria, visa essencialmente responder a essa pergunta. Ver também: ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. *In*: **Coletânea →**

que, por mais relevante que isso seja, não é essa questão que deve pautar o debate. Em primeiro lugar, por tratar-se de questão que parece partir de uma premissa falsa de dualidade[10] de regimes jurídicos de responsabilidade, se objetiva ou subjetiva. Na verdade, há diversos modelos e, mesmo entre aqueles que são supostamente de responsabilidade objetiva, nem por isso são idênticos.[11] Mais importante, portanto, do que essa tentativa de classificação binária de responsabilidade, se objetiva ou subjetiva, é analisar mais de perto e, em detalhes, os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização. É o que se pretende fazer no presente artigo, o qual assume uma abordagem exploratória, de primeiras

→ **do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais**. Revista dos Tribunais: São Paulo, 2019, no prelo; 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. *In*: **Cadernos Jurídicos** – Direito digital e proteção de dados pessoais, Escola Paulista de Magistratura, ano 21, n. 53, jan.-mar. 2020. Disponível em: <https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902>. Acesso em: 01 maio 2020.

10 Exceção feita à Caitlin Sampaio Mulholland, que se orienta por três sistemas de responsabilidade civil na LGPD. Ver: MULHOLLAND, Caitlin Sampaio. Palestra no Webinar IBERC #2 – A Responsabilidade Civil na Lei Geral de Proteção de Dados. Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC, 19 set. 2019.

11 A respeito da responsabilidade objetiva ou pelo risco, António Menezes Cordeiro afirma: "Numa leitura simplista, poder-se-ia afigurar que a responsabilidade pelo risco, nas suas várias concretizações, se reconduziria a uma responsabilidade delitual, mas sem os requisitos da culpa e da ilicitude. Não é, de todo, assim. A responsabilidade civil traduz, em cada uma das suas manifestações típicas, um modelo complexo. Os seus diversos pressupostos interagem uns com os outros, de tal modo se alterar, adaptando-se ao conjunto. Ainda quando conservem uma identidade linguística, já não são os mesmos, obrigando a uma reconstrução, modelo a modelo." (CORDEIRO, António Menezes. **Tratado de direito civil português**, vol. II, t. III: gestão de negócios, enriquecimento sem causa, responsabilidade civil. Coimbra: Almedina, 2010, p. 597). Por exemplo, no caso da responsabilidade por fato de terceiro, trata-se de responsabilidade objetiva – os responsáveis respondem "ainda que não culpa de sua parte" (art. 933, CC). Nessa modalidade de responsabilidade objetiva não se exige nada dos responsáveis elencados no art. 932, CC além do vínculo com o lesante (pais e filhos, ou empregadores e empregados, entre outros). No caso da responsabilidade por fato do produto ou do serviço, apesar de tratar-se de responsabilidade também objetiva – "independentemente da existência de culpa", como dizem os arts. 12 e 14, *caput*, do CDC –, para que haja responsabilização, o legislador exige o pressuposto especial do defeito relativo ao produto ou ao serviço (arts. 12 e 14, CDC).

impressões, e que busca compreender qual é a racionalidade jurídica[12] subjacente ao regime de responsabilidade civil contido na LGPD.

O artigo está dividido em 03 (três) partes. A primeira, na linha de outros trabalhos,[13] faz uma análise histórica do texto da LGPD, abrangendo, inclusive, dispositivos para além daqueles diretamente ligados à responsabilidade civil. Desta forma, o objetivo foi desvendar se a estrutura normativa da LGPD estimula ou desincentiva a discussão de culpa. A segunda propõe-se a analisar alguns elementos normativos em específico, os quais são centrais para desvendar qual será o espaço ocupado pela culpa no regime jurídico firmado na LGPD. Em especial, se as obrigações atribuídas aos agentes de tratamento de dados são de meio ou de resultado e, de forma ainda mais detida, os incisos do artigo 44 que traçam parâmetros de aferição em torno da reprovabilidade da conduta danosa. A terceira é uma espécie de colagem das duas anteriores onde se tecem conclusões e reflexões em torno da racionalidade jurídica do regramento da LGPD para a responsabilização dos agentes de tratamento de dados.

A hipótese deste trabalho considera que há uma espécie de gradiente que pode ser um filtro ou um catalisador da culpa enquanto um dos pressupostos da responsabilidade civil. Ao qualificar de forma intensa quais são as obrigações dos agentes de tratamento de dados, e, ainda, ao traçar parâmetros com alta vagueza normativa para mensurar a reprovabilidade de uma conduta danosa, há uma considerável margem interpretativa para que a culpa exerça, ao final, um papel na determinação da responsabilidade civil dos agentes de tratamento. Dessa forma, a principal contribuição do

12 CORDEIRO, A. Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019, pp. 779.

13 ZANATTA, op. cit., no prelo; TASSO, op. cit..

artigo é mapear quais são tais elementos normativos e, com isso, extrapolar uma falsa dualidade entre regimes de responsabilidade civil subjetiva ou objetiva como sendo o cerne da dogmática do regime jurídico de responsabilidade civil formatado na LGPD.

2. A (IN)EVOLUÇÃO DO TEXTO DA LGPD: A DISPUTA TRAVADA EM TORNO DO PAPEL DA CULPA NA DEFINIÇÃO DO REGIME DE RESPONSABILIDADE CIVIL COM UM OLHAR PARA O TODO DA LGPD

A LGPD é fruto de quase dez anos de debate público. Essa discussão deixou pistas hermenêuticas valiosas e, em especial, uma lente por meio da qual considerar os trabalhos preparatórios da lei. A esse respeito, é importante destacar que houve forte disputa em torno da definição do modelo de regime de reponsabilidade civil, a qual não se deu apenas na seção e dispositivos diretamente dedicados ao tema, mas, também, em torno de outros elementos normativos que indiretamente calibram o regime jurídico da reponsabilidade dos agentes de tratamento de dados.

No que diz respeito ao primeiro eixo, é importante destacar: a) o abandono deliberado do regime de responsabilidade civil objetiva e; b) a adoção de técnica legislativa mais prescritiva quanto às excludentes de reponsabilidade civil.

A primeira versão do então anteprojeto de lei de proteção de dados pessoais, bem como a proposta legislativa do Senado Federal expressamente adotavam um regime de reponsabilidade civil objetiva. Enquanto a primeira preceituava que "o tratamento de dados [seria] uma atividade de risco"[14], a segunda estabelecia

14 Disponível em: <http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf>, ver tabela comparativa adiante nesse artigo.

que os agentes da cadeia responderiam, "independentemente da existência de culpa",[15] pela reparação dos danos.

A partir da segunda versão do anteprojeto de lei, ganhou força a opção por um regime de reponsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública[16] e em audiência pública realizada na Câmara dos Deputados[17-18], essa escolha foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos antes aventados – "independentemente de culpa" ou "atividade de risco" – que eliminariam a culpa como um dos pressupostos da responsabilidade civil.

15 Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&ts=1571776630206&disposition=inline>, ver tabela comparativa adiante nesse artigo.

16 INTERNETLAB. **O que está em jogo no debate sobre dados pessoais no Brasil?.** 2016. Disponível em <https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Um dos autores desse relatório, Bruno Bioni, à época pesquisador do Grupo de Políticas Públicas para o Acesso à Informação/GPoPAI da USP, apresentou contribuição em defesa de um regime de responsabilidade civil objetiva.

17 Na ocasião da audiência pública, realizada em 03.05.2017, Rafael Zanatta, representando o Idec, defendeu um regime de responsabilidade objetiva e solidária, fundando-se no diálogo com as demais fontes legislativas, na vulnerabilidade dos consumidores e no estímulo à segurança jurídica e à confiança dos usuários. Leonardo Bessa, representando o Brasilcon, defendeu um regime de responsabilidade objetiva e solidária, tendo em vista o diálogo das fontes e a vulnerabilidade dos consumidores. E Leandro Alvarenga, representando a Confederação Nacional de Dirigentes e Lojistas, criticou a adoção de um regime de responsabilidade solidária, por excluir pequenos lojistas do acesso à informação (e dificultar o acesso ao crédito) e não levar em conta a atuação individual. Disponível em: <https://www.youtube.com/watch?v=-tU53jLMSyk>. Acesso em: 30 abr. 2020.

18 ZANATTA, op. cit., p. 11: "A tensão também ficou clara em dois textos de posição produzidos por entidades distintas: de um lado, o **Manifesto sobre a Futura Lei de Proteção de Dados Pessoais**, coordenada por Brasscom, Abranet e outras associações; de outro, a **Carta Aberta à Comissão Especial de Tratamento e Proteção de Dados Pessoais** produzida pelo Idec. Observando-se as contribuições do setor privado à Comissão Especial de Tratamento e Proteção de Dados Pessoais – em especial, BSA, Facebook, Brasscom, Febraban, ABMED e ANBC –, nota-se, também, um posicionamento massivo contra as regras de responsabilidade solidária".

1ª versão do anteprojeto	Art. 6º O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei.
2ª versão do anteprojeto	Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.
PLC 53/2018	Art. 42. O responsável ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável, hipótese em que o operador equipara-se a responsável, salvo nos casos de exclusão previstos no art. 43 desta Lei; II – os responsáveis que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto no Título III da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor). § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

LGPD	Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Tabela comparativa entre os dois textos citados e o final da LGPD

Além disso, o texto foi gradualmente esculpido para delimitar quais seriam as excludentes de responsabilidade civil. Até a aprovação do substitutivo de autoria do Deputado Orlando Silva, as versões anteriores do texto eram, senão silentes, extremamente tímidas com relação aos contornos para a definição de ilicitude de

uma conduta, bem como com relação ao seu nexo de causalidade para deflagrar a responsabilização dos agentes de tratamento. É, apenas, nesse último estágio da discussão legislativa que são prescritos tais pilares fundantes do regime jurídico da responsabilidade civil da LGPD.

Em vez de simplesmente espelhar as excludentes do CDC, o legislador optou por eximir a responsabilização dos agentes de tratamento de dados caso comprovem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II). Da mesma forma, quando a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados,[19] há ressalva de que tal responsabilização somente é deflagrada se não foram adotadas as "medidas *aptas* a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação"[20]. Trata-se de elementos que afasta a responsabilização do sistema de responsabilidade civil objetiva.

Ao completar um regime jurídico que se orienta pela discussão da culpa, não se pode negligenciar a inserção do princípio da *accountability*, acompanhada dos chamados relatórios de impacto

19 O art. 44, parágrafo único, fala em obrigação de indenizar por danos causados em decorrência de "violação da segurança dos dados". Com base em referência nele expressa, esse dispositivo deve ser lido em conjunto com o art. 46, *caput*. Disso depreende-se que a "violação da segurança dos dados" configura-se nos casos em que, com os dados pessoais, ocorre: (i) acessos não autorizados; ou (ii) situações acidentais ou ilícitas de destruição, perda, alteração, comunicação; ou (iii) qualquer outra forma de tratamento inadequado ou ilícito.

20 Artigo 46 da LGPD: "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei. § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."

à proteção de dados pessoais[21] e, de forma mais ampla e geral, o estímulo e reforço à capacidade dos agentes de tratamento de dados pessoais de auto-organização. Ao longo dos trabalhos preparatórios da LGPD, foi dedicada uma seção específica sobre "Boas Práticas e da Governança". Trata-se de elementos que, ainda que indiretamente, reforçam um regime de responsabilidade civil de natureza subjetiva.

Além do próprio *nomen iuris* do referido princípio, a sua definição aponta para que haja juízo de valor em torno da conduta do agente de tratamento de dados para a sua responsabilização. Nesse sentido, aliás, há conexão expressa entre este princípio e o mencionado elemento de responsabilidade civil mais voltado a um sistema de natureza subjetiva.

Com relação aos chamados relatórios de impacto à proteção de dados pessoais, trata-se de instrumento que foi ganhando cada vez mais protagonismo ao longo dos trabalhos preparatórios da lei. Enquanto na segunda versão do anteprojeto de lei de proteção de dados era referido uma única vez, passa a ser mencionado

21 "Art. 4º [...] § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais." "Art. 10 [...] § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial." "Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público." "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." "Art. 55-J. Compete à ANPD: XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; § 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório."

oito vezes no desenho final da LGPD. Além disso, o texto aprovado ressalta que tal ferramenta deveria ser ativada para os casos em que as atividades de tratamento de dados fossem de "alto risco". É uma gramática que, mais uma vez, não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado, afastando-se um regime de natureza objetiva.

Por fim, deve ser também destacado que a parte relativa à "segurança e boas práticas", que antes era um título do capítulo da tutela administrativa, passa a ser um capítulo próprio. Em termos topográficos e de técnica legislativa, ganha autonomia e, principalmente, passa a ser referenciado como um gatilho para deflagrar a responsabilidade civil dos agentes de tratamento de dados. Mais uma vez, há uma estrutura normativa que prioriza um juízo de valor em torno da conduta do lesante.

Em resumo, os trabalhos preparatórios da LGPD deixam claro que sua política legislativa refutou deliberadamente um regime de reponsabilidade civil objetiva. Mais do que isso, há outros elementos normativos que, direta ou indiretamente, convergem para que haja um juízo de valor em torno da culpa do lesante. Algo que não está apenas cristalizado no rol de excludentes de responsabilidade, mas, também, na principiologia e em outras partes importantes e integrantes do corpo normativo da LGPD. É uma racionalidade inescapável e que está por trás da lógica do regime de responsabilidade civil em questão.

3. RESPONSABILIDADE EM CASO DE "VIOLAÇÃO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS PESSOAIS" E DE "VIOLAÇÃO DA SEGURANÇA DOS DADOS"

Ainda que criticável em termos de técnica legislativa,[22] a LGPD estabelece dois gatilhos para a responsabilidade civil dos agentes de tratamento de dados, quando há a "violação à legislação de proteção de dados pessoais" ou a "violação da segurança dos dados". Ambas são calibradas pela noção de tratamento irregular, prevista no artigo 44, a qual procura sistematizar critérios para aferição da culpa dos agentes de tratamento de dados a esse respeito.

Mesmo que superada a discussão, concluindo-se que o regime de responsabilidade civil adotado pela LGPD é mesmo subjetivo, esse artigo é central para a construção de uma dogmática que pode reduzir ou ampliar o espaço a ser ocupado pela culpa para fins de deflagração da responsabilidade dos agentes de tratamento de dados.

3.1. Tratamento irregular

O art. 44 prevê que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado."

22 Não há razão para tal bifurcação, uma vez que as consequências são as mesmas (obrigação de indenizar) e, em especial, que essas duas hipóteses de reponsabilidade civil são reunidas no artigo 44 sob a noção ampla de "tratamento irregular".

Antes das "circunstâncias relevantes", mencionada no *caput* do referido artigo, é necessário analisar uma questão: a relação do tratamento irregular com a hipótese de violação à legislação de proteção de dados pessoais.

3.1.1. Dubiedade de critérios quanto à violação à segurança dos dados: medidas aptas (art. 44. parágrafo único) *versus* a segurança que dele se pode esperar (art. 44, II)

A noção de tratamento irregular apresenta desconformidades. Da sua leitura, percebe-se que ele visa conectar-se tanto com a hipótese de responsabilidade por violação da legislação, quanto da segurança. Por outro lado, a previsão de tratamento irregular encontra-se prevista no *caput* de dispositivo (art. 44) que abarca, em seu parágrafo único, a responsabilidade por violação da segurança.

Se a figura do tratamento irregular conecta-se igualmente com ambas as hipóteses de responsabilidade, melhor seria prever sobre a irregularidade em dispositivo autônomo, permitindo a essa regra ficar equidistante das duas hipóteses de violação de normas da LGPD. Da forma como está, a previsão sobre irregularidade do tratamento está no mesmo dispositivo do que a violação da segurança, o que sugere ao intérprete uma conexão mais próxima (ou quiçá exclusiva) da noção de regularidade do tratamento para com a violação da segurança, do que para com a violação à legislação da proteção de dados. E mais: melhor ainda seria um dispositivo que previsse, no *caput*, que os agentes de tratamento responderiam pelos danos decorrentes de tratamento irregular de dados. E, em parágrafo, houvesse a explicação do conteúdo do tratamento irregular.[23]

23 Essa questão da dispositivos dos artigos não deixa de ter reflexos materiais. Segundo Patricia Peck Pinheiro, o art. 44 "traz as condições de demonstração da ilicitude do tratamento de dados pessoais, assim como ocorre com o artigo 6° do GDPR, que pontua as condições de licitude do tratamento de dados pessoais." (PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: Comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraivajur, 2018, p. 101). Note-se que o art. 6º do GPDPR, ou melhor RGPD →

Essa má técnica legislativa pode, contudo, ser parcialmente explicada. Essa previsão de tratamento irregular corresponde à transposição para a LGPD de previsão do CDC que regula defeito do serviço. O art. 14, § 1º do CDC prevê: "O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido." É exatamente o conteúdo que foi espelhado nos incisos do artigo 44 da LGPD.

CDC	**LGPD**
Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - **o resultado e os riscos que razoavelmente dele se esperam;** III - **a época em que foi fornecido.** § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas. § 3º O fornecedor de serviços só não será responsabilizado quando provar: I - que, tendo prestado o serviço, o defeito inexiste; II - a culpa exclusiva do consumidor ou de terceiro. § 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.	Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; **III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.** Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Tabela Comparativa CDC *vs* LGPD

➔ conforme sua sigla em português, encontra correspondência material no art. 7º da LGPD, que trata dos requisitos para o tratamento de dados pessoais. Esse dispositivo, por sua vez, está diretamente ligado à hipótese de "violação à legislação de proteção de dados pessoais", prevista no art. 42, *caput*. Essa leitura da autora sobre o conteúdo do dispositivo deixa de fora, portanto, a relação entre tratamento irregular e violação da segurança dos dados. Nesse caso, a associação teria de ter incluído o art. 32 do RGPD, o qual prevê os parâmetros para determinação das medidas de segurança exigíveis para tratamento de dados.

Trata-se, portanto, de previsão que tem maior vocação para fornecer elementos para orientar a concretização de falha de segurança do tratamento de dados. Isso explica, inclusive, o fato de previsão de irregularidade estar no mesmo dispositivo que a violação da segurança dos dados e ter com ela maior proximidade e interação material.

A segunda desconformidade é de conteúdo. O art. 44, parágrafo único, prevê que os agentes de tratamento de dados respondem, ao deixarem de adotar medidas de segurança aptas a proteger os dados pessoais (art. 46) e, assim, derem causa ao dano. A irregularidade aqui, para utilizar uma nomenclatura da própria LGPD, é a não adoção, por parte do controlador e operador, das medidas de segurança aptas a proteger os dados pessoais. Por outro lado, o art. 44, *caput*, diz que o tratamento será irregular quando não fornecer a segurança que o titular dele pode esperar. Vê-se, portanto, que, de um lado, tem-se como pressuposto as medidas de segurança aptas a proteger os dados pessoais. E, de outro, tem-se a segurança que o titular dele pode esperar. Em face disso, questiona-se: em caso de violação da segurança dos danos, o agente responde se ele não adotar as medidas de segurança aptas a protegê-los, ou se o tratamento não fornecer a segurança que o titular dele pode esperar?

Note-se que são critérios distintos. Para ficar apenas em um exemplo: o titular pode esperar que o tratamento forneça segurança maior ou menor que aquela garantida pela adoção das medidas de segurança aptas a proteger os dados pessoais. Os critérios geram questionamentos diferentes. De um lado, o que são medidas de segurança aptas? São aquelas que potencialmente garantem a segurança, ou apenas aquelas que seguramente o fazem? De outro lado, quando a lei fala em "segurança que o titular dele pode esperar", o critério é subjetivo ou objetivo? Trata-se do que a pessoa do titular de dados do caso concreto pode esperar, devendo-se então levar em conta o seu nível especial de conhecimento ou ignorância? Ou critério objetivo, falando de um titular padrão?

3.1.2. Conectando inobservância da legislação e o não fornecimento de segurança esperada, a partir do conceito de "legítimas expectativas de segurança"

No tópico anterior, chegamos à conclusão de que tratamento irregular não é noção autônoma e, mais especificamente, que o não fornecimento da segurança que o titular pode esperar (art. 44, *caput*) tem de coincidir em conteúdo com "deixar de adotar as medidas de segurança" aptas a proteger os dados pessoais (art. 44, parágrafo único, c/c art. 46, *caput*).

No entanto, qual é o conteúdo disso? Analisando detidamente, percebe-se que apenas um deles oferece elementos para uma concretização e delimitação do conteúdo. Parece-nos que é o não fornecimento da segurança que o titular pode esperar do tratamento (art. 44, *caput*). Isso se deve, em primeiro lugar, pelo fato de o critério da adoção de tratamentos aptos a proteger os dados pessoais ser demasiadamente amplo. Ele confere apenas um critério mínimo, ou quiçá nem isso. De fato, seria ilógico pensar que o agente teria de adotar medidas inaptas para proteger os dados pessoais. Contudo, o universo de medidas aptas é demasiadamente amplo. Por exemplo, a rigor poderiam ser consideradas medidas aptas a proteger os dados pessoais, tanto uma desproporcionalmente mais custosa do que as demais, quanto uma outra cuja eficácia tivesse sido confirmada e disseminada apenas após o evento danoso, mas antes da decisão judicial de responsabilidade. Mas, apesar de aptas, seriam essas medidas exigíveis, ou seja, que o agente deveria ter adotado sob pena de responsabilização? Entendemos que não.

Por outro lado, é bem mais frutífera a análise do critério de irregularidade do tratamento "quando não fornecer a segurança que o titular dele pode esperar". Mas o que isso significa exatamente? Em primeiro lugar, não é a segurança cujo fornecimento de fato se espera, mas sim aquela que se "pode esperar". No primeiro caso, seria uma mera constatação fática. No segundo, há aí

um *filtro jurídico*: aquilo que, do ponto de vista jurídico, o titular está autorizado a esperar. Não se trata de qualquer expectativa de segurança, mas sim de expectativas juridicamente legítimas.[24] Vai-se trabalhar aqui, assim como se trabalha no CDC, com "legítimas expectativas de segurança". Trata-se de conceito jurídico indeterminado, "cujo sentido deve ser concretizado pelos tribunais em vista das circunstâncias do caso concreto"[25].

Um exemplo que ilustra bem os desdobramentos práticos de tal dogmática proposta é o que se testemunhou recentemente no campo da criptografia. Foi apenas mais recentemente que se desenvolveu e se disseminou a chamada criptografia assimétrica de "ponta a ponta"[26], de sorte que hoje é uma expectativa de segurança que se pode esperar dos chamados aplicativos de mensagens instantâneas. Em um passado não muito distante, em particular antes dos escândalos de espionagem "Snowden", tal tecnologia de segurança da informação não estava disseminada e, muito provavelmente, não corresponderia a uma expectativa juridicamente tutelável.[27]

24 No CDC, essa questão é mais clara quando se regula responsabilidade por defeito do produto do que por defeito do serviço. No primeiro caso, o CDC prevê que "o produto é defeituoso quando não oferece a segurança que dele legitimamente se espera" (art. 12, § 1.º). No caso da responsabilidade por defeito do serviço, fala apenas que "o serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar" (art. 14, § 1.º). Apesar da distinção, a doutrina não faz diferenciação. Em ambos os casos, entende-se que a expectativa tem de ser legítima. A LGPD inspirou-se no regramento da responsabilidade por defeito do serviço, por isso que não menciona legitimamente. Mas, da mesma forma que acontece no CDC, isso não é sinal de que as expectativas não precisam ser legítimas.

25 REINIG, Guilherme Henrique Lima. **A responsabilidade do produtor pelos riscos do desenvolvimento**. São Paulo: Atlas, 2013, p. 30.

26 Essa discussão é o que está no cerne da ADPF 403-SE: se as ordens de bloqueio do aplicativo WhatsApp, por franquear acesso às mensagens criptografadas dos seus usuários, gera lesão a uma série de direitos fundamentais. A esse respeito, veja-se todo o mapa das argumentações feito pelo InternetLab, disponível em: <http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/>.

27 Na criptografia assimétrica de ponta a ponta, dois tipos de chaves são usados para cada ponta da comunicação, uma chave pública e uma chave privada. As chaves públicas estão disponíveis para qualquer outra pessoa, todos compartilham suas chaves ➔

Um outro exemplo a esse respeito, desta vez projetando um cenário futuro, será quando for escalada a chamada computação quântica.[28] Dado o aumento da capacidade de processamento de informação em termos quantitativos e qualitativos que se experimentará, consequentemente as técnicas de segurança progredirão e, em última análise, haverá a atualização do filtro jurídico hoje existente em torno do que se considera "legítima expectativa de segurança".[29]

Um segundo ponto refere-se à necessidade de delimitar esse "titular", se é a pessoa em si do caso concreto, ou um titular médio. Retornando ao referencial do direito do consumidor, como bem coloca Guilherme Reinig, referindo-se às expectativas de segurança no CDC, "para tal concretização importa, antes de tudo, especificar a perspectiva a partir da qual o juiz deve identificar as expectativas de segurança [...]. Trata-se, em outros termos, da determinação da 'titularidade' da legítima expectativa de segurança. Em linhas gerais, o problema consiste em saber se o legislador adotou um critério subjetivo ou objetivo."[30] Isto é, se vai fazer uma

→ públicas antes da comunicação. ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", Columbia Journal of Transnational Law Online Edition, 17 de outubro de 2016, disponível em: <http://jtl.columbia.edu/from-jurisdictional-battles-to-cryptowars-brazilian-courts-v-whatsapp/>.

28 Em 08.01.2019 foi lançado o primeiro computador quântico de uso comercial do mundo. Contudo, estima-se um período entre cinco e dez anos para que a computação quântica passe a ser adotada nos negócios. Assim, apesar de existente, essa tecnologia não compreenderia o estado da arte da tecnologia (ou meio técnico razoável disponível, nos termos da LGPD), tornando um encargo demasiado excessivo a expectativa de sua adoção. Disponível em <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/como-computacao-quantica-vai-abalar-os-negocios-para-sempre.html>. Acesso em: 29 abr. 2020.

29 Sobre uma discussão mais detida a esse respeito sobre as chamadas técnicas de anonimização, veja-se: BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: **Cadernos Jurídicos** – Direito digital e proteção de dados pessoais, Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020. Disponível em <https://brunobioni.com.br/wp-content/uploads/2020/04/Bioni_Anonimiza%C3%A7%C3%A3o.pdf >. Acesso em: 01 maio 2020.

30 REINIG, op. cit., p. 30.

análise em concreto, ou em abstrato. Tendo como base a pessoa em causa, ou um grupo abstrato de pessoas.

De maneira análoga ao que ocorreu no CDC, o legislador da LGPD não é expresso em relação à solução seguida. No direito do consumidor, uma vez que o CDC trabalha com noção parecida: o produto ou serviço é defeituoso quando não oferece a segurança que o consumidor dele pode esperar (art. 14, § 1.º). A doutrina, contudo, conclui pelo critério objetivo.[31]

Em relação à LGPD, deve-se chegar a conclusão análoga. Nesse sentido, na doutrina nacional sobre proteção de dados, Cots e Oliveira afirmam: "a análise da expectativa deverá sempre ser realizada sobre um caso concreto, utilizando a noção que se espera do homem-médio em relação a determinado tratamento de seus dados."[32]

Dessa maneira, o critério determinante para a imputação de responsabilidade é o da irregularidade do tratamento. Esse critério, por sua vez, é preenchido com base nas legítimas expectativas de segurança que um titular médio pode legitimamente esperar do tratamento de dados em questão.

31 Segundo fundamenta Guilherme Reinig, "o uso da voz passiva sintética na oração subordinada adjetiva restritiva [...], não deixa dúvida de que o legislador optou pelo critério objetivo". E complementa: "Em última instância, as legítimas expectativas de segurança são determinadas pelo chamado 'horizonte da coletividade afetada pela falta de segurança do produto' (*Horizont der durch die fehlende Produktsicherheit betroffenen Allgemeinheit*), o qual nem sempre se confunde com a perspectiva da sociedade em geral. O mencionado horizonte abrange tanto os destinatários ou consumidores do produto como os *bystanders*. Como, porém, a consideração dos interesses destes não altera significativamente os critérios de verificação da existência de defeito, não há problema algum em se apontar como titular das expectativas de segurança o consumidor médio ou ideal-típico. Nesse sentido, esta noção é um instrumento conceitual de identificação das legítimas expectativas de segurança do setor social afetado pelos riscos relacionados ao produto." (REINIG, op. cit., p. 30).

32 COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. São Paulo: RT, 2019, p. 186.

3.1.3. Circunstâncias relevantes: conectando o artigo 43 ao 50 da LGPD para um juízo de culpa caso a caso

Analisa-se agora as circunstâncias relevantes para determinação da segurança que o titular médio pode esperar do tratamento de dados. O legislador elencou três circunstâncias: I – o modo pelo qual o tratamento é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; e III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Antes de mais, é importante notar o uso da terminologia "entre as quais" no *caput* do artigo 44. Trata-se, portanto, de elenco não exaustivo das circunstâncias para determinar a segurança que o titular pode esperar do tratamento de dados pessoais, bem como quando uma atividade de tratamento de dados é capaz de violar as normas de proteção de dados em sentido *latu sensu*. Trata-se de uma abertura normativa importante, na medida em que a vagueza normativa do artigo 44, em especial dos incisos I e II, pode ser preenchida por outros elementos normativos da própria LGPD.

Um possível caminho para dar densidade normativa a tais incisos é colá-los ao que preceitua o artigo 50, em especial os §§ 1º e 2º. Ao considerar que os agentes de tratamento de dados devem estabelecer mecanismos de mitigação de "riscos" das suas atividades de tratamento de dados, referidos dispositivos apontam que se deverá levar em consideração respectivamente: (i) a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular; (ii) a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados.

Dessa forma, o modo pelo qual é realizado um tratamento de dados (inciso I) e os riscos que razoavelmente dele se esperam (inciso II) são calibrados diretamente por tais variações. A estrutura normativa da LGPD parte do pressuposto que haverá uma alta variação do potencial lesivo entre as mais diferentes atividades

de tratamento de dados, o que tornará determinante avaliar-se a maneira pela qual estas devem ser executadas e os riscos que delas derivam.

Volta-se ao que foi mencionado anteriormente (tópico 1), a (in) evolução do texto da LGPD não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado. Pelo contrário, demanda-se uma análise casuística para se desdobrar um juízo de valor sobre o modo pelo qual deve ser realizado um tratamento de dados e os riscos que dele razoavelmente se esperam.

Alguns exemplos e considerações podem ser elucidativos. De um lado, é notório que dados de cartão de crédito detêm um risco maior diante do interesse de terceiros fraudadores, do que em relação a endereços de e-mail.[33] A mesma coisa com relação ao CPF do que outros dados cadastrais para fins de fraudes bancárias. De outro, é uma análise que não olha para o porte ou o tamanho do agente de tratamento de dados, mas que é voltada para a atividade de tratamento de dados em si. Por exemplo, pense-se no caso de uma empresa nascente de tecnologia, com apenas cinco colaboradores, que fornece uma solução de inteligência artificial para automatizar diagnósticos e prognósticos na área de oncologia. Para tanto, é necessário manipular um grande volume de dados sensíveis de pacientes de uma série de hospitais e laboratórios. Tal atividade de tratamento de dados é mais arriscada do que aquela praticada por uma grande rede de supermercados, com mais de quinhentos colaboradores, que não tem sequer um programa de fidelidade dos seus consumidores.

Portanto, os agentes devem ajustar suas medidas de segurança para corresponder à probabilidade e gravidade de uma violação em face dos possíveis impactos nos direitos e liberdades dos

33 De maneira análoga, lecionando sobre segurança no tratamento de dados com base no art. 32 do RGPD, ver: MORGENROTH, Sven. ***GDPR Article 32***: Security of Data Processing. Disponível em: <https://www.netsparker.com/blog/web-security/gdpr-article-32-security-data-processing/>. Acesso em: 30 mar. 2020.

titulares dos dados. É, então, vital separar e estimar esses riscos variados e, em seguida, aplicar medidas de segurança. A política legislativa da LGPD leva em consideração que tem como objeto regulado uma plêiade de relações jurídicas e que apresentam uma multiplicidade de efeitos colaterais distintos, devendo-se investigar a culpa do agente de tratamento de dados de forma casuística.

3.1.4 Circunstâncias relevantes: as técnicas de tratamento de dados disponíveis à época (inciso III do artigo 43)

Por fim, ainda como um critério que compõe a noção de tratamento irregular, o artigo 44 dispõe que se devem levar em consideração "as técnicas de tratamento de dados pessoais *disponíveis à época* em que foi realizado". Como já apontado, a legislação consumerista inspirou a LGPD. O produto ou serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, como risco que razoavelmente se espera *e a época* em que foi colocado em circulação ou fornecido (art. 12, § 1º, III e art. 14, § 1º, III, CDC)

Essa previsão reflete a necessidade de se determinar um momento a partir do qual se afere a irregularidade do tratamento.[34] A questão a se responder, contudo, diz respeito à cognoscibilidade e exigibilidade de adoção das medidas de segurança para que elas sejam consideradas como disponíveis à época em que

34 Essa indispensabilidade já foi reconhecida no direito do consumidor em relação ao juízo de defeito do produto ou serviço, sendo os argumentos aqui aproveitáveis. Segundo analisa Guilherme Reinig: "Diversos fatores, como o aumento das necessidades de segurança da sociedade e especialmente o desenvolvimento de novas tecnologias, concorrem para que a segurança que legitimamente se espera do produto não seja constante, modificando-se com o passar do tempo. Por isso, é necessário o estabelecimento de um instante decisivo para a avaliação da defectibilidade do produto. Esse instante ou momento é, de acordo com o texto legal, aquele em que o produto é colocado em circulação. Se o produto corresponder à segurança que dele legitimamente se espera no mencionado instante ou momento, ele não poderá ser considerado defeituoso, ainda que haja uma posterior elevação das legítimas expectativas de segurança." (REINIG, op. cit., p. 36)

foi realizado o tratamento de dados. Ou seja, considera-se como disponível à época do tratamento as medidas de segurança perceptíveis e acessíveis aos agentes de tratamento de diligência comum ou média?

Em relação a essa questão, Márcio Cots e Ricardo Oliveira pontuam que "a LGPD dispõe que as técnicas de tratamento disponíveis à época devem ser consideradas. A regra é importante, especialmente porque utiliza a palavra 'disponíveis', não existentes, o que são coisas completamente diferentes." Os autores propõem, então, dois exemplos: "Imagine, por exemplo, que na Noruega esteja sendo testado um sistema de segurança extremamente eficiente, mas que ainda não está sendo comercializado fora do âmbito daquele país. Ora, o sistema existe, mas não está disponível aos controladores brasileiros. Por outro lado, suponha que após determinado tempo o sistema passe a ser comercializado no Brasil, mas pelo valor de 50 milhões de dólares a licença." Em face disso, questionam: "Isso faz com que o sistema esteja 'disponível' para os controladores brasileiros? Entendemos que não. A palavra 'disponíveis' precisa levar em consideração a possibilidade ou não de o controlador ter acesso a determinado sistema, não o simples fato de ele existir ou ser comercializado fora dos padrões econômicos do controlador sob análise."[35]

De acordo com essa leitura, o critério determinante seria o da diligência média dos agentes de tratamento. Contudo, essa posição não leva em conta que essa previsão foi inspirada em previsão análoga no CDC. Nesse diploma, é necessário verificar se o fornecedor adotou ou não as medidas necessárias para que o produtor ou serviço fornecesse a segurança que o consumidor dele pode esperar, levando-se em conta a época em que o serviço foi fornecido. Contudo, o legislador previu que a responsabilidade do fornecedor seria independentemente de culpa. O critério não é,

35 COTS; OLIVEIRA, op. cit., p. 186.

portanto, o da diligência média do próprio fornecedor e nem a diligência de um fornecedor médio. Isso porque a diligência média do fornecedor, ou a diligência de fornecedor médio são os dois critérios tradicionais para determinar a culpa subjetiva (ou *in concreto*) e objetiva (ou *in abstracto*).

Na LGPD não há previsão de exclusão da culpa análoga a essa do CDC ("independentemente da existência de culpa"). Contudo, como a previsão da circunstância da época em que o serviço foi prestado foi o que deu origem à disposição da LGPD, é possível conceber que o critério almejado é, assim como no CDC, mais rigoroso do que o da culpa.

3.2. Presunção de alguns dos pressupostos de responsabilidade e inversão do ônus da prova quanto aos demais

O art. 43 prevê as excludentes de responsabilidade dos agentes de tratamento. Dessa previsão, é extraível que, em face de dano decorrente de tratamento de dados, presume-se: (i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; e (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento.

Acontece que, além dessa presunção geral de dois elementos da responsabilidade civil dos agentes de tratamento, a LGPD prevê também a possibilidade de o juiz inverter o ônus da prova a favor do titular dos dados quando a alegação for verossímil, quando houver hipossuficiência ou quando a produção de provas for excessivamente onerosa (art. 42, § 2.º). Como compatibilizar?

O art. 43 implica a presunção automática de alguns elementos da responsabilidade civil, mas não de todos. Contando com essa presunção, resta ainda ao lesado, em geral, alegar e provar: (i) a realização de (algum) tratamento de dados pessoais – não sendo necessário provar que foi realizado pelo réu; (ii) o dano sofrido; e (iii) o nexo causal entre o tratamento de dados realizado e o dano.

A compatibilização entre as previsões do art. 43 e art. 42, § 2.º é, então, a seguinte: caso a alegação da vítima seja verossímil, ou haja hipossuficiência para produção de provas, ou a produção seja excessivamente onerosa, o juiz poderá inverter o ônus da prova em relação a esses três últimos elementos. Como resultado, a vítima não precisará provar nenhum elemento da responsabilidade, ficando a cargo dos agentes de tratamento o ônus de provar a sua não ocorrência.

Uma inversão tão extremada do ônus da prova é justificada pela, igualmente dramática, hipossuficiência do titular de dados. Como observam Tarcisio Teixeira e Ruth Armelin, essa hipossuficiência torna-se "facilmente constatável quando se tem uma sociedade permeada pela cultura do *Big Data*, em que há uma coleta massiva de dados, muitas vezes até desnecessária." Em face dessa realidade, complementam os autores, "o titular de dados se encontra em uma posição claramente desfavorável, em que beira [a]o impossível saber quais de seus dados estão sendo tratados, de que forma isso tem sido feito e quem seriam os agentes de tratamento."[36]

Com isso, o regime jurídico da responsabilidade civil estipulado pela LGPD traz uma erosão bastante significativa dos filtros da responsabilidade civil em favor do titular dos dados. Ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil.

36 TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. *In*: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 322.

Presunção automática-legal	Presunção mediante inversão do ônus da prova em juízo
(i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento	Resta ao lesado provar: (i) o dano sofrido; e (ii) o nexo causal entre o tratamento de dados realizado e o dano.
(artigo 43, I e II, da LGPD)	(artigo 42, § 2º da LGPD)

3.3. Obrigação de meio *versus* de resultado: a significação dos termos aptas, eficazes e eficientes

Uma última discussão importante para a definição do regime jurídico de responsabilidade civil da LGPD, é considerar se as obrigações atribuídas aos agentes de tratamento de dados são de meio ou resultado. Isto porque, na prática, no caso de uma obrigação de resultado, a não consecução do resultado almejado implica uma presunção de culpa em relação ao inadimplemento.

O princípio da responsabilidade e prestação de contas prescreve que deve haver pelos agentes de tratamento de dados pessoais a "demonstração (...) da *adoção* de medidas *eficazes* e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da *eficácia* dessas medidas". O dispositivo chega a ser prolixo, já que duplica o uso do termo eficazes-eficácia.

Tais adjetivos abrem margem interpretativa para considerar que a LGPD atribuiu uma obrigação de resultado, na medida em que indicam normativamente que não basta apenas adotar – para usar o verbo de ambos os dispositivos – medidas a evitar o tratamento inadequado de dados, mas, sobretudo, que tais ações sejam eficientes.

Por outro lado, o conceito de *privacy by design*,[37] previsto no artigo 46 da Lei, prevê que os "agentes de tratamento devem *adotar* medidas de segurança, técnicas e administrativas *aptas* a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Por sua vez, o já citado artigo 50 da LGPD prevê que a aptidão dessas medidas deve ser ajustada de acordo as características da atividade de tratamento de dados em questão, em especial "a gravidade dos riscos" que dela derivam para o titular.

Esses outros dois dispositivos parecem prescrever uma *norma de conduta* que encerra uma obrigação de meio. Isto porque enuncia-se quais elementos devem ser considerados para que um fim seja alcançado, mas sem vincular o sujeito passivo dessa obrigação à consecução deste objetivo.

Em resumo, há, mais uma vez, uma possível dubiedade na moldura normativa da LGPD quanto ao tipo de obrigação que foi alocada aos agentes de tratamento de dados. Um olhar mais focado nos adjetivos trazidos pelo princípio da responsabilidade e prestação de contas abre caminho para uma possível obrigação de resultado, enquanto os dispositivos relacionados à *privacy by design* e boas práticas indicam uma obrigação de meio que poderia, em última análise, modular o referido termo eficiência contido no referido princípio.

37 BIONI, Bruno Ricardo. Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito ainda elusivo de Privacy by design. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). **Direito & Internet IV**: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, v. 1, 2019.

4. CONCLUSÃO

Ainda que a LGPD tenha esculpido um regime de responsabilidade civil subjetiva, não se pode negligenciar que as barreiras para a deflagração do dever de indenizar foram substancialmente diminuídas. Em particular diante da presunção automática-legal da culpa do lesante, a qual pode ser somada à inversão do ônus da prova em juízo quanto aos demais pressupostos da responsabilidade civil. Se isto for, ainda, combinado com uma interpretação elástica em torno da noção de tratamento irregular, especialmente quanto à obrigação dos agentes de tratamento de dados pessoais adotarem as técnicas "disponíveis à época do tratamento" que se desdobrem em um alto nível de diligência quanto ao estado da arte e da técnica como já o vem fazendo parte da doutrina consumerista, então se tornará extremamente difícil o agente de tratamento de dados afastar a sua culpa.[38]

Em poucas palavras, deve-se avançar para além da constatação binária de se o regime jurídico de responsabilidade civil da LGPD é de natureza objetiva e ou subjetiva. Isto porque, não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Ainda que possa parecer paradoxal, o resultado pode ser um regime jurídico de responsabilidade civil subjetiva com uma espécie de alto grau de objetividade.

38 SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 4ª ed. Atlas Jurídico: São Paulo, 2015, p. 221: "E, mesmo no Brasil, onde a matéria era tradicionalmente regida pela responsabilidade subjetiva, as cortes já recorriam a expedientes bastante objetivistas, como a presunção, tomada em sentido quase absoluto, de responsabilidade do motorista que atinge a parte traseira do automóvel alheio (...) por meio da simples adoção de parâmetros bastante elevados e rígidos de comportamento diligente, ou ainda por força de uma inversão insuperável do ônus probatório da demonstração de culpa".

BIBLIOGRAFIA

ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", **Columbia Journal of Transnational Law** Online Edition, 17 de outubro de 2016. Disponível em: http://jtl.columbia.edu/from-jurisdictional-battles-to-cryptowars-brazilian-courts-v-whatsapp/. Acesso em: 01 maio 2020.

ACCIOLY, Hildebrando; NASCIMENTO E SILVA, G. E. do; CASELLA, Paulo Borba. **Manuel de Direito Internacional Público.** 24ª ed. Saraiva: São Paulo, 2019.

BIONI, Bruno Ricardo. **Compreendendo o conceito de anonimização e dado anonimizado.** Cadernos Jurídicos – Direito digital e proteção de dados pessoais, Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020. Disponível em: <https://brunobioni.com.br/wp-content/uploads/2020/04/Bioni_Anonimiza%C3%A7%C3%A3o.pdf>. Acesso em: 01 maio 2020.

_____. Nota do coordenador. **Revista do Advogado**, n. 144, nov., 2019.

_____. **País precisa ser competitivo em uma economia de dados.** Valor Econômico, 19 jul 2018. Disponível em < https://valor.globo.com/opiniao/coluna/como-o-brasil-pode-inovar-na-protecao-de-dados-pessoais.ghtml >.

_____. Abrindo a caixa de ferramentas da *LGPD* para dar vida ao conceito ainda elusivo de Privacy by design. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). **Direito & Internet IV -** Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, v. 1, 2019.

BRUNO, Marcos Gomes da Silva. Da responsabilidade e do ressarcimento de danos. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de dados comentada. São Paulo: RT, 2019.

CORDEIRO, António Menezes. **Tratado de direito civil português**, vol. II, t. III: gestão de negócios, enriquecimento sem causa, responsabilidade civil. Coimbra: Almedina, 2010.

CORDEIRO, António Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Revista dos Tribunais: São Paulo, 2019.

_____. Da responsabilidade civil pelo tratamento de dados pessoais. *In*: BARBOSA, Mafalda Miranda; ROSENVALD, Nelson; MUNIZ, Francisco (Coord.). **Desafios da nova responsabilidade civil**. São Paulo: Editora JusPodivm, 2019, p. 49-64.

COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, 28 (2012), 14-24.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. São Paulo: RT, 2019.

GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. **Caderno especial LGPD**, p. 167-182. São Paulo: RT, nov. 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**, vol. 120, 2018, p. 469-483, nov.-dez. 2018.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 6. ed. São Paulo: RT, 2016.

_____. **A internet das coisas e os riscos do admirável mundo novo.** Consultor Jurídico, 29 mar. 2017. Disponível em: <https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo>. Acesso em: 01 maio 2020.

MORGENROTH, Sven. **GDPR Article 32**: Security of Data Processing. Disponível em: <https://www.netsparker.com/blog/web-security/gdpr-article-32-security-data-processing/>. Acesso em: 30 mar. 2020.

MULHOLLAND, Caitlin Sampaio. Palestra no Webinar IBERC #2 – A Responsabilidade Civil na Lei Geral de Proteção de Dados. Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC, 19 set. 2019.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraivajur, 2018.

REINIG, Guilherme Henrique Lima. **A responsabilidade do produtor pelos riscos do desenvolvimento**. São Paulo: Atlas, 2013.

SCHERTEL, Laura Mendes; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista dos Tribunais: **Revista de Direito do Consumidor**, vol. 120/2018, p. 469 – 483, Nov - Dez/2018.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 4ª ed. Atlas Jurídico: São Paulo, 2015.

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 – Direito digital e proteção de dados pessoais, Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020. Disponível em: <https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902>. Acesso em: 01 maio 2020.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. *In*: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 297-326.

ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. *In*: **Coletânea do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2019, no prelo.

"Já no primeiro papo, Bruno mostrou seu jeito: direto, objetivo, analítico, estratégico, mas ao mesmo tempo empático, escutador, compreensível. Eram os idos de 2012, ambos na mesma aula na velha SanFran, a centenária Faculdade de Direito da USP. Depois de debates em sala, pegamos o metrô na Praça da Sé. Ali engatamos a primeira de muitas conversas que perduram até hoje. Depois desse episódio, viajamos para lados diferentes do oceano, ele para o Canadá, eu para a Ásia e o velho continente. Mantivemos contatos intermediados pela paixão em comum: a privacidade. A volta ao Brasil, em 2014, logo resultou numa visita ao Porão, recanto da SanFran onde todos se encontram para socializar por décadas a fio. Nesse momento nasceu uma incrível colaboração e amizade que perdura intensamente até hoje, que teve como contexto o desenvolvimento da Lei Geral de Proteção de Dados, nossa querida LGPD, e resultou na fundação do Data Privacy Brasil, hoje uma das principais instituições do país focada na educação e pesquisa em privacidade e proteção de dados. Esse mais novo livro do Bruno, agora na forma de coletânea, é como ele: direto, objetivo, analítico, estratégico, preciso, mas sem perder a maestria (e a magia) na condução do leitor a um conteúdo único no país sobre o tema. Convido a todos e a todas a conhecerem a bela visão de mundo que tenho a oportunidade de acompanhar diariamente com meu grande amigo."

Renato Leite Monteiro