PROTEÇÃO DE DADOS PESSOAIS: PRIVACIDADE VERSUS AVANÇO TECNOLÓGICO

Cadernos Adenauer

3

ANO XX 2019

PROTEÇÃO DE DADOS PESSOAIS: PRIVACIDADE VERSUS AVANÇO TECNOLÓGICO

KONRAD ADENAUER STIFTUNG

EDITORA RESPONSÁVEL
Anja Czymmeck

COORDENAÇÃO EDITORIAL E REVISÃO
Reinaldo J. Themoteo

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO
Claudia Mendes

IMPRESSÃO
Stamppa

ISSN 1519-0951

Cadernos Adenauer XX (2019), nº3
Proteção de dados pessoais: privacidade versus avanço tecnológico
Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019.
ISBN 978-85-7504-230-4

FUNDAÇÃO KONRAD ADENAUER
Representação no Brasil: Rua Guilhermina Guinle, 163 · Botafogo
Rio de Janeiro · RJ · 22270-060
Tel.: 0055-21-2220-5441 · Telefax: 0055-21-2220-5448
adenauer-brasil@kas.de · www.kas.de/brasil
Impresso no Brasil

Sumário

Apresentação

■ Este número da série Cadernos Adenauer é dedicado ao tema da proteção de dados pessoais, uma vez que o uso e a proteção dos dados das pessoas têm ocupado crescentemente o debate público, sobretudo a partir da Lei Geral de Proteção de Dados Pessoais, sancionada m 14 de agosto de 2018, com o objetivo de normatizar diversos aspectos relacionados ao tratamento dos dados das pessoas. À medida que as tecnologias da informação se desenvolvem e complexificam, o volume de dados que circula em meio digital cresce de modo significativo, de modo que hoje em dia temos o chamado Big Data, possibilitando lidar adequadamente com volumes e variedades muito grandes de informações, em velocidade muito alta.

Desde os primórdios da internet, muitos progressos foram alcançados, abarcando o rápido desenvolvimento de novas tecnologias que nos possibilitaram a conexão online: computadores, modens, recursos de rede, e mais recentemente a popularização de smartphones e tablets que abriram campo ao uso móvel dos recursos online. Os aplicativos de mensagens instantâneas, por exemplo, não só mudaram a forma como as pessoas se comunicam no dia-a-dia, mas também afetaram a dinâmica na própria política, ao permitir que pessoas se troquem ideias e se organizem em grupos criados em tais aplicativos, cujo conteúdo não pode ser acessado por quem esteja fora dos mesmos devido ao fato de serem criptografados. A greve dos caminhoneiros de 2018 em diversos estados brasileiros é um caso emblemático da influência de tais aplicativos, bem como a campanha eleitoral e os debates realizados nas redes sociais.

Os hábitos de consumo encontram-se profundamente entrelaçados ao mundo digital, onde é possível comprar desde comida a equipamentos de última geração usando um celular, onde os aplicativos de transporte, sejam eles carona em automóveis ou aluguel de patinetes elétricos, impactam a mobilidade urbana, onde recursos avançados de navegação GPS estão presentes nesses serviços

tanto como nos bolsos mesmo de quem eventualmente não é usuário de um desses serviços, mas pode usar seu GPS para se deslocar para onde queira. Recursos de vigilância, localização e bloqueio que vêm transformando e abrindo novos horizontes no setor de segurança. Em algumas localidades da cidade do Rio de Janeiro encontram-se em fase de implantação o uso de tecnologia de reconhecimento facial de pessoas em tempo real, a exemplo de outras metrópoles em outros países. As tecnologias de informação transformaram o conceito de home office algo cada vez mais conhecido e viável, para diversas áreas de atuação profissional, possibilitando novos arranjos no mundo do trabalho. A digitalização no mundo corporativo, bem como no setor público, acena com promissoras possibilidades de agilidade em serviços e desburocratização. O lazer também vem sendo grandemente impactado pelos avanços das tecnologias de comunicação: seja com o streaming que tem mudado a forma como muitas pessoas assistem filmes e séries, seja com os jogos online, os quais atualmente ganham cada vez mais destaque e praticantes.

Em todos os casos acima elencados temos equipamentos e internet de alta performance mais acessível como elementos comuns. E no contexto desse cenário tecnologicamente cada vez mais complexo, avulta-se o imenso volume de dados que trafega pelas redes a cada minuto. Informações que muitas vezes precisam ser protegidas em função de direitos autorais, dados pessoais que devem ser resguardados adequadamente, ao abrigo dos crimes virtuais e de propaganda abusiva, sem que os donos dessas informações sejam expostos sem o seu consentimento. A preservação da privacidade é um dos grandes desafios que se apresenta. O caso da Cambridge Analytica evidencia a necessidade da proteção aos dados pessoais, os quais podem ser usados inclusive com finalidade política. O tema do tratamento dos dados é importante não somente por causa da tecnologia já existente e demanda tratamento adequado e atual por parte da lei, mas também em função de toda uma revolução tecnológica que se avizinha, a conjugar elementos que já se fazem presentes em nosso cotidiano, junto a outros que estão em fase de implementação: a quarta revolução industrial, a fazer convergir elementos digitais, físicos e biológicos no mundo do trabalho; a internet das coisas; a expandir o alcance da web a usos que seriam inimagináveis a poucos anos. Com a implantação da tecnologia 5G nos próximos anos, mal podemos imaginar o alcance das novas possibilidades, como carros autônomos, videoconferências de alta qualidade e confiabilidade, e toda essa gama de inovações que trazem impactos de ordem social, política e econômica traz também o desafio de lidar de maneira adequada com os dados das pessoas.

Com o objetivo de contribuir nos debates sobre a temática, reunimos artigos que trazem análises sobre diversos aspectos da Lei de Proteção Geral de Proteção de dados pessoais, como uma visão geral da lei, considerações sobre o Marco Civil da Internet, as relações entre ciberativismo e proteção de dados, a regulamentação da proteção aos dados no mundo corporativo, os dados no âmbito da quarta revolução industrial, a questão da privacidade e inclui também um capítulo sobre como proteger os nossos dados pessoais no ambiente virtual. Com a expectativa de que esta publicação possa estimular debates e reflexões, desejamos a todas e todos uma boa leitura.

Anja Czymmeck
Diretora da Fundação Konrad Adenauer no Brasil

A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica

ANTONIA ESPÍNDOLA LONGONI KLEE
ALEXANDRE NOGUEIRA PEREIRA NETO

RESUMO

■ O artigo analisa a regulamentação do tratamento de dados pessoais, inclusive nos meios digitais, estabelecida pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que entrará em vigor plenamente em agosto de 2020. Faz um panorama geral das disposições legislativas, principalmente seu objetivo, seus fundamentos e seu âmbito de aplicação. Examina alguns conceitos legais, os princípios norteadores da proteção de dados no Brasil e os requisitos para seu tratamento. Propõe a interpretação e a aplicação da Lei em diálogo com todo o ordenamento jurídico brasileiro, principalmente com o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet no Brasil. Ainda, visando à proibição do retrocesso, sugere que a interpretação e a aplicação da LGPD devem ser pautadas pelos princípios estabelecidos na Constituição da República de 1988, principalmente a privacidade, o sigilo de dados e a proteção do consumidor.

ABSTRACT

■ The article examines the regulation of the processing of personal data, including in digital media, established by the General Personal Data Protection Act (LGPD), Nº. 13.709, of August 14, 2018, which will be fully effective in August 2020. It gives an overview of the main legislative provisions, especially their purpose, their rationale and their scope. It examines some legal concepts, the guiding

principles of data protection in Brazil and the requirements for their treatment. It proposes the interpretation and application of the act in dialogue with the entire Brazilian legal system, especially with the Consumer Protection Code and the Brazilian Internet Civil Framework. Still, aiming at the prohibition of retrogression, it suggests that the interpretation and application of LGPD should be based on the principles established in the Constitution of 1988, especially privacy, data confidentiality and consumer protection.

I. INTRODUÇÃO

■ Em 14 de agosto de 2018, foi sancionada no Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), que recebeu o nº 13.709, e estabeleceu um regime geral de proteção de dados pessoais. Alguns dispositivos dessa Lei entraram em vigor em 28 de dezembro de 2018. Outros, entrarão em vigor em 14 de agosto de 2020. Explica-se: quando da publicação da Lei nº 13.709/2018, foram vetados pela Presidência da República os dispositivos que dispunham sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, por vício de iniciativa formal (a criação de tais órgãos é de iniciativa do Poder Executivo e não do Poder Legislativo)[1]. Recentemente, a Lei nº 13.853, de 8 de julho de 2019, alterou a Lei nº 13.709/2018, incluindo os arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, para dispor sobre a criação a ANPD e a composição do Conselho. Esses dispositivos, segundo a alteração realizada na Lei em 2019, já estão em vigor.

Mendes e Doneda afirmam que:

> A lei aprovada proporciona ao cidadão garantias em relação ao uso de seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor

1 Pinheiro informa: "Ao sancionar a Lei 13.709/2018 o Presidente Temer vetou alguns artigos que se mostravam incongruentes com a Constituição Nacional, como a criação de um órgão regulador, procedimento que só pode ser iniciado pelo executivo e estava com um erro em sua iniciativa ao ser proposto pela Câmara". PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais*, São Paulo, v. 1000, p. 313, fev. 2019.

público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização[2].

A LGPD deverá ser interpretada e aplicada à luz dos princípios garantidos pela Constituição da República de 1988, tais como a dignidade da pessoa humana, a privacidade, o sigilo de dados e a proteção do consumidor, de maneira a dialogar com as demais fontes normativas do ordenamento jurídico brasileiro. Essas fontes normativas são o Código Civil, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet no Brasil, a Lei do Cadastro Positivo e a Lei do Acesso à Informação, pois todas elas asseguram direitos relacionados à proteção de dados e à privacidade, no seu campo de aplicação. É preciso ressaltar que está tramitando no Congresso Nacional o Projeto de Lei nº 3.514/2015, que objetiva alterar o CDC para incluir disposições sobre a proteção do consumidor no comércio eletrônico[3]. Essa atualização do CDC é extremamente importante e necessária e espera-se que ocorra antes da entrada em vigor da LGPD, em 2020.

A LGPD complementa o marco regulatório brasileiro da Sociedade da Informação "ao compor, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, o conjunto normativo que moderniza o tratamento da informação no Brasil"[4]. A entrada em vigor da LGPD não poderá ser um retrocesso nas garantias dos direitos fundamentais dos cidadãos brasileiros. No que toca ao uso econômico dos dados, a LGPD também não pode significar um retrocesso na garantia fundamental de proteção dos direitos dos consumidores. A LGPD inspira-se no modelo europeu de proteção de dados, "amparado na Convenção do Conselho da Europa 108 de 1981, na

2 MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 566, 2018.

3 BRASIL. Projeto de Lei nº 3.514, de 4 de novembro de 2015. Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9º do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=00AE6ABCC278FD3C457C8E81FD188271.proposicoesWebExterno1?codteor=1408274&filename=PL+3514/2015>. Acesso em: 14 ago. 2019.

4 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 470, 2018.

Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados (Regulamento 2016/679)"[5].

Abaixo será apresentado um panorama da LGPD.

2. OBJETIVO DA LEI GERAL DE PROTEÇÃO DE DADOS

■ A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. As normas gerais contidas na LGPD são de interesse nacional e devem ser observadas pela União, pelos Estados, pelo Distrito Federal e pelos Municípios.

Dados pessoais são aquelas informações que permitem identificar a pessoa a quem dizem respeito. A sua proteção tem como objeto (1) o direito à intimidade e (2) o direito à identidade pessoal. Enquanto o primeiro importa na autodeterminação informativa[6], o segundo visa a impedir que a identidade pessoal seja alterada por informações inexatas ou incompletas. A LGPD significa uma evolução da autodeterminação informativa em favor do direito à proteção dos dados pessoais[7]. Se bem aplicada, protegerá a privacidade dos usuários e de seus dados pessoais de maneira mais adequada e segura.

Os meios digitais facilitaram a comunicação e o intercâmbio de informações pessoais. Isto é, o avanço da tecnologia aumenta o risco potencial da utilização abusiva dessas informações, e acentua a vulnerabilidade do direito à privacidade.

---

5 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 470, 2018.

6 Para um exame mais detalhado sobre o direito à autodeterminação informativa, ver LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. *Revista de Direito Bancário e do Mercado de Capitais*, São Paulo, n. 37, p. 59, jul. 2007.
Ver, também, CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade (Org.). *Responsabilidade civil*: direito à informação: dever de informação, informações cadastrais, mídia, informação e poder, internet. São Paulo: Revista dos Tribunais, 2010. v. 8. (Doutrinas essenciais). p. 343-392.

7 LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. *Revista de Direito do Consumidor*, São Paulo, ano 17, n. 67, p. 225, jul./set. 2008.
Ver, também, CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade (Org.). *Responsabilidade civil*: direito à informação: dever de informação, informações cadastrais, mídia, informação e poder, internet. São Paulo: Revista dos Tribunais, 2010. v. 8. (Doutrinas essenciais). p. 343-392.

Assim, é necessário que o ordenamento jurídico ofereça "instrumentos que assegurem que a fruição das novas vantagens proporcionadas pela tecnologia possa ocorrer de forma proporcional à manutenção das expectativas de privacidade [...]"[8]. É isso que se espera da correta interpretação e aplicação da LGPD.

Mendes e Doneda asseveram que a LGPD objetiva a proteção dos dados do cidadão, independentemente de quem realiza o seu tratamento, aplicando-se tanto ao setor privado como ao setor público (empresas e Governo), sem distinção de tratamento de dados, inclusive pela Internet[9]. Blum e Schuch são categóricos: a importância da proteção dos dados pessoais está no fato de que a informação passou a ser um bem extremamente valorizado na sociedade e no mercado ("a informação é o ativo mais valioso da atual sociedade, servindo de instrumento de conhecimento, poder e controle"), porque a partir dela é possível traçar perfis de comportamento, tais como econômico, familiar, político, profissional e de consumo[10] e fundamentar a tomada de decisões econômicas, políticas e sociais.

O objetivo da LGPD é a proteção dos dados pessoais dos indivíduos, com a finalidade de preservar a sua personalidade. Em última *ratio*, a LGPD visa à proteção dos direitos de personalidade dos indivíduos e das garantias constitucionais decorrentes.

3. FUNDAMENTOS DA PROTEÇÃO DE DADOS NO BRASIL

■ A disciplina da proteção de dados pessoais tem como fundamentos alguns princípios consagrados no ordenamento jurídico brasileiro: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

---

8 DONEDA, Danilo. Considerações sobre a tutela da privacidade e a proteção de dados pessoais no ordenamento brasileiro. In: CONRADO, Marcelo; PINHEIRO, Rosalice Fidalgo (Coord.). *Direito privado e Constituição*: ensaios para uma recomposição valorativa da pessoa e do patrimônio. Curitiba: Juruá, 2009. p. 87.

9 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 472, 2018.

10 BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

A LGPD está amparada na ideia central de que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações, principalmente daquelas que as identificam, que são os dados pessoais, possibilitando a limitação desse processamento[11], conforme a boa-fé, que deve pautar todas as relações jurídicas.

O principal fundamento da Lei é a proteção dos direitos fundamentais dos cidadãos, sejam eles consumidores ou não. A relevância da proteção de dados nas relações de consumo está no fato de que a informação tem valor econômico e pode significar uma vantagem competitiva para as empresas que utilizam os dados pessoais de seus consumidores para fazer publicidade e ofertar produtos e serviços a um público consumidor em potencial, inclusive nos meios digitais. Com a entrada em vigor da LGPD, "os modelos de negócios desenvolvidos com base no uso de dados precisarão instituir novos procedimentos de tratamento que obedeçam às novas regras"[12].

A informatização dos meios para o tratamento de dados pessoais tornou a necessidade de regulamentação ainda mais urgente. Isso porque a informática e os meios eletrônicos ampliam a capacidade de armazenamento da informação (hoje, com a "nuvem", ela é praticamente ilimitada) e possibilitam o cruzamento e a combinação de dados para a realização de perfis econômico, social, político, religioso, de consumo, etc.[13]

Santos e Taliba assinalam que "da boa-fé e da segurança decorrem os demais princípios que deverão guiar o comportamento das empresas que coletam e tratam, de qualquer forma, dados pessoais"[14], conforme será analisado a seguir.

11 BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

12 PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais*, São Paulo, v. 1000, p. 310, fev. 2019.

13 MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista De Direito Civil Contemporâneo*, São Paulo, v. 9, p. 40, 2016.

14 SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 227-228, dez. 2018.

4. ÂMBITO DE APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

■ A LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

A própria Lei excepciona a sua aplicabilidade, ao dispor que não se aplica ao tratamento de dados pessoais: realizado por pessoa natural para fins exclusivamente particulares e não econômicos; realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (esse tratamento será regido por legislação específica); ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Percebe-se que o âmbito de aplicação da LGPD é bastante amplo, com o intuito de garantir a proteção de dados pessoais dos indivíduos em um maior número de circunstâncias possíveis. Entretanto, a Lei contém exceções, que devem ser interpretadas taxativamente (*numerus clausus*).

5. CONCEITOS LEGAIS IMPORTANTES

■ A LGPD define alguns conceitos que nortearão a sua interpretação e aplicação. É um ponto bastante positivo da Lei. Entre os conceitos trazidos no texto legal, destaque deve ser dado às definições de dado pessoal, de dado pessoal sensível, dado anonimizado, banco de dados, tratamento e consentimento. Mas a LGPD não se restringe a apenas esses conceitos, trazendo outros. Os conceitos estabelecidos pela Lei são:

Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
Dado pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
Dado anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
Banco de dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
Agentes de tratamento	O controlador e o operador
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
Anonimização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados
Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado
Transferência internacional de dados	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
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
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
Órgão de pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
Autoridade nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. A importância na definição desses conceitos no texto legal está no fato de servirá de guia para a correta interpretação e aplicação da lei, bem como da fiscalização com relação ao seu fiel cumprimento

6. PRINCÍPIOS NORTEADORES DA INTERPRETAÇÃO E DA APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

■ Segundo a LGPD, as atividades de tratamento de dados pessoais deverão observar a boa-fé e uma série de princípios norteadores da atividade. Entre os princípios elencados pela Lei, deve-se dar destaque ao da finalidade, que 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. Esse princípio "vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta"[15]. Disso decorre a ideia de que "o tratamento de dados pessoais é indissociável de uma determinada função [...]"[16].

Também devem ser destacados os princípios da adequação e da necessidade, segundo os quais "os tratamentos de dados devem ser adequados, relevantes e limitados à sua necessidade"[17]. Isto é: deve haver a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, e a 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. Vê-se que a Lei procura garantir a transparência das relações abrangidas por sua aplicação: o agente de tratamento deverá ser transparente com o titular dos dados e bem informá-lo acerca de sua atividade.

Além desses princípios, devem ser observados o livre acesso dos titulares à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; a qualidade dos dados dos titulares com relação a sua exatidão, clareza, relevância e atualização, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; a transparência, que é a garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; a segurança, decorrente da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados

15 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 474, 2018.

16 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 474, 2018.

17 VENTURA, Leonardo Henrique de Carvalho. Considerações sobre a nova lei geral de proteção de dados pessoais. *Revista Síntese Direito Administrativo*, Porto Alegre, v. 13, n. 155, p. 60, nov. 2018.

e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; a prevenção, que é a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; a não discriminação, baseada na impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; a responsabilização e a prestação de contas, consubstanciadas na 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.

Os princípios elencados devem nortear a atividade da coleta de dados e de seu tratamento. Conforme afirmam Blum e Schuch, "nos procedimentos de tratamento de dados, devem ser respeitados os direitos constitucionais e fundamentais dos titulares dos dados, preservando a sua intimidade, vida privada, honra e imagem"[18]. Da mesma forma, quando houver uma relação de consumo, deve ser observado o art. 43 do CDC, em conjunto com o art. 7º do Marco Civil da Internet no Brasil, com a redação dada pela LGPD.

Santos e Taliba exemplificam os seguintes princípios: i) minimização dos dados (não pode haver coleta irrestrita de informações, pois a LGPD impõe que sejam coletados apenas os dados minimamente necessários para a finalidade do serviço). Nas relações de consumo, essa ideia deve ser observada desde a concepção do serviço ou do produto a ser ofertado, configurando o que se convencionou chamar de *privacy by design*. Isso porque, inexistindo finalidade clara e adequação da coleta, o tratamento poderá ser considerado abusivo; ii) adequação do tratamento dos dados à sua finalidade (os dados coletados deverão ser utilizados apenas para as finalidades específicas devidamente informadas aos titulares); iii) *privacy by default*[19], ou privacidade por padrão, segundo o que o consentimento não é mais a única forma de legitimar o tratamento de dados, conforme se depreende da leitura do art. 7º da LGPD[20].

18 BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

19 "O tratamento de dados pessoas exige a adoção de medidas técnicas e organizativas adequadas, devendo o responsável pelo tratamento de dados ser capaz de comprovar a adoção de orientações internas e de medidas que respeitem os princípios da proteção de dados desde a sua concepção e da proteção de dados por padrão". SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 231, dez. 2018.

20 SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 227-228, dez. 2018.

7. DOS REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

■ Segundo Mendes e Doneda, o tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize[21]. Isso porque a LGPD determina que o tratamento de dados pessoais somente poderá ser realizado em hipóteses determinadas: mediante o fornecimento de consentimento pelo titular; para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307/1996 (Lei de Arbitragem); para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; 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 para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (CDC e Lei do Cadastro Positivo, por exemplo).

O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados seus direitos e os princípios previstos na LGPD.

Destaque deve ser dado à necessidade de consentimento válido do titular dos dados, pois é o principal requisito de validade de todos os atos atrelados ao tratamento dos dados pessoais. A LGPD determina que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular e deverá referir-se a finalidades determinadas. Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais

21 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 472, 2018.

cláusulas contratuais. Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei. O consentimento deve ser expresso, livre e informado, mediante manifestação própria. Por isso, as autorizações genéricas para o tratamento de dados pessoais serão nulas. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Nas relações de consumo, faz-se importante destacar que "o consentimento é considerado 'livre' quando se dá a opção do usuário de utilizar o serviço sem ser obrigado a aceitar as condições impostas"[22]. Isso é: o fornecedor do produto ou do serviço não pode proibir o acesso ao bem de consumo caso os dados solicitados não sejam fornecidos pelo consumidor. Blum e Schuch acrescentam: "O consentimento é 'informado' quando concedido após a leitura de regras claras, completas e inteligíveis sobre o tratamento de dados pessoais e é 'expresso' quando ocorre de forma destacada de outras cláusulas contratuais e por meio de ação específica do titular, como na prática do *opt-in* e *opt-out*[23].

8. DIREITO AO ACESSO FACILITADO ÀS INFORMAÇÕES SOBRE TRATAMENTO DE DADOS

■ Da mesma forma, a LGPD garante ao titular dos dados o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade específica do tratamento; da forma e da duração do tratamento, observados os segredos comercial e industrial; da identificação do controlador; das informações de contato do controlador; das informações sobre o uso compartilhado de dados pelo controlador e a finalidade; das responsabilidades dos agentes que realizarão o tratamento; e dos direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso aos seus dados. Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o

22 BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

23 BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos elencados no art. 18 da LGPD.

9. O LEGÍTIMO INTERESSE

■ O legislador tratou de regulamentar o legítimo interesse do controlador, que somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: apoio e promoção de atividades do controlador; e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e seus direitos e liberdades fundamentais.

Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. Ademais, o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, e 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.

Mendes e Doneda afirmam que "a hipótese de tratamento de dados pessoais baseada nos interesses legítimos do controlador é relevante, ao reconhecer que outras pessoas – além do titular do dado – podem ter interesses protegidos juridicamente no tratamento de dados. O exemplo trazido por eles é o tratamento de dados pessoais realizado pelo empregador para o controle de seus empregados[24].

Deve-se frisar que o legítimo interesse do controlador "deverá ter relação com a atividade empresarial exercida, com a natureza do dado coletado, estar muito bem fundamentado e, como visto, estar de acordo com os princípios, precisamente com o da transparência, e com as vedações legais relativas a determinados compartilhamentos"[25].

24 MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista De Direito Civil Contemporâneo*, São Paulo, v. 9, p. 40, 2016.

25 SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 229, dez. 2018.

10. DO TÉRMINO DO TRATAMENTO DE DADOS

■ O término do tratamento de dados pessoais ocorrerá quando: a finalidade foi alcançada ou os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; houver o fim do período de tratamento; o titular comunicar, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou quando houver determinação da autoridade nacional, por violação ao disposto na LGPD.

A Lei determina que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

11. DOS DIREITOS DO TITULAR

■ A LGPD dispõe que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento, nos termos do § 5º do art. 8º da Lei.

O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional e pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei. Esses direitos serão

exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento, e deverá ser atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

12. DA RESPONSABILIDADE E DO RESSARCIMENTO DE DANOS

■ 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 Lei, é obrigado a repará-lo. A fim de assegurar a efetiva indenização ao titular dos dados: o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da Lei 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 na Lei; os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos na Lei.

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. Essa previsão legal recebeu influência do CDC, que também contém regra sobre a inversão do ônus da prova em favor do consumidor.

Outra clara influência do CDC é o dispositivo que determina que os agentes de tratamento só não serão responsabilizados quando provarem: que não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. Também se encontra influência do CDC na previsão de 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: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. 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 na Lei, der causa ao dano. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas nos arts. 12 e 14 do CDC.

13. DA SEGURANÇA E DO SIGILO DE DADOS

■ 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. Essas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (*privacy by design*).

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; os riscos relacionados ao incidente; os motivos da demora, no caso de a comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: ampla divulgação do fato em meios de co-

municação; e medidas para reverter ou mitigar os efeitos do incidente. Aqui, da mesma forma, encontra-se na Lei uma forte influência do CDC, a demonstrar o diálogo bastante positivo existente.

14. DAS BOAS PRÁTICAS E DA GOVERNANÇA

■ 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. Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Acredita-se que essa medida estimulará o respeito à boa-fé e à confiança entre as partes envolvidas.

15. DAS SANÇÕES ADMINISTRATIVAS

■ Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total referido acima; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de

acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé, a condição econômica e a cooperação do infrator; a vantagem auferida ou pretendida pelo infrator; a reincidência; o grau do dano; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A LGPD não substitui a aplicação de sanções administrativas, civis ou penais definidas no CDC e em legislação específica.

16. DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

■ A LGPD, com a redação dada pela Lei nº 13.853/2019, passou a dispor sobre a criação, sem aumento de despesa, da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. A avaliação quanto à transformação deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

Compete à ANPD: zelar pela proteção dos dados pessoais, nos termos da legislação; zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos da Lei; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os

quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento da Lei; elaborar relatórios de gestão anuais acerca de suas atividades; 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; ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; arrecadar e aplicar suas receitas e publicar, no relatório de gestão, o detalhamento de suas receitas e despesas; realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos; 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 à LGPD; garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos da LGPD e do Estatuto do Idoso (Lei nº 10.741/2003); deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos; comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; comunicar aos órgãos de controle interno o descumprimento do disposto na LGPD por órgãos e entidades da administração pública federal; articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

17. DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

■ Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; sugerir ações a serem realizadas pela ANPD; elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

18. CONCLUSÃO

■ A entrada em vigor do Regulamento Geral de Proteção de Dados (Regulamento 2016/679) na Europa, em maio de 2018, acelerou a regulamentação da proteção de dados no Brasil, onde a questão vinha sendo discutida desde 2010[26]. Isso porque "o Estado que não possui lei de mesmo nível pode passar a sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da região"[27]. Não é interessante economicamente para o Brasil não poder fazer negócios com os países europeus.

A LGPD é bastante inspirada na regulamentação europeia. Adota um modelo *ex ante* de proteção de dados, "baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação"[28] e na ideia de que o titular pode dispor de seus dados de acordo com seus interesses. Se bem aplicada, estimulará a confiança e trará segurança jurídica para todos os envolvidos no processo de tratamento de dados,

26 Mendes e Doneda informam que a LGPD "é resultado de um esforço de, pelo menos, oito anos de debates e duas consultas públicas, que se iniciaram desde a elaboração da primeira versão do anteprojeto de lei pelo Ministério da Justiça em 2010". MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 566, 2018.

27 PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais*, São Paulo, v. 1000, p. 318, fev. 2019.

28 MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, São Paulo, v. 120, p. 566, 2018.

ao proteger a privacidade dos cidadãos sem inviabilizar a inovação tecnológica e a economia dos negócios. Isso porque o tratamento de dados é permitido, desde que os indivíduos saibam quais dados estão sendo coletados, para quais finalidades e com quem estão sendo compartilhados. A transparência nas relações que têm como objeto dados pessoais é fundamental.

A LGPD garante a proteção do direito fundamental à privacidade ao regulamentar o tratamento de dados pessoais, estabelecendo limites que conferirão legitimidade à atividade. Isto é, o princípio da autodeterminação informativa, previsto em lei, "garante não apenas a possibilidade de oposição ao tratamento de dados, mas, também, a de interagir e intervir no tratamento de dados pelo controlador e pelos terceiros que obrigatoriamente devem ser indicados"[29]. Resta saber se a Lei será cumprida, para dar efetividade às garantias constitucionais da privacidade, da intimidade, da vida privada, do sigilo de dados e dos direitos dos consumidores, em diálogo com as demais leis brasileiras que dispõem sobre a proteção de dados, principalmente o CDC. Esperemos agosto de 2020 e os anos vindouros.

29 SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 235, dez. 2018.

Antonia Espíndola Longoni Klee · Doutora e Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Especialista em Direito Internacional pela UFRGS. Professora de Direito Civil da Faculdade de Direito da Universidade Federal de Pelotas (UFPEL). Professora convidada do Curso de Especialização *Lato Sensu* em Direito do Consumidor e Direitos Fundamentais da UFRGS. Advogada.

Alexandre Nogueira Pereira Neto · Mestre em Direito pelo Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Pelotas (UFPEL). Especialista em Direito Processual Civil pelo Complexo de Ensino Superior de Santa Catarina (CESUSC). Graduado em Direito pelo CESUSC.

REFERÊNCIAS

BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente on-line. *Contraponto jurídico*. Ed. 2019. p. RB-32.1.

BRASIL. 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: 10 ago. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 11 ago. 2019.

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/L8078.htm>. Acesso em: 10 ago. 2019.

BRASIL. Projeto de Lei nº 3.514, de 4 de novembro de 2015. Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9º do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=00AE6ABCC278FD3C457C8E81FD188271.proposicoesWebExterno1?codteor=1408274&filename=PL+3514/2015>. Acesso em: 14 ago. 2019.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade (Org.). *Responsabilidade civil*: direito à informação: dever de informação, informações cadastrais, mídia, informação e poder, internet. São Paulo: Revista dos Tribunais, 2010. v. 8. (Doutrinas essenciais). p. 343-392.

DONEDA, Danilo. Considerações sobre a tutela da privacidade e a proteção de dados pessoais no ordenamento brasileiro. In: CONRADO, Marcelo; PINHEIRO, Rosalice Fidalgo (Coord.). *Direito privado e Constituição*: ensaios para uma recomposição valorativa da pessoa e do patrimônio. Curitiba: Juruá, 2009. p. 87-107.

LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. *Revista de Direito Bancário e do Mercado de Capitais*, São Paulo, n. 37, p. 59, jul. 2007.

LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. *Revista de Direito do Consumidor*, São Paulo, ano 17, n. 67, p. 215-241, jul./set. 2008.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 555-570, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista De Direito Civil Contemporâneo*, São Paulo, v. 9, p. 35-48, 2016.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 469-483, 2018.

PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais*, São Paulo, v. 1000, p. 309-323 fev. 2019.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no brasil e os possíveis impactos. *Revista dos Tribunais*, São Paulo, v. 998, p. 225-239, dez. 2018.

VENTURA, Leonardo Henrique de Carvalho. Considerações sobre a nova lei geral de proteção de dados pessoais. *Revista Síntese Direito Administrativo*, Porto Alegre, v. 13, n. 155, p. 56-64, nov. 2018.

O Marco Civil da Internet e a Proteção de Dados: diálogos com a LGPD

LUÍZA COUTO CHAVES BRANDÃO

RESUMO

■ O período de integração da LGPD ao ordenamento brasileiro desperta o diálogo entre diferentes fontes sobre proteção de dados pessoais. Nesse sentido, busca-se resgatar o histórico e as disposições da Lei n. 12.965/2014, o Marco Civil da Internet, e de seu decreto regulamentador. Os direitos definidos pelo Marco Civil da Internet foram analisados em comparação com os direitos que a LGPD inaugura no Brasil. O decreto n.8.771/2016 foi abordado em suas interfaces com a matéria de proteção de dados pessoais. A partir dessas discussões, o trabalho busca contribuir para uma visão sistemática de interpretação e prática da proteção de dados no Brasil.

ABSTRACT

■ The period of General Data Protection Law (LGPD) integration with the Brazilian system awakens the dialogue between different sources on personal data protection. In this sense, we seek to recover the history and provisions of Law no. 12.965 / 2014, the Civil Mark of the Internet, and its regulatory decree. The rights defined by the Civil Mark of Internet were analyzed in comparison with the rights that LGPD inaugurates in Brazil. The decree n.8.771 / 2016 was addressed in its interfaces with the subject of personal data protection. From these discussions, the paper seeks to contribute to a systematic view of interpretation and practice of data protection in Brazil.

I. INTRODUÇÃO

Sancionada em 2014, a Lei nº. 12.965 recebeu o nome de Marco Civil da Internet (MCI) e é considerada uma carta de direitos para a internet no Brasil. Seu caráter civil – isto é, que não resultou em abordagem criminalizatória do uso da internet – foi elogiado em todo mundo. Não apenas por sua natureza, mas também por seu processo de discussão legislativa, que contou com consultas públicas e abertas, e por ter dado força ao modelo brasileiro de governança da internet. Se o Brasil tornou-se uma referência no campo legislativo e regulatório da internet com a Lei nº. 12.965/2014[1], isso não necessariamente foi sempre assim. Enquanto projeto de lei, o Marco Civil tramitou por muitos anos sem sucesso, apesar dos esforços de diferentes setores, como acadêmicos, representantes da sociedade civil e do setor privado. Os olhos se voltaram para a necessidade de parâmetros legais para a internet no país quando, em 2013, Edward Snowden[2] tornou públicas informações das atividades de vigilância da NSA, que incluíam líderes de estados, como a primeira-ministra alemã Angela Merkel e a então presidente do Brasil, Dilma Rousseff. O escândalo de dimensões internacionais motivou politicamente a aprovação do Marco Civil da Internet como resposta institucional, que também envolveu a realização do Fórum NetMundial[3].

Quando da aprovação da Lei nº. 12.965/2014, o Brasil estava no centro das atenções relacionadas à internet e tecnologias que nela se baseiam. Os compromissos assumidos no país tiveram alcance internacional e continuam a ser discutidos em fori globais[4]. Ainda que sua importância seja inegável, sua proposta de estabelecer as linhas gerais para os direitos relativos à era digital, deixou alguns temas para instrumentos a serem construídos posteriormente. Tal escolha,

1 BRASIL. Lei 12.965, de 23 de abril de 2014. Marco Civil da Internet. 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: 20/08/2019.

2 LEMOS, Ronaldo. Feet on the Ground: Marco Civil as an Example of Multistakeholderism in Practice. In: SOUZA, Carlos Affonso Pereira; LEMOS, Ronaldo; VIOLA, Mario. Understanding Brazil's Internet Bill of Rights. Rio de Janeiro: ITS, 2015, p. 26.

3 CGI.BR. Declaração Multissetorial do NETmundial, 2015. Disponível em: <https://www.cgi.br/publicacao/cadernos-cgi-br-declaracao-multissetorial-do-netmundial/>. Acesso em: 15/05/2019.

4 Ver, por exemplo, a relevância do Brasil no IGF – Internet Global Forum, realizado sob os auspícios da ONU e que já aconteceu duas vezes no país, em 2007 (Rio de Janeiro) e 2015 (João Pessoa). CGI.BR Fórum de Governança da Internet: Relatórios dos dez primeiros anos do IGF, 2018. Disponível em: < https://www.cgi.br/publicacao/cadernos-cgibr-forum-de-governanca-da-internet/>. Acesso em:15/08/2019.

do ponto de vista político-legislativo, foi importante para que o Marco Civil da Internet se estabelecesse como uma espécie de "constituição" e subsídio para a regulamentação da internet no Brasil. Além disso, para que não fosse tão sensível ao avanço da tecnologia, sempre mais rápido que os procedimentos legislativos, e não necessariamente levasse à defasagem da lei. A redação baseada em princípios, diretrizes e definição de direitos, portanto, tem como mérito sua adequação a diferentes situações, mas não consegue atender a algumas matérias mais específicas, como a neutralidade de rede, que foi tratada em decreto regulamentador posterior, a proteção de dados, a cargo da recente Lei nº 13.709/2018[5], e os direitos autorais na internet, que continuam a ser debatidos.

Apesar de não entrar em especificidades no que se refere à proteção da privacidade e dos dados pessoais[6], o Marco Civil da Internet define princípios, diretrizes e direitos pertinentes a esses temas. Dessa forma, ainda com a vigência da Lei Geral de Proteção de Dados (LGPD) prevista para agosto de 2020, a Lei nº 12.965/2014 continua a fazer parte do arcabouço normativo brasileiro que se aplica às interfaces digitais. Aliás, é importante destacar que não apenas à internet ou às tecnologias que se baseiam no Big Data será aplicável a Lei Geral de Proteção de Dados, mas também aos dados coletados e utilizados em outros contextos, inclusive analógicos. Os dados relacionados à internet, por sua vez, também incluem as disposições normativas do Marco Civil da Internet, bem como de seu decreto regulamentador e ainda de outros instrumentos normativos vigentes no Brasil[7]. Na prática, isso quer dizer que a interpretação de qualquer lei não se restringe apenas a ela, como se sua aplicação pudesse ser hermética, mas deve ser integrada ao ordenamento como um todo, inclusive (e principalmente) a direitos e garantias fundamentais já estabelecidos.

5 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 10/08/2019.

6 Destaca-se que privacidade e proteção de dados são conceitos que, embora relacionados, não se confundem. Sobre a diferenciação, ver: DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

7 Entre os méritos da Lei Geral de Proteção de Dados – e de suas congêneres ao redor do mundo – aponta-se o fato de justamente compilar as disposições legais em um único instrumento, com a vantagem de tornar claras, centralizadas e mais acessíveis as regras aplicáveis, e por essa razão ser chamada "geral". De fato, essa característica está presente na LGPD, mas não significa que outros instrumentos foram revogados.

2. DIREITOS ESTABELECIDOS PELO MARCO CIVIL DA INTERNET E PELA LGPD

■ O Marco Civil da Internet estabeleceu, em seu artigo 3º, a proteção à privacidade e aos dados pessoais (incisos II e III) como princípios que disciplinam o uso da internet no Brasil. Dessa forma, o ambiente digital, as atividades e atores nele envolvidos já deveriam ter como orientação ou diretriz a proteção de dados, ainda que se previsse uma lei específica para sua disciplina. Em decisões judiciais, tomadas de decisão e modelos de negócio esses princípios funcionam como norteadores de interpretações, aplicações de normas e adequação legal. Devem ser um parâmetro para escolhas políticas, econômicas, jurídicas e sociais no âmbito da internet no Brasil que também oferecem expectativas de adequação à LGPD.

Em diálogo com a resolução da ONU[8] que reconheceu o acesso à internet como um direito, o MCI também o considera indispensável para o exercício da cidadania[9]e, nesse sentido, elenca os direitos dos usuários para o pleno acesso à internet. Eles se fundamentam na neutralidade de rede, liberdade de expressão e privacidade[10]. No que se refere aos dados pessoais, foram garantidos os seguintes direitos:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...]
> VII – 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;
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e

8 ONU, Resolução A/HRC/32/L.20. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. 2016. Disponível em: < https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20>. Acesso em: 18/08/2019.

9 "Art. 7º O acesso à internet é essencial ao exercício da cidadania [...]." (grifo nosso), Lei nº. 12.965/2014 (Marco Civil da Internet).

10 VIOLA, Mario; e IGATIBA, Gabriel; Privacidade e Dados Pessoais. In: SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord). Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017, p.20.

> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> 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; (grifos nossos)

É possível observar que a lei trata de proteções aos dados pessoais e que algumas delas encontram respaldo em outras normas – como o direito à informação, no caso do inciso VIII, que também está garantido às relações de consumo[11]. Assim como na Lei Geral de Proteção de Dados, estão previstos o não fornecimento a terceiros, o direito de ser informado sobre a coleta e o tratamento de dados pessoais, além da possibilidade de requerer sua exclusão. Apesar de já tratar dessas possibilidades enquanto garantias dos titulares de dados pessoais, o Marco Civil da Internet não se aprofunda tanto quanto a Lei 13.709/2018, que refina e oferece mais detalhes para a disciplina no Brasil.

Ainda que a LGPD ofereça inovações, o Marco Civil da Internet ainda deve ser compreendido como complementar a ela. Isso porque as duas leis estão centradas na perspectiva do titular dos dados pessoais ou, no caso do MCI, dos usuários da internet. Também é possível identificar, a partir de ambos os textos legais, elementos para outro fundamento em comum: a autodeterminação informacional. Esse conceito, que ganha notoriedade nas discussões europeias sobre proteção de dados, leva em conta que a lógica da economia baseada em dados gira em torno de informações[12] construídas sobre e a partir de pessoas.

Em tal cenário, a autodeterminação seria uma forma de proteção frente aos interesses de outros atores da "economia da vigilância" pela qual as pessoas podem determinar, escolher e controlar as informações (extraídas a partir de seus dados)

---

11 A informação, por exemplo, está entre os direitos básicos dos consumidores no Brasil. Ver: 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/l8078.htm>. Acesso em 19/08/2019.

12 Sobre a diferença entre "dado" e "informação" é importante a explicação de Bruno Bioni: "[...] Cabe destacar que dados e informação não se equivalem [...] O dado é o estado primitivo da informação, pois não é algo *per se* que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo intangível, podendo ser deles extraída uma informação." BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019. p. 36.

sobre elas, seus modos de utilização e, inclusive, seu apagamento ou correção. A escolha legislativa do Marco Civil que reflete esse conceito, como em outras regulações pelo mundo, se expressa na ideia de consentimento. Conforme descreve Bruno Bioni, o consentimento:

> Nada mais é do que a liberdade que todo cidadão tem de reger a sua vida, criando, modificando e extinguindo as suas relações em meio à sociedade. Essa mesma autonomia é captada e transportada para a proteção dos dados pessoais, na medida em que é o próprio cidadão quem deve governar seus dados pessoais[13].

O Marco Civil da internet segue a ideia de que o consentimento estaria na base das relações que envolvam a coleta, tratamento, armazenamento e processamento de dados pessoais. O modelo do consentimento, apesar de bem intencionado e fundamentado no exercício da autonomia do titular dos dados, não fica livre de questionamentos. Muitos deles envolvem a eficácia do pedido de consentimento a cada titular de dados tratados, em um contexto em que as interações virtuais geram não apenas uma maior quantidade de dados, mas também aumentam a velocidade (em alguns casos, praticamente instantânea) e potencialidade de usos, trocas e compartilhamentos[14].

Expresso em contratos, documentos longos que ficaram conhecidos como "termos de uso" ou "políticas", o consentimento ficou com o tempo fortemente associado à expressão "Li e aceito", que em muitas situações precedem o registro de usuários em plataformas da internet e outros serviços. De linguagem truncada, extensão considerável e pouca clareza relativa às informações, a possibilidade de exercício da autonomia por meio do titular dos dados pessoais acaba ficando remota na prática. Além disso, a adjetivação do consentimento pelo Marco Civil da Internet como "expresso, livre e esclarecido" tornou-o um ideal quase impossível de se alcançar por meio de um formato contratual e de grande volume de informações. Soma-se a isso o fato de que a velocidade das interações pela internet torna impraticável a leitura – e o esclarecimento – de todos os termos de uso disponíveis ao usuário. Por esses motivos, o consentimento acabou sendo ques-

13 BIONI, Bruno Ricardo. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

14 Sobre os desafios da era digital e a escala que antigiram, ver LEONARDI, Marcel. Tutela e privacidade na internet. Editora Saraiva, 2012.

tionado enquanto fundamento efetivo de exercício de direitos pelos titulares em relação a seus dados[15].

Seguindo as problemáticas relativas ao consentimento, a Lei Geral de Proteção de dados insere no ordenamento brasileiro outras hipóteses para o tratamento de dados pessoais. Nesse ponto, vale ressaltar que a LGPD não descarta o consentimento e, inclusive, mantém a qualificação que vem do texto do Marco Civil da Internet para a manifestação do pensamento "livre, informada e inequívoca" do titular dos dados pessoais para uma finalidade específica de tratamento[16]. A Lei Geral de Proteção de Dados, no entanto, insere outras hipóteses que autorizam o tratamento de dados pessoais[17], para além da hipótese do consentimento, já estabelecida pelo Marco Civil da Internet e reiterada no inciso I do artigo 7º da LGPD. O dispositivo ainda inaugura outras nove possibilidades para o tratamento de dados pessoais no Brasil[18]. Entre elas, o legítimo interesse do controlador ou de terceiro (inciso IX) e o cumprimento de obrigação legal (inciso II). Essas são as hipóteses em que os diversos setores que precisam se adequar à Lei Geral de Proteção de Dados devem basear o tratamento de dados pessoais.

O exercício dessas atividades deve estar em conformidade com a LGPD, quando os dados forem coletados no território nacional, destinem-se ao fornecimento de bens ou serviços no país ou tenham sido coletados no Brasil[19]. Essas são as três situações que caracterizam a regra geral de aplicação da LGPD, que segue a tendência do Regulamento Geral de Proteção de Dados[20] (também conhecido

15 A problemática dos termos de uso que se associaram ao termo "Li e aceito" é debatida desde o início da vigência do Marco Civil da Internet. Um exemplo pode ser encontrado em: BRANDÃO, Luiza. "Li e aceito": muito além de entregar seus dados. IRIS, 2016. Disponível em: <http://irisbh.com.br/li-e-aceito-alem-de-entregar-seus-dados/>. Acesso em: 22/08/2019.

16 Art. 5º Para os fins desta Lei, considera-se: [...] XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Lei 13.709/2018 (LGPD).

17 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. (grifos nossos) Lei 13.709/2018 (LGPD).

18 Art. 7º, Lei 13.709/2018 (LGPD).

19 Art. 3º, Lei 13.709/2018 (LGPD).

20 UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em:< https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT> . Acesso em: 16/08/2019.

pela sigla GDPR)[21]. A lei dialoga ainda com a previsão do artigo 11 do Marco Civil da Internet para aplicação da lei brasileira aos procedimentos que envolvam dados coletados ou qualquer outra fase de seu tratamento no Brasil[22].

Além de seguir a racionalidade do artigo 11 do MCI, a nova lei também se alinha a uma tendência mais expansiva da jurisdição brasileira. Essa é uma postura verificada em outras regulações ao redor do mundo que, superada a lógica de que a internet era um espaço independente do poder estatal (liderada especialmente por John Perry Barlow no final dos anos 90[23]), começaram uma "corrida" legal sobre o espaço digital[24]. O escopo de aplicação alargado significa, na prática, um esforço de adequação que compreende não apenas controladores[25] ou operadores[26] sediados em território nacional, mas todos que operarem ou lidarem com dados pessoais aqui coletados, conforme o parágrafo primeiro do artigo 3º da LGPD e o art. 11 do MCI.

Como discutido anteriormente, as legislações assumiram posturas de proteção à autodeterminação informacional dos titulares de dados pessoais, importantes recursos econômicos da atualidade. Para tanto, a LGPD define direitos relacionados à possibilidade de controle, pelo usuário, do que é efetivamente

21 GDPR é a sigla em inglês para General Data Protection Regulation, pela qual se tornou conhecida foi globalmente debatida, em razão de suas previsões com alto alcance internacional e para além dos países-membros da União Europeia. Sobre os efeitos no Brasil, ver: IRIS, GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa, 2018. Disponível em: <https://irisbh.com.br/publicacoes/gdpr-e-suas-repercussoes-no-direito-brasileiro/>. Acesso em 21/08/2019.

22 Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Lei 12.964/ 2014.

23 BARLOW, John Perry. Declaração de Independência do Ciberespaço, 1996. Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acesso em 22/08/2019.

24 O termo ganha destaque com Bertrand de La Chapelle, do projeto Internet & Jurisdiction, em artigo sobre as tendências jurisdicionais e a necessidade de uma coordenação legal que atenda às demandas transnacionais da internet. Ver: DE LA CHAPELLE, Bertrand; FELLINGER, Paul. Jurisdiction on the internet: how to move beyond the legal arms race, 2016. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Articles/20161014-ORF-PDF.pdf>. Acesso em: 21/08/2019.

25 Art. 5º Para os fins desta Lei, considera-se: [...] VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, Lei 13.709/2018 (LGPD).

26 Art. 5º Para os fins desta Lei, considera-se: [...] VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; Lei 13.709/2018 (LGPD).

realizado com seus dados. Maria Cecília de Oliveira Gomes divide os direitos relativos à proteção de dados em "tradicionais", ou seja, aqueles já presentes no ordenamento brasileiro, em normas esparsas (como o próprio MCI) e os "novos", que passam a vigorar com a LGPD, em 2020. São eles:

- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
- portabilidade dos dados;
- eliminação dos dados pessoais tratados com o consentimento do titular;
- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento;
- direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional;
- direito de oposição nas hipóteses de dispensa de consentimento;
- direito de revisões de decisões automatizadas;
- direito à explicação.[27]

Apesar de os "novos" direitos não encontrarem exata correspondência no Marco Civil da Internet, estão em harmonia com os princípios de proteção aos dados e à privacidade, os quais devem reger o uso da internet e as tecnologias nela baseadas no Brasil. O fundamento de autodeterminação informacional também é compartilhado entre o MCI e a LGPD, os quais devem inspirar, juntos, muito mais um incentivo aos quadros de garantias de titulares de dados pessoais e usuários da internet, bem como segurança jurídica para diversos atores, do que uma rivalidade interpretativa. A Lei Geral de Proteção de Dados, no que se refere às interfaces com as dinâmicas da internet, também deve encontrar no Marco Civil da Internet, pioneiro e já estabelecido na jurisprudência, suporte e complementaridade em seus esforços regulatórios.

27 GOMES, Maria Cecília Oliveira. Novos direitos. GV EXECUTIVO, [S.l.], v. 18, n. 4, p. 34-37, ago. 2019. ISSN 1806-8979. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/79979/76433>. Acesso em: 24 Ago. 2019, p.36.

3. O DECRETO REGULAMENTADOR DO MARCO CIVIL DA INTERNET E A PROTEÇÃO DE DADOS PESSOAIS

■ Algumas matérias do Marco Civil ficaram a cargo de decreto regulamentador. O Decreto nº 8.771, de 11 de maio de 2016[28] tratou, então, de questões como a neutralidade de rede, obrigações e responsabilidades acerca da segurança da informação e também inaugurou previsões sobre a matéria de proteção de dados pessoais[29]. O decreto e também outras mais de 40 normas setoriais[30] eram (e ainda são, durante a *vacatio legis* da LGPD) os instrumentos que ofereciam a tutela da privacidade e dados pessoais no direito brasileiro. Por essa razão, embora o Brasil não estivesse entre os países com leis gerais de proteção de dados, figurava entre aqueles países que possuíam normas sobre essa matéria, e não entre aqueles totalmente desprovidos de regulamentação.

O Decreto nº 8.771/2016 inclui um capítulo que trata "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas". São apresentadas definições que também dialogam com aquelas que passam a vigorar com a Lei Geral de Proteção de Dados:

> I – 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; e
>
> II – tratamento de dados pessoais – toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazena-

28 BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 22/08/2019.

29 GONÇALVES, Pedro Vilela Rezende. O que muda com o decreto de regulamentação do Marco Civil? 2016. Disponível em: < http://irisbh.com.br/publicacoes/o-que-muda-com-o-decreto-de-regulamentacao-do-marco-civil/>. Acesso em: 21/08/2019.

30 Para alguns exemplos de instrumentos normativos sobre proteção de dados, ver: IRIS, Representação ao Ministério Público de Minas Gerais, 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/08/Representacao-FINAL-MP.pdf>. Acesso em: 22/08/2019.

> mento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[31] (grifos nossos)

Esses conceitos também aparecem na Lei Geral de Proteção de Dados, embora com redação menos exemplificativa. No entanto, é possível compreender que os exemplos abarcados pelo Decreto regulamentador do Marco Civil da Internet também estarão sob o escopo da LGPD. Observa-se que a tendência expansionista da definição de dados pessoais, que se baseia na possibilidade de individualização de uma pessoa por meio de seus dados[32], já podia ser encontrada no direito brasileiro por meio do Decreto 8.771/2016. Em razão dessa definição é que, conforme Maria Cecília Gomes, os "cookies" se inserem no conceito de dados pessoais, por se tratarem de "identificadores que podem ser gerados ou coletados a partir do navegador ou dispositivo que você usa, a fim de disponibilizar uma página para você acessar ou ainda identificar o seu perfil de navegação"[33].

Uma vez que os cookies também podem ser utilizados para identificar perfis, direcionar propagandas e influenciar comportamentos de forma individualizada, entre outras finalidades, de acordo com o comportamento do usuário da internet e titular dos dados tratados, são abrangidos pela redação do Decreto nº 8.771/2016 como dado pessoal. Dessa forma, apesar de o assunto não ser pacífico, como aponta Maria Cecília Gomes, a utilização de cookies continua no escopo de proteção a dados pessoais e deve buscar adequação à LGPD, por meio de uma das hipóteses legais que validam o tratamento de dados pessoais, a partir da vigência da lei[34].

Os identificadores expressos no decreto regulamentador do Marco Civil da Internet são um exemplo de como a legislação anterior à Lei Geral de Proteção de Dados pode influenciar sua aplicação, a partir de 2020. Eles também demonstram que o Brasil já trata da matéria, ainda que de forma esparsa, e que os setores envolvidos no tratamento de dados pessoais não estão totalmente alheios a parâmetros de proteção de direitos dos titulares de dados pessoais.

---

31 Art. 9º, Decreto nº 8.771/2016.

32 GOMES, Maria Cecília de Oliveira. Cookie notice: o que é e por que é importante? 2018. Disponível em: <https://baptistaluz.com.br/institucional/midia-publicidade/>. Acesso em 23/08/2019.

33 Idem.

34 Idem.

4. CONCLUSÃO: UM CAMINHO A SEGUIR

Nenhum trabalho em período de vacância de uma lei pode ter o objetivo de estabelecer seus efeitos com precisão ou determinar conclusões exatas sobre como ela será integrada ao ordenamento jurídico. A futurologia não parece ser um caminho útil para os diversos setores envolvidos no tratamento de dados pessoais no Brasil e no mundo. O que se procura oferecer, portanto, nesse capítulo é uma observação de como as normas já definidas pelo Marco Civil da Internet e o Decreto nº 8.771/2016 têm o potencial de diálogo com a Lei Geral de Proteção de Dados.

Por certo, existem questões ainda pendentes quanto a conflitos de normas, hierarquia ou prevalência entre os dispositivos do Marco Civil (e de seu Decreto) e as inovações oferecidas pela LGPD. Entre elas, o consentimento como protagonista do Marco Civil da Internet, enquanto incluído ente outras hipóteses para tratamento de dados pessoais na Lei Geral de Proteção de Dados. Além disso, também a conciliação entre o direito do titular de eliminação de seus dados e as obrigações legais de guarda de dados de acesso definidas pelo Marco Civil da Internet, por exemplo.

As questões de integração da LGPD ao ordenamento jurídico e à prática brasileira relativa ao tratamento de dados pessoais representam o desafio constante de compreender e praticar o Direito de forma sistemática, integrada e inexoravelmente complexa. O Marco Civil da Internet é um exemplo de norma a ser considerada no contexto digital da proteção de dados e também pode ser visto como uma oportunidade de exercício de integração para a construção de um cenário não simples, mas necessário, de diálogo para a proteção de dados pessoais e suas tendências contemporâneas.

Luíza Couto Chaves Brandão · Fundadora e Diretora do Instituto de Referência em Internet e Sociedade - IRIS. Bacharela e mestranda em direito pela Universidade Federal de Minas Gerais (UFMG), fellow da European Summer School on Internet Governance – EuroSSIG (2019), Internet Society – ISOC(2019) e Universidade de Genebra (2017).

REFERÊNCIAS

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 22/08/2019.

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/l8078.htm>. Acesso em 19/08/2019.

BRASIL. Lei 12.965, de 23 de abril de 2014. Marco Civil da Internet. 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: 20/08/2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 10/08/2019.

BARLOW, John Perry. Declaração de Independência do Ciberespaço, 1996. Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acesso em 22/08/2019.

BIONI, Bruno Ricardo. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019.

BRANDÃO, Luiza. "Li e aceito": muito além de entregar seus dados. IRIS, 2016. Disponível em: <http://irisbh.com.br/li-e-aceito-alem-de-entregar-seus-dados/>. Acesso em: 22/08/2019.

CGI.BR. Declaração Multissetorial do NETmundial, 2015. Disponível em: <https://www.cgi.br/publicacao/cadernos-cgi-br-declaracao-multissetorial-do-netmundial/>. Acesso em: 15/05/2019.

CGI.BR Fórum de Governança da Internet: Relatórios dos dez primeiros anos do IGF, 2018. Disponível em: < https://www.cgi.br/publicacao/cadernos-cgibr-forum-de-governanca-da-internet/>. Acesso em:15/08/2019.

DE LA CHAPELLE, Bertrand; FELLINGER, Paul. Jurisdiction on the internet: how to move beyond the legal arms race, 2016. Disponível em: < https://www.internetjurisdiction.net/uploads/pdfs/Articles/20161014-ORF-PDF.pdf>. Acesso em: 21/08/2019.

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

GONÇALVES, Pedro Vilela Rezende. O que muda com o decreto de regulamentação do Marco Civil? 2016. Disponível em: < http://irisbh.com.br/publicacoes/o-que-muda-com-o-decreto-de-regulamentacao-do-marco-civil/>. Acesso em: 21/08/2019.

GOMES, Maria Cecília de Oliveira. Cookie notice: o que é e por que é importante? 2018. Disponível em: <https://baptistaluz.com.br/institucional/midia-publicidade/>. Acesso em 23/08/2019.

GOMES, Maria Cecília Oliveira. Novos direitos. GV EXECUTIVO, [S.l.], v. 18, n. 4, p. 34-37, ago. 2019. ISSN 1806-8979. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/79979/76433>. Acesso em: 24 Ago. 2019.

IRIS, GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa, 2018. Disponível em: <https://irisbh.com.br/publicacoes/gdpr-e-suas-repercussoes-no-direito-brasileiro/>. Acesso em 21/08/2019.

IRIS, Representação ao Ministério Público de Minas Gerais, 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/08/Representacao-FINAL-MP.pdf>. Acesso em: 22/08/2019.

LEONARDI, Marcel. Tutela e privacidade na internet. Editora Saraiva, 2012.

LEMOS, Ronaldo. Feet on the Ground: Marco Civil as an Example of Multistakeholderism in Practice. In: SOUZA, Carlos Affonso Pereira; LEMOS, Ronaldo; VIOLA, Mario. Understanding Brazil's Internet Bill of Rights. Rio de Janeiro: ITS, 2015.

ONU, Resolução A/HRC/32/L.20. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. 2016. Disponível em: < https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20>. Acesso em: 18/08/2019.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord). Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017.

SOUZA, Carlos Affonso Pereira; LEMOS, Ronaldo; VIOLA, Mario. Understanding Brazil's Internet Bill of Rights. Rio de Janeiro: ITS, 2015.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em:< https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT> . Acesso em: 16/08/2019.

VIOLA, Mario; e IGATIBA, Gabriel; Privacidade e Dados Pessoais. In: SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord). Marco Civil da Internet: jurisprudência comentada. São Paulo: Editora Revista dos Tribunais, 2017.

A atuação de organizações ativistas na regulação da proteção de dados pessoais no Brasil: o caso da Lei Geral de Proteção de Dados (Nº 13.709 de 2018)

JONAS VALENTE

RESUMO

■ O presente artigo discute o processo de tramitação e aprovação da Lei Nº 13.709 de 2019, denominada Lei Geral de Proteção de Dados, bem como das alterações nesta promovidas pela Lei Nº 13.853 de 2019. Nesse processo, joga luz sobre a participação de entidades ativistas, especialmente a Coalizão Direitos na Rede, rede de organizações da área de defesa do consumidor, de promoção de direitos digitais e de pesquisa em informação e Internet. Ao analisar a participação desses atores, identifica suas pautas, as estratégias adotadas e êxitos e reveses na comparação entre as propostas e o texto final. Para isso, o artigo tomou as formulações apresentadas em audiências públicas, posicionamentos públicos e entrevistou duas integrantes das entidades que participaram do processo de negociação, bem como um pesquisador que também acompanhou de perto as tratativas.

ABSTRACT

■ This article discusses the process of passing and approving Law Nº. 13,709 of 2019, known as the General Data Protection Lawt, as well as the amendments thereto promoted by Law Nº. 13,853 of 2019. In this process, it sheds light on the participation of activist entities, especially the Network Rights Coalition, a network of organizations in the area of consumer protection, digital rights promotion and information and Internet research. By analyzing the participation of these actors, identifies their agendas, the strategies adop-

ted and successes and setbacks in the comparison between the proposals and the final text. For this, the article took the formulations presented in public hearings, public positions and interviewed two members of the entities that participated in the negotiation process, as well as a researcher who also closely followed the negotiations.

I. INTRODUÇÃO

De forma tardia, o Brasil teve em 2018 a aprovação de uma Lei Geral de Proteção de Dados (Nº 13.709). A LGPD, sigla pela qual ficou conhecida, unificou os princípios, diretrizes, exigências, direitos e responsabilidades relacionados à coleta e tratamento de informações de titulares pelo setor privado e Poder Público, consolidando dispositivos e preceitos dispersos na legislação nacional e preenchendo as lacunas desta em um novo arcabouço normativo. Contudo, o processo não foi rápido nem simples. Ao contrário, teve início na virada da década de 2010, foi objeto de diversas iniciativas dentro do Legislativo Federal, teve sua temática envolvida na tramitação de outras matérias (o Marco Civil da Internet), ganhou forma de proposição do Executivo na iminência do impeachment da ex-presidenta Dilma Rousseff em 2016, teve sua tramitação acelerada a partir deste momento e foi envolta em polêmicas mesmo após a sua aprovação, com vetos pelo presidente Michel Temer, uma nova Medida Provisória alterando parte dos seus trechos e a conversão desta em uma Lei em 2019 (Nº 13.853) que alterou dispositivos importantes e concluiu, até o momento de elaboração do presente trabalho, a complexa jornada desse regulamento.

O caminho tortuoso teve relação com contingências políticas, mas também com a diversidade de agentes e interesses envolvidos. Dentre estes, um conjunto de organizações da chamada sociedade civil com atuação desde os primeiros esboços, em 2010, até a edição da Lei de Conversão (Nº 13.853) em 2019. Esse campo se mobilizou em torno da Coalizão Direitos na Rede, grupo que se conformou ao longo do processo como a representação, mesmo que de maneira difusa e sem procuração para tal na maioria dos casos, dos interesses dos titulares de dados pessoais e da afirmação de direitos relacionados ao tema, da privacidade à liberdade de expressão, passando pela própria proteção de dados pessoais, entendida como uma garantia fundamental dos seres humanos.

O objetivo do presente artigo é fazer uma reconstrução e uma análise deste processo, discutindo a atuação desse campo em torno da Coalizão Direitos na Rede e de que maneira a incidência dessas organizações teve contribuição

no resultado do conteúdo da Lei[1], considerado aí também a sua etapa complementar na figura da Medida Provisória Nº 869 de 2018. Para isso, o texto inicia posicionando as noções de proteção de dados pessoais tomadas como referência para o debate do processo legislativo, bem como a compreensão dessas associações, buscando uma articulação de diferentes referenciais para propor a síntese da denominação de organização ativista. Em seguida, faz uma análise histórica do processo e da participação destes atores políticos. São tomados como material de análise os registros do processo legislativo, as posições públicas de entidades do campo e entrevistas com dois representantes da CDR (Bia Barbosa do Intervozes e Renata Mielli do Fórum Nacional pela Democratização da Comunicação) e de um advogado e professor que acompanhou a evolução desde os debates internos no governo federal até as negociações no Parlamento, Danilo Doneda (docente do Instituto de Direito Público de Brasília). Por fim, o artigo apresenta considerações conclusivas acerca do papel dessas organizações ativistas na construção da LGPD.

2. PRIVACIDADE E PROTEÇÃO DE DADOS

■ Antes de adentrar no processo da Lei e na atuação das organizações ativistas nela, faz-se necessário delimitar o que entendemos por seu objeto e preceitos relacionados a sua regulação. Entre definições mais notórias, Westin (1967, p. 7) a afirma como "a reivindicação de indivíduos, grupos e instituições para determinar por si mesmos quando, como e em que extensão informação sobre eles é comunicada a outros"[2]. Outra referência disseminada é a de Altman (1975, p. 24), que entende o fenômeno como o "controle seletivo do acesso a si [self]"[3]. O autor elenca quatro elementos relativos ao conceito: (1) o controle das fronteiras das relações pessoais; (2) o conflito entre privacidade pretendida e privacidade real, com a variação para além ou para aquém do desejado, não correspondendo ao nível ótimo necessariamente; e (3) a manifestação em diversos níveis, do individual ao coletivo. Dentro das discussões sobre o conceito, há abordagens questionadoras de uma acepção centrada em uma dimensão individual, de um direito apenas do

1 Em razão dos limites do presente texto, não será possível realizar um balanço ponto-a-ponto de como as posições se traduziram no texto final da Lei, mas tal análise será apontada de conjunto e nas questões mais importantes.

2 Tradução própria do original em inglês: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

3 Tradução própria do original em inglês: "selective control of access to the self".

ser de forma descolada dos contextos sociais. É o caso de Burkert (1997), segundo o qual o conceito de privacidade deve estar inserido em uma perspectiva mais ampliada, em uma dimensão "política", estando imerso em um conjunto de direitos relacionados à comunicação e à participação democrática.

Allmer (2013) parte de uma crítica de noções tradicionais sobre privacidade, caracterizadas como de caráter liberal e associadas a um individualismo possessivo autoprotetivo, localizando a vigilância no Estado e afirmando a proteção do indivíduo contra esta para fazer parte das relações de mercado. No lugar dessas acepções, o autor propõe uma abordagem mais crítica, que incorpore as assimetrias de poder na sociedade, as relações de dominação, as lutas de classe, os controles de recursos e a exploração. A vigilância, em especial na Internet, estaria associada à reprodução desse quadro de relações sociais, manifestando-se nas esferas da produção, circulação e do consumo. Uma abordagem mais crítica deveria incorporar essa compreensão, colocando o papel desta prática na proteção dos indivíduos contra as coerções para a reprodução do sistema social. Isso inclui a proteção contra a vigilância na Internet, especialmente a conduzida por corporações.

Nesta trilha mais crítica, Kwecka et al. (2014) argumentam que o conceito está relacionado à realização de outros direitos, como a livre associação e a participação pública. A privacidade não seria a cortina que permite ao indivíduo permanecer no isolamento, mas o elemento que assegura sua inserção livremente na vida em sociedade e no debate público. Os autores ponderam que um dos desafios para avançar neste sentido é a transformação da privacidade em algo renunciável e cambiável por serviços e por benefícios, seja junto ao Estado (como o exemplo da segurança pública) seja junto a uma empresa (como no caso do uso de sites de redes sociais). Esse caráter mais ampliado da privacidade a partir dos desafios postos pela configuração contemporânea do capitalismo e pela disseminação das tecnologias digitais e práticas de coleta e processamento de dados ensejou uma derivação para a afirmação do conceito de proteção de dados pessoais, segundo Doneda (2006)[4]. Mais do que uma concepção ampliada, o tema está diretamente

4 A necessidade de funcionalização da proteção da privacidade faz, portanto, com que dela defluísse uma disciplina de proteção de dados pessoais. A proteção dos dados pessoais compreende, basicamente, pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias – especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a conceitualística, na qual o direito à privacidade era limitado por uma tutela de índole patrimonialística, e

relacionado à qualidade das democracias contemporâneas. A proteção de dados continua uma utopia necessária e precisa ser assegurada para garantir a natureza democrática dos sistemas políticos (RODOTÁ, 2009).

3. AS ENTIDADES ATIVISTAS E O PROCESSO DA LGPD

■ A construção da LGPD teve uma série de atores envolvidos representando diversos setores: empresas de tecnologias da informação, indústria, emissoras de TV, instituições financeiras, agronegócio, governo federal, procuradores, investigadores, acadêmicos, entre outros. Nossa atenção será voltada ao que definiremos aqui como um campo organizado em torno da defesa de direitos dos usuários relacionados às comunicações, à Internet e às tecnologias digitais. Este campo reuniu organizações de defesa do consumidor (como o Instituto Brasileiro de Defesa do Consumidor e o Instituto Proteste), de ativismo nas comunicações e liberdade de expressão (Fórum Nacional pela Democratização da Comunicação, Intervozes – Coletivo Brasil de Comunicação, Centro de Estudos de Mídia Alternativa Barão de Itararé, Artigo XIX), de ativismo já no campo da Internet (Coding Rights, Internet sem Fronteiras, Coletivo Digital, NUPEF, Ibidem) e redes de pesquisadores acadêmicos (Rede Latino-americana de Estudos sobre Vigilância, Tecnologia e Sociedade – Lavits, Grupo de Pesquisa sobre Políticas de Acesso à Informação – GEPoPAI, Instituto de Tecnologia e Sociedade do Rio – ITS Rio e Internetlab).

Essas entidades, com atuação importante em pautas da área como na aprovação do Marco Civil da Internet (Lei Nº 12.965 de 2014) (CRUZ, 2015), reuniram-se em torno de uma rede denominada Coalizão Direitos na Rede, surgida em 2016 com o intuito de reunir associações preocupadas com diversas iniciativas de retrocesso às liberdades e direitos na Internet promovidas no âmbito do Executivo, Legislativo e Judiciário. Tal atuação pode ser localizada dentro do que Gohn (2013) identifica como a nova forma de associativismo da sociedade civil brasileira a partir dos anos 1990, na qual entidades deste campo atuam focadas em agendas de universalização de direitos e defesa da justiça social na intervenção nos processos de elaboração de políticas públicas. "A participação passa a ser concebida como intervenção social periódica e planejada, ao longo de todo o circuito de

---

de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa." (DONEDA, 2006, p. 16).

formulação e implementação de uma política pública, porque toda a ênfase passa a ser dada nas políticas públicas" (p. 240).

Ao examinar o processo do Marco Civil da Internet, Solagna (2015), inspirado em Shaw (2011), adota o conceito de "especialistas insurgentes"[5]. Discutindo uma nova forma de ativismo relacionada à Rede Mundial de Computadores, Goldsmith e Wu (2006) trabalham com a ideia de *geekativismo* para designar um tipo de ativismo específico de defesa de liberdades no âmbito do ambiente online. Tomando também o autoreconhecimento da rede e de suas organizações como o campo da "sociedade civil", adotaremos aqui o termo de "organizações ativistas", tomadas como associações formadas por indivíduos que partilham de uma agenda política apresentada e reivindicada não apenas para sua própria representação, mas para um coletivo mais amplo e que atuam com vistas a incidir em processos políticos, especialmente na formulação e implementação de políticas. No caso em exame, tais organizações atuaram como redes de coalizão, marcadas por movimentos de consenso na medida em que "os atores compartilham solidariedade e uma interpretação do mundo, possibilitando-lhes encadear atos e eventos específicos em uma perspectiva de mais longo prazo" (DIANI e BISON, 2010, p. 224).

3.1 A tramitação da LGPD e a atuação das organizações ativistas

■ Embora o Brasil tenha demorado para aprovar sua Lei Geral, já havia no arcabouço legal do país normas e dispositivos relacionados ao tema. A Constituição Federal, em seu mais central artigo sobre direitos (5º), elenca entre as garantias serem "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A Carta Magna determinou também a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações

5 Embora o foco de Shaw (2011) seja a ascensão de ativistas da área de software livre a postos no interior do aparelho estatal do Executivo brasileiro em 2003 e da atuação que fizeram no âmbito deste espaço, exemplo que cabe apenas parcialmente no objeto em análise no artigo já que tal atuação ocorreu até a deposição da presidente Dilma Rousseff em 2016, a interpretação de Solagna para o conceito aplicando-o à atuação no Marco Civil parece-nos interessante. "O conceito de insurgents experts fornece uma dimensão de análise interessante para explicar o ativismo que se situa entre tecnologia e política e que atua na formulação e na proposição de agendas para a área de TIC e Internet. Dessa forma, os atores envolvidos não são considerados apenas "especialistas" técnicos, mas indivíduos identificados com ideias de liberdade de expressão, privacidade e direitos relativos à Internet, que lançam mão de recursos e estratégias para influenciar a agenda governamental" (SOLAGNA, 2015, p. 52).

telefônicas", excetuando situações previstas em lei para investigação ou ordens judiciais.

Mais recente, o Marco Civil da Internet avançou afirmando não somente a privacidade, mas a proteção de dados como princípios das atividades na Rede Mundial de Computadores no país, já relacionando esta última a uma regulação específica ao incluir o aposto "na forma de lei". A despeito do reconhecimento da necessidade de uma Lei Geral de Proteção de Dados, que já era discutida na época da aprovação do Marco Civil, disciplinou parcialmente a matéria. Entre os direitos estavam a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação", bem como a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial".

Além disso, incluiu entre as garantias das pessoas a proibição de fornecimento de dados a terceiros, inclusive registros de conexão e acesso a aplicações de Internet, admitindo estas "mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (em mais uma referência a uma futura lei geral). Da mesma forma, elencou entre os direitos que a coleta e armazenamento só poderiam ocorrer para finalidades que: "a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet". A seção II (Artigos 10 a 12) detalha a proteção de registros e dados pessoais. Os Artigos preveem a guarda por tempo determinado e o repasse somente em caso de ordem judicial, com a exceção do acesso a dados cadastrais por autoridades administrativas "que detenham competência legal para a sua requisição". Por fim, a seção elenca punições a violações destes direitos, como multa de até 10% do faturamento do grupo no Brasil, suspensão temporária das atividades que envolvam os atos e proibição do exercício dessas atividades.

No Executivo, o governo federal passou a promover consultas públicas e debates para a formulação de um anteprojeto de lei de proteção de dados pessoais ainda antes da aprovação do Marco Civil, na virada da década de 2010. Por meio da plataforma "culturadigital.br"[6] foi lançada uma consulta pública sobre o tema e sobre uma redação inicial[7], conduzida até 2011. Contribuições da sociedade civil abordaram o conjunto dos temas da proposta, do conceito de dados pessoais aos direitos do titular (GPoPAI, 2015). No âmbito deste processo, proliferaram

6 Disponível em: http://culturadigital.br/dadospessoais/.

7 Versão disponível em: http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf.

discussões com participação da sociedade civil, como workshops promovidos pelo Comitê Gestor da Internet (CGI, 2011). Apesar disso, Danilo Doneda (2019), que participou da formulação no Ministério da Justiça, considera que nessa primeira fase o projeto não possuía apoio político dentro do governo federal.

No Congresso, um dos projetos mais antigos foi o PL 4069 de 2012, do deputado Milton Monti (PR-SP), que "dispõe o tratamento de dados pessoais e dá outras providências". A descrição focada no tratamento, e não da proteção, indica a linha da proposta, mais liberal e menos protetiva. A despeito de afirmar o direito à privacidade e à proteção de dados, a redação definia o objeto como algo que permite "a identificação exata" (e não qualquer forma de identificação), excluía dos dispositivos dados relativos a atividades comerciais e previa a necessidade de consentimento somente para o tratamento de dados sensíveis e de pais para a hipótese de crianças, cabendo a titulares de dados "normais" apenas o direito ao bloqueio do tratamento e garantias relativas a segurança e acesso não devido. O texto não criava uma estrutura institucional de fiscalização nem sanções, adotando neste último caso as do Código de Defesa do Consumidor.

De autoria do Poder Executivo, o PL 5276 de 2016 era mais amplo e com viés mais protetivo. A matéria foi objeto de intenso debate por diversos segmentos durante a sua elaboração (ZANATTA, 2015), que contou com consulta pública e embates no interior do governo federal no período anterior à derrubada da presidenta Dilma Rousseff por um processo de *impeachment*. O PL objetiva "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Art. 1º); dispõe sobre o tratamento de dados de qualquer por indivíduo ou pessoa jurídica independentemente do local desde que a coleta ou o processamento ocorram no país ou o seu objeto seja destinado a cidadão ou entidade brasileira (Art. 3º); abarca todo "dado relacionado à pessoa natural identificada ou identificável", diferenciando como sensíveis as informações sobre origem racial ou étnica, convicções religiosas ou políticas, filiação a associações e dados relacionados à saúde ou vida sexual (Art. 5º); fixa princípios para o tratamento como a definição de finalidade específica, a adequação e a necessidade relacionadas ao propósito informado no momento da coleta, o livre acesso do usuário, a transparência e a não discriminação (Art. 6º); exige o consentimento e permite o tratamento em hipóteses específicas (Art. 7º), estabelece exigências de transparência e disponibilização de informações ao usuário (Art. 8º), entre outras disposições.

Enviado às vésperas do impeachment da presidenta Dilma Rousseff em 2016, o PL 5276 foi distribuído para diversas comissões. Organizações da sociedade ci-

vil atuaram juntamente a parlamentares para que partidos sensíveis a abordagens mais protetivas se colocassem para posições-chave na tramitação (BARBOSA, 2019). A primeira comissão era a de trabalho (CTASP), na qual a Coalizão atuou para que um relator mais sensível a sua agenda, o que acabou ocorrendo com o deputado Orlando Silva (PC do B-SP). "Essa mobilização para ter um relator na primeira comissão que tinha um diálogo aberto com o movimento foi determinante durante toda a tramitação", avalia Renata Mielli (2019), uma das ativistas envolvidas na atuação da Coalizão. Em 26 de outubro de 2016, a Câmara criou uma comissão especial sobre o tema para substituir a tramitação nas comissões para onde havia sido distribuído o PL 5276/16 e para analisar três matérias: o PL 4060/12, o PL 5276/16 e o PL 6291/16. A presidência foi ocupada por Bruna Furlan (PSDB-SP) e a relatoria, por Orlando Silva (PC do B-SP). A comissão realizou diversas audiências públicas. Mielli (2019) avalia que a existência da comissão também foi importante para o resultado. A complexidade do tema ensejou a sua prorrogação, medida anunciada no início de 2018. Foram realizados seminários temáticos, inclusive um de caráter internacional (10 e 11 de maio de 2017), bem como diversas audiências públicas[8]. No histórico traçado pelo relator em seu parecer da matéria apreciado em plenário (SILVA, 2018) aparece a participação de representações de diversas organizações[9] em várias dessas ocasiões.

Entre as numerosas contribuições dessas entidades para o debate, destacamos: (1) uma concepção expansionista para a definição e dados pessoais, que incluísse aspectos identificáveis e relacionados ao titular; (2) a constituição de uma autoridade regulatória com amplos poderes, independente, com autonomia financeira e independência administrativa; (3) problemas do conceito vago de "legítimo interesse", receio de que este justifique qualquer tipo de tratamento e relevância de permiti-lo dentro de uma correlação com a finalidade da coleta; (4) não condicionamento de prestação de serviços ao fornecimento de dados pelo usuário; (5) responsabilidade objetiva e solidária dos tratadores de dados; e (6) a separação clara entre dados pessoais e sensíveis.

8 "As audiências foram importante para que parlamentares fossem entendendo o tema, mapeando as polêmicas e para amadurecer o diálogo entre os setores" (MIELLI, 2019).

9 Entre elas Instituto Brasileiro de Defesa do Consumidor (Idec), Coding Righs, Intervozes, Internetlab, Centro de Estudos de Mídia Alternativa Barão de Itararé, Rede de Pesquisa sobre Vigilância, Tecnologia e Sociedade (Lavits), Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI), Instituto Beta para Internet e Democracia (Ibidem), Intituto Proteste, Artigo 19, Open Knowledge Foundation, Fórum Nacional pela Democratização da Comunicação (FNDC), Laboratório de Estudos sobre Imagem e Cibercultura da UFES (Labic) e Instituto de Tecnologia e Sociedade do Rio (ITS Rio).

As organizações da sociedade civil também se manifestaram durante a tramitação por meio de notas e outros tipos de posicionamentos públicos. Logo após o envio do PL 5276/16, um enunciado defendeu a sua aprovação (GpoPAI et al., 2016). Nela destacam o seu conteúdo como resultado de ampla construção coletiva, com mais de duas mil contribuições, e como sistematização dos "conceitos e princípios de proteção de dados pessoais, delimitando de maneira clara seu escopo de aplicação e os critérios interpretativos necessários para a sua aplicação". Além disso, destacava a previsão de uma autoridade competente, por mais que tal órgão não tivesse sido desenhada na redação enviada ao Congresso pelo Executivo. O segmento defendia ali o que considerava ser a síntese mais bem acabada e possível dos debates entre os diversos segmentos de modo a preservar princípios e diretrizes regulatórias coerentes com suas bandeiras no tocante à proteção dos dados, aos direitos dos usuários e a uma estrutura institucional capaz de assegurar a sua efetividade.

Deposta a presidente Dilma Rousseff, uma nova gestão assumiu sob o comando do agora ex-presidente Michel Temer. E com ela, uma nova agenda de cunho mais liberal. E, com ela, um projeto apresentado no Senado Federal ganhou protagonismo: o PL 330 de 2013, de autoria do senador Antônio Carlos Valadares. Ainda em 2016, na Comissão de Meio Ambiente da Casa, o relatório do senador Aloysio Nunes (PSDB-SP), aliado do novo bloco político no Executivo, passou a figurar como principal alternativa para a aprovação de uma legislação. Em 2017, o parlamentar foi nomeado ministro das Relações Exteriores e a matéria foi assumida pelo senador Ricardo Ferraço (PDMB-ES) na Comissão de Assuntos Econômicos. Com isso, abriu-se uma competição entre as duas casas para ver quem adiantaria a tramitação. A avaliação era que o primeiro projeto aprovado fixaria a linha do debate político no Parlamento. Em maio de 2018, a matéria ganhou urgência para avaliação no Plenário do Senado.

Na avaliação de Danilo Doneda (2019), o destravamento da tramitação tem relação com a acolhida dentro do Congresso, com forças políticas que entenderam a relevância da matéria, sem um antagonismo entre partidos políticos. Bia Barbosa (2019) acredita que teve muita importância que o tema ganhou na sociedade, especialmente com a divulgação do escândalo do uso ilegal dos dados de dezenas de milhões de pessoas pela empresa de marketing digital Cambridge Analytica obtidos de apps no Facebook e empregados para influenciar processos políticos, como as eleições nos Estados Unidos e em Trinidad e Tobago e o referendo sobre a permanência do Reino Unido na União Europeia, popularmente conhecido como "Brexit". Outro fator importante foi a entrada em vigor do

Regulamento Geral de Proteção de Dados da União Europeia, que exigia nas atividades envolvendo a coleta e tratamento de dados com trocas em outros países os mesmos níveis de proteção instituídos.

Na tramitação da Câmara, a ativista relata que a Coalizão Direitos na Rede realizou reuniões com o relator na Comissão Especial, Orlando Silva (PC do B-SP), e com lideranças partidárias. Ela destaca que uma medida chave de mediação do conteúdo entre os atores políticos para a formulação do substitutivo do relator foi a organização de uma mesa de negociação criada para analisar a redação ponto-a-ponto, que ocorreu nos meses de abril e maio. O relatório inicial havia acolhido bastante do conteúdo do PL 5276 e das posições das organizações ativistas. Contudo, a pressão de segmentos empresariais era intensa. Na mesa de negociação, posições de diversos setores foram apresentadas. Conforme relata Barbosa (2019), a Coalizão atuou para manter uma série de dispositivos criticados por associações empresariais, como conceitos de dados pessoais e sensíveis, obrigação de consentimento, regras específicas para crianças e a exigência de relatórios de impacto em algumas situações. Contudo, outros interesses dos segmentos empresariais foram contemplados, como a exceção do consentimento para a análise de crédito[10]. A Coalizão buscou melhorar pontos, como retirar a exceção da aplicação da Lei ao Poder Público em atividades de segurança pública, mas não obteve sucesso. Ainda às vésperas do relatório, a rede seguiu em diálogo com o relator e pressionou por pontos importantes, como a redação sobre a hipótese de legítimo interesse para um uso pelos processadores de dados distinto daquela finalidade que deveria ser informada no momento da coleta. Doneda (2019) assinala que as organizações conseguiram se consolidar não apenas como grupos de pressão mas também como referência técnica no debate na Câmara.

Na outra Casa Legislativa, o PL 330 caminhava a passos largos. A Coalizão Direitos na Rede, que já havia lançado a campanha "Seus Dados São Você", divulgou nota pontuando críticas ao PL 330. Entre elas: (1) exceções ao poder público, como no caso do direito de oposição pelo titular, bem como não na aplicação a atividades de inteligência e infrações penais, (2) nos casos de legítimo interesse ausência da obrigação de apresentação de relatórios de impacto e teste de proporcionalidade pelos agentes econômicos; (3) falta de tratamento adequado de dados sensíveis para evitar abusos; (4) falhas em regras específicas para crianças

10 Além de uma bandeira do setor financeiro, essa modalidade de tratamento era prevista na proposta que instituía o Cadastro Positivo também em tramitação na Câmara e essas instituições buscavam evitar que a Lei Geral pudesse dificultar o uso compulsório de dados para essa finalidade.

considerando sua condição especial; (5) a possibilidade de um dado permanecer com um controlador mesmo após o fim do seu uso, de forma anonimizada; (6) não detalhamento do instrumento do relatório de impacto em um determinado tratamento de dados, considerado pela rede fundamental em casos como decisões automatizadas, elaboração de perfil comportamental e quando envolvesse dados sensíveis; e (6) não previsão da autoridade nacional de proteção de dados[11].

Nos bastidores, a corrida se intensificou. Enquanto no Senado, o PL 330 contava com apoio do governo e havia avançado para análise em plenário, na Câmara o relator, Orlando Silva, buscava com o presidente da casa, Rodrigo Maia (DEM-RJ), a inclusão da matéria para votação. Segmentos continuavam pressionando por mudanças, influenciando as redações que seriam efetivamente apreciadas. No dia 29 de maio, o PL 330 estava na pauta do Senado. Segundo Bia Barbosa, em razão de um desgaste entre o presidente da Casa, Eunício Oliveira (PMDB-CE), e o governo, a sessão daquele dia foi encerrada sem analisar o projeto. A poucos metros dali, o presidente da Câmara colocou o substitutivo de Silva (2018) em votação, que recebeu apoio do conjunto dos partidos. Na sessão, o texto foi elogiado como resultado de uma construção envolvendo todos os segmentos e partidos. Os deputados, capitaneados pelo relator, haviam vencido a disputa com o Senado. Contudo, a matéria ainda precisava passar por esta casa (agora sob o nome de Projeto de Lei da Câmara 53 de 2018), que poderia alterar a sua redação. Teve início então uma nova movimentação dos agentes em cima do relator nomeado, senador Ricardo Ferraço (PSDB-ES), o mesmo do PL 330.

Neste momento, formou-se um amplo campo de apoio ao PL envolvendo não apenas a Coalizão Direitos na Rede, mas também segmentos empresariais do setor de tecnologia (representados pela Associação Brasileira de Empresas de Tecnologia da Informação e da Comunicação – Brasscom e pela Associação Brasileira das Empresas de Software – ABES), incluindo grandes agentes do setor, como Google e Facebook. A resistência e pressão pela alteração ficou concentrada, sobretudo, no segmento de instituições financeiras, representadas pela Federação Brasileira de Bancos. Ao mesmo tempo, no governo federal também havia desconfortos com o projeto, especialmente após o Executivo ter sido um ator distante e pouco protagonista no conteúdo da matéria aprovada na Câmara e por desejar regras mais flexíveis para o tratamento e compartilhamento de in-

11 "Nós tentamos articular para tentar atrasar a tramitação do PL 330 a partir da apresentação de emendas e acelerar o processo do PL 5276. Mas houve uma combinação de fatores. A ação da Coalizão foi determinante, mas a mesa de negociação foi importante, bem como a articulação do relator com a Mesa Diretora", relata Renata Mielli (2019).

formações pelo Poder Público, o que disciplinaria a sua própria atuação na matéria. Uma das resistências era a Autoridade Nacional, já que esta seria a estrutura institucional de fiscalização e aplicação dos dispositivos da Lei e da ação do Poder Público, incluindo o próprio governo. Em meio a estes debates, a coalizão ampla divulgou nota (ACTANTES et AL., 2018) em que defende o órgão com um caráter independente funcional, administrativa e financeiramente. Somente com a sua criação "é que se foi possível alcançar uma tutela efetiva da privacidade dos cidadãos, ao mesmo tempo em que se propiciou a segurança jurídica na aplicação desta para os atores regulados".

Em manifesto (ABA et al. 2018), a frente ampla cobrou a aprovação do PLC 53 dos senadores, classificando a proposta como "uma lei de proteção de dados clara e principiológica, que equilibra a posição central do indivíduo com o dinamismo econômico de um país criativo e inclinado à inovação". A reivindicação foi manifestada também em carta própria da Coalizão Direitos na Rede (CDR, 2018b). Nesta, a rede ressaltou este como "o resultado possível e maduro de diálogo e negociação intensa entre diversos interessados na consolidação de uma moderna lei geral de proteção de dados pessoais". Representantes da rede percorreram lideranças e gabinetes no Senado, a exemplo do que já havia sido feito na Câmara. Frente à pressão dos diversos segmentos, entre eles as organizações ativistas, Ferraço decidiu não propor alterações e a proposta foi aprovada no Senado no dia 10 de julho, também por unanimidade.

Os desacordos do governo e pressões de setores empresariais, se não motivaram a mudança da redação no Senado, apareceram na forma de vetos do presidente Michel Temer no momento da sanção da Lei. A elaboração desses vetos também foi objeto de intensa disputa política. A mencionada carta da coalizão ampla foi um exemplo importante da atuação deste segmento na principal polêmica: a criação da autoridade. Embora houvesse uma resistência de mérito e de caráter político, esta aparecia no argumento de que haveria um vício formal na criação do órgão uma vez que tal previsão não veio de projeto do Executivo. Do outro lado, organizações ativistas e empresas favoráveis ao projeto da Câmara defendiam que a sua presença no PL 5276/16, de autoria do Executivo e incorporado no substitutivo aprovado na Câmara, eliminava tal vício, posição expressa em carta ao governo (CDR, 2018c). Doneda (2019) avalia que a permeabilidade às posições das organizações ativistas vista nos parlamentares não se repetiu no governo federal. O Executivo demonstrava uma visão mais liberal e menos protetiva da legislação, em correspondência a sua agenda política e econômica no viés de aprofundamento do neoliberalismo no país e restrição de direitos.

Em agosto de 2018, o presidente Michel Temer não apenas vetou a autoridade, mas outros pontos, como o Conselho Nacional de Proteção de Dados, a proteção dos solicitantes de informações do Poder Público pela Lei de Acesso à Informação (LAI), as sanções administrativas para agentes que violassem os dispositivos da Lei e a obrigação de publicidade no compartilhamento de dados entre entes públicos. Na cerimônia em que anunciou os vetos, Temer afirmou que editaria uma Medida Provisória criando a autoridade. A Coalizão se posicionou questionando a decisão. "Os vetos realizados pelo governo federal ao texto aprovado no Parlamento podem comprometer a eficácia da legislação sancionada" (CDR, 2012d). Em dezembro, faltando pouco tempo para o fim da gestão de Temer, a frente ampla novamente cobrou do governo a criação da Autoridade Nacional e do Conselho Nacional de Dados Pessoais (ABAP et al., 2018), afirmando a necessidade de sua independência e autonomia, da restauração das sanções previstas no projeto aprovado no Congresso e assegurando corpo técnico competente para as suas funções[12].

Nos últimos dias de sua gestão, editou a MP 869/18, que alterou a natureza institucional da Autoridade em relação ao texto do Congresso, mas foi além e reconfigurou outros dispositivos, além de reduzir as sanções previstas. O Instituto Brasileiro de Defesa do Consumidor (IDEC, 2019) apontou um conjunto de problemas no texto da MP: (1) ampliação do escopo do tratamento para fins de Segurança Pública, como a permissão a pessoas de direito privado controladas pelo Poder Público para tratarem a integralidade de dados, criando mecanismo para empresas públicas e fundações coletarem dados sem necessidade de consentimento; (2) autorização para compartilhamento de dados referentes à saúde, abrindo possibilidade para comercialização dessas informações; (3) fim da revisão de decisões automatizadas por pessoa natural, um pleito importante das organizações ativistas em função dos riscos de discriminação e abuso neste tipo de procedimento; (4) majoração das hipóteses de transferência de dados pelo Poder Público a entes privados, sem consentimento do titular; (5) retirada de obrigação de informar o titular em casos onde não era obrigatório o consentimento, como no cumprimento de obrigações legais e na execução de políticas públicas; e (6)

12 "Essa Autoridade deverá gozar de características imprescindíveis tais como independência e autonomia decisória; o mandato fixo de seus dirigentes; a manutenção do rol de atributos listados no art. 56 do PLC 53/2018, objeto de veto presidencial; ser composta por um corpo funcional estritamente técnico para realizar o gerenciamento deste tema perante seus múltiplos e distintos atores; e ter em sua estrutura um conselho consultivo multissetorial" (ABAP et al., 2018).

a modelagem da Autoridade Nacional vinculada à Presidência e sem garantia de autonomia financeira, diferentemente do modelo defendido pelas organizações ativistas, além de retirar competências do órgão, como a realização de auditorias (instrumento chave de fiscalização) e a regulamentação da produção de relatórios de impacto em situações de alto risco. Como dispositivo simbólico da MP, foi incluído um dispositivo segundo o qual a atuação da Autoridade deveria seguir a lógica da "mínima intervenção estatal".

A atuação dos grupos políticos ganhou nova intensidade com o início da tramitação da MP em 2019, em uma nova configuração do Executivo com a gestão de forças ultraliberais e de traços autoritários sob o comando do novo presidente Jair Bolsonaro (PSL), e do Congresso Nacional, cuja legislatura teve a majoração da presença de parlamentares conservadores e a diminuição das bancadas de legendas vinculadas a agendas de promoção de direitos[13]. Consagrado como grande articulador da Lei Geral, o deputado Orlando Silva (PC do B-SP) assumiu a relatoria da MP na Comissão Mista criada para escrutinar a matéria. Seu relatório, ao qual foram apresentadas 170 emendas, recuperou uma série de dispositivos da redação aprovada pelo Congresso em 2018, como notou a Coalizão Direitos na Rede em posicionamento público (CDR, 2019a). Um item restaurado foi a revisão de decisões automatizadas por pessoa natural (e não por sistemas automatizados, o que reduz o direito à explicação e cria uma tendência de reforço das decisões). O relatório de Silva também restabeleceu sanções da redação da Lei aprovada pelo Congresso, vetadas por Michel Temer e ignoradas na MP. Já no tocante à Autoridade, a pressão de novos grupos empresariais e da nova gestão no Executivo foi forte o suficiente para vetar no relatório o modelo fixado pela Lei 13.708/18. A mediação realizada terminou por delimitar um órgão subordinado à Presidência, mas de caráter transitório, devendo sua natureza ser reavaliada em dois anos. A Coalizão manteve sua defesa do órgão com independência administrativa e funcional e independência financeira, mas admitiu os limites da negociação[14].

13 "Foi uma nova correlação de forças, com muitos parlamentares que não haviam acompanhado o debate em 2018 e com uma inclinação política mais liberal, além da pressão mais forte das empresas e de novos segmentos empresariais que não haviam atuado no ano anterior" (BARBOSA, 2019).

14 Consideramos que a previsão de transitoriedade colocada no modelo proposto no relatório é um passo que permitirá a construção de uma Autoridade de Proteção de Dados Pessoais com essas características, ante as atuais limitações orçamentárias impostas à criação de um órgão na administração indireta.

Segundo Barbosa (2019), as pressões de segmentos empresariais e do Executivo Federal e a correlação de forças no Congresso não possibilitaram a retomada integral do conteúdo da Lei 13.709 dado pelo Congresso. A ativista destaca que na tramitação da MP houve uma diversificação de segmentos empresariais atuando como grupos de pressão, como companhias envolvidas no tratamento de dados de saúde e startups. Essa presença resultou em redações flexibilizantes, como a previsão de compartilhamento de dados de saúde para obtenção de ganhos econômicos e a possibilidade de reduzir obrigações na Lei para startups[15]. A MP foi aprovada na forma do Projeto de Lei de Conversão Nº 07 de 2019. Ainda assim, o presidente Jair Bolsonaro vetou um conjunto de artigos. A Coalizão veio novamente a público condenar os vetos (CDR, 2019b), argumentando que eles "desrespeitam os acordos firmados no Congresso Nacional e pede que os parlamentares, dentro da prerrogativa que cabe ao Poder Legislativo, revertam questões importantes no texto do ponto de vista dos direitos da população". O grupo elencou entre os dispositivos suprimidos problemas graves na exclusão da possibilidade de revisão de decisões automatizadas por pessoa natural, na retirada das sanções de suspensão parcial ou total de um banco de dados e na revogação da proteção de requerentes de informações públicas por meio da Lei de Acesso à Informação (LAI).

4. CONSIDERAÇÕES CONCLUSIVAS

■ A Lei Geral de Proteção de Dados foi um avanço importante no arcabouço legal brasileiro. Em um cenário de crescimento das tecnologias digitais, da coleta e tratamento de dados em informação e aplicações inteligentes (VAN DIJCK, 2014; BARRETO e VALENTE, 2019) em um número crescente de atividades, do aprofundamento das práticas de vigilância (LYON, 2013) e da emergência do poder de grandes empresas especializadas neste tipo de negócio, em especial monopólios digitais como Google, Facebook, Amazon e Apple (VALENTE, 2019),

15 "A sociedade civil perdeu mais coisas neste relatório do que a lei tinha nos garantido. Foram abertas algumas exceções, como para startups e para empresas de inovação sema avaliar tamanho das empresas e impacto destas empresas. Ganharam excepcionalidades. Fio inserida excepcionalidade para saúde. Por outro lado, o relatório conseguiu recuperar algumas prerrogativas que tinham sido vetadas da autoridade que tinham sido vetadas e não tinham sido reinseridas via MP. Achamos que do ponto de vista do ganho da autoridade, relatório foi positivo. Mas em aspectos do restante da Lei, o relatório por correlação de forças desfavorável abriu flexibilizações, deixando pra autoridade definir questões que a lei definida" (BARBOSA, 2019).

o avanço sobre os titulares de dados para extrair suas informações requer um arcabouço protetivo adequado de modo a não aprofundar as assimetrias de poder entre indivíduos, de um lado, e agentes econômicos e instituições públicas, de outro. Seu resultado incorporou diversos direitos e dispositivos importantes previstos em legislações de referência, como o Regulamento Geral de Proteção de Dados, mas a segunda etapa de tramitação, a partir dos vetos de Temer e especialmente em 2019 refletiu a hegemonia de forças políticas e de segmentos empresariais com uma visão mais focada na liberalização do tratamento e menos na proteção do titular.

No exame do processo de tramitação da LGPD, identificamos o campo de organizações ativistas, especialmente aquelas organizadas em torno da Coalizão Direitos na Rede, como um ator político com a compreensão dessas mudanças, dos riscos do ascenso das práticas de coleta e da vigilância e coadunado com a perspectiva de defesa da proteção de dados como direito dos indivíduos e das coletividades não apenas na dimensão relativa da privacidade mas em seu sentido ampliado (DONEDA, 2006; ALLMER, 2013), relacionando também a garantias como a liberdade de expressão e a própria autonomia do indivíduo frente a corporações e Estados.

Desde a consulta ao anteprojeto de lei em 2010 à tramitação no Congresso, essas entidades apresentaram um programa consistente com esses conceitos, materializado em posições protetivas em diversos aspectos da legislação, como: (1) a conceituação de dados pessoais e dados sensíveis; (2) o escopo de aplicação da lei; (3) a necessidade do consentimento livre e informado como hipótese chave para a coleta, tratando as demais como exceções; (4) a afirmação de direitos dos titulares, como oposição a tratamento, correção de informações, exclusão de registros e revisão de decisões automatizadas; (5) o reconhecimento de públicos vulneráveis, com crianças e adolescentes ou segmentos cujo tratamento de dados sensíveis teria potencial discriminatório; (6) restrição do escopo de coleta e exceções, explicitando a necessidade de finalidade específica; (7) previsão de instrumentos adequados de fiscalização, como auditorias, relatórios de impacto e sanções que assegurem o respeito aos mecanismos da Lei; e (8) desenho da autoridade com independência financeira, autonomia administrativa e funcional, corpo técnico adequado e dotada de prerrogativa regulamentadora e poderes de atuação não somente sobre empresas como também a órgãos públicos.

Para além de uma agenda robusta, as organizações ativistas lançaram mão de métodos diversos de articulação e pressão. Podemos classificar as estratégias em cinco frentes: (1) formulação – transformação das concepções teóricas e políticas

em propostas concretas nos distintos momentos de tramitação, da consulta do anteprojeto a emendas nas votações em comissões e no Plenário das casas legislativas; (2) mobilização de apoios na sociedade, envolvendo outras organizações ativistas não afeitas inicialmente ao tema; (3) articulação com segmentos empresariais, o que ocorreu desde a tramitação no Congresso até as disputas acerca dos vetos e cuja maior expressão é a coalizão ampla para manutenção do projeto de lei aprovado na Câmara em 2018 e em defesa da Autoridade Nacional; (4) pressão e negociação juntamente ao Executivo Federal, prática adotada tanto na gestão de Michel Temer para a negociação dos vetos quanto na de Jair Bolsonaro para discutir a MP 869; e, principalmente, (5) mobilização, articulação e negociação no Parlamento, abrangendo desde o incentivo a parlamentares assumirem posições-chave na tramitação até o debate dos conteúdos dos relatórios e textos votados em comissões e nos plenários, bem como convencimento das bancadas sobre as opiniões relacionadas às agendas deste campo.

No tocante à efetividade dessa atuação, faz-se necessário tomar cuidado para não inflar nem desconsiderar a importância da atuação das organizações ativistas. A avaliação de Mielli (2019), uma das lideranças do processo, assinala o papel do grupo em incluir dispositivos protetivos e resistir a movimentos de ofensiva pela sua retirada, mesmo em uma conjuntura adversa[16]. Doneda (2019) avalia a incidência da rede como muito importante. "Amplificou grupos de pressão social e conseguiu articular essas demandas de uma forma que incrivelmente conseguiu disputar com outras forças". Ele acrescentou que os ativistas estavam tão bem preparados quanto representantes de outros segmentos. Aproximamo-nos desse balanço, reconhecendo as contribuições das organizações ativistas em diversos aspectos, entre os quais destacamos: (1) a pressão interna no governo federal para a conclusão e envio do PL 5276/16; (2) a mobilização de parlamentares sensíveis a sua agenda durante a tramitação, em especial do relator, que teve papel chave no êxito da aprovação; (3) a sensibilização de bancadas e lideranças no Congresso; (4) a movimentação pública e a articulação juntamente a diferentes segmentos para evitar retrocessos quando das pressões empresariais; e (5) o questionamento dos vetos e da ofensiva envolta na MP 869.

Com isso não estamos afirmando que as organizações ativistas lograram incluir toda sua agenda na redação aprovada. Como tentamos mostrar, ainda que

16 "Foi um processo de redução de danos diante do novo cenário mais adverso. Setores econômicos que haviam aberto mão de pontos viram no novo Congresso um quadro para recolocar suas demandas. Apesar de termos perdido, conseguimos impedir que o retrocesso fosse maior", (MIELLI, 2019).

sinteticamente, a Lei foi objeto de intensa pressão por parte de segmentos empresariais e de gestões do Executivo Federal com pouco ou nenhum compromisso com um arcabouço mais protetor, o que se refletiu especialmente nas mudanças resultantes da MP 869 e a lei correspondente desta (Nº 13.853 de 2019). Contudo, dada a correlação de forças, as estratégias da Coalizão Direitos na Rede e das organizações ativistas foram bem-sucedidas parcialmente em incluir pontos importantes na legislação, em impedir ou dificultar uma série de descaracterizações de mecanismos protetivos e de pautar o tema da proteção de dados como um desafio nacional contemporâneo. No momento em que este artigo era escrito, a batalha estava longe de terminar. Ao contrário, ela passava então a novos embates, como a montagem da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados, a discussão da regulamentação da Lei em diversos aspectos e a admissão das já limitações desta em razão da evolução das práticas de coleta e tratamento, como na chamada "Internet das Coisas" em que tais procedimentos ocorrem de formas complexas e não tão claras no tocante ao titular. A perspectiva é que o tema permaneça objeto de discussões regulatórias no futuro, com a Coalizão Direitos na Rede continuando a atuar.

Jonas Valente · Doutor em sociologia da tecnologia pelo Programa de Pós-Graduação do Departamento de Sociologia da Universidade de Brasília. Pesquisador do Laboratório de Políticas de Comunicação da mesma instituição.

REFERÊNCIAS

ABA et al. Em defesa da aprovação, pelo Senado, do Projeto de Lei da Câmara no 53 de 2018. ABA et al. 13 de julho de 2018.

ABAP et al. Manifesto pela criação imediata da autoridade nacional de proteção de dados pessoais. Abap et al. 06 de dezembro de 2018.

ACTANTES et al. Carta em defesa da Autoridade de Proteção de Dados Pessoais. 13 de junho de 2018.

ALLMER, T. Critical internet surveillance studies and economic surveillance. In: Internet and Surveillance. Routledge, 2013, p. 144-164.

ALTMAN, I. The environment and social behavior. Monterey, CA: Brooks/Cole, 1975.

BARBOSA, B. Entrevista ao autor. 2019.

BARRETO, HMR. VALENTE, JCL. Datificação da economia e impactos nos mercados das comunicações digitais: uma análise do Google e do Grupo Globo. Revista Eptic, v. 21(3), set. 2019.

BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21 ago. 2019.

_____. Lei Nº 12.965, que estabelece princípios, garantias, direitos e deveres para a Internet no Brasil. 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 ago. 2019.

_____. Lei Nº 13.709 de 2018. Lei Geral de Proteção de Dados. 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 21 ago. 2019.

_____. Medida Provisória Nº 869 de 2018. Acesso em: 21 ago. 2019.

_____. Lei Nº 13.853 de 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. 8 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm>. Acesso em: 21 ago. 2019.

CÂMARA DOS DEPUTADOS. Projeto de Lei 5276 de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento e da dignidade da pessoa natural. 13 de maio de 2016. Disponível em: < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 21 ago. 2019.

CÂMARA DOS DEPUTADOS. Redação final do PL 4060 de 2012. Câmara dos Deputados. 29 de maio de 2018. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1665276&filename=Tramitacao-PL+4060/2012>. Acesso em: 21 ago. 2019.

CDR. Nota da Coalizão Direitos na Rede sobre o Projeto de Lei do Senado no 330/2013. Coalizão Direitos na Rede. 29 de maio de 2018a. Disponível em: <https://direitosnarede.org.br/c/nota-cdr-sobre-pls330-13/>. Acesso em: 18 ago. 2019.

____. Carta ao Senado pela imediata aprovação do PLC 53/2018. Coalizão Direitos na Rede. 25 de junho de 2018b. Acesso em: 18 ago. 2019.

____. Temer: sancione sem mudanças a lei de Proteção de Dados! Não ataque essa conquista do povo brasileiro! Coalizão Direitos na Rede. 31 de julho de 2018c. Acesso em: 18 ago. 2019.

____. Vetos de Temer ameaçam eficácia da Lei de Proteção de Dados Pessoais. Coalizão Direitos na Rede. 15 de agosto de 2018d. Acesso em: 18 ago. 2019.

____. Um novo compromisso com a democracia e a proteção de dados pessoais é necessário. Coalizão Direitos na Rede. Maio de 2019a. Acesso em: 18 ago. 2019.

____. Sobre os vetos presidenciais à LGDP e à criação da Autoridade Nacional de Proteção de Dados. Coalizão Direitos na Rede. 6 de agosto de 2019. Acesso em: 18 ago. 2019.

COMITÊ GESTOR DA INTERNET. Governo e Sociedade discutem Anteprojeto de Lei sobre Proteção de Dados Pessoais. Comitê Gestor da Internet. Online. Disponível: <https://www.cgi.br/noticia/releases/governo-e-sociedade-discutem-anteprojeto-de-lei-sobre-protecao-de-dados-pessoais/>. Publicado em: 6 abr. 2011. Acesso em: 18 ago. 2019.

CRUZ, Francisco Carvalho de Brito. Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet. Diss. Universidade de São Paulo, 2015.

DIANI, M. BISON, I. Organizações, coalizões e movimentos. Revista Brasileira de Ciência Política. 2010;3:219.

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar; 2006.

_____ . Entrevista ao autor. 2019.

GOLDSMITH, J.; WU, T. Who Controls the Internet?: Illusions of a Borderless World. Oxford University, 2006.

GPoPAI. Contribuições à Consulta Pública do Anteprojeto de Lei/APL de Proteção de Dados Pessoais. GPOPAI. Disponível em: <http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/07c449c076fabbb00f3d3b850e063417.pdf>. Julho de 2015. Acesso em: 18 ago. 2019.

GEPoPAi et al. Carta Aberta de Apoio ao PL 5276/2016. 2 de junho de 2016. Disponível em: <http://intervozes.org.br/wp-content/uploads/2016/06/Carta-Aberta.-PL-Dados-Pessoais.02.06.2016.pdf>. Acesso em: 18 ago. 2019.

GOHN, M.C. Sociedade Civil no Brasil: movimentos sociais e ONGs. Meta: Avaliação. 2013 Sep 18;5(14):238-53.

IDEC. Medida Provisória Nº 869 – Análise da criação da Autoridade Nacional de Proteção de Dados. Instituto Brasileiro de Defesa do Consumidor. 2019.

KWECKA, Z. et al. I am Spartacus: privacy enhancing technologies, collaborative obfuscation and privacy as a public good. Artificial Intelligence and Law, v. 22, Issue 2, June, 2014.

LYON, D. The information society: Issues and illusions. John Wiley & Sons, 2013.

MIELLI, R. Entrevista ao autor. 2019.

RODOTÁ, Stefano. Data protection as a fundamental right. In: Reinventing Data Protection?, Springer, Dordrecht, 2009. pp. 77-82.

SENADO FEDERAL. Projeto de Lei 330 de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências.13 de agosto de 2013. Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>.

SILVA, O. Parecer do relator ao PL 4060 de 2012 para apreciação em Plenário. Câmara dos Deputados. 29 de maio de 2018.

SOLAGNA, F. A formulação da agenda e o ativismo em torno do Marco Civil da Internet 2015. 201 f., il. Dissertação (mestrado em filosofia e ciências humanas) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015.

SHAW, A. Insurgent Expertise: The Politics of Free/Livre and Open Source Software in Brazil. Journal of Information Technology & Politics, v. 3, n. 8, p. 253–272, 2011.

VALENTE, JCL. Tecnologia, informação e poder: das plataformas online aos monopólios digitais. 2019. 400 f., il. Tese (Doutorado em Sociologia) – Universidade de Brasília, Brasília, 2019.

VAN DIJCK, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, v. 9, n. 12, 2014.

ZANATTA, R A. F. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. Direito e Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, 2015.

WESTIN, A. Privacy and freedom. New York: Athenaeum, 1967.

A gestão de dados pessoais por grandes empresas: considerações geopolíticas e jurídicas

MARIA AMÁLIA OLIVEIRA DE ARRUDA CAMARA
WALTER DE MACEDO RODRIGUES

RESUMO

■ Este trabalho trata como empresas multinacionais de tecnologia da informação lidam com diferentes ordenamentos jurídicos a respeito de proteção de dados pessoais e privacidade. As leis que surgem neste cenário podem advir de interesses de Estados em conflitos geopolíticos e que, muitas vezes, podem convergir para o direcionamento das empresas para o detrimento dos titulares dos dados. Fazendo um estudo comparado de diferentes legislações, percebe-se a possibilidade de nações violarem, com fundamento de segurança nacional, a proteção de dados pessoais e de direitos correlatos de seus titulares. As repercussões de tais violações foram avaliadas na medida que estudou-se como os modelos de gestão das empresas podem proporcionar uma maior segurança em processos de *compliance* com a normativa nacional, e na escolha pela defesa dos direitos dos titulares dos dados. Tentando identificar os modelos mais interessantes para a proteção de dados, este trabalho também propôs a utilização de *privacy by design* como uma possibilidade para mitigar a ação de decisão humana no processo de *compliance*, como uma forma de tecnologia que já garanta essa proteção em sua concepção.

ABSTRACT

■ This paper is about how multinational information technology companies deal with different legal systems regarding personal data protection and privacy. The laws that emerge in this scenario may come from the interests of national

states in geopolitical conflict, and it can converge on companies to the detriment of data subjects. In a comparative study of different laws, we realize the possibility of several national violations on the protection of personal data and related rights of their holders, on grounds of national security. The repercussions of such violations were assessed as we studied how corporate management models can provide greater security in national regulatory compliance processes, and in choosing to defend data rights holders. The paper identifies the most interesting models for this scenario. This work also proposes the use of privacy by design as a possibility to mitigate the human decision action in the compliance process, as a technology that already guarantees this protection in your conception.

1. INTRODUÇÃO

■ Nos últimos tempos, a preocupação com a privacidade dos dados pessoais tem sido um ponto nevrálgico do universo jurídico. Casos como recentes escândalos de privacidade envolvendo o Facebook, onde 14 milhões de usuários tiveram suas informações privadas expostas sem seus consentimentos, devido a um mero erro de *software*, são paradigmáticos na discussão normativa sobre responsabilidades, sanções e contenção de danos, no caso de vazamento de dados pessoais (KUCHLER, 2018). Além do vazamento de dados, no início de 2018, o Facebook estava sob investigação devido ao uso de dados pessoais de usuários pela empresa de consultoria política Cambridge Analytica. Foram coletadas à época informações pessoais de aproximadamente 87 milhões de usuários do Facebook sem seu consentimento explícito de acesso (HERN, 2018), que possibilitaram campanhas de marketing direcionado que conseguiram com sucesso eleger candidatos pelo mundo.

Não desconsiderando a importância de outras legislações e discussões anteriores a GDPR – General Data Protection Regulation[1] pareceu ter sido uma reação direta a uma possível ameaça ao modelo de democracia presente em regulamentar a ferramenta do *big data* (EUROPEAN PARLIAMENT, 2018). Grandes empresas passaram a, especialmente nos primeiros dias da legislação vigente, ou enfrentar multas milionários ou ter uma maior discricionariedade como lidariam com questões de *compliance*. As gigantes de tecnologia, por sua vez, encontraram-se em meio a um conflito internacional de entes estatais.

1. Regulamento Geral de Proteção de Dados. Tradução livre.

É inegável que, para se atingir maior eficiência na mobilidade, consumo, economia e outros aspectos da vida quotidiana, quão maior a quantidade de dados fornecida pelos usuários, maior é a precisão dos perfis traçados, a individualização de demandas e otimização de resultados almejados por cada indivíduo. Isto, de fato, parece ser por demais vantajoso para usuários desse tipo de tecnologia. Mas a opacidade sobre a forma de como os dados são tratados evoca preocupações legítimas com a privacidade. Esse obstáculo relativamente novo, típico do século XXI, é, certamente, a maior desafio que empresas e negócios que lidam com coleta e tratamento de dados devem vencer.

Ora, se o tratamento de dados por grandes empresas representa um problema para a própria democracia representativa, dado ao fato de que campanhas políticas têm sofrido manipulação por problemas de gestão de dados, pode-se argumentar que o não *compliance* das mesmas a normas que garantam a proteção de dados pessoais é um perigo latente a tais regimes. Isto é reforçado se levado em consideração que grandes empresas têm figurado como atores importantes no cenário político internacional. Visto o limite jurisdicional das legislações que garantam a proteção de dados pessoais, o comprometimento de tais informações ao ultrapassar fronteiras pode também estar a mercê do interesse de entes estatais, ocorrendo fora do escrutínio da lei, porém tendo consequências significativas.

Mais do que a necessidade de coibir tais práticas através da devida regulamentação, é importante entender como estas são distintas entre si. Logo, deve-se conhecer melhor quais são os interesses envolvidos na confecção e aplicação destas normas, uma vez que grandes empresas de tecnologia têm demonstrado o potencial interferir indiretamente na confecção delas por oferecerem ferramenta que possibilitem aparelhamento de cargos eleitos. A efetivação da proteção de dados então demonstra ser um problema multifacetado, abrangendo questões econômicas, políticas, jurídicas, de gestão e de informática. Este trabalho propõe-se explorar alguns problemas referentes a estas áreas do conhecimento, na expectativa de que possa avistar potenciais soluções.

2. PROBLEMAS GEOPOLÍTICOS À COOPERAÇÃO JURÍDICA INTERNACIONAL NO DIREITO DIGITAL

■ Legislações e sua aplicação são orientadas pelo que chamamos de fontes materiais do Direito. Economicamente, a transnacionalidade das regulamentações de proteção de dados pode parecer uma possível barreira de acesso ao mercado interno a uma empresa estrangeira. Tomando como exemplo a GDPR, nos seus

recitais 1º c/c 2º, 3º e 23º, pode abranger em seu escrutínio qualquer tipo de atividade com fins comerciais e de monitoramento de dados de cidadãos e residentes da União de empresa estrangeira. As possíveis sanções às violações das normas no código estabelecidas pode resultar na suspensão dos serviços da empresa estrangeira, como previsto no recital 4º. O *compliance* às normas da GDPR tornam-se uma necessidade para a continuidade de realização de práticas comerciais.

Observando os princípios da cooperação internacional e dos agentes interessados, pode-se assumir que há uma tendência dos ordenamentos jurídicos bem como empresas de convergirem na criação e aderência à normas que venham a garantir os direitos dos titulares de dados pessoais (UERPMANN-WITTZACK, 2010, p. 17). Logo, pode-se também argumentar que esta possibilidade não encontraria respaldo empírico. Numa perspectiva geopolítica, entretanto, devido ao potencial do tratamento de dados em poder influenciar em comportamentos humanos, a aplicação da legislação no tocante a empresas multinacionais de grande porte tem recebido um tratamento diferenciado, deixando evidente a instrumentalização de normas para atender a interesses nacionais.

No primeiro semestre de 2018, o mundo experimentou duas grandes crises de privacidade: em março, quando o escândalo da Facebook e Cambridge Analytica estourou, para, logo depois, em maio pela inauguração da europeia GDPR (DAVIES, 2019). O escândalo da Cambridge Analytica chamou a atenção e a indignação da mídia geral, do público, de parlamentares e legisladores de todo o planeta. As pessoas passaram a demonstrar que se preocupam com a violação de sua privacidade e possíveis abusos do poder informacional que grandes corporações detentoras de dados pessoais poderiam exercer sobre seus usuários. Esse escândalo tem sido um dentre muitos outros que indicam que a privacidade também se refere à autonomia, dignidade, empoderamento e autodeterminação das pessoas. Por essa perspectiva, a privacidade é também uma condição necessária para a democracia material. Ao mesmo tempo, a GDPR que, à época do escândalo, estava em fase de elaboração, finalmente entrou em vigor em toda a União Europeia a partir de 25 de maio de 2018, trazendo obrigações bem mais rigorosas para quem usa dados pessoais, assim como novos direitos para indivíduos, não somente na jurisdição europeia.

No Reino Unido, a Information Commissioner's Office (ICO)[2], antes mesmo da vigência da GDPR, já estava conduzindo uma investigação sobre aná-

2 A ICO no Reino Unido é a equivalente a ANPD no Brasil, sendo a instituição reguladora da proteção à privacidade e do tratamento de dados pessoais.

lise de dados para fins políticos e, quando estoura o escândalo da Cambridge Analytica, conseguiu um mandado para inspecionar as próprias instalações da empresa. Os desafios em responder imediatamente aos relatórios da Cambridge Analytica levaram, em grande parte, à ICO a concessão de poderes novos e mais fortes como o Projeto de Lei de Proteção de Dados do Reino Unido (agora a Lei de Proteção de Dados de 2018) ao passar pelo Parlamento. Em julho de 2018, a ICO publicou seu relatório Democracy Disrupted (ICO, 2018a). Na atualização da ICO sobre sua investigação em análise de dados em campanhas políticas, a ICO anunciou sua intenção de multar o Facebook por falta de transparência e segurança relacionadas à coleta de dados que violam a Data Protection Act 1998 (a lei de proteção de dados do Reino Unido em vigor em A Hora). A ICO também emitiu um aviso de execução contra o QI agregado para exigir que eles deixem de processar os dados pessoais de cidadãos do Reino Unido ou da UE obtidos de organizações políticas do Reino Unido ou de outra forma para fins de análise de dados, campanha política ou qualquer outro objetivo publicitário.

No relatório, a ICO também anunciou sua intenção de instaurar um processo criminal contra a SCL Elections (ICO, 2018a), empresa controladora da Cambridge Analytica, por não cumprir um aviso de execução emitido pela OIC para exigir que eles negociem adequadamente com a solicitação do professor David Carroll de acessar sua conta. dados. Então, em outubro de 2018, a ICO multou o Facebook em £ 500.000 por violar a lei anterior de proteção de dados do Reino Unido (ICO, 2018b). Ao discutir as inúmeras razões para impor a multa máxima, a ICO observou que "as informações pessoais de pelo menos um milhão de usuários do Reino Unido estavam entre os dados coletados e, consequentemente, corriam o risco de uso indevido". Essa multa era o máximo permitido pela lei anterior; se sua substituição, o GDPR, estivesse em vigor no momento da violação dos dados da Cambridge Analytica, a ICO poderia multar o Facebook em 4% do faturamento anual total da empresa em todo o mundo, o que seria superior a 1 bilhão de libras.

Atualmente, o Facebook está apelando dessa multa. Em novembro de 2018, a ICO publicou seu relatório ao Parlamento sobre o uso da análise de dados em campanhas políticas (ICO, 2018a). Entre suas descobertas, a ICO destacou uma desconsideração perturbadora da privacidade pessoal dos eleitores pelos atores do ecossistema da campanha política – de empresas de dados e corretores de dados para plataformas de mídia social, grupos de campanha e partidos políticos. O relatório estabelece que a ICO continua investigando a Cambridge Analytica e analisando os materiais que apreendeu no decorrer desta investigação. Em janeiro

de 2019, a ICO multou a empresa controladora da Cambridge Analytica, a SCL Elections, por não cumprir um aviso de execução da ICO e, em março de 2019, emitiu multas para a licença por voto (ICO, 2019).

Destaca-se então como o insurgente interesses na confecção da regulamentação da GDPR deu-se pelo potencial que tratamento de dados teria em interferir em processos democráticos. Tanto que em se tratando de proteção de dados, já existiam legislações tratando de proteção de dados por parte de outros países membros. Além do exemplo europeu, a instrumentalização das normas de proteção de dados pode ser vista também por parte dos Estados Unidos. No caso do "banimento da empresa Huawei", a ordem executiva em promover "Segurança da Tecnologia da Informação e Comunicação e da Cadeia de Produção" restringe a utilização de equipamentos de empresas estrangeiras que possam "armazenar comunicar vastas quantidades de informações sensíveis", qualificados também os dados pessoais (Sessão 3 – Definições, "c")[3]. Consecutivamente, adicionou a empresa chinesa na "Lista de Entidades" de restrição de comercialização do Birô de Indústria e Segurança (EUA, 2019). Sob alegação de proteger dados sensíveis, bem como a integridade do tráfego de informações em si, são alegações ofuscadas por um contexto de "guerra comercial" entre China e Estados Unidos (COWEN, 2019).

Porém, observando a legislação chinesa no tocante ao assunto, é possível notar que existem normas das quais podem sim oferecer uma possibilidade do governo legalmente exigir que empresas forneçam dados sensíveis à requisição do governo. O artigo 7 da Lei Nacional de Inteligência da China de 2017 diz que...

> ...uma organização ou cidadão deve dar suporte, assistência e cooperação ao trabalho de inteligência nacional que esta (companhia) ou ele (cidadão) saiba
> - O Estado deve proteger o indivíduo ou organização que der suporte, assistência ou cooperação ao trabalho de inteligência nacional.[4] (DONTAI, 2019).

3 Tradução livre de "*store and communicate vast amounts of sensitive information*". ESTADOS UNIDOS. Executive Order on Securing the Information and Communications Technology and Services Supply Chain, de 15 de maio de 2019. Disponível em: <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>. Acesso em: 19/08/2019.

4 Tradução livre de: "*An organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.*"

Por sua vez, no Capítulo III, art. 22 da Lei de Contra-Espionagem da China, existe a seguinte previsão:

> Quando um órgão de segurança do Estado investiga e entende que há uma situação de espionagem e coleta evidência relevante, as organizações e indivíduos relevantes devem providenciá-las veridicamente e não devem recusar-se.[5] (DONTAI, 2019).

Estas duas peças legislativas deixam claro que é possível que órgãos de segurança nacional tenham alcance sobre o controle de dados pessoais de companhias chinesas. Não obstante, é necessário estar ciente de que no que tange a transparência do sistema de direitos, de freios e contrapesos em funcionamento em seu sistema legal, há opacidade o suficiente para que o acesso aos dados aconteça sem resistência por parte de agentes estatais. Ilustrando esta situação, vale citar a notícia postada pelo comitê partidário da Suprema Corte Chinesa que alegou "traçar limites à noção ocidental de independência judicial e separação de poderes"[6].

Um importante exemplo disto é a tentativa de emulação da GDPR pela China. Na redação do art. 8, inc. 7 da Lei de Medidas de Gerenciamento de Segurança de dados, se observa que...

> A coleta e regras de uso (de dados pessoais) devem ser claras, específicas, simples e fácil de entender e acessíveis. Elas devem destacar o seguinte conteúdo: 7. Canais e métodos para que informação pessoal estejam sujeitas a uma revogação de consentimento, bem como de acesso, correção e deleção de informação pessoal.[7] (TAI et. al, 2019).

… e combinado com o art. 9º que assegura que...

---

5 Tradução de livre de: "*When the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse."* . DONTAI, Xi Jinping Thought: Implications for Chinese Trade and Relations. 2018. Tradução de: <http://www.jc.gansu.gov.cn/art/2017/3/16/art_21842_218728.html> Disponível em: <http://dontai.com/wp/2018/11/02/xi-jinping-thought-implications-for-chinese-trade-relations/>. Acessado em: 19/08/2018.

6 Tradução livre, "*A meeting of the Supreme Court's party committee on Wednesday said China would draw boundaries with the West's notion of "judicial independence" and "separation of powers", the state-run China News Service said*." (WEE, 2015).

7 Tradução livre, "Article 8: The collection and use rules shall be clear, specific, simple and easy to understand, and accessible. They shall highlight the following content: 7. Channels and methods for the personal information subject to revoke consent, as well as to access, correct, and delete personal information;" disponível em: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-se curity-management-measures/>. Acessado em: 19/08/2019.

> "Se regras de coleção e uso estão incluídas na política de privacidade, elas devem estar juntas correspondentemente e serem claras, para facilitar a redação. Operadores de rede podem coletar informação pessoal somente se os usuários forem informados da regra de sua coleta e uso, bem como explicitamente concordarem com elas" (grifo nosso)[8], (TAI et. al, 2019).

Note que em teoria existe a possibilidade do cidadão consentir e requerer exclusão de dados pessoais que estejam sob a detenção de um terceiro. Isto parece não se aplicar a programas do governo que dependem da coleta de dados pessoais, como é o sistema de crédito social. Em decisão das próprias cortes do país, mais de 5,5 milhões de pessoas foram banidas de realizar viagens, resultando no impedimento de 17,5 milhões de compras de passagens de avião e trem (KUO, 2019).

Não obstante, deve-se lembrar que as primeiras alegações de que a Huawei estava realizando coleta indevida de dados e informações datam das denúncias de Edward Snowden, que revelou a utilização por parte da Agência de Segurança Americana de *backdoors*[9] para submeter a vigilância entidades estrangeiras, inclusive a Huawei, numa operação nomeada "Shotgiant". Tais documentos apontaram que o conhecimento do governo americano de que estava havendo uma operação de coleta indevida de dados (DUNHAM et. al., 2014) foi através de uma coleta indevida de dados per si (WARDELL, 2013).

Existem também, porém, precedentes legais para a realização de tais operações nos Estados Unidos. O "Ato de Inteligência e Vigilância Estrangeira" de 1978 permite através de autorização judicial de uma corte que opera em sigilo a coleta de dados e informações sob o pretexto de segurança nacional no combate a espionagem estrangeira e terrorismo (ESTADOS UNIDOS, 2019). Documentos que vieram a ser desclassificados posteriormente expuseram como o governo americano pagou companhias multinacionais para que entrassem em *compliance* com normas de segurança nacional que lhes permitiram acesso a dados e informações de usuários de em extensão ainda não conhecida (MACASKILL, 2013). O papel das companhias multinacionais foi então chave, estas servindo também de meio para coleta, tratamento e repasse dos dados.

---

8 Tradução livre, "Article 9: If rules for collection and use are included in the privacy policy, they should be correspondingly assembled and clear, to facilitate reading. Network operators may collect personal information only after the user is informed of the rules for collection and use and explicitly agrees to them.". *Bis, idem.*

9 Um meio de acessar um sistema de computador ou de encriptação de informação que contorna os mecanismos de segurança costumeiros deste sistema. (ROUSE, 2017)

3. PROBLEMAS NA GESTÃO DE DADOS PESSOAIS NAS EMPRESAS MULTINACIONAIS DE TI

Tendo estes casos em mente, é possível observar como o cruzamento de dados pessoais influencia na produção normativa, tanto diretamente, com ações para a regulamentação das companhias que permitem coleta e tratamento destes, como indiretamente, seja pela capacidade destas companhias de eleger indivíduos que possam interferir na regulamentação. Grandes empresas de tecnologia parecem apresentar um papel duplo, tanto econômico quanto estratégico-político, podendo fornecer o aparato tecnológico necessário para realizar operações ilícitas em território estrangeiro, mas em *compliance* com as normas de uma nação rival. Devido a esta importância estratégica, multinacionais de tecnologia são confrontadas então com a escolha de como lidar com interesses de Estados nacionais conflitantes mas potenciais clientes ou limitadores ao acesso de seus respectivos mercados. O processo da gestão de dados vai consequentemente ter a interferência da direção da empresa, uma vez que as decisões em relação a *compliance* podem interferir, como visto no início do item anterior, no acesso a determinado mercado. Por muito tempo este tem sido o dilema da Google, no que diz respeito ao acesso ao mercado chinês.

A resistência oferecida num primeiro momento pela companhia em aderir às demandas de censura do governo chinês durante os anos 2000 e a mudança na direção pela incorporação ao grupo Alphabet em 2015 teve como primeira tomada de instância a mudança aparentemente simbólica do lema "Não Seja Mal" (*Don't Be Evil*), em maio de 2018. Meses depois, documentos vazados tornaram público o projeto "Libélula" (*Dragonfly)*, que tinha como objetivo lançamento de uma plataforma de pesquisa da que se adequasse às normas chinesas. O destaque neste evento foi o protagonismo dos funcionários da Google, que primeiramente em carta pública demonstraram preocupação no desenvolvimento de tal projeto, bem como repúdio a possibilidade de a companhia contribuir para a degradação de direitos trabalhando em parceria com países com histórico de violações de direitos humanos (ACKERMANN, et. al., 2018).

Este exemplo do modelo de gestão participativa da Google permite uma maior liberdade do seu empregado em assumir posições de liderança e de protagonismo na empresa. Apesar da GDPR ter figuras bem definidas como a do

controlador, processador e DPO[10], muitas decisões são de competência da chefia da empresa. A hipótese de contribuição dos demais colaboradores em construir e preservar uma política ou cultura institucional não configura uma extrapolação indevida de função. No caso em apreço, a possibilidade de expressar-se livremente, especialmente quando a cúpula de determinada organização passa a tomar decisões que podem implicar em violações legais, é uma contribuição positiva não só para a sociedade como um todo, mas para a própria lógica de gestão da empresa (MANIMALA, 2013).

Numa situação similar, a companhia tem engajado no financiamento e incentivo de desenvolvimento de tecnologia em inteligência artificial na capital chinesa, abrindo lá um laboratório de pesquisa (PENG, 2017). Em paralelo, a Google encerrou um contrato que realizava com o Pentágono também em pesquisa em inteligência artificial (GRIFFIN, 2018). Tanto o antigo contrato como o novo foram questionados por grupos de empregados da empresa, que entendiam que inteligência artificial se qualifica como uma tecnologia de "de uso duplo", ou seja, tem uma serventia tanto para fins civis quanto militares (COMISSÃO EUROPEIA, 2009). Sendo o caso da segunda finalidade, as mesmas companhias que são parcerias nas iniciativas de pesquisa em inteligência artificial na China com a Google tem também sido responsáveis pelo desenvolvimento do sistema de segurança da província de Xinjiang, onde mais de 1 milhão de cidadãos de minorias étnicas têm sido detidos em campos de concentração (GALLAGHER, 2019), o que foi possível mediante a coleta de dados sensíveis e padrões de comportamento que possibilitaram a sua identificação, categorização e então possível cerceamento de liberdade estratégico.

Na superfície, o que passa a parecer é que como é da natureza de uma empresa a busca pela maximização do lucro, demais questões éticas e de natureza legal estariam subservientes aos interesses econômicos. Porém, deve-se perguntar se a sobrevivência desta empresa, quando atingido determinado porte, passa a se tornar uma questão política devido ao interesse do ente estatal. O potencial de desenvolvimento de tecnologia e de infraestrutura, face a leis de segurança nacional outras normas que regulamentem atividades no estrangeiro, que as tratem como peça chave para determinado planejamento estratégico, talvez extrapole a convencionalidade dos modelos de gestão de proteção de dados.

10 Processador e DPO, neste caso, correspondem aos operadores e encarregados da LGPD, qualificados respectivamente nos incisos VII e VIII do art. 5 da lei.

Infelizmente, apesar da resistência e consciência por parte dos colaboradores da empresa, isto não tem sido o suficiente para poder prevenir que a mesma se associar a atividades que culminam no cerceamento de direitos humanos, quiçá aos direitos dos titulares de dados. Entretanto, devido a sua importância como multinacional, é notável como questões acerca da administração interna da companhia venha a ganhar interesse midiático, sendo possível ser neste artigo estudado por ter se tornado informação de fácil acesso. A importância da gestão de multinacionais passou a ser uma discussão sobre a gestão de dados pessoais dos milhões de usuários que dela têm utilizado serviços, tornando-se parte discussão das normas nacionais de proteção de dados. A consciência de que agentes estatais de interesses conflitantes passam a interferir diretamente

Uma situação similar pode ser o caso do Facebook e a Cambridge Analytica. Foi somente através do protagonismo de um empregado é que o caso veio a público, este tendo sido responsável por revelar como práticas que vieram a ser consideradas ilícitas pela GDPR estavam diretamente interferindo no processo democrático de diversos países. Se a violação de dados pessoais partisse de decisão de corte especial americana sob o fundamento do interesse de segurança nacional e em teor sigilo, estaria o indivíduo que reporta o vazamento de dados ou desvio de finalidade da sua utilização (como é hoje a função legal do controlador[11, 12]), incorrendo em quebra de sigilo ou de segredo de justiça? Afinal, o vazamento de dados de determinada nação pode significar o *compliance* com as normas de segurança nacional da outra[13]. Em meio a esta falta de segurança jurídica, resta então a gestão da empresa ou do protagonismo de seus membros em construir uma cultura institucional, bem como a qual orientação política a empresa se orientará para que promova certos valores em detrimento de outros.

A autonomia da empresa e seus colaboradores de tomar uma decisão é visível nestes casos, mas isto é garantido pela manutenção de liberdades individuais, transparência do processo de regulamentação e da primazia da separação das questões estatais das econômicos. Estes limites tornam-se muito menos claros em países menos democráticos, onde poder político e poder econômico tendem a se comunicar, seja pelo aparelhamento do Estado ou pelo aparelhamento de empresas. Um exemplo disto são as oligarquias russas, que controlam recursos o suficientes que são capazes de influenciar políticas públicas (RACHINSKY, 2005). Apesar de ser formalmente uma democracia, é possível observar perse-

11 Art. 33 da GPDR.
12 Art. 48 da LGPD.
13 Previsão de uso estendida pela GDPR aos estados membros da União, nos termos do art. 23.

guições sistemáticas e cerceamento seletivo de direitos, onde as estruturas que teoricamente seriam capazes de oferecer freios e contrapesos são na verdade subservientes aos poderes políticos dominantes, não havendo então "prestação de contas" por parte do poder público (BRETTER, 2005). A concentração de poder econômico também reflete na cultura de gestão deste país, onde há centralização no topo linha de comando, de onde ordens diretas são endereçadas a subordinados sem muita consulta (PAIK, 2002). O que isto tem representado para a gestão de proteção de dados, em especial dados de cidadão estrangeiros, é em falta de transparência bem como uma prática de agências governamentais em contratação de multinacionais estatais para realização de coleta indevida de dados (DOFFMAN, 2019).

Seguindo esta mesma tendência, uma pesquisa de Balding e Clarke (2019) tentou responder através de pesquisa em registros disponibilizados publicamente a propriedade da Huawei com objetivo de conferir se esta tinha conexões com o governo chinês, uma das alegações que fundamentaram as represálias impostas à empresa pelo governo americano. De acordo com a pesquisa, há uma escassez de informação publicamente disponíveis de como se dá a governança dentro da empresa. Entretanto, dentro do que é sabido, teoricamente todos funcionários têm participação nos lucros através de ações administradas pela entidade sindical da qual estes estão vinculados compõem a mesa diretora da empresa, bem como exercer em nome dos empregados os direitos de voto (BALDING, 2019, p. 6). Membros sindicais, por sua vez, respondem à Federação Chinesa Sindical, que tem controle exercido diretamente pelo Partido Comunista Chinês. Este partido, por sua vez, é o líder do "sistema de cooperação multipartidário" (WIPO, p. 3), logo, o protagonista principal na governança do país.

Comparando estes dois cenários, modelos de gestão mais democráticos, comumente implementados em multinacionais de países de democracias já consolidada, têm proporcionando maior transparência quanto a práticas adotadas. Nestes modelos, problemas quanto a violação de privacidade de usuários acabaram por vir a superfície, seja através de autoridades reguladoras, judiciário ou até ações individuais ou organizadas de empregados, situação somente possível com um empoderamento dos mesmos suficiente, seja através da mídia ou seja através de instâncias representativas. Lembrando que, independente do modelo de gestão, vazamentos e utilização indevida de dados pessoais vem acontecendo com uma frequência regular, tendo em vista que estes incidentes não dizem respeito somente a uma situação administrativa da empresa, mas também uma questão de segurança da informação.

4. SOLUÇÕES DE TECNOLOGIA PARA PROTEÇÃO DOS DIREITOS DOS TITULARES

■ Os debates acerca de quais modelos de gestão seriam adequados para o tratamento de dados pessoais pode ser dirimido se considerado o uso "privacidade desde a concepção (*privacy by design*). Tal conceito fora talvez explorado pela primeira vez por Ronald Hes (2000), que citou a possibilidade de implementação de determinadas ferramentas para diminuir a possibilidade de uma plataforma ser um ponto possível de comprometimento de dados pessoais. Uma característica interessante para a companhia que utiliza de uma tecnologia que lhe impossibilita de alguma maneira de tratar diretamente dos dados de usuários pode lhe impedir de confrontar questões éticas das quais possa a colocar numa situação em que esta deva escolher *compliance* entre diferentes normas. Este foi o caso do Whatsapp no Brasil, que por usar de tecnologia P2P na sua comunicação, não sofreu as sanções de descumprimento previstas no art. 12 do Marco Civil, bem como não tinha meios de fornecer as informações pelas autoridades requeridas fossem interceptadas (STF, 2016).

Das ferramentas observadas, pode-se citar o uso de assinaturas digitais para que possa encriptar os dados do titular de maneira que estes possam somente ser operados pela plataforma da qual o consentimento fora concedido. Da mesma maneira pode ser utilizada uma assinatura digital cega, em que a identidade do titular nunca seja compartilhada, mas o fato de ter realizado a assinatura seja a chave para acessar determinado serviço que tenha os dados pessoais como imprescindível. Ou então, o uso de um pseudônimo digital, que teoricamente teria efeito similar quanto a ocultação da identidade do usuário. De maneira genérica, o autor destaca que soluções mais complexas possam ser evitadas se houver uma minimização estratégica da quantidade de dados a serem coletados para se atingir determinado fim, incorrendo na hipótese de que os dados coletados nunca sejam o suficiente para poder identificar um indivíduo. Em todo caso, se determinada plataforma implementar um pseudo-domínio que permita anonimização dos dados coletados, este não pode permitir que quaisquer informações sejam ventiladas – tanto por falha do programa, quanto por uma individualização de algum processo computacional que resulte numa variável que dê unicidade aos dados coletados, tornando possível identificação.

Um exemplo prático destas diretrizes seria na utilização de VPNs. As *Virtual Private Networks* (VPNs)[14] estão se tornando cada vez mais comuns enquanto solução de transporte de dados eficiente na atual infraestrutura da *internet*. Essas VPNs usam a infraestrutura de rede pública dos provedores de serviços de *internet* para estabelecer serviços seguros e confiáveis de acordo com os Contratos de Nível de Serviço[15] assinados. Nessas redes, o gerenciamento de recursos é um dos principais desafios enfrentados pelos provedores, onde cada VPN pode ter diferentes requisitos, juntamente com uma enorme diversidade de garantias de serviço, a depender do tipo e do modelo de negócio, bem como das tecnologias envolvidas. As crescentes demandas por estes serviços de VPN com certos requisitos de satisfação e de manutenção da qualidade do serviço demandam que os provedores utilizem eficientemente seus recursos de largura de banda. Modelos para fornecer esquemas eficientes e eficazes de alocação de recursos são de máxima relevância. Baseando-se nos atuais modelos de gestão, que tentam interações diretas com os provedores, é possível identificar alguns problemas ligados há limitações ligadas ao custo e à eficácia, em termos de tempo de resposta. Essas limitações podem levar a altos índices de insatisfação dos usuários. Dessa forma, nos últimos anos, tem havido um crescente interesse em fornecer modelos eficientes de gerenciamento automatizado para alocação de recursos em VPNs. Entretanto, apesar de representarem uma solução viável, estudos mostraram que de tais plataformas ainda são susceptíveis a falhas a serem exploradas, existentes de maneira deliberada ou não, que podem acabar por comprometer a identidade dos usuários (IKRAM, 2016). Esbarra-se de outra maneira no mesmo problema anteriormente estudado, que é a confiança na governança da companhia, apesar de reduzir o risco ao desenho do aplicativo.

Tendo em consideração a necessidade da utilização de um código aberto, governança de maneira distribuída, transparência e supervisão independente, pode-se esboçar uma solução com base em tecnologia *blockchain,* utilizando-se de um *smart contract* para gerenciamento automatizado da plataforma. Nesta hipótese, a rede poderia oferecer três tipos de *tokens*: o primeiro, que funcionaria

14 Redes Privadas Virtuais são redes de comunicação privadas construídas sobre uma rede de comunicação pública. Assim, o tráfego de dados é feito através da rede de comunicação pública, seguindo seus protocolos padrões. Funciona como se fosse um túnel construído sobre uma infraestrutura pública, como a *internet*.

15 Contratos de Nível de Serviço são contratos típicos assinados entre um prestador de serviços de TI e seu usuário. O objeto do contrato é o tipo e as características do serviço, seus níveis de qualidade, as responsabilidades, direitos e deveres das partes, bem como eventuais compensações caso o nível da qualidade do serviço não seja mantido.

como as ações preferenciais sem direito a voto, dispostas no art. 15, §2º da Lei n.º 6.404/76, disponíveis as empresas que tivessem interesse de veicular propaganda direcionada, por exemplo, sendo calculada por um algoritmo que adequaria a oferta e demanda a determinado público alvo recortado do conjunto de dados pessoais que encriptados de maneira pseudo-anônima na *blockchain.* O segundo tipo de *token* seria emitido para desenvolvedores de aplicações e da plataforma, tendo estes direito a voto, sendo possível então a gestão direta da plataforma. Estes seriam recompensados com *tokens* do tipo 1 a depender do quanto significativa for a contribuição para a plataforma, cuja avaliação seria feita pelos seus pares (outros desenvolvedores), e talvez usuários e as próprias empresas que estariam interessadas na contratação dos serviços que necessitassem do tratamento de dados. O terceiro tipo de *token* seria disponibilizado para os mineradores, bem como outros que disporiam não só de poder de processamento que seria necessário para o tratamento, mas também espaço em disco para o armazenamento dos dados armazenados na plataforma. Diferente da proposta anterior, aqui incorre-se em todos os problemas atualmente atrelados ao desenvolvimento de plataformas de tecnologia *blockchain,* como a complexidade da tecnologia possibilitando a existência de falhas, a escalabilidade da rede, custos ou velocidade de transação e até na permanência dos usuários em torno do mesmo protocolo de consenso, evitando *forks* que potencialmente comprometessem a rede.

Uma outra solução que não depende de tecnologia *blockchain* mas de regulamentação residiria também predileção a ferramentas que não as do controlador, mas sim de terceiros autorizados cujo escrutínio público lhes garantisse permissão de tratamento dos dados. Este terceiro se limitaria ao armazenamento e tratamento, somente a realizando quando a empresa interessada e o usuário final demonstrassem interesse na realização do serviço. Este terceiro teria o desenvolvimento da plataforma, gestão e transparência gerido por entidade internacional ou nacional que pudesse operar livremente cujo único objetivo seria garantir a proteção dos dados pessoais e o desenvolvimento da tecnologia. Nesta última hipótese restaria questionar se a concentração dos dados num só "alvo" resultaria em dados bem mais significativos do que o modelo atualmente desordenado de coleta e tratamento de dados.

CONCLUSÃO

■ Através deste estudo, é perceptível como a gestão de dados pessoais impõem problemas significativos na gestão de empresas multinacionais de tecnologia, bem

como possíveis barreiras de mercado e dilemas éticos vez em que a própria tecnologia pode acabar sendo subvertida para violação dos direitos dos titulares de dados, direitos humanos ou até comprometimento de processos democráticos. Este poder dá contornos a um cenário internacional em que estas companhias passam de coadjuvantes a protagonistas, não só sendo operacionalizadas para fins de garantir interesses Estatais, mas prevalecendo-se de uma liberdade em adequar-se a situações econômica e politicamente mais interessantes possíveis. Leis de proteção de dados e demais normas tornam-se então ferramentas de política internacional, não prezando pelos princípios da cooperação internacional e dos agentes interessados, tornando a efetiva garantia dos direitos dos titulares uma questão secundária. Dito isto, não significa que não houve ganhos a garantias individuais. Aqui, discute-se, fundamentalmente, as motivações de tais normativas.

Observada possíveis soluções ao problema, tendo em consideração que a proibição do uso de determinada tecnologia é ainda muito difícil de ser observado à nível de *software,* privacidade desde a concepção pode ser a chave para soluções de privacidade, não deixando à mercê da volição que não a do titular a disposição dos dados pessoais. Tal solução, porém, requer desenvolvimento de tecnologias e métodos de gestão a elas integrados, levando em consideração também que multinacionais não necessariamente teriam interesse de adotar tais ferramentas. Levando em consideração como coisas como propaganda direcionada podem acabar influenciando em processos democráticos, assim sendo processo regulatórios, é imperativo que usuários e empregados tenham como meta empoderar-se em relação à estas multinacionais de tecnologia, bem como sempre foi o fenômeno de luta por direitos face a entidades estatais.

Maria Amália Oliveira de Arruda Camara · Doutora em Ciência Política (2012) e em Direito (2010) pela Universidade Federal de Pernambuco (UFPE). Professora no Curso de Direito da Universidade de Pernambuco (UPE). Gerente de Desenvolvimento da Pró-Reitoria de Extensão da UPE. Membro de corpo editorial da Revista de Extensão da UPE. Coordenadora do grupo de pesquisa e extensão Smart Cities - Cidades Inteligentes/UPE. Coordenadora da pós-graduação em Direito Digital pela Faculdade Egas Moniz. amalia.camara@upe.br

Walter de Macedo Rodrigues · Professor da pós-graduação em Direito Digital pela Faculdade Egas Moniz. Pesquisador do Grupo Direito e Conflitos Oriundos da Pós-Modernidade pela UPE, certificados pelo CNPq. Coordenador do Grupo de Pesquisa em Democracia Líquida pela Liga Pernambucana de Direito Digital. Possui graduação em Direito pela Universidade Federal de Pernambuco (2019), atuando principalmente nos seguintes temas: Direitos Digital, Direito Econômico e pesquisa empírica em Direito. mrwalterde@outlook.com

BIBLIOGRAFIA

ACKERMANN, Rebecca. We are Google employees. Google must drop Dragonfly. Medium, 2018. Disponível em: <https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-mu st-drop-dragonfly-4c8a30c5e5eb>. Acesso em: 19/08/2019.

AHLGREN, Matt. 20 + Facebook estatísticas e fatos para 2019. W. 2 de abril de2019. Disponível em: <https://www.websitehostingrating.com/pt/facebook-statistics/>. Acesso em: 7 de maio de 2019.

BALDING, Christopher et. al. Who Owns Huawei. Social Science Research Network. ISSN 1556-5068. 8 de maio de 2019. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669>. Acesso em: 19/08/2019.

BAUERLE, Nolan. What are Blockchain's Issues and Limitations? Coindesk, 2019. Disponível em: <https://www.coindesk.com/information/blockchains-issues-limitations>. Acesso em: 19/08/2019.

BLAKE, S.; BLACK, D.; CARLSON, M.; DAVIES, E.; WANG, Z.; WEISS, W. An architecture for differentiated services. Network Working Group RFC 11 (5: December) (1998) 2475.

BORGESIUS, Frederik J. Zuiderveen et al. Online Political Microtargeting: Promises and Threats for Democracy. Utrecht Law Review. Vol. 14. Ed. 1. Amsterdam: 2018. Disponível: https://www.ivir.nl/publicaties/download/UtrechtLawReview.pdf. Acessado: 23/08/2019.

BOSS, A. H.; KILIAN, W. The United Nations Convention on the Use of Electronic Communications in International Contracts became effective with respect to 5 states. EU has not become party to that convention. 2008. Disponível em: <http://www.uncitral.org/pdf/english/texts/electcom/ 06-57452_Ebook.pdf>. Acesso em :23 de agosto de 2019.

BOUILLTE, E.; MITRA, D.; RAMAKRISHNAN, K. The structure management of service level agreements in networks. IEEE Journal on Selected Areas in Communications 20 (4: Jun) (2002) 691–699.

BOYLES, J. L.; SMITH, A.; MADDEN, M. Apps and privacy: More than half of app users have uninstalled or decided to not install an app due to concerns about their personal information. Internet & Technology. Pew Research Center. Disponível em: <http://www. pewinternet.org/2012/09/05/main-findings-7/>. Acesso em: 11 de maio de 2019.

BRETTER, Zoltán. Hungary and Poland in Times of Political Transition. Selected Issues. PAJĄK-PATKOWSKA, Beata et. al. Faculdade de Ciência Política e Jornalismo da Universidade Adam Mickiewicz. Poznan: 2016. Disponível em: <http://helwecja.amu.edu.pl/wp-content/uploads/2013/05/Hungary-and-Poland_tre%C5%9B%C4%87.pdf>. Acesso em: 19/08/2019.

CAVOUKIAN, Ann. Privacy by Design – The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices.

CHAPPEL, Chris. China Uncensored. 2019. Disponível em:<https://www.youtube.com/channel/UCgFP46yVT-GG401TgXn-04Q>. Acesso em: 19/08/2019.

CHENG, Y.; ZHUANG, W. ; LEON-GARCIA, A.; HU, R.Q. Efficient resource allocation for sla based wireless/wireline interworking. Proceedings of the Second IEEE International Conference on Broadband Networks, 1 (2005) pp. 561–570.

COMISSÃO EUROPEIA. Regulamento (CE) nº 428/09 do Conselho de 5 de Maio de 2009: qe cria um regime comunitário de controlo das exportações, transferências, corretagem e trânsito de produtos de dupla utilização. Bruxelas: Jornal Oficial da União Europeia, 2009. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Acx0005> Acesso em: 19/08/2019.

COWEN, Tyler. What the U.S.-China Trade War is Really About. Bloomberg Opinion: Politics & Policy. 15 de julho de 2019. Disponível em: <https://www.bloomberg.com/opinion/articles/2019-07-15/u-s-china-trade-war-s-main-i ssues-are-taiwan-and-huawei>. Acesso em: 19/08/2019.

DAVIES, Tom. One Year on from the Cambridge Analytica Scandal. PrivSec Report. 18 de março de 2019. Disponível em: <https://gdpr.report/news/2019/03/18/one-year-on-from-the-cambridge-analytica-scand al/>. Acesso em: 01/09/2019

DINEV, T.; MCCONNELL, A. R.; SMITH, H. J. Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. Information Systems Research, 26(4), 639–655., 2015. Disponível em: <https://doi.org/10.1287/ isre.2015.0600>. Acesso em: 11/07/2019.

DOFFMAN, Zak. Russia's Secret Intelligence Agency Hacked: Largest Data Breach In Its History. Forbes, 2019. Disponível em: <https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/#1d3bcf06b115>. Acesso em: 19/08/2019.

DONTAI. Huawei and US National Security: Thoughts. 2019. Disponível em: <http://dontai.com/wp/2019/05/23/huawei-and-us-national-security-thoughts/>. Acesso em: 19/08/2019.

DUNHAM, Will et. al. NSA infiltrates serves of China telecom giant Huawei: report. Washington: Reuters, 22 de março de 2014. Disponível em: <https://www.reuters.com/article/us-usa-security-china-nsa/nsa-infiltrates-servers-of-chi na-telecom-giant-huawei-report-idUSBREA2L0PD20140322>. Acesso em:

EMARKETER. Most mobile users will delete an app if concerned about security: Users are asked to share different types of information when downloading apps. Retail & Ecommerce: Mobile. Diaponível em: <https://www.emarketer.com/Article/ Most-Mobile-Users-Will-Delete-App-Concerned-About-Security/1013488>. Acesso em: 01 de setembro de 2019.

ESTADOS UNIDOS. Addition of Certain Entities to the Entity List (final rule), de 16 de maio de 2019. Bureau of Industry and Security, U.S. Department of Commerce. Disponível em: <https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019>. Acesso em: 19/08/2019.

ESTADOS UNIDOS. Executive Order on Securing the Information and Communications Technology and Services Supply Chain, de 15 de maio de 2019. Disponível em: <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>. Acesso em: 19/08/2019.

ESTADOS UNIDOS. Foreign Intelligence Surveillance Act. Atualizado por Steven Aftergood, em 20 de maio 2019. Disponível em: <https://fas.org/irp/agency/doj/fisa/>. Acesso em: 19/08/2019.

EUROPEAN PARLIAMENT. PS_TA-PROV(2018)0433. Texts Adopted – Provisional Edition. Disponível em: <http://www.europarl.europa.eu/doceo/document/TA-8-2019-0441_EN.html>. Acessado em: 19/08/2019.

FEDERAL TRADE COMMISSION. Path social networking app settles FTC charges it deceived consumers and improperly collected personal information from users' mobile address books. Federal Trade Commission: Protecting America's Consumers. 28 de fevereiro de 2013. Disponível em: <https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived>. Acesso em: 4 de junho de 2019.

GALLAGHER, Ryan. Google Employees Uncover Ongoing Work on Censored China Search. The Intercept, 4 de março de 2019. Disponível em: <https://theintercept.com/2019/03/04/google-ongoing-project-dragonfly/>. Acesso em: 19/08/2019.

GALLAGHER, Ryan. Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal. The Intercept, 1 de agosto de 2018. Disponível em: <https://theintercept.com/2018/08/01/google-china-search-engine-censorship/>. Acesso em: 19/08/2019.

GALLAGHER, Ryan. How U.S. Tech Giants are Helping to Build China's Surveillance State. The Intercept. 2019. Disponível em: <https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/>. Acesso em: 19/08/2019.

GOOGLE. Community Guidelines. Disponível em: <https://about.google/community-guidelines/>. Acesso em: 19/08/2019.

GRIFFIN, Erin. Google won't Renew Controversial Pentagon AI Project. Wired, 2018. Disponível em: <https://www.wired.com/story/google-wont-renew-controversial-pentagon-ai-project/>. Acesso em: 19/08/2019.

HAUNG, Y.; HO, J. Distributed call admission control for a heterogeneous pcs network. IEEE Transaction on Computing 51 (12: Nov) (2002) 1400–1409.

HERN, A. Far more than 87m Facebook users had data compromised, MPs told. The Guardian. 17 de abril de 2018. Disponível em: <https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica>. Acesso: 7 de julho de 2019.

HES, Ronald et. al. Privacy-Enhancing Technologies: The path to Anonymity. Haia: Registratiekamer, V. 11., agosto de 2000. Disponível em: <https://www.researchgate.net/publication/243777645_Privacy-Enhancing_Technologies_The_Path_to_Anonymity/link/56e6850708ae68afa1138167/download>. Acesso em: 19/08/2019.

IKRAM, Muhammad et. al. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. CSIRO. Santa Monica: Proceedings of the 2016 Internet Measurement Conference, p. 349-364, 2016. Disponível em: <http://dx.doi.org/10.1145/2987443.2987471>. Acesso em: 19/08/2019.

INFORMATION COMMISSIONER'S OFFICE. ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information. 25 de outubro de 2018b. Disponível em: <https://ico.org.uk/facebook-fine-20181025>. Acesso em: 01/09/2019.

INFORMATION COMMISSIONER'S OFFICE. Investigation into the use of data analytics in political campaigns: a report to Parliament. 6 de novembro de 2018a. Disponível em: <https://ico.org.uk>. Acesso em: 01/09/2019.

INFORMATION COMMISSIONER'S OFFICE. SCL Elections prosecuted for failing to comply with enforcement notice. 9 de janeiro de 2019. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-election s-prosecuted-for-failing-to-comply-with-enforcement-notice/>. Acesso em: 01/09/2019.

JEE, Charlotte. China's Social Credit System Stopped Millions of People from Buying Travel Tickets. MIT Technology Review: Artificial Intelligence, Cambridge: 2019. Disponível em: <https://www.technologyreview.com/f/613070/chinas-social-credit-system-stopped-millions-of-people-buying-travel-tickets/>. Acessado: 19/08/2019.

KOBIE, Nicole. The Complicated Truth about China's social credit system. WIRED: 2019. Disponível em: <https://www.wired.co.uk/article/china-social-credit-system-explained>. Acesso em: 19/08/2015.

KUCHLER, H. Software bug made millions of Facebook users' private posts public: As many as 14m users were affected by the error, which was not caught for 10 days. Financial Times. Disponível em: <https://www.ft.com/content/49749f5e-6a8b-11e8-b6eb-4acfcfb08c11>. Acesso em: 01/09/2011.

KUO, Lily. China bans 23m from buying travel tickets as part of 'social credit' system. Beijing: The Guardian, 1 de março de 2019. Disponível em: <https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system>. Acesso em: 19/08/2019.

LAI, F.S.; MISIC, J.; CHANSON, S.T. Complete sharing versus partitioning: quality of service management for wireless multimedia networks. Proceedings of the 7th IEEE International Conference on Computer Communications and Networks, (1998).

MACASKILL, Ewen et al. Snowden document reveals key role of companies in NSA data collection. New York: The Guardian, 1 de novembro de 2013. Disponível em: <https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms>. Acesso em: 19/08/2019.

MACASKILL, Ewen. NSA paid millions to cover Prism compliance costs for tech companies. New York: The Guardian, 23 de agosto de 2013. Disponível em: <https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-pai d>. Acesso em: 19/08/2019.

MANIMALA, Mathew, J. et. al. Distributed leadership at Google: Lessons from the billion-dollar brand. Ivey Business Journal: Improving the Practice of Management. ed. Maio, 2013. Disponível em: <https://iveybusinessjournal.com/publication/distributed-leadership-at-google-lessons-fr om-the-billion-dollar-brand/>. Acesso em: 19/08/2019.

MARK, J.W.; WONG, T.C.; JIN, M.; BENSAOU, B.; CHUA, K.C. Resource allocation for multiclass services in cellular systems. Proceedings of the IEEE International Conference in Communication Systems, (2000).

PAIK, Yongsun. et. al. Comparing US and Russian management styles: the influence of cultures on cooperative business ventures. International Journal of Human Resources Development and Management. DOI: 10.1504/IJHRDM.2002.001036. Vol 2. Ed. 3-4. 2002. Disponível em: <https://www.inderscienceonline.com/doi/pdf/10.1504/IJHRDM.2002.001036>. Acesso em: 19/08/2019.

PENG, Tony. Google Opens China AI Center. Medium. 2017. Disponível em: <https://medium.com/syncedreview/google-opens-china-ai-center-8af187b66970>. Acesso em: 19/08/2019.

PRIVACY INTERNATIONAL. Cambridge Analytica, GDPR – 1 year on – a lot of words and some action. 30 de abril de 2019. Disponível em: <https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-l ot-words-and-some-action>. Acesso em: 01 de setembro de 2019.

RACHINSKY, Andrei, et. al. The Role of Oligarchs in Russian Capitalism. Journal of Economic Perspectives. Vol. 19. Nº 1. 2005. p. 131-150. Disponível em: <http://econ.sciences-po.fr/sites/default/files/file/guriev/GurievRachinsky.pdf>. Acesso em: 19/08/2019.

ROUSE, Margaret. Backdoor (computing). SearchSecurity, 2017. Disponível em: <https://searchsecurity.techtarget.com/definition/back-door>. Acesso em: 19/08/2019.

SHERIDAN, Kelly. Businesses Calculate Cost of GDPR as Deadline Looms. DarkReading.com. 12 DE ABRIL DE 2018. DISPONÍVEL EM: <https://www.darkreading.com/risk/businesses-calculate-cost-of-gdpr-as-deadline-looms/d/d-id/1331527?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>. Acesso em:04/08/2019.

SUPREMO TRIBUNAL FEDERAL. Audiência Pública: Marco Civil da Internet, Ação Direta de Inconstitucionalidade 5.527. Min. Rel. Rosa Weber. Bloqueio Judicial do Whatsapp. Arguição de Descumprimento de Preceito Fundamental 403. Min. Rel. Edson Fachin. Disponível em: <http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf>. Acessado em: 19/08/2019.

THE GUARDIAN. Watchdog investigates links between Canadian data firm and Vote Leave. 11 de julho de 2018. Disponível em: <https://www.theguardian.com/technology/2018/jul/11/watchdog-investigates-links-between-data-firm-aggregateiq-and-leave-campaigns>. Acesso em: 01/09/2019.

UERPMANN-WITTZACK, Robert. Principles of Internacional Internet Law. Vol. 11. Issue 11. German Law Journal. DOI: doi:10.1017/S2071832200020204. Disponível em: <https://www.cambridge.org/core/journals/german-law-journal/article/principles-of-inte rnational-internet-law/3E9B0ED4BABDC582FA1A053DDD454987>. Acesso em: 19/08/2019.

WARDELL, Jane. Former CIA boss says aware of evidence Huawei spying for China. Sydney: Reuters, 19 de julho de 2013. Disponível em: <https://www.reuters.com/article/us-huawei-security/former-cia-boss-says-aware-of-evidence-huawei-spying-for-china-idUSBRE96I06I20130719>. Acesso em: 19/08/2019.

WEE, Sui-Lee. China's top court says no to West's model of judicial independence.

Beijing: Reuters, 2015. Disponível em: <https://in.reuters.com/article/china-law/chinas-top-court-says-no-to-wests-model-of-judicial-independence-idINKBN0LU07M20150226>. Acesso em: 19/08/2019.

WIPO. The Constitution law of People's Republic of China. 2019. Disponível em: <https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn147en.pdf>. Acesso em: 19/08/2019.

WORLD ECONOMIC FORUM. In 2020, Asian economies will become larger than the rest of the world combined – here's how. Disponível em: <https://www.weforum.org/agenda/2019/07/the-dawn-of-the-asian-century/>. Acesso em: 06 de agosto de 2019.

Os dados no contexto da quarta revolução industrial

ANTONIO RAMALHO DE SOUZA CARVALHO

RESUMO

■ Normalmente, a quarta revolução industrial é compreendida como sendo a convergência das tecnologias dos mundos digitais, físicos e biológicos, onde os dados são elementos fundamentais de sua consolidação. Nesta nova realidade, a importante questão tratada neste artigo é como lidar com os dados, no contexto da quarta revolução industrial, a partir de sua aplicação. A metodologia de pesquisa adotada foi o estudo dos dados e sua aplicação, com ênfase na ética, a partir de diferentes fontes de evidências. Em primeiro lugar, foi estudado os elementos da quarta revolução industrial, tendo como base diferentes teóricos, para em seguida, compreender sobre a aplicação dos dados. Ao final do artigo, verificou-se que os dados permeiam o mundo físico e digital, dentro de um verdadeiro ecossistema, em um ciclo de vida que abrange desde a produção dos dados até o seu descarte. Os dados impactam diretamente no desenvolvimento da economia e na estabilidade social, oferecendo oportunidades e ameaças. Novos termos passam a configurar na realidade da quarta revolução industrial, entre eles a Computação em Nuvem, o Big Data, a Inteligência Artificial, a Mineração de Dados, Internet das Coisas, Aprendizado de Máquinas, Ataques Cibernéticos e Proteção de Dados Pessoais, demonstrando a importância da aplicação dos dados.

ABSTRACT

■ Usually, the fourth industrial revolution is understood as the convergence of the technologies of the digital, physical and biological worlds, where data are fundamental elements of its consolidation. In this new reality, the important issue addressed in this article is how to deal with the data, in the context of the fourth industrial revolution, from its application. The research methodology adopted was the study of data and its application, with emphasis on ethics, from different sources of evidence. Firstly, we studied the elements of the fourth industrial revolution, based on different theorists, and then to understand about the application of data. At the end of the article, it was found that the data permeate the physical and digital world, within a true ecosystem, in a life cycle that ranges from the production of data to its disposal. The data directly impact the development of the economy and social stability, offering opportunities and threats. New terms come to form in the reality of the fourth industrial revolution, among them Cloud Computing, Big Data, Artificial Intelligence, Data Mining, Internet of Things, Machine Learning, Cyber Attacks and Protection of Personal Data, demonstrating the importance of applying the data.

INTRODUÇÃO

■ A quarta revolução industrial não é apenas sobre novos meios de produzir e processar dados ou sobre automatizar e desenvolver robôs autônomos, trata-se da conectividade de uma demanda cada vez mais intensa e mais transparente solicitada pela sociedade pela transformação social, estrutural e tecnológica que atenda ao propósito de cada ser humano e de cada ser vivo, numa clara configuração de um ecossistema onde o virtual e o físico se complementam.

Tudo o que fazemos tem contrapartida no mundo físico e digital, do amanhecer ao anoitecer. Nossas ações constantemente criam dados que migram para algum lugar, gerando soluções, facilidades e alternativas de consumo. Torna-se praticamente impossível os titulares controlarem seus próprios dados.

Estudiosos estimam que, em dez anos, existirá uma grande transformação da indústria, onde os dados *off-line* passarão a ser *on-line*, o que gerará cada vez mais dados que, por sua vez, poderão ser usados de forma inteligente para levar a ajustes internos e melhorias de performance.

Os dados são o novo petróleo, mantra repetido por consultores, executivos e interessados na digitalização. Para Ajay Banga, CEO da Mastercard, a compara-

ção faz sentido, exceto por um pequeno detalhe: "A diferença é que o petróleo vai acabar um dia. Os dados, não"[1].

Com a necessidade crescente da busca de soluções otimizadas e facilidades operacionais, as organizações incorporam-se de dados e tecnologias gerados em prol da transformação digital, posicionando-se, mesmo que de forma embrionária, na quarta revolução industrial, o que representa um desafio vital para a sociedade, sendo que, mais do que os aspectos tecnológicos que a singulariza, é um processo que depende de uma eficiente compreensão pelas pessoas.

Trata de uma onda de transformação surfada no barateamento, miniaturização e aumento da capacidade de produção de dados.

Nesse cenário de transformação, os sistemas convencionais de produção tornam-se gradualmente obsoletos, devido ao surgimento de novos processos, novos produtos e novos modelos de negócios emergentes da estratégia digital, ou seja, o processo produtivo automatizado migra para um processo decisório de investimento em tecnologias, com base em infinitos dados que estão disponíveis em tempo real. Lembrando, nem todos os dados levantados pesam igualmente em um processo decisório, entretanto devem ser utilizados de maneira consciente e competitiva.

A quarta revolução industrial não é uma opção. Ela já é uma realidade e todo o setor produtivo deve estar mobilizado para que o país esteja apto a acompanhar esta nova revolução. "Entendemos que inovar e fazer acontecer a indústria do futuro é um compromisso que deve mobilizar a todos [...]", conforme palavras de Ricardo Alban, presidente da Federação das Indústrias do Estado da Bahia – FIEB, quatriênio 2018-2022[2].

Ter o olhar para a quarta revolução industrial, também conhecida como Indústria 4.0, Manufatura Avançada, Indústria Inteligente, Era do *Big Data* ou da Internet das Coisas, entre outras nomenclaturas, é ter obrigatoriamente um olhar para uma nova gestão das organizações, onde pessoas, dados e tecnologias se complementam em suas ações e finalidades, sendo os dados transformados em inteligência competitiva aplicada em diferentes segmentos.

---

1 Afirmação feita por Ajay Banga, CEO da Mastercard, durante o Master Minds, evento de inovação da Mastercard realizado em São Paulo – Brasil, no dia 05 de julho de 2019. Revista Época Negócio de 05/07/2019. Disponível em https://epocanegocios.globo.com/Empresa/noticia/2019/07/

2 ESTÚDIO CORREIO. Rumo à quarta revolução industrial: Empresas terão que se adaptar à Indústria 4.0, já em curso, para viabilizar os negócios e a competitividade. 25 maio 2018. Disponível em: https://www.correio24horas.com.br/noticia/nid/rumo-a-quarta-revolucao-industrial Acesso em 26 maio 2018.

Para que os líderes consigam alocar os esforços numa migração da informatização para uma resposta autônoma de resultados, é importante entender o que a quarta revolução industrial envolve o comportamento das pessoas, a transformação dos dados em inteligência competitiva e as tecnologias habilitadoras da transformação digital. Diante do disposto, a questão importante a ser tratada neste artigo é como lidar com os dados, no contexto da quarta revolução industrial, a partir de sua aplicação.

A metodologia adotada neste artigo foi o estudo da aplicação dos dados, com ênfase em ética e aplicação dos dados. Trata de um estudo do tema "dados" com foco temporal a partir de 2011, quando termo indústria 4.0 foi cunhado na Alemanha.

Esta forma de investigação tem por si mesma um caráter particularizador, já que seu poder de generalização é limitado na medida em que a validade de suas conclusões permanece contingente. As etapas do estudo foram assim conduzidas (MIGUEL, 2007, p. 221):

- definição da estrutura conceitual teórica, tendo como tema central os "dados" na quarta revolução industrial;
- planejamento do caso, a partir do problema de pesquisa, tendo como delimitador a realidade nacional;
- coleta de informações por meio de uma observação direta e fontes de evidências, tais como documentos, relatórios e contato direto com pessoal envolvido em áreas do conhecimento da quarta revolução industrial;
- análise das informações coletadas apoiado na base teórica pesquisada;
- descrição do papel fundamental da aplicação dos dados.

O delineamento da pesquisa apoiou-se em diferentes fontes de evidências, com ênfase na quarta revolução industrial. Ao escolhê-las, familiariza-se com cada um dos elementos, considerando-as como entidades autônomas, que interagem entre si (EISENHARDT, 1989).

QUARTA REVOLUÇÃO INDUSTRIAL

■ Cada revolução industrial é consequência da transformação de dois vetores: tecnologia e organização social (SIMÃO FILHO; PEREIRA, 2014, p. 45). Tendo como base esses setores:

- a primeira revolução industrial: foi provocada pelo surgimento da máquina a vapor e início do desenvolvimento do pensamento econômico liberal, com a publicação, por Adam Smith, da obra "*An inquiry into the nature and cause of the wealth of Nations*";
- a segunda revolução industrial: teve início no início do século XX, impulsionada pela linha de montagem e pela proposta de Frederick Taylor na utilização de métodos cartesianos na administração de empresas;
- a terceira revolução industrial: iniciou na década de 60 do século XX, como a robotização e automação, tendo como organização social o plano de Marshall, que gerou o fluxo de investimentos e o impulso pela inovação;
- a quarta revolução industrial: da qual a sociedade vive no momento, é defendida por Schwab como sendo a convergência das tecnologias dos mundos digitais, físicos e biológicos (SCHWAB, 2017, p.23). Os três fatores que sustentam essa revolução, ou indústria 4.0, é assim apresentada por Schwab: velocidade das mudanças e da interconexão, criando um círculo virtuoso e acelerado de progresso tecnológico; amplitude e profundidade da mudança, capaz de produzir inovações em uma alta frequência; impacto sistêmico, com transformações de sistemas inteiros entre países, dentro deles, na sociedade nas organizações e nos indivíduos. A quarta revolução industrial ainda não apresenta claramente o vetor organização social (BARBOSA; BAISSA, ALMEIDA, 2018, p. 3)

As principais tecnologias associadas à quarta revolução industrial, segundo Schwab (2017, p. 23) estão relacionadas a três mundos (digital, físico e biológico):

- Internet das coisas: onde objetos do nosso dia-a-dia passam a se conectar por intermédio da Internet (mundo digital);
- Blockchain: solução que interliga interessados sem a necessidade de intermediários e que busca a desburocratização (mundo digital);
- Plataformas digitais: ambientes digitais capazes de oferecer serviços a custo marginal de acesso (mundo digital);
- Veículos autônomos: veículos que se movimentam sem a ação humana (mundo físico);
- Impressão 3D: impressão por camadas que possibilita muita personalização (mundo físico);
- Robótica avançada: inclusão de robôs para desempenhar tarefas variadas (mundo físico);

- Novos materiais: desenvolvimento de materiais mais leves, mais fortes e recicláveis e adaptáveis, possibilitando a criação de novos produtos (mundo físico);
- Manipulação genética: valorizando a biologia sintética, onde as limitações são éticas (mundo biológico).

Nesta mesma linha, a Confederação Nacional da Indústria (2016, 12), em estudo que trata dos desafios da quarta revolução industrial no Brasil, aponta a Internet das Coisas, o *Big Data*, a Computação em Nuvem, a Robótica Avançada, a Inteligência Artificial, novos materiais e as novas tecnologias de manufatura aditiva (impressão 3D) e manufatura híbrida (funções aditivas e de usinagem em uma mesma máquina) como sendo as principais tecnologias habilitadoras dessa revolução.

Conforme Schwab (2018, p. 324), o ser humano está mais consciente do poder transformador da tecnologia e do impacto na sociedade. As tecnologias são muito mais que conjuntos de máquinas, ferramentas ou sistemas interligados à produção e ao consumo. As tecnologias são vetores que moldam valores e perspectivas sociais. É por meio delas que interpretamos o mundo e moldamos o futuro da sociedade, ou seja, todas as partes interessadas devem internalizar o fato de que os resultados do avanço tecnológico estão ligados às nossas escolhas em cada nível de desenvolvimento e implantação, seja como cidadão, gestor ou representante da sociedade.

Outra pesquisa, elaborada por Carvalho (2018), quanto aos principais elementos teóricos e práticos aderentes à quarta revolução industrial, destacaram-se três vertentes, sendo elas: social, estrutural e tecnológico, sendo representados conforme Quadro 1.

QUADRO 1. Principais elementos teóricos e práticos aderentes à quarta revolução industrial

	Social
Pessoas e Talentos na quarta revolução industrial:	aspectos relevantes para a motivação e fortalecimento das equipes na quarta revolução industrial.
Legislação:	legislação sobre tratamento de dados pessoais, fluxo de dados internacional e acordos internacionais.
Economia circular:	modelo econômico circular, que associa o crescimento econômico a um ciclo de desenvolvimento positivo contínuo, que preserva e aprimora o capital natural, otimiza a produção de recursos e minimiza riscos sistêmicos, com a administração de estoques finitos e fluxos renováveis.

	Estrutural
Big Data:	entendimento teórico e prático do processo de Big Data, envolvendo tarefas como coleta, armazenamento, processamento e visualização de dados, métodos fundamentais para profissionais da quarta revolução industrial.
Design Thinking:	pensamento pluralista e sistêmico, visando o desenvolvimento e adaptabilidade aos desafios da quarta revolução industrial.
Lean Manufacturing:	eliminação do desperdício. aumento do valor ao cliente. e aumento da competitividade das organizações que atuam na quarta revolução industrial.
Análise de Riscos:	riscos, e incertezas aderentes, bem como oportunidades associadas à quarta revolução industrial.
Governança Organizacional aplicada à Quarta revolução industrial:	particularidades da governança e dos modelos de negócios emergentes presentes na quarta revolução industrial.
Práticas Ágeis em Gestão de Projetos:	especificidades e técnicas do método ágil de gerenciamento de projetos.
Sistema Complexo:	sistema com muitos agentes interagentes que exibem comportamentos emergentes não triviais e auto organizados.
Marketing digital:	atividades com o objetivo de atrair novos negócios, criar relacionamentos e desenvolver uma identidade de marca, por meio da Internet.
Inovação disruptiva:	práticas de gestão e a dinâmica da inovação tecnológica disruptiva.
Startup:	ferramentas que possibilitem a criação e manutenção de uma startup.
	Tecnológico
Internet das Coisas (IoT):	elementos e fundamentos da Internet das Coisas (IoT) e o seu emprego na integração e monitoramento dos meios físicos.
Manufatura Aditiva e avançada:	prática e as formas de modelagem de produto por meio da manufatura aditiva.
Inteligência Artificial:	conceito os de Inteligência Artificial, técnicas de aprendizado e algoritmos aplicados na quarta revolução industrial.
Robótica avançada:	sistemas mecânicos motorizados, controlados manualmente ou automaticamente por circuitos elétricos.
Realidade Virtual e Aumentada:	princípios da tecnologia da Realidade Virtual e aumentada incluindo óptica, displays, estereopsia, rastreamento, e as principais plataformas de hardware.
Manipulação genética:	valorizar a biologia sintética, onde as limitações são éticas.
Veículos autônomos:	ter os conceitos dos veículos que se movimentam sem a ação humana.

Fonte: Adaptado de Carvalho (2018).

De acordo com Angeloni (2002), esses três sistemas ou "dimensões" possibilitam a formação e a consolidação da seguinte estrutura sistêmica na era do conhecimento:

- Sistema social: diz respeito à necessidade de se considerar o agente humano nas organizações e o desenvolvimento de ações coordenadas para a ampliação do conhecimento;

- Sistema estrutural: inclui trabalhar aspectos como cultura e estrutura organizacional, com o objetivo de direcioná-la para uma gestão participativa; e
- Sistema tecnológico: a infraestrutura tecnológica – computadores, redes de comunicação de dados, softwares – disponibilizada para criar, armazenar e compartilhar conhecimentos é necessária ao gerenciamento do conhecimento.

Por fim, em pesquisa realizada pela *Deloitte Touche Tohmatsu Limited*, sociedade privada de responsabilidade limitada estabelecida no Reino Unido com 1600 executivos, verificou-se que as empresas estão nos estágios iniciais de maturidade de aplicação e aproveitamento do potencial da quarta revolução industrial, o que aumenta o risco e as incertezas de sua aplicabilidade. A pesquisa enfatizou quatro vertentes (DELOITTE, 2018):

- Impacto social: a Quarta Revolução Industrial poderá criar um mundo mais justo e estável;
- Estratégia: tende para uma abordagem holística, explorando recursos essenciais e aprimorando novos produtos para atender uma ampla parte de interessados;
- Talento e força de trabalho: criação de oportunidades de treinamento, tanto dentro da organização quanto nas comunidades carentes, fortalecendo uma cultura de aprendizado e colaboração;
- Tecnologia: a tecnologia deve apoiar um amplo espectro de responsabilidades e partes interessadas necessárias para prosperar na quarta revolução industrial.

Existem diferentes vertentes de compreensão da quarta revolução industrial, mas com certeza impactará diretamente no crescimento econômico, na produtividade das empresas e nos empregos (SCHWAB, 2017).

As outras revoluções industriais foram identificadas por seus efeitos na sociedade humana somente após a sua passagem, entretanto, a quarta revolução industrial está sendo percebida já na atualidade, permitindo assim, a sociedade antecipar-se aos seus efeitos (BARBOSA; BAÍSSA; ALMEIDA, 2018, p. 10).

Conforme Anderson, Rainie e Luchsinger (2018), as capacidades para se obter sucesso será, primeiramente, entender, gerenciar e manipular dados, e, em seguida, encontrar significado e valor em dados combinados com o problema, condição ou oportunidade que os dados estão descrevendo.

Os dados se tornam cada vez mais parte dos atuais e futuros sistemas de manufatura, obrigando abordagens sofisticadas para avaliar a sua confiabilidade, uma vez que a confiabilidade avalia a probabilidade de que os dados desempenhem o seu propósito adequadamente, por um período de tempo especificado, respeitando o ciclo de vida dos dados.

APLICAÇÃO DOS DADOS NA QUARTA REVOLUÇÃO INDUSTRIAL

■ Drucker (1994, p. 16) enfatiza que os recursos básicos das novas organizações deixaram de ser o capital, os recursos naturais e a mão-de-obra, para passar a ser o conhecimento e o valor organizacional criado por intermédio de dados, produtividade e inovação[3].

Conforme Antonelli e Quéré (2004, p. 1), a identificação do conhecimento é vista como um bem econômico, cujo dados são a base para a sua efetivação e transformação em inteligência competitiva.

Segundo Drucker (1994, p. 164), as organizações – pessoas, estrutura e tecnologia – não mais necessitam estar dentro do mesmo conjunto. É necessária, apenas, a interligação por intermédio dos dados, e ressalta que o ponto focal do conhecimento é sempre a pessoa, que tem por incumbência utilizá-lo, agregar valor e disseminá-lo.

Na quarta revolução industrial existem cinco principais domínios passando por grandes mudanças e que as empresas precisam se atentar: clientes, competição, inovação, valor e dados[4].

Para Laudon e Laudon (1998, p. 10), baseados no pensamento de Platão – filósofo grego que viveu entre os anos de 428 a 348 a.c., os dados são os fatos brutos,

3 De forma genérica, as inovações podem ser radicais ou incrementais. A inovação radical é entendida como o desenvolvimento e introdução de um novo produto, processo ou forma de organização da produção inteiramente nova. Para Lemos (2000, p. 158), este tipo de inovação pode representar uma ruptura estrutural com o padrão tecnológico anterior. "Estas e algumas outras inovações radicais impulsionaram a formação de padrões de crescimento, com a conformação de paradigmas tecno-econômicos" (FREEMAN, 1988 apud LEMOS 2000, p. 158). A inovação incremental, conforme Freeman (1988 apud Lemos, 2000, p. 159), refere-se à "introdução de qualquer tipo de melhoria em um produto, processo ou organização da produção dentro de uma instituição, sem alteração na estrutura industrial". Lemos (2000, p. 159) relata exemplos de inovações incrementais, sendo que muitas delas podem ser aparentemente imperceptíveis, mas geram crescimento da eficiência técnica, aumento da produtividade, redução de custos, aumento de qualidade e otimização de processos.

4 Conforme David Rogers, autor de quatro livros sobre marcas e estratégia digital, incluindo *A rede é seu cliente*, e seu mais novo, *The Digital Transformation Playbook* (2016), considerado um dos grandes estudiosos de estratégia digital e branding da Columbia Business School.

o fluxo infinito de coisas que estão acontecendo no momento e que já aconteceram no passado, a informação é o conjunto de dados aos quais os seres humanos deram forma para torná-los significativos e úteis e o conhecimento considerado o conjunto de ferramentas conceituais e categorias usadas pelos seres humanos para produzir, armazenar, transformar, analisar e descartar os dados (Figura 1).

FIGURA 1. Ciclo de vida do dado

Fonte: AMARAL, 2016, p. 6.

Compreender o ciclo de vida dos dados é indispensável para encontrar melhores maneiras de desenvolver a economia, promover o desenvolvimento social e manter a estabilidade social (YU; ZHAO, 2019).

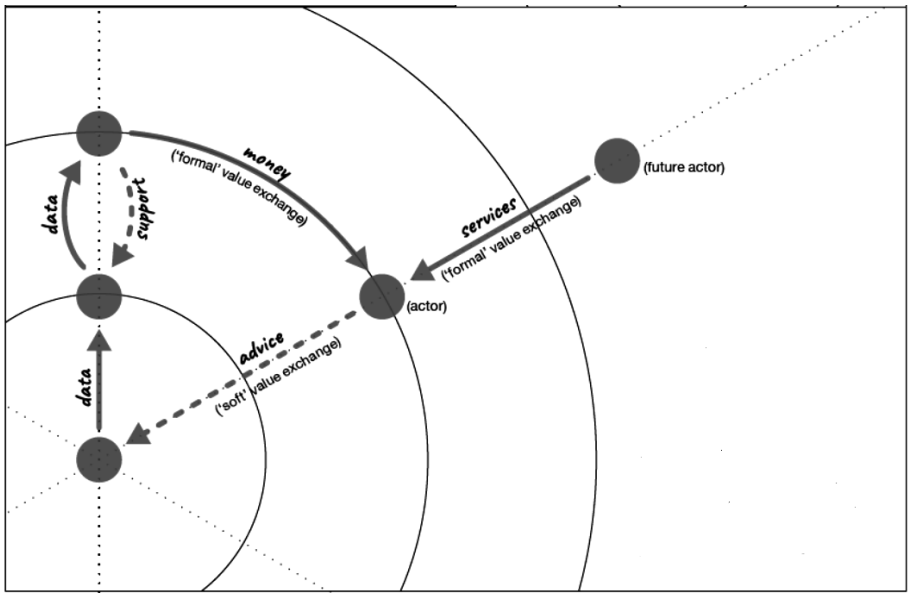
Além do ciclo de vida, a *Open Data Institute* apresenta ser importante a compreensão do ecossistema dos dados (Figura 2), que considera os dados envolvidos, atores existentes, suporte para a coleção e o compartilhamento de dados e os ganhos das trocas estruturadas e não estruturadas de dados, como fluxo de valor dos dados e as oportunidades.

O mapeamento exige que seja considerado diferentes atores, relacionamentos e ideias no sistema. Trata de um processo colaborativo envolvendo as diferentes partes interessadas. O produto é útil como uma ferramenta de comunicação para apoiar o envolvimento no ecossistema de dados.

Os dados contribuem a potencializar o crescimento das empresas e a deixá-las mais competitivas, sendo o segredo extrair o verdadeiro valor dos dados, aqueles que vão gerar mudanças ou aperfeiçoamento nos negócios. Segundo um estudo do Boston Consulting Group (BCG), as empresas mais maduras na transformação digital e que se tornaram orientadas a dados registraram até 30% de maior eficiência e aumentaram em 20% as receitas[5].

5 Informação disponibilizada pela Associação Brasileira de Marketing Direto – ABEMD, referente ao Estudo que comprova que dados podem otimizar processos e aumentar a eficiência dos negócios. Disponível em: https://abemd.org.br/noticias/estudo-comprova-que-dados-podem-otimizar-processos-e-aumentar-a-eficiencia-dos-negocios, acesso em 05 de agosto de 2019.

FIGURA 2. Data Ecosystem Mapping



Fonte: OPEN DATA INSTITUTE, 2019.

Chegar à tomada de decisão apenas nos dados brutos, sem uma análise, sem uma interpretação inteligente de sua potencialidade como informação e conhecimento é potencializar as falhas.

Sendo assim, Gomes e Braga (2017) definem a inteligência competitiva como um processo sistemático e ético, interruptamente avaliado de identificação, coleta, tratamento e análise de dados (ordenar, regular e captar as relações que existem nos dados e nas informações recolhidas, logicamente ordenadas) e disseminação de informação, viabilizando o seu uso no processo decisório e na prospecção de cenários.

O processo de criação de inteligência competitiva está intimamente associado às duas funções essenciais, a de adaptação e de inovação, na medida em que se adaptam as informações recolhidas às situações novas (PASSOS; FERREIRA, 2016).

Ainda, conforme Gomes e Braga (2017), a inteligência competitiva é uma forma de agregar valor à informação e aos dados, fortalecendo seu caráter estratégico, propiciando a tomada de decisão, com foco na elevação da capacidade criativa do capital intelectual da organização, visando a disponibilização de produtos e serviços, como uma aprendizagem constante da empresa.

Senge (1990) informa que a aprendizagem resulta em práticas e mudanças de atitude, e não simplesmente na assimilação de novos dados, informações e formação de novas ideias. O real aprendizado só ocorre quando há um *feedback loop*, ou seja, quando os modelos mentais que guiam os comportamentos são alterados pelas próprias respostas que eles provocam. É necessário que as pessoas se engajem na compreensão de seus comportamentos e em atitudes de cooperação e participação com outros (KNELLER, 1978, p. 60, apud TERRA, 1999).

Para Spiegel et al. (2005), cada modelo de organização possui uma forma de resposta ao mercado, e muitas não são capazes de manobras rápidas de adaptação quando enfrentam mudanças rápidas. Também, não existe um consenso de uma definição para inteligência competitiva (PASSOS; FERREIRA, 2016).

A vida digital está aumentando as capacidades humanas e interrompendo atividades humanas antigas. Os sistemas orientados por código se espalharam para mais da metade dos habitantes do mundo em informações e conectividade ambientais, oferecendo oportunidades inimagináveis e ameaças sem precedentes (ANDERSON; RAINIE; LUCHSINGER, 2018).

Uma grande preocupação é o abuso da utilização dos dados criados. Um exemplo de abuso pode ocorrer por meio da Inteligência Artificial que, na sua maioria, está e estará nas mãos de empresas que buscam lucros ou governos que buscam poder. Valores e ética muitas vezes não são incorporados aos sistemas digitais. Esses sistemas são globalmente interligados e não são fáceis de regular ou controlar (ANDERSON; RAINIE; LUCHSINGER, 2018).

É por isso que existe a necessidade de uma ética dos dados, para que os algoritmos criados visem o benefício da sociedade e não de alguns poucos detentores do poder e da riqueza. A ética dos dados se preocupa com os problemas morais decorrentes da coleta, análise e aplicação de grandes conjuntos de dados. Confiança e transparência são temas cruciais na ética digital (SCHWAB, 2018).

Diante da importância de uma atitude ética dos dados, a *Open Data Institute* desenvolveu a ferramenta *Data Ethics Canvas*[6], com quinze questões, para quem coleciona, compartilha ou usa dados, de modo a avaliar os impactos nas pessoas e na sociedade. O Canvas busca um pensamento crítico quanto o objetivo principal do uso dos dados e quem poderia ser afetado negativamente com a sua utilização.

Conforme Schwab (2018), os três elementos particularmente relevantes no olhar da ética digital são: uso irrestrito de grande volume de dados; crescente de-

6 Canvas disponível em https://theodi.org/knowledge-opinion/ pela *Open Data Institute*, com sede no Reino Unido. Fundada pelos senhores Tim Berners-Lee e Nigel Shadbolt em 2012, com a missão de conectar, equipar e inspirar pessoas de todo o mundo a inovar com dados.

pendência de algoritmos para a execução de tarefas, configuração de escolhas e tomada de decisão; e a redução gradual do envolvimento humano – ou mesmo de fiscalização – sobre os processos automatizados.

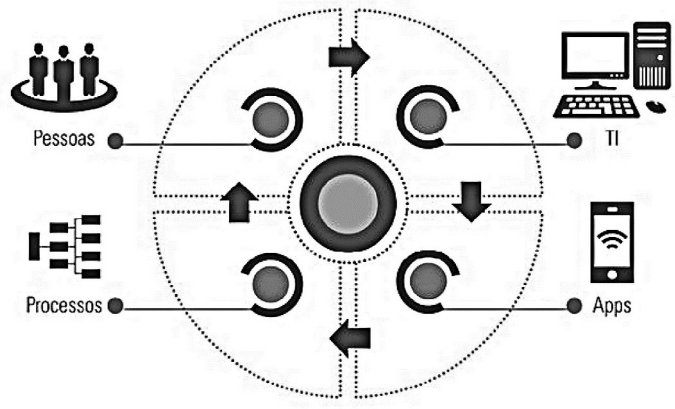
Uma das formas de tratar os dados com ética deve ser por intermédio da aplicação consciente da *Data Science*, a ciência que transforma grande quantidade de dados brutos em insight e conhecimento para a tomada de decisão, da produção ao descarte, muito além de um olhar meramente estatístico, composta por uma governança de dados (outras ciências, modelos, tecnologias, processos e demais procedimentos relacionados ao dado) (AMARAL, 2016)

Para a implantação da ciência de dados, tem-se a profissão de Cientista de Dados, considerada pelo Fórum Econômico Mundial como uma das profissões mais relevantes para o mercado até 2020. Conforme Amaral (2016), o Cientista de Dados é o profissional que possui conhecimento multidisciplinar, competências em gerenciamento de projetos, liderança e familiaridade com equipes de especialistas.

A popularização dessa profissão é resultado do advento da quarta revolução industrial, que alinha a Computação em Nuvem, o *Big Data* e a Inteligência Artificial.

A Computação em Nuvem é uma plataforma acessada via Internet que permite acesso, sob demanda, a um conjunto de dados e recursos de computação configuráveis, envolvendo um amplo espectro de pessoas, processos, tecnologias e aplicações para a manutenção de um serviço contínuo (Figura 3).

FIGURA 3. Elementos que devem ser pensados no modelo de Resiliência



Fonte: SANTOS, 2018.

A Computação em Nuvem está se tornando cada vez mais complexa, sendo que a definição "resiliência" vem no sentido de descrever a capacidade de sistemas complexos (pessoas, processos, tecnologias e aplicações) de se auto organizarem frente a situações difíceis, adaptando-se à evolução da infraestrutura dos mais modernos datacenters do mercado, onde, humanamente, é impossível acompanhar tudo o que ocorre nas milhares de máquinas virtuais que rodam sobre centenas de redes, acessando milhares de volumes de disco.

Atualmente, 95% dos dados armazenados não são estruturados, o que traz um novo desafio de transformação dos dados em inteligência competitiva (GANDOMI; HAIRDER, 2015). Uma alternativa é se apoiar no *Big Data,* associado a grandes volumes de dados. O processo envolve tarefas como coleta, armazenamento, processamento e visualização de dados

O Big Data pode ser definido como "fenômeno de massificação de elementos de produção e armazenamento de dados, bem como o processo de tecnologias, para extraí-los e analisá-los" (AMARAL, 2016, p. 12). Trata de dados produzidos com volume, velocidade, variedade, veracidade e valor, em diferentes formatos, em altíssima quantidade, incluindo informações digitais, vídeos e imagens.

Conforme estudo de Yu e Zhao (2019) na China, os usuários da Internet encontram-se em uma prisão transparente, na qual todos os seus comportamentos e dados pessoais estão sob a estrita supervisão de um terceiro olhar, sendo a essência do *Big Data* seguir os dados que o público cria.

Na quarta revolução industrial, a análise dos dados começa a migar de amostral para ser aplicada a 100% do universo de dados, eliminando risco, apreendendo com os dados e criando vantagem competitiva e novos produtos e serviços.

A Mineração de Dados explora o universo de dados à procura de padrões consistentes, como regras de associação ou sequências temporais, para detectar relacionamentos sistemáticos entre variáveis.

Conforme Gandomi e Hairder (2015), a heterogeneidade, o ruído e o tamanho massivo do Big Data exigem o desenvolvimento de algoritmos eficientes do ponto de vista computacional que possam evitar armadilhas de grandes volumes de dados.

A mineração, considerada uma das bases de sustentação da Inteligência Artificial e da Inteligência Competitiva, é uma forma de melhor conhecer as pessoas, organizações, padrões e tendências às quais elas estão agregadas, normalmente complementada pela análise dos dados.

Para Kaplan e Haenlein (2019, p. 15), a Inteligência Artificial é definida como a capacidade do sistema de interpretar corretamente dados externos, apren-

der a partir desses dados e utilizar essa aprendizagem para atingir objetivos e tarefas específicos, por meio de uma adaptação flexível. Ela vem alterando como as pessoas e empresas se relacionam com tecnologia.

Para Fábio Coelho, CEO do Google, a longo prazo, as máquinas farão boa parte das funções repetitivas, sendo repassadas para a Inteligência Artificial, deixando para os humanos as atividades mais artísticas e intelectuais (ACADEMIA CEO, 2019). Cada vez mais os equipamentos irão fornecer dados.

Os dados externos são obtidos meio da Internet das Coisas e Big Data, utilizados como entradas para identificar regras e padrões subjacentes, baseando-se em abordagens de aprendizado de máquina. Ainda, Kaplan e Haenlein (2019) esclarecem que o aprendizado de máquina é uma parte essencial da Inteligência Artificial, embora a inteligência seja mais ampla do que o aprendizado, pois abrange a capacidade do sistema de perceber dados (por exemplo, processamento de linguagem natural ou reconhecimento de voz / imagem) ou controlar, mover e manipular objetos com base em aprendizado. informação seja um robô ou outro dispositivo conectado.

Percebe-se uma grande preocupação pela integridade dos dados, uma vez que a maioria dos ataques cibernéticos subverte o fluxo desejado e aproveita-se das vulnerabilidades para a corrupção do sistema informacional como um todo, uma vez que os dados pessoais e organizacionais estão cada vez mais valiosos, devido ao seu uso mais amplo e a exploração comercial.

A coleta e transmissão de dados pessoais inevitavelmente resultam na divulgação desses dados, o que potencialmente ameaça à segurança pessoal. Consequentemente, há uma necessidade urgente de proteger os direitos relativos ao uso e transações envolvendo dados (YU; ZHAO, 2019). No Brasil, a proteção dos dados é regulada pela promulgação da Lei Geral de Proteção de Dados Pessoais[7], com base no respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem e aos direitos humanos de liberdade e dignidade das pessoas, entre outros valores.

Um forte aliado à Inteligência Artificial é a Internet das Coisas. A Internet das Coisas é a ferramenta com mais potencial de modernizar os negócios nos próximos três anos, seguida por inteligência artificial[8] que vem se expandindo ra-

7 Lei 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção e o tratamento de dados pessoais, inclusive nos meios digitais, pelas empresas públicas ou privadas, entes públicos e pessoas físicas.

8 Conforme a Pesquisa da KPMG Inovação na indústria de tecnologia 2019 (*Technology Industry Innovation Survey)*, com 740 líderes da indústria de tecnologia, as dez ferramentas que irão

pidamente em bilhões de fontes e dispositivos de dados inteligentes interconectados, levando tudo à conectividade (OWEIS et al, 2016), ou seja, todos os objetos conectados à Internet, agindo de modo inteligente e sensorial. Com o desenvolvimento da tecnologia máquina-máquina, espera-se que uma elevada quantidade de dispositivos heterogêneos conectados à Internet das Coisas, em um futuro muito próximo.

Contribui com a popularização da Internet das Coisas a vinda da tecnologia 5G, a próxima geração de transferência de dados em dispositivos móveis. "*O 3G nos deu a primeira conexão de verdade no celular. O 4G marcou a era do streaming. O 5G transformará os celulares nos nossos bolsos em supercomputadores"* (JULIO, 2019).

A Agência Nacional de Telecomunicações (Anatel) estima que o Brasil já possui cerca de 20 milhões de conexões máquina-máquina. A previsão é que o número salte para 42 milhões em 2020. No mundo todo, até 2025, o total de objetos conectados deve ficar entre 100 milhões e 200 milhões. "*Até 2025, cada cidadão brasileiro terá, em torno de si, sete equipamentos máquina-máquina – seja um relógio que está conectado, seja a televisão, seja o carro*"[9].

CONSIDERAÇÕES FINAIS

■ A quarta revolução industrial é o resultado da convergência de informações dos mundos digitais, físicos e biológicos (SCHWAB, 2017, p.23), onde os dados são as partículas presentes em todas as transações e comunicações, permitindo o entendimento do processo de transformação social, estrutural e tecnológico. Diversas tecnologias são mapeadas como tecnologias habilitadoras dessa nova realidade, entanto, trata-se de um mundo ainda em transformação, sendo percebida na atualidade, onde os dados possuem um papel central.

O principal impulso para a quarta revolução industrial são os dados. O surgimento e desenvolvimento da Indústria 4.0 está criando pressão sobre os fabricantes para recolher e analisar dados, a fim de se manterem competitivos no mercado.

---

mudar as empresas a curto prazo serão: 1ª Internet das Coisas, 2ª Automação Robótica de Processos, 3ª Inteligência Artificial e Aprendizado de Máquina, 4ª *Blockchain*, 5ª Robótica e automação, incluindo veículos autônomos, 6ª Realidade aumentada, 7ª Realidade virtual, 8ª Rede social e tecnologias colaborativas, 9ª Biotecnologia e saúde digital e 10ª Plataformas de compartilhamento.

9 Palavras do Secretário de Políticas de Informática, Maximiliano Salvadori Martinhão, do Ministério da Ciência, Tecnologia, Inovações e Comunicações, Brasil, 2017.

Os dados estão permeando o mundo físico e digital, dentro de um verdadeiro ecossistema que abrange desde a sua produção até o seu descarte dos dados, impactando diretamente no desenvolvimento da economia, da promoção e estabilidade social, espalhados em todo mundo, oferecendo oportunidades e ameaças.

A composição ordenada dos dados por um processo sistemático e ético possibilita, uma interpretação inteligente de sua potencialidade, transformando-os em subsídio para a inteligência competitiva.

As empresas que aderirem à quarta revolução industrial deverão se utilizar de monitoramento online dos dados. O aumento da maturidade do nível de automação e digitalização dos dados visam a garantia de maior agilidade, controle, segurança e eficiência. O modelo de produção deverá ser seguro contra os Ataques Cibernéticos e acidentes.

Novas tecnologias, processos e competências surgem e são necessárias para a aplicação consciente e transformador dos dados, apoiada pela Data Science, que possibilita a transformação de dados brutos em modelos, tecnologias, processos e soluções relacionados aos dados.

Novos termos passam a configurar na realidade da quarta revolução industrial quando olhamos diretamente os dados, entre eles destacam-se a Computação em Nuvem, o *Big Data*, a Inteligência Artificial, a Mineração de Dados, Internet das Coisas, Aprendizado de Máquinas, Ataques Cibernéticos e Proteção de Dados Pessoais.

A sociedade está mais consciente do poder transformador da tecnologia e do valor e necessidade de segurança do uso dos dados, já que eles permitem a comunicação entre máquinas, ferramentas, sistemas e pessoas que estão interligadas para a produção e busca de bens e serviços que nortearão o desenvolvimento das próximas gerações.

Por fim, é importante enfatizar que, para gerar valor, obter vantagem competitiva e se consolidar na quarta revolução industrial é fundamental a utilização de dados como ativos estratégicos, por meio de análises e recursos que permitam transformar os dados em informações e conhecimento, que identificam propósitos da sociedade, de forma ética, onde os dados sejam considerados ativos cada vez mais valiosos.

Antonio Ramalho de Souza Carvalho · Doutor em Ciências pelo Instituto Tecnológico de Aeronáutica - ITA. Assessor em Gestão Estratégica de Projetos de PD&I no Comando da Aeronáutica. Professor efetivo da Fundação Armando Álvares Penteado – FAAP onde coordena o curso de Gestão Estratégica de Projetos. Autor de diversos artigos publicados em livros, revistas e eventos.

REFERÊNCIAS

ACADEMIA CEO. Tecnologia da Informação: uma revolução na gestão. 4 jun 2019. Disponível em: https://www.academiaceo.com.br/blog/2019/06/tecnologia-da-informacao-uma-revolucao-na-gestao, acesso em 07 jul 2019.

AMARAL, Fernando. Introdução a ciência de dados: mineração de dados e Big Data. Rio de Janeiro: Alta Books, 2016.

ANDERSON, J.; RAINIE, L.; LUCHSINGER, A. Artificial Intelligence and the Future of Humans. Pew Research Center: Internet & Technology. December 2018. Disponível em: https://www.pewinternet.org/2018/12/10/artificial-intelligence-and-the-future-of-humans/ Acesso em: 03 de julho de 2018.

ANGELONI, Maria Terezinha (coord.). Organizações do conhecimento. São Paulo: Saraiva, 2002.

ANTONELLI, Cristiano; QUÉRÉ, Michel. The governance of the generation and dissemination of localized technological knowledge. Italia: Università di Torino and Fondazione Rosselli, 2004. Disponível em http://www.fondazionerosselli.it/The governance of the generation and dissemination of localized technological knowledge.doc. Acesso em 12 de junho de 2005.

BARBOSA, M. T. J; BAISSA, M; ALMEIDA, M. T. Surge uma nova sociedade. In: SILVA, Elcio B et. al (Org.). Automação e sociedade: quarta revolução industrial, um olhar para o Brasil. Rio de Janeiro: Brasport, 2018. Cap. 1. p. 3-12

BARBOSA, Marcos T. J., BAISSA, Marcos, ALMEIDA, Marcos T. Surge uma nova sociedade (cap. 1). BRITO DA SILVA et al. Automação & Sociedade: Quarta Revolução Industrial, um olhar para o Brasil. Rio de Janeiro: Brasport, 2018.

CARVALHO, A. R. S. Abordagem sociotécnica da indústria 4.0. In: XV Simpósio de excelência em gestão e tecnologia - SEGET – Indústria 4.0 e o uso de tecnologias digitais. Associação Educacional Dom Bosco: Rezende – RJ, 2018.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. Desafios para a indústria 4.0 no Brasil. Brasília: Confederação Nacional da Indústria - CNI, 2016.

DELOITTE. The Fourth Industrial Revolution is here are you ready? 2018. Disponível em: https://www2.deloitte.com/br/pt.html. Acesso em 24 de maio de 2018.

DRUCKER, Peter F. Sociedade pós-capitalista. São Paulo: Pioneira, 1994.

EISENHARDT, Kathleen M. Building theories from case study research. The Academy of Management Review, v. 14, n. 4, p. 532-550, Oct. 1989.

GANDOMI, A.; HAIRDER, M. Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management. Elsevier, v.35, n. 2. p. 137-144. 2015.

GOMES, E.; BRAGA, F. Inteligência competitiva em tempo de Big Data: analisando informações e identificando tendências em tempo real. Rio de Janeiro: Alta books, 2017.

JULIO, Rennan A. Dados são o novo petróleo[...] Época Negócios. 05 jul 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-

diz-ceo-da-mastercard.html?utm_source=facebook&utm_medium=social&utm_campaign = post Acesso em 07 de julho de 2019.

KAPLAN, Andreas; HAENLEIN, Michael. Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. Business Horizons, Elsevier, v. 62, ed. 1, jan-fev 2019, p. 15-25.

LAUDON, Kenneth C.; LAUDON, Jane Price. Sistemas de informação com internet. Tradução de Dalton Conde de Alencar. Rev. Téc. De Cristina Bacellar. Information Systems and the Internet. Rio de Janeiro: LTC, 1998.

MIGUEL, Paulo Augusto Cauchick. Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. Produção [online], v. 17, n.1, p. 216-229, jan./Apr. 2007.

OPEN DATA INSTITUTE. Data Ecosystem Mapping. London: 2019 Disponível em: https://theodi.org/article/data-ecosystem-mapping-tool. Acesso em 3 de agosto de 2019.

OWEIS, N. E. *et. al.* Internet of Things: overview, sources, applications and challenges. In: Proceedings of the Second International Afro-European Conference for Industrial Advancement (AECIA) 2015. Cham. 2016, p. 57-67.

PASSOS, A; FERREIRA, T. D. M. Terasac: o livro da inteligência competitiva. São Paulo: Livrus, 2016.

SANTOS, Tiago. Fundamentos da computação em nuvem. Senac: São Paulo, 2018.

SCHWAB, K. A quarta revolução industrial. São Paulo: Edipro, 2017.

SCHWAB, K. Aplicando a quarta revolução industrial. São Paulo: Edipro, 2018.

SENGE, Peter. The fifth discipline. New York: Doubleday, 1990.

SIMÃO FILHO, A.; PEREIRA, S. L. A empresa ética em ambiente ecoeconômico: a contribuição da empresa e da tecnologia da automação para um desenvolvimento sustentável inclusivo. São Paulo: Quartier Latin do Brasil, 2014.

SPIEGEL, Eric A. Et al. Test Your Company's DNA. Electric Perspectives. Washington: Mar/Apr 2005. v.30, n. 2. p.32.

TERRA, José Claudio C. Knowledge management: concepts and exploratory study of the managerial practices of brazilian companies. Seminário de Pesquisa – Gestão do Conhecimento: práticas das empresas brasileiras. 25 ago. 1999. FEA/USP: São Paulo, 1999.

YU, Xiaolan; ZHAO, Yun. Dualism in data protection: Balancing the right to personal data and the data property right. Computer Law & Security Review. ScienceDirect. Elsevier, maio 2019.

Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP

MARIA CELINA BODIN DE MORAES
JOÃO QUINELATO DE QUEIROZ

RESUMO

■ As noções tradicionais de privacidade e de divulgação mostram-se insuficientes e inadequadas diante das tecnologias presentes na sociedade da informação, demandando do intérprete um cuidadoso exame dos novos instrumentos para a proteção da pessoa humana no âmbito do tratamento dos dados pessoais. Com o advento da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), no contexto de assunção dos dados pessoais como bens jurídicos essenciais, assume relevo o direito à autodeterminação informativa como vetor de proteção dos dados pessoais. Quanto à responsabilização civil, um novo regime se faz presente. Cumpre investigar aqui sua potencialidade como instrumento de natureza multifuncional que apresenta, no que tange a danos causados pelos agentes de tratamento de dados, além da função comum compensatória, uma função de prevenção e dissuasão, vindo a criar, desse modo, um reforço para a garantia da proteção da privacidade dos dados pessoais.

ABSTRACT

■ The traditional notions of privacy and disclosure are both insufficient and inadequate given the technologies present in the information society, demanding from the interpreter a careful examination of the new instruments for the protection of the human person in the context of the processing of personal

data. With the advent of the General Law on the Protection of Personal Data (Law 13.709/2018), in the context of the assumption of personal data as essential legal assets, the right to informational self-determination as a vector of protection of personal data is emphasized. As for civil liability, a new system is present. It is an instrument of a multifunctional nature which presents, concerning the damage caused by data processing agents, the common objective of compensation, and additionally seems to pursue deterrence and prevention objectives, which in this case means a reinforcement to ensure the protection of the privacy of personal data.

INTRODUÇÃO

■ Kenny, 17 anos, estudante, foi vítima do ataque silencioso de um *hacker* em seu computador, que obteve acesso à câmera de seu laptop e o gravou em ato íntimo. Hector, empresário, 45 anos, casado e pai de duas filhas, foi vítima de *hackers* que invadiram seu smartphone e captaram vídeos e sons de sua infidelidade conjugal. Sob ameaças de divulgação do material, Hector e Kenny são chantageados a roubarem um banco e a entregarem o dinheiro à quadrilha de *hackers*, expondo a fragilidade dos dados pessoais e sua relevância para a identidade pessoal daqueles indivíduos. Os casos são ficcionais e foram exibidos no episódio *Shut Up and Dance,* da série *Black Mirror*, mas espelham-se em situações concretas que desafiam a privacidade nesses tempos de novas tecnologias.[1] Na vida real, casais ingleses foram filmados em relações íntimas por suas *smart-tvs* [2] e cidadãos americanos, segundo o *The Wall Street Journal* estariam sendo monitorados pelo FBI por meio das câmeras de seus laptops.[3] Nem mesmo as opções de "navegação anônima" oferecidas por alguns programas mostram-se seguras: estudo recente mostra que o Facebook e o Google monitoram acessos a sites de pornografia ao redor do mundo, sugerindo que ações de acesso ilegal

1 Como noticiou um jornal inglês, não é coincidência o aumento das vendas de capas ou protetores de câmeras de laptops. *The Guardian*, "*Why is everyone covering up their laptop cameras?*", acesso em 30 ago. 2019.

2 Casais foram surpreendidos com o envio automático de imagens privadas a sites pornográficos de imagens obtidas por suas Smart-Tvs. (*Smart TV hackers are filming people having sex on their sofas – and putting it on porn sites*). Disponível em https://metro.co.uk/2016/05/23/smart-tv-hackers-are-filming-people-having-sex-on-their-sofas-and-putting-it-on-porn-sites-5899248/, acesso em 30 ago. 2019.

3 "*FBI Taps Hacker Tactics to Spy on Suspects*". *The Wall Street Journal*, acesso em 30 ago. 2019.

a dados pessoais vem não só de agentes desconhecidos da web mas, inclusive, desses grandes operadores.[4]

No Brasil, como se sabe, os chefes dos três poderes já foram alvos de ações de espionagem. Nunca foi tão atual a afirmação de Rodotà: "assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão deixando transparente".[5]

O homem de lata que anseia um coração deixou as longínquas narrativas de *O Mágico de Oz* (1939) e passou a ocupar a realidade contemporânea por meio da Internet das Coisas (*Internet of Things* ou *IoT)*: robôs que têm sentimentos, máquinas que pensam e aprendem sozinhas, TVs que captam as emoções de seus telespectadores e, assim, podem recomendar-lhes filmes.[6]

Em um contexto de tão frequente inovação, a ficção torna-se realidade, a multidão torna-se nua e a proteção de dados pessoais assume caráter indispensável ao progresso democrático e social.[7] No Brasil, há muito despontam mecanismos legislativos com o objetivo de proteger os dados pessoais: desde a previsão constitucional do *habeas data*, à proteção dos dados dos consumidores promulgada pelo CDC,[8] até a cláusula geral de tutela da privacidade no art. 21 do Código Civil

4 "*Facebook and Google Trackers Are Showing Up on Porn Sites*". *The New York Times*, acesso em 30 ago. 2019.

5 Relatório da *Autorità Garante per la tutela dei dati personali,* apresentado por Stefano Rodotà ao Presidente da República Italiana em 2000. (BODIN de MORAES, Maria Celina. Apresentação. In: RODOTÀ, Stefano. *A vida na sociedade de vigilância.* Privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 8).

6 "Em poucas palavras, a IoT representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet possibilitando não só a comunicação e realização de funções específicas entre coisas, como gerando a cada vez mais constante a coleta, transmissão, guarda e compartilhamento de dados entre objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas". (MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: REIA, Jessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo (Org.). *Horizonte presente:* tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito, Fundação Getúlio Vargas, 2019, p. 486).

7 Como se afirmou em outra oportunidade, "a multidão não é mais 'solitária' e anônima; está nua. A digitalização das imagens e as técnicas de reconhecimento facial consentem extrair o indivíduo da massa, identifica-lo e segui-lo. O *data mining,* a incessante pesquisa de informações sobre o comportamento de qualquer pessoa, gera uma produção contínua de 'perfis' individuais, familiares, territoriais, de grupo. A vigilância não conhece fronteiras". (BODIN DE MORAES, Maria Celina. Apresentação. In: RODOTÀ, Stefano. *A vida na sociedade de vigilância.* Privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 9).

8 O CDC, no art. 43, assegura ao consumidor o acesso às informações constantes em bancos de dados, facultando-lhe a possibilidade de requerer sua correção quando inexatos.

em 2002,[9] diversos foram os instrumentos jurídicos que, pouco a pouco, foram reconhecendo os dados pessoais como bens jurídicos merecedores de tutela. Foi, na realidade, a partir da dogmática desenvolvida acerca da tutela da privacidade[10] que se atentou para o merecimento de tutela dos dados pessoais.[11]

A normatividade do Código Civil, contudo, especialmente o capítulo dedicado aos direitos da personalidade (arts. 11 a 21), por ter sido elaborado sob a lógica ultrapassada da década de 1960, é insuficiente para responder aos desafios práticos hodiernos, que demandam soluções diferenciadas.[12] O texto constitucional, diversamente, tutela os dados pessoais a partir da proteção à intimidade (art. 5º, X), do direito à informação (art. 5º, XIV), do direito ao sigilo de comunicações e dados (art. 5º, XII) e, ainda, da garantia individual ao conhecimento e correção de informações sobre si pelo *habeas data* (art. 5º, LXXII). É na tentativa majoritariamente bem-sucedida de ampliar a proteção aos dados pessoais no Brasil, ao lado das ferramentas constitucionais já existentes, que entra em vigor a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018 ou LGPD), inaugurando a disciplina regulatória nacional de proteção de dados pessoais, refletindo, em grande parte, a estrutura do "Regulamento Geral sobre a Proteção de Dados" (*General Data Protection Rule*), em vigor na União Europeia desde maio de 2018. [13]

9 CC, art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

10 A doutrina diverge acerca das expressões privacidade, intimidade, segredo e, segundo Bruno Lewicki, "o conjunto das situações hoje ligadas à proteção da vida privada representa um 'conglomerado de interesses diversos', configurando as inúmeras e variáveis facetas de um conceito em ampliação constante". (LEWICKI, Bruno. *A privacidade da pessoa humana no ambiente de trabalho.* Rio de Janeiro: Renovar, 2003, p. 31).

11 Assim, Stefano RODOTÀ. *A vida na sociedade da vigilância*, cit., *passim*.

12 V., nesse sentido, BODIN DE MORAES, Maria Celina. *Danos à pessoa humana*. Uma leitura civil-constitucional dos danos morais. 2. ed. rev. Rio de Janeiro: Processo, 2017, p. 126 e ss. Como se sabe, o capítulo dos Direitos da Personalidade do Código de 2002 foi elaborado para o Anteprojeto de Código Civil do Prof. Orlando Gomes, em 1963, sendo o art. 21 a única novidade desta matéria do Projeto Reale.

13 Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN, acesso em 30 ago. 2019.

I. DO SILÊNCIO AO CONTROLE: NOVAS DIMENSÕES DO DIREITO À PRIVACIDADE

■ O direito à privacidade foi originalmente pensado a partir da lógica do direito a ser deixado só (*the right to be left alone*), em lapidar estudo de Warren e Brandeis, de 1890.[14] Para os autores, a proteção da privacidade decorria da garantia de não invasão na esfera individual por qualquer mecanismo não autorizado.[15] Sendo o nascimento da privacidade historicamente associado à desagregação da sociedade feudal e a um contexto no qual a privacidade e a intimidade eram privilégios burgueses, a construção de espaços privados acentuou-se com as Revoluções industriais, privilegiando a burguesia que, cada vez mais, se isolaria em relação às demais classes.[16]

Analisando o conceito criado por Warren e Brandeis, observou-se que o princípio da privacidade foi pensado a partir do ideal burguês patrimonial (e não existencial), assinalando que "as formas de tutela jurídica da privacidade naquele determinado momento histórico se reportam aos instrumentos de proteção da posse e propriedade."[17] De certa maneira a lógica proprietária permanece, infelizmente, como vetor de orientação das normas protetivas da privacidade, embora, como já assinalara há muito Stefano Rodotà, os interesses postos em questão não sejam redutíveis à ótica proprietária.[18]

---

14 "*The protection afforded to thoughts, sentiments and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be left alone. (…) If we are correct in this conclusion, the existing law affords a principle which may be invoked to protect the privacy of the individual from their invasion either by the too enterprising press, the photographer, or the possessor of any modern device for recording or reproducing scenes or sounds*". (WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, Vol. IV, December 15, 1890, Nº 5, p. 205-206, ora disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, acesso em 30 ago. 2019).

15 "O direito a ser deixado em paz não foi construído meramente como a expressão da era de ouro da burguesia, que havia protegido sua esfera imaterial por mesmo da mesma proibição ao esbulho que por muito tempo foi a principal característica da propriedade imobiliária. Sob o impulso dado por Louis Brandeis, emergiu uma visão na qual a privacidade foi vista também como proteção a minorias e opiniões dissonantes" (RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 16).

16 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 27.

17 MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT), cit., p. 489.

18 "(...) devendo-se considerar, a essa altura, o tema da privacidade como parte integrante das dimensões mais gerais da garantia dos direitos civis e da organização da democracia, os interesses em questão não são redutíveis à esfera individual e, de qualquer forma, exprimem valo-

Progressivamente, a privacidade passou a ser lida não só sob sua dimensão negativa – segundo a qual se acreditava que a proteção da privacidade adviria da mera abstenção de terceiros e de não invasão dos espaços privados – mas, também, sob sua dimensão positiva, que demanda, tanto do legislador como dos agentes de tratamentos de dados em geral, uma atuação na proteção das garantias atinentes à circulação de dados pessoais. Esta tutela positiva passa a ser chamada de *autodeterminação informativa*, é incorporada no art. 2º, II, da LGPD e foi definida por Rodotà como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[19]

As cada vez mais criativas formas de coleta e tratamento de dados pessoais na atualidade renovam o direito à autodeterminação informativa como instrumento de promoção da pessoa, sendo premente que se abandone a lógica proprietária que ainda recai sobre os dados pessoais – no sentido de que os dados pessoais podem ser objeto de apropriação tal qual bem móveis – para uma lógica protetiva das relações pessoais e dos direitos subjetivos. A proteção da intimidade por vias da mera não interferência na esfera individual cede espaço à tutela positiva e proativa, isto é, que garanta ao titular o conhecimento pleno das formas de tratamento, finalidade e destino de seus dados.[20] Na lição de Rodotà, é muito fraca a concepção meramente negativista sobre os dados pessoais segundo a qual se lançam proibições de coletas de dados pessoais, proibições essas que, na verdade, são o ponto de partida e não de chegada.[21]

A partir da mudança da perspectiva constitucional introduzida pela cláusula geral de tutela da pessoa humana, fundada no art. 1º, III, da Constituição, bem como da prevalência das relações existenciais face às relações patrimoniais,

---

res irredutíveis à lógica puramente proprietária" (RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 53).

19 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 15, conceito elaborado com base em histórica decisão da Corte Constitucional alemã.

20 "Parece cada vez mais frágil a definição de 'privacidade' como 'o direito a ser deixado só', que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito". (RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 24).

21 "Não parece somente inadequada, portanto, a tendência da *deregulation* e do mercado, mas parece pobre também uma perspectiva ligada apenas a um fortalecimento das defesas individuais 'passivas', feitas de proibições da coleta de determinadas informações e de direitos 'indisponíveis', subtraídos às transações consensuais. Tudo isso continua sendo necessário: porém como um ponto de partida e não de chegada". (RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 58).

começa-se a impor restrições à vontade individual, comprimindo a autonomia privada patrimonial e cedendo espaço à proteção primordial da pessoa. A mesma orientação volta-se, agora, para a proteção dos nossos dados pessoais: não se pode, em nome da livre iniciativa, coletar, tratar e transferir dados pessoais sem a observância de princípios gerais protetivos dos titulares. Conquanto os dados pessoais possam ser vistos como bens jurídicos apropriáveis e circuláveis, a privacidade não o é, de modo que a coleta e o tratamento de dados pessoais deve ser precedida de medidas rigorosas e eficazes de proteção, especialmente em relação aos dados sensíveis, núcleo duro da dignidade humana.[22]

Percebe-se, então, a inadequação das definições tradicionais jurídico-institucionais que dizem respeito à privacidade e intimidade diante dos atuais desafios de processamento de dados, não sendo mais possível, na lição atualíssima de Rodotà, "considerar os problemas da privacidade somente por meio de um pêndulo entre 'recolhimento' e 'divulgação'; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder".[23]

Em razão da insuficiência da mera e indesejável proibição geral de coleta e tratamento de dados pessoais é que se deve superar o antigo direito a ser deixado só, incorporar nas práticas legislativas o direito à autodeterminação informativa e, indo além, garantir a liberdade substancial (e não meramente formal) para o consentimento na coleta de seus dados pessoais, assegurando que o usuário jamais se torne refém da (falsa) opção de consentimento para o consumo de bens e serviços essenciais da vida contemporânea.

22 "Lamenta-se, (...), que a LGPD, embora tenha acertadamente atentado, em diversos dispositivos, à distinção entre dados sensíveis e dados econômicos (notadamente na Seção II de seu Capítulo II), não tenha feito qualquer gradação da tutela dispensada a essas duas categorias de dados no Capítulo III, onde dispôs sobre os "direitos" do titular" (SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na Lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. *Revista Pensar*. Fortaleza, 2019, p. 13. Disponível em https://periodicos.unifor.br/rpen/article/view/9407/pdf, acesso em 30 ago. 2019). Os autores citam ainda a lição de Stefano Rodotà sobre a tutela menos intensa devida aos dados econômicos e sua distinção para com os dados sensíveis: "Procura-se individuar o 'núcleo duro' da privacidade em torno dos dados relativos a opiniões políticas, sindicais ou de qualquer outro gênero, fé religiosa, raça, saúde, hábitos sexuais. Ao mesmo tempo, tende-se a liberalizar a circulação de informações pessoais de cunho econômico" (*A vida na sociedade da vigilância*, cit., p. 78).

23 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 25.

2. A LEI BRASILEIRA DE PROTEÇÃO DOS DADOS PESSOAIS

2.1. Princípios no tratamento de dados pessoais

■ A Lei Geral de Proteção de Dados dispõe, no art. 6º, que o tratamento dos dados pessoais deverá observar a boa-fé e outros dez princípios cardeais, quais sejam os princípios da i) finalidade; ii) adequação, iii) necessidade; iv) livre acesso, v) qualidade dos dados, vi) transparência, vii) segurança, viii) prevenção, ix) não discriminação e x) responsabilização e prestação de contas.[24]

Pelo *princípio da finalidade*, depreende-se que a coleta de dados pessoais deverá ter um propósito específico, previamente definido e informado ao titular, sendo vedada a utilização dos mesmos dados pessoais posteriormente à sua coleta para outra finalidade. Danilo Doneda assevera que esse princípio limita a livre circulação e transferência de dados pessoais a terceiros.[25] O usuário, portanto, deve ser informado de que uma vez coletado seus dados eles serão usados para a finalidade determinada e que não poderão compartilhados com terceiros.

O *princípio da não discriminação*, contido no inciso IX do art. 6º da LGPD, implica a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. O dispositivo parece revelar que o legislador admitiu o tratamento distintivo dos dados pessoais, desde que não abusivo e lícito. Em outras palavras, seria possível que uma instituição financeira, por exemplo, precifique o crédito, com base em dados como o nível de inadimplência, funcionando os princípios gerais de direito, a boa-fé objetiva e o abuso como critérios determinantes da licitude ou não da discriminação. Ao revés desta prática, encontra-se o uso discriminatório de dados pessoais nas relações de trabalho, com a circulação desautorizada de listas entre empregadores com informações pessoais de seus empregados, já vêm há muito demonstrando o caráter nocivo do uso não consentido de dados pessoais, vedação agora reafirmada pela LGPD.[26]

---

24 V., sobre o tema, SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na Lei geral de proteção de dados pessoais, cit., p. 9.

25 "Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição de transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade" (DONEDA, Danilo. *Da privacidade à proteção de dados*, cit., p. 216).

26 "Listagem elaborada pela empresa com dados pessoais do ex-empregado. Divulgação. Dano moral independente de eventuais efeitos na vida profissional do trabalhador A Corte Regional entendeu que há prejuízo à imagem, à intimidade e à dignidade do trabalhador cujos dados pessoais se encontram inseridos em um banco cadastral elaborado pela Reclamada, destinado a consulta por outras empresas em face de provável contratação, independentemente do resul-

O uso distintivo de dados pessoais já era legítimo por força da Lei do Cadastro Positivo (Lei n. 12.414/2011), que autorizava o *credit scoring* para fins de concessão de crédito mediante coleta de dados pessoais. Em 2019, por meio da Lei Complementar n. 116/2019, alterou-se o sistema de consentimento do cadastro positivo: no cenário anterior vigorava o modelo *opt in* (a abertura do cadastro requeria autorização prévia do titular) e agora se adota o modelo *opt out* (o cadastro é aberto automaticamente e se encerra quando o consumidor assim solicita). O formato inicial representou uma baixa adesão ao cadastro positivo e, por isso, os gestores de bancos de dados demandaram a alteração legislativa.

O Superior Tribunal de Justiça reconheceu a licitude do sistema de *credit scoring* por meio do Recurso Repetitivo REsp 1.419.697, Tema 710, tendo ali sido fixadas as seguintes teses: "O sistema '*credit scoring*' (...) é prática comercial lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo) (...). Na avalição do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem com as informações pessoais valoradas".[27] Fica assegurado ao consumidor o direito de ter pleno conhecimento sobre todos os mecanismos usados em seu desfavor para ter conhecimento sobre a metodologia usada para o cálculo de seu *score*.[28]

Se por um lado o sistema de *credit scoring* tem a potencialidade de garantir o barateamento do crédito ao bom pagador, por outro ele pode esconder práticas discriminatórias que tragam em seu bojo discriminação racial e étnica, afetando

---

tado na vida funcional do mesmo. (TST, 2ª T, AIRR nº 558/2003-091-09-40.3, Rel. José Ronald C. Soares, publ. 23.03.2007).

27 STJ, Segunda Seção, REsp n. 1.419.697, Rel. Min. Paulo de Tarso Sanseverino, j. 12.11.2014, DJe 17.11.2014. V. o enunciado da Súmula 550: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo".

28 "Em relação ao sistema *credit scoring*, o interesse de agir para a propositura da ação cautelar de exibição de documentos exige, no mínimo, a prova de: i) requerimento para obtenção dos dados ou, ao menos, a tentativa de fazê-lo à instituição responsável pelo sistema de pontuação, com a fixação de prazo razoável para atendimento; e ii) que a recusa do crédito almejado ocorreu em razão da pontuação que lhe foi atribuída pelo sistema *Scoring*" (STJ, Segunda Seção, Tema Repetitivo 915, REsp 1.304.736/RS, Rel. Min. Luís Felipe Salomão, julg. em 24.02.2016).

emprego, locação, seguros e empréstimos por meio da transferência desautorizada de dados pessoais a terceiros.[29] A atenção especial deve se voltar, nessa hipótese, para os chamados *dados sensíveis*, definidos pela LGPD como "dado sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II).

O *princípio do consentimento*, que consiste na livre manifestação, informada e inequívoca, mediante a qual o titular concorda com o tratamento de seus dados pessoais para determinada finalidade, apresenta destaque frente a outros princípios contidos da LGPD. É a partir do consentimento que se analisará a legitimidade ou não da coleta, tratamento e armazenamento dos dados pessoais no caso específico.

Ao passo que a tecnologia domina atividades triviais do ser humano, nossa dependência às inovações aumenta e para que tenhamos acesso a uma gama de serviços essenciais, a abdicação da privacidade e dos dados pessoais parece inevitável. O usuário, portanto, torna-se *refém* do "consentimento" para a aquisição de produtos e serviços cada vez mais essenciais à vida em sociedade.[30] Ao tratar do consentimento, será preciso ir além das "caixas de seleção" de concordância com os termos de uso de plataformas digitais[31] ou de fornecedores de serviços e,

29 "*Credit Scores in America Perpetuate Racial Injustice. Here's How*" (*The Guardian*. Disponível em https://www.theguardian.com/commentisfree/2015/oct/13/your-credit-score-is-racist-heres-why, acesso em 30 ago. 2019). No Brasil, é comum que os empregadores, no ato de contratação ou até mesmo ao longo do vínculo laboral, peçam exames laboratoriais a seus funcionários, exames que não têm nenhuma relação com a função desempenhada, ficando o empregado sujeito compulsoriamente a fornecer dados pessoais sensíveis, como urina e sangue. Em recente julgado, o empregado, ao consultar-se com médico do empregador, ao relatar sentir fraqueza e tontura, foi instado a fazer exame de sífilis e HIV, de modo que a notícia do pedido de exame espalhou-se entre seus colegas de trabalho, recebendo ele a alcunha de aidético. Na demanda, foi o empregado indenizado em R$ 5.000,00 a título de danos morais. (TRT-4ª Reg., 2ª Seção de Dissídios Individuais, Ac. 0020696-94.2018.5.04.0000, Rel. Alexandre Correa da Cruz, julg. em 28.04.2019).

30 "Para estar no mundo da tecnologia e usufruir da sua potencialidade de conveniências e utilidades é necessário renunciar à proteção dos dados pessoais, que se tornam, em grande medida, a moeda de troca padrão desses serviços" (MULHOLLAND, Caitlin; A tutela da privacidade na internet das coisas (IoT), cit., p. 493).

31 Ver, nesse sentido, QUINELATO DE QUEIROZ, João. *Responsabilidade civil na rede.* Danos e liberdades à luz do Marco Civil da Internet. Rio de Janeiro: Editora Processo, 2019, p. 78-79. Como já se defendeu na referida obra, pode-se dizer que os termos e as condições de uso – conjunto de regras estabelecidas unilateralmente pelo provedor de aplicações aos usuários para uso de suas plataformas – têm natureza jurídica de contrato de adesão. Segundo Caio Mário da Silva Pereira "chamam-se *contratos de adesão* aqueles que não resultam do livre debate entre as partes, mas provêm do fato de uma delas aceitar tacitamente cláusulas e condições

pensando a médio prazo, é preciso garantir mecanismos que efetivamente permitam o usuário a não consentir com a cessão de seus dados pessoais sem que isso acarrete a impossibilidade de acesso a uma gama de facilidades essenciais à vida moderna. O consentimento, no estado atual da arte, configura-se como um "tudo ou nada": ou se concorda por meio de um clique com os termos de uso unilaterais que tradicionalmente requerem a autorização irrestrita para uso de seus dados pessoais ou não se terá acesso a produtos e serviços. Esse "tudo ou nada" não se apresenta como ferramenta adequada para a tutela da pessoa humana, sendo premente a construção de soluções mais eficazes e que garantam, na prática e não só na *mens legis,* o direito à autodeterminação informativa.

2.2. A figura da autoridade nacional de proteção de dados pessoais

■ Promulgada em 8 de julho de 2019, fruto da conversão da Medida Provisória 869/2018, a Lei n. 13.853/2019 criou a figura da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). O objetivo primordial da Autoridade é, qual órgão da administração pública, zelar, implementar e fiscalizar o cumprimento da LGPD no território nacional, mediante a aplicações de multas pecuniárias aos infratores.

As atividades típicas da ANPD incluem, exemplificativamente, a competência de i) dispor sobre padrões e técnicas utilizados em processos de anonimização de dados pessoais sensíveis; ii) determinar o término imediato de tratamento inadequado de dados pessoais por cento controlador; iii) regulamentar a portabilida-

---

previamente estabelecidas pela outra" (SILVA PEREIRA, Caio Mário da. *Instituições de direito civil.* Contratos. v. III. 20. ed. Rio de Janeiro: Gen Forense, 2016, p. 65). A utilidade prática de se investigar a natureza jurídica destes instrumentos é determinar a incidência da disciplina específica dos contratos de adesão, mormente o comando ora contido nos arts. 423 e 424 do Código Civil. A jurisprudência já se manifestou quanto à abusividade de quaisquer condições constantes dos termos e condições de uso do Facebook nas hipóteses em que se viole os direitos da personalidade. Foi o que o Tribunal de Justiça do Estado do Paraná decidiu ao analisar se para uso do aplicativo *Lulu* seria suficiente a autorização de acesso aos dados pessoais do usuário por meio da adesão aos termos de uso do Facebook. A sentença condenou o aplicativo ao pagamento de R$ 2.000,00 a título de danos morais. No julgado, destacou-se que "no momento da adesão, não há nenhuma advertência ao usuário dos riscos de utilização, inclusive quanto à possibilidade de compartilhamento de seus dados pessoais". Prossegue o juiz, definindo que o mero aceite na cessão de dados pessoais nos aplicativos por meio dos termos de adesão não são suficientes, "sobretudo quando empregado em aplicativo que obtém tais dados na rede social sem nenhuma autorização expressa" (TJPR, 2º Juizado Especial Cível de Maringá, Proc. nº 0015216-72.2013.8.16.0018, Juiz Fernando Swain Ganem, julg. em 18.06.2015).

de de dados pessoais de um controlador a outro; iv) assegurar o respeito a todos os direito dos titulares.[32]

A criação da ANPD, ainda que bem-vinda para assegurar a regulamentação da Lei Geral de Proteção de Dados Pessoais, passou por vetos presidenciais que além de ignorarem o amplo processo de debate público que se submeteu a LGPD, comprometeram seriamente a eficácia e efetividade da dita Autoridade, representando tais vetos um significativo retrocesso no grau de proteção do titular em comparação com a redação aprovada pelo Congresso Nacional.

Excluiu-se a possibilidade de a pessoa física ter o direito de ter revistas por pessoas naturais as decisões tomadas de maneira exclusivamente automatizada, por algoritmos, contida no vetado § 3º do art. 20 da LGPD.[33]. Em suas razões de veto, aduziu o Presidente da República que a possibilidade de revisão humana de processos automatizados "inviabilizará os modelos atuais de planos de negócios de muitas empresas",[34] dando prioridade à tutela patrimonial de pessoas jurídicas em detrimento da proteção dos direitos da personalidade da pessoa humana, em contrariedade com os princípios fundamentais da Constituição.

A sanção presidencial alterou a anterior proibição de compartilhamento de dados pessoais no âmbito do Poder Público, sob o argumento de que tal proibição geraria "insegurança jurídica, tendo em vista que o compartilhamento de

32 A estrutura da ANPD estará temporariamente, nos dois primeiros anos de sua existência, ligada à estrutura da Presidência da República e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial, nos termos do art. 55-A §1º da Lei 13.853/2019. Espera-se que a insegurança jurídica criada pela nomeação exclusiva pelo poder executivo possa ser atenuada com a garantia de autonomia técnica e decisória da ANPD prevista pelo art. 55-B da lei.

33 A redação original do item era a seguinte: "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 3º (vetado): A revisão de que trata o *caput* deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados".

34 Razões de veto, contidas na Mensagem nº 288 de 8.07.2019: "A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das *startups*, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária" (Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm, acesso em 30 ago. 2019).

informações relacionadas à pessoa natural identificada ou identificável, é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas".[35] Criou-se assim uma autorização genérica e irrestrita para que dados pessoais possam ser compartilhados entre entes da administração pública sem a anuência do titular quanto ao seu compartilhamento, um verdadeiro cheque em branco em confronto com a privacidade das pessoas.

Os vetos presidenciais mais preocupantes, contudo, dizem respeito à eliminação das sanções administrativas de suspensão ou proibição do funcionamento da atividade relacionada ao tratamento de dados para aqueles que violassem a norma, antes contidas nos incisos X, XI e XII §§ 3º e 6º da Lei n. 13.709. Os mecanismos – revogados sob a justificativa de "a propositura legislativa, ao prever as sanções administrativas de suspensão ou proibição do funcionamento/exercício da atividade relacionada ao tratamento de dados, gera insegurança aos responsáveis por essas informações" –, em síntese, previam a suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador ou até mesmo a suspensão definitiva. A exclusão das referidas prerrogativas sancionatórias à ANPD esvazia a capacidade sancionatória da agência praticamente reduzindo à pó a eficácia prática da LGPD e deixando o usuário à mercê de penalizações casuísticas e não previstas em lei.

2.3. Um novo sistema de responsabilidade civil

■ Para Pablo Salvador "o direito a danos tem uma especificidade clara e distinta se for analisado do ponto de vista do remédio típico que é paradigmático: as ações de reparação e compensação de danos. Somente remédios dão unidade ao direito a danos.[36] Com efeito, temos a cada dia mais hipóteses de responsabilidades espe-

35 Razões de veto, contidas na Mensagem nº 288 de 8.07.2019. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm, acesso em 30 ago. 2019.

36 Pablo SALVADOR CODERCH (Ed.) et al. *Derecho de Daños*. Análisis, aplicación e instrumentos comparados, 7. ed., 2018. Disponível em http://www.indret.es, acesso em 30 ago. 2019. E continua o autor: "*Pero casi nada más lo hace: hoy en día, en un país occidental tecnológicamente avanzado es crecientemente difícil de concebir que una abogada esté especializada, al mismo tiempo, en litigación derivada de difamación, de protección de datos, de daños masivos, de accidentes de circulación, de daños biofarmacéuticos, de prevención de riesgos laborales, de exposición a sustancias tóxicas, etc. La razón es que el derecho de daños descansa sobre regulaciones crecientemente intrincadas y su conocimiento y dominio es, en la práctica, condición necesaria de la viabilidad de un escrito de demanda de reclamación de cantidad por daños y perjuicios. Nadie*

ciais, tornando impossível a tarefa de sistematizar a disciplina da responsabilidade civil. Basta pensar em quantas sistemas diferentes temos apenas ao interno do Código Civil.

O sistema de responsabilidade civil da LGPD, previsto nos artigos 42 a 45, mostra-se especialíssimo, sendo talvez a principal novidade da lei, e reflete o disposto no inciso X do art. 6º da Lei que prevê o princípio da "responsabilização e prestação de contas, isto é, a 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". O legislador pretendeu não apenas mandar ressarcir, mas quer prevenir e evitar a ocorrência de danos.

Assim, esta responsabilidade especial, à semelhança do que ocorre no Regulamento europeu, está articulada em torno de três noções fundamentais, que devem ser somadas: i) dano, ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação. Com efeito, o regime demanda que o dano seja resultante de violação da LGPD e que tenha sido causado por um agente de tratamento dos dados para então impor a obrigação de ressarcir a parte lesada.

Com efeito, só podem obrigados a reparar esse dano dito "de violação da privacidade" dois protagonistas da lei: os controladores e os operadores, que respondem solidariamente. Já no que se refere às vítimas, trata-se de "outrem", segundo o disposto no *caput* do art. 42, significando dizer que a vítima não se resume aos titulares dos dados, podendo estender-se a qualquer pessoa que sofra um dano resultado de uma violação do RGPD, até mesmo uma pessoa jurídica que considere que o processamento ilegal de dados relativos aos seus funcionários ou feito por um concorrente cause-lhe danos.

Isso poderia fazer crer, ao observador menos atento, que ao determinar o regime de responsabilidade civil que consta dos arts. 42 e seguintes,[37] teria o le-

domina a la vez el acoso sexual, la difamación, la litigación por inhalación de sustancias tóxicas o los accidentes de aviación. Ya no. Mas queda bien anclado en el análisis de los remedios, el cual presta algún otro punto de apoyo a la idea de la unidad positiva del derecho de daños – es decir, a la idea de que este se define por algo más que por su contraposición al derecho de contratos, al derecho penal y al derecho regulatorio". (p. 38)

37 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. (Grifou-se) § 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 controla-

gislador da LGPD optado pelo regime da responsabilidade civil subjetiva, considerando seja a imprescindibilidade do descumprimento (a mencionada violação da lei) por parte do causador, seja a excludente de responsabilidade prevista no inciso II do art. 43, LGDP, determinar a prova de inexistência de falta (*rectius*, violação à legislação) pelo tratador de dados, seja, enfim, a ausência de qualquer menção legislativa à responsabilidade objetiva sem culpa, são todos mecanismos típicos do regime subjetivo.[38]

A possibilidade de inversão do ônus probatório em favor da vítima, configurado no art. 42 § 2º da LGPD,[39] não representa favorecimento que resolverá o usual calvário probatório a que toda vítima tem que se submeter. A regra trazida na LGPD continua sendo a exigência da prova do descumprimento por parte do tratador dos dados e a exceção, mediante decisão fundamentada e após a instauração judicial da demanda, é apenas a sua inversão.

A eventual adoção do regime objetivo de responsabilidade civil poderia ser defendida a partir da constatação de risco atrelado à coleta e tratamento dos dados pessoais, tal qual consta na exposição de motivos do projeto de lei que originou a LGPD, tarefa árdua ao exegeta à luz do enunciado pouco técnico do art. 927 do Código Civil.[40]

Por outro lado, a adoção do regime objetivo apresentaria, para os especialistas, um dilema consubstanciado no empecilho do desenvolvimento de novas

---

dor, 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 (...).

38 LGDP. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I – que não realizaram o tratamento de dados pessoais que lhes é atribuído; *II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados*; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (Grifou-se).

39 LGPD. Art. 42, § 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.

40 "A redação da cláusula geral do parágrafo único do art. 927 não se mostra rigorosa, uma vez que toda e qualquer atividade pode implicar 'riscos para os direitos de outrem'. A excessiva abertura da cláusula tem sido criticada por deixar ao arbítrio do julgador a definição da natureza da responsabilidade, permitindo a fluidez da noção de atividade de risco a instituição de regimes de responsabilidade sem culpa que não estejam caracterizados em lei". (BODIN DE MORAES, Maria Celina. Risco, solidariedade e responsabilidade objetiva. In: *Na medida da pessoa humana:* estudos de direito civil-constitucional. Rio de Janeiro, Editora Processo, 2016, p. 386).

tecnologias tão bem-vindas ao dia a dia do usuário. Com efeito, afirma-se que a adoção do regime objetivo ampliaria o número de demandas ressarcíveis, inibiria o desenvolvimento e a indústria, supostamente, não veria atratividade no desenvolvimento de novas tecnologias de tratamento de dados no Brasil. Assim como no início do processo de industrialização, com fundamento na ideologia liberal baseado no modelo individualista-liberal de responsabilidade, propugnava-se a exclusão de qualquer responsabilização por atividades perigosas como um meio de evitar que o progresso técnico viesse a ser dificultado pelo pagamento de indenizações, argumentando-se em suma, que a objetivação da responsabilidade no tratamento de dados pessoais inibiria o desenvolvimento de novas tecnologias.[41] Cuida-se de falso dilema pois a história já demonstrou que a adoção dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não limitaram o desenvolvimento de novas tecnologias. Ao contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade fundado na atenção e no cuidado para com o lesado.[42] Ademais, já pontuava Rodotà, o argumento de eventual aumento dos custos de proteção dos dados pessoais para as empresas não é decisivo, vez que não se pode estimar que interesses ligados à proteção de dados pessoais dos titulares sejam de *status* inferior aos interesses empresariais.[43]

A adoção do regime de responsabilidade civil objetiva fundada no risco da atividade, assim, à luz do art. 927, parágrafo único do Código Civil e *ex vi* do aparente risco contido na atividade, pareceria ser um caminho para assegurar a mais efetiva proteção ao titular dos dados pessoais.[44] Como já se sustentou, o

41 "No início do processo, ainda com fundamento na ideologia liberal, propugnava-se a exclusão de qualquer responsabilização por atividades perigosas, sustentando-se a aplicação da regra segundo a qual 'as perdas devem ficar onde caírem', como meio de evitar que o progresso técnico viesse a ser dificultado pelo pagamento de indenizações". (BODIN DE MORAES, Maria Celina. Risco, solidariedade e responsabilidade objetiva, cit., p. 391).

42 GONÇALVES, Carlos Roberto. *Responsabilidade civil*. 9. ed. São Paulo: Saraiva, 2006, p. 25.

43 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 53.

44 Pode-se argumentar, não sem razão, que a lei especial (LGPD), ao trazer o regime de responsabilidade civil subjetivo, prevalece em face do Código Civil pelo critério da especialidade, de modo que a atração do regime objetivo fundado na cláusula geral de atividade de risco contida no art. 927, parágrafo único do Código Civil não seria instrumento capaz de atrair o regime objetivo. Por outro lado, parece-nos que de acordo com a hermenêutica mais adequada, o critério da especialidade não é o único (mas tão somente um de tantos outros disponíveis)

sistema atual de responsabilidade civil parece ao menos indicar para a subversão da antiga coerência do sistema ao superar, em casos cada vez mais numerosos, a identificação do culpado, melhor protegendo assim as vítimas lesadas, ao atribuir o dever de indenizar àquele que com sua atividade – como o tratador de dados – gera ocasião ou oportunidade de dano.[45]

A nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de "prestação de contas". Esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa" encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente".

Até hoje, como é sabido, as empresas simplesmente cumprem o expediente fornecendo um *kit* de documentos (formulários de informações e consentimento, política de privacidade, documento de segurança etc.) aos quais ninguém realmente presta atenção. A partir de 2020, quando a lei entra em vigor plenamente, qualquer organização a ela sujeita deverá provar: i) que avaliou e, se necessário, redesenhou adequadamente o processamento de dados pessoais; ii) que as medidas de segurança implementadas são adequadas e eficazes; iii) que aplica uma política de privacidade interna com obrigações claras, ações concretas vinculadas a cada uma e que foram designados os responsáveis pelo cumprimento; iv) que nomeou um encarregado e que exige esse mesmo cumprimento responsável de seus funcionários e na sua cadeia de terceirização.

Além disso, um novo mapa de consequências foi introduzido em caso de descumprimentos: i) em questões administrativas, o montante das sanções previstas no regulamento indica a relevância que a proteção de dados pessoais adquirirá: até 50 milhões de reais ou 2% do faturamento anual global da empresa para as infrações mais graves (art. 52); ii) a criação de uma nova variedade de ações coletivas de responsabilidade civil; iii) a obrigação de comunicar à Agência e às partes interessadas os eventos de "violação de dados" ou violações da segurança, o que

---

para auxiliar o intérprete na aplicação da norma, de modo que havendo colisão de um ou mais critérios deverá prevalecer aquele que efetivamente assegurar a máxima tutela da pessoa humana em razão da cláusula geral contida no art. 1º III da Constituição Federal.

45 BODIN DE MORAES, Maria Celina. Risco, solidariedade e responsabilidade objetiva, cit., p. 401.

abrirá o caminho para novas reivindicações de indenização pelas empresas e indivíduos afetados.[46]

Em termos práticos, estes novos princípios requerem que as empresas analisem quais os dados que tratam, com que finalidade e que tipo de operações de tratamento levam a cabo. Exige-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais, terá não apenas que cumprir a lei, mas também terá que provar que está em conformidade com a Lei. Caberá às empresas, em vez de à Administração Pública, a responsabilidade de identificar os próprios riscos e escolher e aplicar as medidas apropriadas para mitigá-los.

2.4. A proteção de dados pessoais nas relações de consumo

■ É cediço que o maior volume de dados pessoais, na prática, é colhido no âmbito das relações de consumo, sendo premente a indagação: estando o julgador diante da análise de coleta ou tratamento irregular de dados pessoais, a qual diploma deverá ele recorrer? *Ab initio,* duas advertências devem, contudo, serem assumidas. A primeira é a de que o ordenamento jurídico é unitário e, assim o sendo, deverá ser interpretado sistematicamente e não em tiras, de modo que a indagação sobre qual instrumento se amolda adequadamente à uma relação pode ser substituída pela indagação acerca de qual (ou quais) é o instrumento que efetivamente assegura a tutela da pessoa naquela relação concreta.[47] A segunda é que uma vez que o consumidor é tutelado pela própria Carta Maior e tem seu direito à proteção de dados assegurado constitucionalmente, seriam dispensáveis instrumentos infralegais específicos para que se viabilizasse a proteção dos dados pessoais do consumidor. A edição de norma posterior pelo legislador tem o condão de regular em detalhes a tutela e o regime de responsabilidade, tutela que não seria negada

46 Nesse sentido, o direito à indenização por danos por infração não é novo; a novidade é que será mais fácil provar o evento prejudicial que determina a responsabilidade: a discussão estará, dentro do perímetro dessa responsabilidade, entre outros fatores.

47 Já se disse que "acolher a construção da unidade (hierarquicamente sistematizada) do ordenamento jurídico significa sustentar que seus princípios superiores, isto é, os valores propugnados pela Constituição, estão presentes em todos os recantos do tecido normativo, resultando, em consequência, inaceitável a rígida contraposição direito público x direito privado. Os princípios e valores constitucionais devem estender-se a todas as normas do ordenamento, sob pena de se admitir a concepção de um *mondo in frammenti*, logicamente incompatível com a ideia de sistema unitário" (BODIN DE MORAES, Maria Celina. A caminho de um direito civil constitucional. In: *Na medida da pessoa humana*, cit., p. 9).

ao consumidor e titular de dados pessoais caso não fosse editada norma regulamentadora, esvaziando ainda mais a utilidade, para fins de merecimento de tutela, sobre a adequação desse ou aquele instrumento legislativo. Afinal, a proteção da pessoa, determinada pelo constituinte originário, não pode ficar à mercê da atuação do constituinte derivado por estar a pessoa na cimeira do ordenamento.

De toda sorte, antevendo-se possíveis discussões jurisprudenciais, poder-se-ia cogitar de aparente antinomia entre o artigo 43 do CDC[48] e os arts. 42 e 45 da LGPD, inaugurando a discussão ainda acerca do regime de responsabilidade civil aplicável à proteção dos dados pessoais na seara consumerista. Cuidando-se de tratamento de dados no âmbito de relações de consumo, responderia o controlador de forma subjetiva e mediante prova da culpa, à luz do art. 42 da LGDP e à luz do art. 186 do Código Civil, ou responderia objetivamente à luz do art. 14 do CDC por haver falha na prestação do serviço ou no fornecimento do produto?

A LGPD assume a defesa do consumidor como um de seus fundamentos (art. 2º VI) e no art. 45 estabelece que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente". Uma leitura desavisada do dispositivo e contrária à unidade do ordenamento poderia levar à conclusão incorreta de que a LGPD não se aplica às relações de consumo, sendo acertado concluir que o art. 45 quer, em verdade, apontar para que o regime de responsabilidade civil do controlador ou operador de dados pessoais no âmbito das relações de consumo será objetivo quando violada qualquer disposição da própria LGPD ou de quaisquer garantias de proteção de dados pessoais nas relações de consumo contidas nos arts. 43 a 44 do CDC. Em outras palavras, estando o intérprete diante da violação dos princípios e garantias do titular de dados pessoais no âmbito de relações de consumo, aplicar-se-á o regime de responsabilidade civil objetiva contida no art. 14 do CDC, com fulcro no art. 45 da LGPD e, no que diz respeito ao rol de garantias e direitos do titular de dados pessoais e dos deveres dos tratadores e coletores de dados pessoais, aplica-se a LGPD em sua inteireza.

Por derradeiro e acerca das implicações de dados pessoais no âmbito das relações de consumo, deve-se destacar, ainda, o retrógrado veto presidencial conferido ao anterior art. 55-K da LGPD, que estabelecia ser competência da Autoridade Nacional de Proteção de Dados a tarefa de articular sua atuação com o Sistema Nacional de Defesa do Consumidor, integrante do Ministério da Justiça, com

48 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.

vistas ao desenvolvimento de políticas específicas de proteção de dados pessoais às relações de consumo. Ainda que essa integração possa ser executada na prática sem o dispositivo em vigor, o veto presidencial pode indicar a indesejável indiferença quanto à vulnerabilidade especial do consumidor titular de dados pessoais que deva ser destinatário de políticas públicas específicas.

3. NOTAS CONCLUSIVAS

■ A cessão de dados pessoais passa a ser condição para acesso a bens e serviços essenciais, de modo que consentir ou não com seu uso não tem se apresentado como opção efetivamente viável contemporaneamente. No Brasil, o metrô de São Paulo utilizará reconhecimento facial junto aos seus diários 3 milhões de passageiros.[49] No Rio de Janeiro, já está em fase de testes pela Secretaria de Segurança Pública o sistema de reconhecimento facial que erroneamente levou à prisão uma senhora inocente.[50] Recentemente, uma consumidora viu-se refém da violação de seus dados pessoais decorrentes da falha na prestação de serviços de operadora de telefone celular que, em razão da má prestação dos serviços, teve seu WhatsApp invadido por duas vezes.[51] A cada passo dado, o cidadão cede seus dados pessoais sem ter consentido ou mesmo sem sequer saber. Ilustrativo desse dilema foi a recente divulgação de que o Facebook havia contratado diversos transcritores de conteúdo de áudio de seus usuários.[52]

No esforço de aprimoramento das ferramentas de proteção da privacidade, é rica a advertência de Rodotà para a importante revisão dos critérios de classificação das informações pessoais

> segundo uma escala de valores renovada, na qual deveria ser garantido o máximo de opacidade às informações suscetíveis de originar práticas discriminatórias e o máxi-

49 "Metrô de São Paulo terá vigilância com reconhecimento facial". (Folha de São Paulo, https://www1.folha.uol.com.br/cotidiano/2019/07/metro-de-sp-tera-vigilancia-com-reconhecimento-facial.shtml, acesso em 30 ago. 2019).

50 Jornal O Globo. Disponível em https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913, acesso em 30 ago. 2019.

51 TJSP, 22ª C. de Dir. Priv., Ap. Cív. 1105778-06.2018.8.26.0100, Rel. Des. Roberto Mac Cracken, julg. em 02.08.2019.

52 "*Facebook Inc. has been paying hundreds of outside contractors to transcribe clips of audio from users of its services, according to people with knowledge of the work*". Agência Bloomberg. Disponível em https://www.bloomberg.com/amp/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio, acesso em 30 ago. 2019.

> mo de transparência àquelas que, referindo-se à esfera econômica dos sujeitos, concorrem para embasar decisões de relevância coletiva.[53]

O binômio regular ou não regular expõe um falso dilema, já que a verdadeira dúvida não é se deve o Estado regular ou não a proteção de dados pessoais mas, sim,

> à possibilidade de atribuir um valor orientador, para o futuro, a categorias e conceitos que, como o dos contratantes hipossuficientes ou da privacidade, foram elaborados para situações em que a informação como um recurso ainda não ocupava posição central.[54]

A rapidez com que inovações tecnológicas são introduzidas no cotidiano agudiza a ancianidade do Direito e mostra como ele fica sempre atrás nessa corrida e, inevitavelmente, não consegue corresponder aos desafios que lhe são postos.[55] Desse modo, na busca de mecanismos eficazes para a proteção efetiva dos titulares de dados pessoais, é preciso que se garanta que o não consentimento para determinadas utilizações não implique em vedação absoluta de acesso a determinados bens e serviços. O consentimento do titular de dados pessoais e sua autodeterminação informativa não podem estar à mercê do tudo ou nada dos termos e uso de condições de plataformas e aplicativos, sendo premente que, na prática, seja assegurado ao usuário o acesso a bens, serviços e facilidades tecnológicas essenciais para a vida em democracia sem que se exija que o titular se despida de todo e qualquer dado pessoal por meio de cliques instantâneos, sob pena de a autodeterminação informativa tornar-se letra morta da lei.

As características peculiares da hipótese de responsabilidade civil em questão – que se expressam principalmente na regulação detalhada das obrigações comportamentais do controlador e do operador de dados, com um novo foco no perfil de gerenciamento de riscos, especialmente relacionado ao uso da inovação

53 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 35.

54 RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 57.

55 "As inovações tecnológicas potencializam a velhice do Direito. Vivemos num momento em que a tecnologia se desenvolve a largos passos e o Direito não consegue acompanhar o seu ritmo. Não se tratando de ciência preditiva, o Direito sempre fica atrás na corrida com – ou para alguns, contra – a tecnologia. De fato, começam a surgir conflitos e questionamentos que devem ser respondidos ou referidos pelo Direito, sempre depois que eles se apresentam como resultado do uso de novas tecnologias" (MULHOLLAND, Caitlin. O direito à privacidade na Internet das Coisas (IoT), cit., p. 485).

tecnológica – possibilita garantir a efetividade do recurso de compensação, adaptando-o às especificidades da atividade de processamento de dados pessoais e aos requisitos de proteção que ele apresenta. Desse modo, criou-se um modelo, por assim dizer, mais maduro de responsabilização civil, no qual se vai além da responsabilidade dos agentes, tendo-se em vista, especialmente, a evitação de danos. Admitida sua natureza multifuncional, não foram postos obstáculos ao lançamento dessa figura complexa de responsabilidade especial descrita pelos art. 42 e seguintes da LGPD, no mesmo feitio do regulamento europeu.

Estando a Constituição no ápice do ordenamento e sendo fundamento axiológico primeiro de todo o sistema, a introdução da cláusula geral de tutela da pessoa humana contida no art. 1º III impõe a proteção da privacidade não somente a partir da ótica proprietária[56] segundo a qual os dados pessoais seriam bens móveis objeto de mera apropriação mas, ao revés, da prevalência do aspecto não patrimonial dos dados pessoais (como atributos indissociáveis à sua dignidade) em face de seu aspecto patrimonial. E, para tanto, é fundamental a instituição de ferramentas verdadeiramente eficazes.

56 "Não é apenas uma certa preguiça intelectual ou a incapacidade de vislumbrar além da lógica proprietária os fatores que continuam a atribuir ao tema da privacidade um valor que não corresponde mais à dimensão efetiva que os problemas institucionais das informações assumiram. No fundo, existem razões precisas de política do direito que fazem com que isto aconteça". (RODOTÀ, Stefano. *A vida na sociedade de vigilância*, cit., p. 49-50).

Maria Celina Bodin de Moraes · Professora Titular de Direito Civil da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ) e do Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Doutora em Direito Civil pela Universidade de Camerino, Itália. E-mail: mcbm@puc-rio.br

João Quinelato de Queiroz · Doutorando e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professor de Direito Civil do IBMEC. Advogado. E-mail: joaoquinelato@gmail.com.

REFERÊNCIAS

BODIN DE MORAES, Maria Celina. Apresentação. In: RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008.

_____. Danos à pessoa humana. Uma leitura civil-constitucional dos danos morais. 2. ed. revista. Rio de Janeiro: Editora Processo, 2017.

_____. Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Editora Processo, 2016.

DONEDA, Danilo. Da privacidade à proteção de dados. Rio de Janeiro: Renovar, 2005.

GONÇALVES, Carlos Roberto. Responsabilidade civil. 9. ed. São Paulo: Saraiva, 2006.

LEWICKI, Bruno. A privacidade da pessoa humana no ambiente de trabalho. Rio de Janeiro: Renovar, 2003.

MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: REIA, Jessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo (Org.). Horizonte presente: tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito, Fundação Getúlio Vargas, 2019, p. 485-495. Disponível em <https://bibliotecadigital.fgv.br/dspace/handle/10438/27448>, acesso em 30 ago. 2019.

QUINELATO DE QUEIROZ, João. Responsabilidade civil na rede. Danos e liberdades à luz do Marco Civil da Internet. Rio de Janeiro: Processo, 2019.

RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008.

SALVADOR CODERCH, Pablo. (Ed.) Derecho de Daños. Análisis, aplicación e instrumentos comparados. 7. ed., 2018. Disponível em http://www.indret.es, acesso em 30 ago. 2019.

SCHREIBER, Anderson. Novos paradigmas da responsabilidade civil. Da erosão dos filtros da reparação à diluição dos danos. São Paulo: Atlas, 2015.

_____. PEC 17/19: Uma Análise Crítica. Carta Forense. Disponível em http://www.cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345, acesso em 30 ago. 2019.

SILVA PEREIRA, Caio Mário da. Instituições de direito civil. v. III. Contratos. 20. ed. rev. e atual. Caitlin Mulholland. Rio de Janeiro: Gen Forense, 2016.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. Revista Pensar, Fortaleza, 2019. Disponível em <https://periodicos.unifor.br/rpen/article/view/9407/pdf >, acesso em 30 ago. 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, vol. IV, Dec. 15, 1890, nº 5. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, acesso em 30 ago. 2019.

Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais

IRINEU FRANCISCO BARRETO JUNIOR
SAMYRA HAYDÊE DAL FARRA NASPOLINI

RESUMO

■ Este artigo analisa a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709, de 14 de agosto de 2018), especialmente nos quesitos que determinam a obrigatoriedade de consentimento do titular para tratamento de dados pessoais. Sua problematização é situada no contexto da Sociedade da Informação, era inaugurada pelo avanço tecnológico informático do qual decorreu uma completa erosão da privacidade e da intimidade, decorrentes das inúmeras possibilidades de exploração mercantil dos dados pessoais. Adota a premissa de que não existem dados inexpugnáveis na Internet e o uso das aplicações informáticas, associado à inteligência artificial e ao Big Data, tornam urgente o desenvolvimento de mecanismos que possam assegurar ao titular dos dados pessoais autonomia quanto ao destino dos seus registros. Conclui não ser plausível qualquer prognóstico otimista quanto à preservação da intimidade dos usuários das aplicações informáticas *via web* e pela premência de garantias aos usuários de ferramentas tecnológicas, legítimos titulares dos seus dados, de que poderão determinar quais informações consentem em tornar públicas. Conduta esta denominada *autodeterminação informacional*.

ABSTRACT

■ This paper analyzes the Brazilian Personal Data Protection Law (Law 13.709, of August 14, 2018), focusing on the issues that determine the holder's obligatoriness

consent to process personal data. Its problematization is situated in the context of the Information Society, was inaugurated by the computing technological advance, which resulted in a complete erosion of privacy and intimacy, resulting from the numerous possibilities of personal data commercial exploration. The assumption is that there is no impregnable data on the Internet and the use of computer applications, associated to artificial intelligence and Big Data make it necessary to develop mechanisms that can ensure the personal data holder autonomy as to the destination of their records. It concludes that it's not plausible any optimistic prognosis regarding the preservation of the users privacy of web-based computer applications and the urgency of guaranteeing the users technology tools, legitimate holders of their data, that they will be able to determine which information they consent to make public. This is called *informational self-determination*.

INTRODUÇÃO

A sociedade contemporânea tem sido impulsionada, nas últimas décadas, por um novo estágio de desenvolvimento econômico marcado pelo avanço tecnológico e pela propulsão de uma nova indústria de geração de valor, cuja matéria prima essencial advém da avalanche de dados gerada na utilização das aplicações tecnológicas e disseminada em escala mundial pela internet. Atualmente, esses fenômenos confundem-se com as práticas mais comezinhas, cotidianas, provocando a naturalização de práticas que, mesmo corriqueiras, inauguram novos paradoxos para as quais ainda não se vislumbram equacionamento, dentre os quais destaca-se a completa aniquilação de qualquer possibilidade de privacidade no mundo virtual.

O crescimento exponencial da valoração de dados pessoais, disponibilizados com o uso da internet e de aplicativos, deriva da possibilidade de formulação de sofisticados perfis, individuais ou de segmentos sociais, que passam a ser aplicados em orientação de anúncios publicitários, análises de mercado, prospecção de tendências de investimento, probabilidade de aquisição de bens e até mesmo na formulação de *clusters* de cidadãos com o intuito de direcionamento de campanhas eleitorais – amplia-se nas agendas sociais e jurídicas, em escala global, a necessidade de estabelecer mecanismo que regulem a coleta, uso, armazenamento, tratamento e proteção de dados pessoais.

Necessária a ressalva de que não é adequado olvidar os inegáveis avanços advindos com a tecnologia informacional, nas décadas recentes, nas áreas das comunicações interpessoais, medicina e saúde, economia, educação, cultura, acesso ao conhecimento, pesquisa científica e, em suma, nas mais diversas áreas da so-

ciabilidade humana. Não obstante, "com a crescente adesão ao uso da Internet, têm-se desenvolvido uma sensação ainda difusa, entre os seus usuários, de que *não existe qualquer possibilidade de sigilo, privacidade e intimidade on-line"*(BARRETO JUNIOR, 2015, p.418). Mais do que isso, o uso da rede oferece informações para um movimento em sentido reverso, no qual anúncios de produtos e ofertas de mercadorias em *websites*, mensagens recebidas por correio eletrônico, *pop-ups* e várias outras comunicações publicitárias que o usuário recebe, são orientadas pelo uso que ele próprio faz da *Internet*. (BARRETO JUNIOR, 2015, p.418).

Este artigo situa o novo estágio de desenvolvimento tecnológico e econômico denominado como Sociedade da Informação e a resposta do poder legislativo brasileiro formatada com o intuito de mitigar a *hiperexposição* dos usuários da internet, denominada Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709, de 14 de agosto de 2018), que passará a gerar efeitos em agosto de 2020, com foco específico na determinação de consentimento e livre esclarecimento do titular para tratamento de dados.

1. SOCIEDADE DA INFORMAÇÃO E OS PARADOXOS ENTRE AVANÇO TECNOLÓGICO E PROTEÇÃO DA PRIVACIDADE

■ A revolução tecnológica ocorrida nos meios de comunicação deu origem a uma nova era denominada como *Sociedade da Informação*. A sua principal característica é a viabilidade tecnológica do acesso a informações advindas de qualquer lugar do mundo em tempo quase real, de forma inédita na história pretérita. Denota-se que a *informação é o centro gravitacional* desta nova era e, em outras palavras, é possível afirmar que o tratamento de dados adquire novos patamares de valor comercial. Barreto Junior (2015, p. 410) ao tratar do tema esclarece que:

> O advento do *Informacionalismo* é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no qual há uma gradativa valoração da informação como mercadoria e fator de geração de valor econômico (...). As megacorporações informativas (*Google*, *Facebook* e *Yahoo*, entre outras) acumulam vestígios de informações sobre os usuários da Internet, tais como seus padrões de navegação, compras realizadas on-line, preferências culturais, religiosas e ideológicas, *websites* de interesse, verbetes e expressões pesquisadas nos *websites* de busca, entre outras, "*impressões digitais eletrônicas"* que servem para estabelecer uma categorização minuciosa de cada usuário na rede. (BARRETO JÚNIOR (2015, p. 410)

Para a exata compreensão dos efeitos da Sociedade da Informação e da urgência que impõe à adoção de práticas que protejam dados pessoais, torna-se inexorável estabelecer a vinculação entre *informação* e seu *valor monetário*. Marcelo Xavier de Freitas Crespo (2011, p. 38) destaca que "a informática se transformou em importantíssimo instrumento de informação e esta, por seu turno, tornou-se valioso bem econômico". Para Vieira e Evangelista (2015: p. 524- 533), as aplicações de Inteligência Artificial – recurso tecnológico que permite o desenho de sofisticados algoritmos que oferecem respostas às indagações humanas – buscam obter dados dos sujeitos e analisa-los enquanto agentes econômicos e, principalmente, agentes de consumo: "o que desejam, o que compram, quando e como o fazem, quanto estariam dispostos a pagar por esses desejos, e assim por diante. "

Nesse cenário, a aplicação de tecnologias de tratamento e interpretação dos dados pessoais, tais como o *Big Data*[1] *(*CUKIER; MAYER-SCHÖNBERGER, 2012*)*, análise semântica, mineração de dados e inteligência artificial, têm possibilitado a coleta e organização de gigantescos bancos de dados, padronizados e individualizados, para cada usuário da rede. Com a convergência tecnológica propiciada pelos smartphones, os dados disseminados pelo uso da internet podem ser vinculados, "cruzados" como conceituado em análises quantitativas, com atributos individuais, tais como nome, sexo, idade, endereço eletrônico, CPF e rendimentos. É possível imaginar a meticulosidade dos perfis elaborados a parti desse cruzamento, entre dados individualizados, e o perfil de consumo, cultural, ideológico, religioso e futebolístico, por assim dizer, de cada pessoa.

Além das questões relacionadas à privacidade e à intimidade, imprescindíveis socialmente, várias indagações surgem quando é assumida a premissa de que *não existem dados inexpugnáveis na Internet*. São atingidos, dessa forma, patamares inéditos de aplicação das tecnologias da informação na derrocada de barreiras clássicas entre o público e privado.

Viera e Evangelista (2015, p. 524- 533) apontam um aspecto crucial na compreensão das aplicações mercantis de dados pessoais. Esses dados *sequer precisam referenciar indivíduos de forma específica, nominal*, para que sejam úteis: "eles já são valiosos enquanto tendências de mercado, ou como informação geral sobre

1 "Big Data é qualquer tipo de dado – estruturado ou não – como um texto, áudio, vídeo, cliques, registros e outros. Big Data é mais do que apenas uma questão de tamanho: é uma oportunidade de descobrir insights em novos tipos de dados e conteúdo, para tornar o seu negócio mais ágil. " In: CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. Big Data – Como Extrair Volume, Variedade, Velocidade e Valor da Avalanche de Informação Cotidiana. Rio de Janeiro: Campus, 2012.

grupos estratificados da sociedade (por variáveis demográficas, culturais ou comportamentais). " Apontam "o que fornece valor a esse "produto audiência" é a vigilância: é ela que permite construir perfis ricamente detalhados dos membros dessa audiência, e sem ela não seria possível exibir anúncios profundamente customizados, variando de acordo com o membro da audiência, o dispositivo que ele utiliza, o local em que ele se encontra, o seu comportamento de navegação... (VIEIRA; EVANGELISTA, 2015: p. 524- 533). "

Ainda mais que, conforme assinalado por Vieira e Evangelista (2015: p. 524-533) a vigilância estatal clássica não é o único tipo de olhar ao qual as pessoas atualmente são expostas. "Há um amplo espectro de mecanismos e práticas de vigilância que são operadas por outros atores, sob uma lógica distinta: a vigilância que denominaremos de mercantil. " Essa vigilância materializa-se nos mecanismos "cada vez mais sofisticados e abrangentes de publicidade online comportamental (incluindo os mecanismos de coleta de dados que a alimentam) e atravessa hoje uma boa parte de toda troca de informações realizada no globo. " Nessa perspectiva, dois fatores multiplicam o potencial da vigilância mercantil:

Da perspectiva do primeiro desses fatores, existe uma grande demanda por uma publicidade lucrativa, que alie eficiência e baixo custo. Da perspectiva do segundo fator, *sites e aplicativos de smartphones são espaços publicitários com características novas em relação às mídias analógicas: por um lado, eles são comparativamente abundantes* (sua quantidade não é limitada pelas concessões estatais ou pela largura do espectro, como no caso dos canais de televisão), *e muito flexíveis para a exibição de publicidade (podem exibir anúncios diferentes para cada membro da audiência, e o custo operacional dessa customização é relativamente baixo)*; e por outro lado, as tecnologias utilizadas na internet e em smartphones permitem que todo o comportamento de sua audiência seja registrado e equacionado visando aumentar a eficiência dessa publicidade (VIEIRA; EVANGELISTA, 2015: p. 524- 533).

A vigilância *on-line* tornou-se, portanto, cada vez mais intensa sobre os usuários da rede mundial de computadores, percepção que tem sido disseminada, mesmo que de forma ainda difusa, entre os usuários das tecnologias informáticas.

A resposta oferecida pelo poder legislativo brasileiro para mitigar a superexposição daqueles que se utilizam das ferramentas tecnológicas e, como contrapartida, cedem seus dados pessoais reside na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709, de 14 de agosto de 2018). A próxima unidade deste artigo aborda aspectos da LGPD previstos com o intuito de determinar a obrigatoriedade de consentimento do titular para tratamento dos dados pessoais.

2. DETERMINAÇÃO DE CONSENTIMENTO DO TITULAR PARA TRATAMENTO DE DADOS PREVISTA NA LGPD

■ Conforme vislumbrado nas décadas recentes, é possível estabelecer um prognóstico de que o ritmo dessa máquina de produção de valor, *alimentada por dados,* recrudescerá nos próximos anos. E ainda que não é plausível qualquer previsão otimista quanto à preservação da intimidade dos usuários das aplicações informáticas e da internet. Torna-se consensual a necessidade de que os usuários de ferramentas tecnológicas, legítimos titulares dos seus dados, possam limitar as informações que desejam, ou não, tornar públicas, com o intuito de proteger sua privacidade. "Trata-se da autodeterminação informacional fundada na perspectiva de que o próprio usuário deve ter controle sobre as suas informações pessoais, autodeterminando-se." (RODOTÁ, 2015, p. 267)

O desenvolvimento da informática colocou em crise o conceito de *privacidade*, e, a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em banco de dados. (RODOTÁ, 2015, p. 267)

Ainda segundo Stefano Rodotá (2015, p. 267) destaca que, inicialmente, a proteção à privacidade era estática (negativa – correspondente ao que não fazer), enquanto que nos tempos atuais ela é dinâmica (positiva – correspondente ao controle de nossas próprias informações):

A distinção entre o direito ao respeito da vida privada e familiar e o direito à proteção dos dados pessoais não é bizantina. O direito ao respeito da vida privada e familiar reflete, primeira e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para tomada de medidas – *i.e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos. (...) É de fato o fim da linha de um longo processo evolutivo experimentado pelo conceito de privacidade – de uma definição original de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser constituída. (Grifos nossos). (RODOTÁ, 2015, p. 267)

No intuito de mitigar essa vigilância extrema, e para que se possa desenvolver um ecossistema de confiança para as sociedades e suas economias baseadas em dados, é imprescindível respeitar as legítimas expectativas dos usuários (BIONI,

2017), quando são levados a ceder seus dados pessoais em troca das aplicações e serviços. Essas iniciativas são necessárias para preservar direitos muito caros na tradição liberal contemporânea, direitos de proteção do indivíduo contra a violação da sua intimidade pelo *Estado* e, hodiernamente, pelo *Mercado*.

Com esse intuito, adentrou no ordenamento jurídico brasileiro a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709, de 14 de agosto de 2018), que passará a gerar efeitos em agosto de 2020 assim que superada a *vacatio legis*. O *ethos* dessa lei é orientado à *autodeterminação do usuário, legítimo titular dos dados pessoais, quanto à aplicação e tratamento aos quais serão submetidos seus registros informáticos*. Essa autodeterminação repousa na necessidade de manifestação expressa de consentimento e esclarecimento do titular dos dados pessoais quanto à autorização para destinação dos seus rastros digitais. Bioni (2019, p.134) assinala que a análise dos princípios e a maneira pela qual a LGPD disseca o consentimento ao longo do seu corpo normativo "acabam por revelar uma forte preocupação (...) sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais (BIONI, 2019, 134).

Ainda segundo Bioni, "o consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral (BIONI, 2019, 134). " Na sua leitura da LGPD:

Grande parte dos seus princípios tem todo seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento dos seus dados e, ainda ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais modernos, como adequação e necessidade, em que o tratamento dos dados deve responder às legítimas expectativas do seu titular. (BIONI, 2019, 1345)

O rol de fundamentos da LGPD, expressos no seu artigo 2º, apontam taxativamente para os preceitos basilares da proteção da privacidade e avançam conceitualmente até a autodeterminação do titular dos dados. Expressam *in verbis*: "I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

Em consonância com seus fundamentos, conforme exposto acima, a LGPD reafirma o alinhamento transnacional brasileiro com os direitos humanos e alude

à dicotomia que eventualmente ocorre entre direitos fundamentais ao assegurar, concomitantemente, a *liberdade de expressão e o desenvolvimento econômico* limitados pela *proteção da privacidade e da autodeterminação informativa* dos usuários da rede e de aplicações informáticas. Será necessário acompanhar a aplicação da LGPD pelos tribunais, superada a *vacatio legis*, frente aos paradoxos provocados pela *exploração industrial* dos dados, *vis* à *vis* a determinação de consentimento dos usuários para tratamento dos seus registros.

A LGPD avança, no rol do seu artigo 5º, em importantes definições sobre dados pessoais[2], dados sensíveis e anonimizados, titularidade, tratamento e consentimento – sem os quais é inviável assegurar os parâmetros mínimos de proteção da privacidade e voltados a assegurar o protagonismo dos usuários quanto às suas pegadas digitais.

> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

2 SETZER define *dado* "como uma sequência de símbolos quantificados ou quantificáveis. Quantificável significa que algo pode ser quantificado e depois reproduzido sem que se perceba a diferença para com o original. (...) também são dados fotos, figuras, sons gravados e animação, pois todos podem ser quantificados ao serem introduzidos em um computador, a ponto de se ter eventualmente dificuldade de distinguir a sua reprodução com o original. É muito importante notar-se que, mesmo se incompreensível para o leitor, qualquer texto constitui um dado ou uma sequência de dados. Isso ficará mais claro no próximo item. Com essa definição, um dado é necessariamente uma entidade matemática e, desta forma, é puramente sintático. Isto significa que os dados podem ser totalmente descritos através de representações formais, estruturais. Sendo ainda quantificados ou quantificáveis, eles podem obviamente ser armazenados em um computador e processados por ele." SETZER, V. W. Dado, informação, conhecimento e competência. DataGramaZero – Revista de Ciência da Informação, Rio de Janeiro, n.0, dez. 1999. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html. Acesso: 07 ago. 2019.

> (...)
> 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;
> XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (...).

Conforme o exposto no artigo 5º e, não obstante, a LGPD categorizar distintamente os dados entre *pessoais, sensíveis e anonimizados*, é necessário aduzir que para alcançar efetividade e produzir efeitos a Lei deverá enfrentar entraves tecnológicos significativos. Existem tecnologias disponíveis e que permitem a conexão entre bancos de dados distintos (*linkage*, mesclagem, análises de *clusters*), gerados pela avalanche informacional. A privacidade torna-se cada vez mais inatingível uma vez que se perdeu, com a tecnologia, a possibilidade de assegurar a diferença entre pessoa identificada e identificável. A dicotomia entre dados anônimos (sigilosos) e dados pessoais identificáveis não é mais viável em decorrência do aparato tecnológico e das técnicas de *linkage* de bancos de dados, além do georreferenciamento que mapeia a distribuição geográfica dos dados ao monitorar a circulação dos smartphones.

Ao instalar aplicativos em seus aparelhos, o usuário é instado a autorizar que o novo programa acesse dados sobre chamadas realizadas pelo aparelho, localização, fotos, mídias e demais arquivos do dispositivo. Sem esse aceite o aplicativo não permite a exploração de suas funcionalidades pelo usuário, sinalizando um dos principais desafios a serem enfrentados pela LGPD.

É notório ainda que a aplicação de tecnologias como *Big Data*[3], análise semântica e inteligência artificial tem propiciado a agregação de registros dispersos em bancos de dados padronizados e individualizados para cada usuário da rede.

3 "Big Data é qualquer tipo de dado – estruturado ou não – como um texto, áudio, vídeo, cliques, registros e outros. Big Data é mais do que apenas uma questão de tamanho: é uma oportunidade de descobrir insights em novos tipos de dados e conteúdo, para tornar o seu negócio mais ágil." (CUKIER, MAYER-SCHÖNBERGER, 2012).

Com a convergência tecnológica, dados que abrangem categorias como nome, sexo, idade, endereço eletrônico, CPF, rendimentos, associados ao perfil cultural, ideológico e aos padrões de consumo de cada usuário da internet, tem potencializado a captação e geração de riqueza – por intermédio direto da utilização e venda desses dados pessoais.

Recorde-se ainda que a anonimização não impede que os dados sejam usados para formulação de perfis grupais e categorização de *clusters* conforme gênero, raça/cor, orientação sexual, religiosa, política, deslocamentos geográficos etc. E a partir desses agrupamentos extrair valor dos registros pessoais. A tecnologia pode, ela própria, mitigar a relevância do consentimento do titular uma vez que, mesmo tratados e tornados anônimos, os dados podem sem muito precisos na elaboração de agregados de registros que, mesmo indiretamente, são muito eloquentes sobre quem são, o que fazem e o que pensam seus donos originais.

Quanto ao tratamento enquanto técnica cuja implementação transforma os dados, de meros registros informáticos em informação, a LGPD o define como" toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (LGPD, 2018, artigo 5º).

A prolixa quantidade de aplicações abrigadas sob a nomenclatura *tratamento* impõe novos desafios ao intuito de assegurar a autonomia do titular dos dados sobre suas destinações. Evidente que novas regras de *compliance* serão formuladas para adequar empresas, órgãos de pesquisa, prestadores de serviços e mesmo a administração pública ao novo paradigma de proteção de dados propalado pela LGPD, outrossim é evidente que será uma tarefa desafiadora assegurar que suas determinações sejam efetivadas.

O artigo sexto determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé, ser pautado por princípios que assegurem seus propósitos legítimos e cujas finalidades sejam informadas ao titular, com tratamento limitado ao mínimo necessário para a realização de suas finalidades e determinações que assegurem a qualidade dos dados, transparência e segurança na sua armazenagem e tratamento. Reza ainda que devam ser adotadas medidas preventivas que mitiguem a ocorrência de danos em virtude do tratamento de dados pessoais. Ainda nesse artigo, determina que os dados não sejam tratados em aplicações que possam gerar discriminação (tratamento para fins discriminatórios ilícitos ou abusivos) e ainda a necessidade de res-

ponsabilização e prestação de contas pelo agente que promove o tratamento dos dados pessoais.

A ratificação da autodeterminação do titular como requisito para tratamento de dados pessoais ressurge no artigo sétimo da LGPD. Este somente poderá ser efetuado mediante o fornecimento de consentimento pelo titular, determina o inciso que ocupa o degrau superior da topografia do referido artigo. Bioni afirma que franquear ao cidadão o controle sobre seus dados pessoais é eixo encontrado pela referida lei para conciliar o rol de fundamentos e determinações nela contido (BIONI, 2019, p.110). O autor afirma que "tão importante quanto este elemento volitivo é assegurar que o fluxo informacional atenda suas legítimas expectativas (BIONI, 2019, p.110). " Somadas estas ao intuito de preservação dos seus direitos de personalidade, têm-se uma interpretação do *ethos* da LGPD que emergirá após o *vacatio legis* com a missão de mitigar a erosão da privacidade assistida na Sociedade da Informação, como um indelével efeito inesperado do avanço tecnológico.

Importante salientar que o Marco Civil da Internet/MCI, Lei 12.965 de 2014, preconizou anteriormente a preocupação de *assegurar e garantir os direitos dos cidadãos em ambiente eletrônico*, sendo que também determinava expressamente à necessidade do consentimento do usuário "para a coleta, o uso, o armazenamento e o tratamento de seus dados pessoais, tal como para a sua transferência a terceiros. " (BIONI, 2018). Assim, o MCI dedica vários dispositivos para qualificar o consentimento e estabelecer uma orientação de como ele deve ser utilizado. Neste sentido, Bioni afirma que:

> Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. (2018).

Na LGDP o consentimento é figura central e aparece em inúmeros artigos, seguindo as previsões pretéritas do Marco Civil da Internet e a tendência mundial de conceder ao cidadão a responsabilidade de resguardar a proteção dos seus dados pessoais. Segundo Bioni, "o progresso geracional normativo da proteção dos dados pessoais assinala, destarte, um percurso no qual o consentimento emerge, é questionado e se reafirma como sendo o seu vetor central. Com isso, o titular dos dados pessoais permanece sendo o seu ponto focal. " (BIONI, 2018)

Patrícia Pinheiro observa que, ao longo dos anos, o consentimento foi sendo valorizado em razão da *"sensibilidade e vulnerabilidade"* das informações pessoais e, segundo a autora, garantir que os titulares tenham conhecimento de que devem consentir no uso dos seus dados e ainda "possuem o direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, primordial para a assegurar a liberdade e a privacidade". (PINHEIRO, 2018, 65).

Segundo Bioni, na LGPD "há uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento. " (BIONI, 2018). É o que passaremos a analisar aqui. No inciso I do artigo sétimo a LGPD é taxativa em afirmar que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – Mediante o fornecimento de consentimento pelo titular; (grifos nossos)
> O artigo sétimo trata, portanto, de dois conceitos centrais na LGPD, o *consentimento*, detalhado no artigo oitavo e o *tratamento* de dados pessoais, regulado no artigo nono. Conforme visto anteriormente nas definições trazidas pelo artigo quinto, para os fins da LGPD considera-se consentimento: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. " (Inciso XII) e tratamento:
> X – (...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Art. 5º LGPD)

Conforme estas disposições e as determinações do artigo oitavo a LGPD vai exigir que o consentimento previsto no inciso I do art. sétimo deverá ser "fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (*caput*). No caso do consentimento por escrito, a cláusula que o confere deve estar destacada das demais atribuições do contrato (§ 1º) e o § 4º veda, sob pena de nulidade, as autorizações genéricas, devendo o consentimento referir-se a finalidades determinadas. Por fim, os parágrafos 5º e 6º garantem que o consentimento pode ser revogado a qualquer tempo pelo seu titular.

O § 3º determina a vedação do tratamento mediante vício de consentimento e o § 2º deixa claro que o ônus da prova de que o consentimento foi obtido em

conformidade com o disposto nesta lei caberá ao controlador. Depreende-se do disposto a existência na LGPD de várias adjetivações atribuídas ao consentimento, sendo que esse "deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico." (BIONI, 2018)

Bioni problematiza o protagonismo do consentimento como sendo *refratário*, uma vez que coloca dúvidas sobre a capacidade dos titulares dos dados pessoais em exercer um controle efetivo sobre seus dados pessoais. Apresentando vários argumentos que vão desde a hipervulnerabilidade do titular dos dados pessoais até o questionamento da racionalidade dos mesmos ao consentir no tratamento de seus dados. O referido autor afirma que esse paradigma, conhecido como "autodeterminação informacional" deve ser reavaliado:

> Nessa conjuntura, faz-se necessário reavaliar tal estratégia regulatória e a própria compreensão do conteúdo do que é autodeterminação informacional. Devem-se canalizar esforços para identificar a problemática em torno de uma estratégia regulatória e dogmática anacrônica pensada nos anos 1980, que enfrente uma demanda social dos anos 2000. E, assim, verificar como ser encarado esse descompasso, balanceando soluções que, por um lado, empoderem o titular dos dados pessoais, e, por outro lado, não deixem apenas sobre seus ombros a proteção de suas informações pessoais. (BIONI, 2018).

No artigo nono a questão fulcral é a transparência das informações do tratamento de dados (PINHEIRO, 2018, 67), de tal maneira que "o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva" (*caput*), referindo-se essas informações à finalidade específica do tratamento (I), à forma e duração do mesmo (II), identificação e informações de contato do controlador (III e IV), ao uso compartilhado quando houver (V), às responsabilidades dos agentes que realizarão o tratamento (VI) e os direitos do titular que devem ser mencionados de forma explícita (VII).

O § 1º do artigo nono volta a tratar da questão do consentimento, prevendo a nulidade do mesmo nos casos em que as informações oferecidas ao titular "tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca."

Também se referindo ao consentimento, o § 2º adverte que se houver mudança de finalidade para o tratamento de dados, nas situações em que esse con-

sentimento é requerido, tal mudança deverá ser informada ao titular podendo este revogar o consentimento, se não assentir com a alteração.

Quanto aos dados pessoais sensíveis, analisados anteriormente e estabelecidos, no inciso II do artigo quinto da LGPD, como aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico", esses, segundo a artigo décimo primeiro da lei, apenas poderão ser tratados mediante o consentimento dado de forma específica e destacada para finalidades previstas e determinadas, não obstante o referido artigo apresente algumas exceções.

Assim, mais uma vez encontramos a necessidade do consentimento para a realização do tratamento de dados. Com relação aos dados sensíveis o consentimento é intrínseco à validade da ação, todavia há algumas situações em que tal consentimento pode ser relativizado (excetuado), tais como, cumprimento de obrigação legal ou regulatória pelo controlador (a); realização de estudos por órgão de pesquisa (c), exercício regular de direitos (d), proteção da vida ou da incolumidade física do titular ou de terceiros (e); garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (g). Segundo Patrícia Pinheiro,

> os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa.

Os casos aos quais se refere a alínea (c) são regulamentados pelo artigo décimo terceiro que preceitua que em casos em que órgãos de pesquisa realizem estudos de saúde pública, esses poderão ter acesso a bases de dados pessoais desde que realizem o tratamento dos dados dentro do órgão para a finalidade específica do estudo assegurando sempre que possível "a anonimização ou pseudoanimização[4] dos dados".

4 Segundo o §4º do artigo 13 "pseudonimização 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 tratamento de dados pessoais de crianças e de adolescentes mereceram tratamento específico no artigo décimo quarto da LGPD, uma vez que nesse caso o consentimento para o tratamento deverá ser dado por pelo menos um dos pais ou pelo responsável legal. (§ 1º), excetuando-se o caso no qual a coleta de dados seja necessária para contatar os pais ou o responsável legal. (§ 3º). O controlador deverá "realizar todos os esforços razoáveis" para averiguar se o consentimento dos pais ou responsáveis foi realmente dado por eles (§ 5º). Pinheiro considera que merece destaque a preocupação contida no § 5º, uma vez que "o ambiente digital possibilita inúmeros meios de burlar os procedimentos de identificação; dessa forma, cabe aos controladores garantir que o consentimento é real e válido" (2018, 75)

Importante observar o que asseveram Fuller e Soares (2018) ao afirmarem que a erosão da privacidade pode representar violações dos mais diversos direitos, desde aqueles assegurados constitucionalmente, direitos da personalidade (nome, honra, imagem, intimidade e privacidade) e até mesmo direitos de propriedade autoral e intelectual, não obstante a legislação nem sempre tenha demonstrando-se efetiva "em acompanhar os avanços tecnológicos, principalmente em seu aspecto penal (FULLER; SOARES, 2018, *passim*)."

Perante a Sociedade da Informação e a erosão global da privacidade, no Brasil e no mundo, as comunidades jurídicas têm desenvolvido elementos normativos com o intuito de mitigar os efeitos derivados da economia de dados. Não obstante as enormes benesses do avanço tecnológico, é premente que no horizonte próximo que seja equacionado esse paradoxo.

CONSIDERAÇÕES FINAIS

■ Nesse novo estágio de desenvolvimento do Capitalismo impulsionado pelo avanço tecnológico, no qual são dissolvidas as fronteiras entre dispositivos informáticos e a sociedade, a interação entre computadores, *smartphones* e sociedade, mediada pela Internet, tem provocado reflexos em todos os aspectos da vida humana e pode ser considerada a marca mais visível da era digital. Reitera que o fator primordial de geração de riqueza na Sociedade da Informação são os *dados*: registros informáticos sobre transações financeiras, movimentações econômicas, padrões de uso de *smartphones* ou da Internet, de uma maneira abrangente.

Uma vez que as tecnologias propiciaram o aumento da coleta, processamento e análise de bancos de dados, é necessário intensificar a determinação para que haja transparência quantos esses mecanismos de tratamento de dados pessoais. E,

ainda, a quais aplicações esses dados serão submetidos, com quais finalidades, se serão comercializados, cedidos ou vendidos para terceiros, usados para orientar publicidade ou impulsionamento de postagens de cunho eleitoral, têm-se percebido em pleitos recentes em todo o mundo.

O imperativo da proteção da privacidade e da autodeterminação informacional tornam-se ainda mais prementes caso considerada a hipótese, bastante plausível, de que regimes políticos autocráticos usem dados pessoais e perfis em redes sociais de seus opositores para promoverem perseguição, expurgos, prisões ou banimento daqueles que se erguem contra esse status quo.

Em resposta a esses movimentos houve nos anos recentes um movimento de aperfeiçoamento das legislações nacionais e supranacionais voltadas à proteção de dados pessoais e manutenção de um ambiente virtual mais ético e transparente. Destaca-se a reforma da diretiva da comunidade europeia – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Nenhuma medida terá efetividade se não houver também uma mudança no padrão de utilização da internet pelos usuários. O ambiente virtual deve preservar os paradigmas do real.

Em síntese, retomando o exposto por Bioni (2017), desenvolve-se a necessidade de formulação de um novo conceito de privacidade associado a uma liberdade positiva (não mais negativa, que se refere ao controle da aplicação das informações pessoais a ser exercido pelo dono desses dados, ou seja, a assunção da autodeterminação informacional quanto à aplicação dos dados pessoais). Reside na possibilidade de que, aquele que cede os dados, possa exercitar o controle sobre a captação (coleta), tratamento aos quais são submetidos seus registros pessoais e tomar conhecimento das aplicações aos quais serão submetidos. A privacidade historicamente foi associada a uma liberdade negativa, ao direito de não mostrar algo, de não expor, esconder, cobrir. A privacidade, portanto, não parece mais executável em tempos de economia alimentada pela coleta, tratamento e geração de valor a partir de dados pessoais disseminados pela internet.

Evidente que ainda pairam dúvidas muitos significativas quanto à efetividade da LGPD. Apesar das determinações normativas quanto à necessidade do livre esclarecimento e consentimento como requisito para a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, inauguradas com o Marco Civil da Internet, não é o que se verifica em termos práticos. Relatos constantemente comprovam a necessidade de efetivação desta proteção, que poderá advir com

a efetiva vigência da Lei Geral de Proteção de Dados, ou de ações judiciais que questionem essas fragilidades.

A impossibilidade de prever qual será a capacidade jurídica e a força política da autoridade nacional de proteção de dados, preconizada para ser responsável pela aplicação da lei, reveste de opacidade qualquer prognóstico. Não obstante e independente das determinações da lei, urge uma postura mais crítica dos usuários de aplicações tecnológicas quanto a tomada de consciência da quase impossibilidade de privacidade no ambiente informático. E na exigência pelo protagonismo informacional.

Irineu Francisco Barreto Junior · Pós Doutor em Sociologia pela Faculdade de Filosofia, Letras e Ciências Humanas (FFLCH), da Universidade de São Paulo – USP. Doutor em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo – PUC-SP. Professor do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). Docente Convidado da Escola Superior da Advocacia da OAB – SP – ESA e do Instituto de Direito Público de São Paulo – IDC. Analista de Pesquisas da Fundação Seade – SP.

Samyra Haydêe Dal Farra Naspolini · Doutora em Direito pela Pontifícia Universidade Católica de São Paulo. Professora do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). É professora da Faculdade de Direito de Sorocaba – FADI, onde leciona a disciplina de Metodologia da Pesquisa Jurídica. É membro associado e Diretora Executiva do Conselho de Pesquisa e Pós-Graduação em Direito – CONPEDI e da Associação Brasileira de Ensino do Direito – ABEDi. Recebeu em 2013 o Prêmio Jabuti pela organização do livro Educação Jurídica.

REFERÊNCIAS

ABRAMOVAY, Ricardo. Inteligência artificial pode trazer desemprego e fim da privacidade. *Jornal Folha de S. Paulo*, 02 de abril de 2017. Caderno Ilustríssima. Disponível em: http://www1.folha.uol.com.br/ilustrissima/2017/04/1871569-inteligencia-artificial-pode-trazer-desemprego-e-fim-da-privacidade.shtml. Acesso em: 02. Abr. 2017.

BARRETO JUNIOR, Irineu Francisco. Atualidade do conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (Coord.). O Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

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

BARRETO JUNIOR, Irineu Francisco; VENTURI JÚNIOR, Gustavo. Dados pessoais na internet: análise do seu status enquanto mercadoria na sociedade da informação. *Anais do 41º. Encontro Anual da ANPOCS.* Disponível em: http://www.anpocs.com/index.php/papers-40-encontro-2/gt-30/gt02-25/10599-dados-pessoais-na-internet-analise-do-seu-status-enquanto-mercadoria-na-sociedade-da-informacao/file> Acesso em 10.nov. 2107.

BAUMAN, Zygmunt. Modernidade Líquida. Rio de Janeiro: Jorge Zahar Editores, 2001.

BAUMAN, Zygmunt. Vigilância Líquida: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, p. 9.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais.* Palestra proferida na Fundação Seade, São Paulo, em 13 de dezembro de 2017.

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

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. 5 ed. São Paulo: Paz e Terra, 2001. v I, a sociedade em rede.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data – Como Extrair Volume, Variedade, Velocidade e Valor da Avalanche de Informação Cotidiana.* Rio de Janeiro: Campus, 2012.

FULLER, Greice Patrícia; SOARES, Roger da Silva Moreira. A tutela penal dos dados empresariais na sociedade da informação no ordenamento jurídico brasileiro. REVISTA JURÍDICA DA PRESIDÊNCIA, v. 20, p. 408, 2018.

FULLER, Greice Patrícia; FIGUEIREDO, Leide Priscila. Compliance empresarial e tutela penal na sociedade da informação. REVISTA DOS TRIBUNAIS (SÃO PAULO. IMPRESSO), v. 996, p. 573-588, 2018.

LIMA, Cintia Rosa Pereira; BIONI, Bruno Ricardo. Apontamentos sobre a Adjetivação do Consentimento Implementada pelo Artigo 7, Incisos VIII e IX do Marco Civil da Internet a Partir da "Human Computer Interaction" e da "Privacy By Default". In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coordenadores).

Direito & Internet III – Tomo I: Marco Civil da Internet (Lei 12.965/2014). São Paulo: Quartier Latin do Brasil, 2015.

MARANHÃO, Juliana. A pesquisa em inteligência artificial e Direito no Brasil. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 09. Dez. 2017.

NASPOLINI, Samyra. H D. F.; BRANDAO, C. A Obrigação da Instituição Financeira na Proteção do Consumidor de Crédito Bancário no Contexto da Globalização. REVISTA DE DIREITO DO CONSUMIDOR, v. 119, p. 203-226, 2018.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: comentários à Lei 13.709/2018. São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553608324/cfi/3!/4/4@0.00:48.7. Acesso em: 19 ago. 2019.

RODOTÀ, Stefano. (traduzido por: DONEDA, Danilo; MORAES, Maria Celina Bodin) A Vida na Sociedade da Vigilância: A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SETZER, V. W. Dado, informação, conhecimento e competência. DataGramaZero -

Revista de Ciência da Informação, Rio de Janeiro, n.0, dez. 1999. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html. Acesso: 07 ago. 2019.

VIEIRA, Miguel Said; EVANGELISTA, Rafael. A máquina de exploração mercantil da privacidade e suas conexões sociais. 30 Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios. 13 a 15 de maio, 2015. Rio de Janeiro, Brasil, p. 524- 533.

Publicações anteriores dos *Cadernos Adenauer*

Para assinar ou adquirir os *Cadernos Adenauer*, acesse: www.kas.de/brasil

Infraestrutura e desenvolvimento no Brasil (n. 2, 2019)

Eleições 2018 e perspectivas para o novo governo (n. 1, 2019)

Fake news e as eleições 2018 (n. 4, 2018)

Combate à corrupção no Brasil (n. 3, 2018)

Política e mercado (n. 2, 2018)

Participação política feminina na América Latina (n. 1, 2018)

Reforma política (n. 4, 2017)

Megacidades (n. 3, 2017)

Poder Legislativo sob múltiplos olhares (n. 2, 2017)

Política e Poder Judiciário (n. 1, 2017)

Repensando a política externa brasileira: em busca de novos consensos (n. 4, 2016)

Política local e Eleições 2016 (n. 3, 2016)

Mudanças climáticas: o desafio do século (n. 2, 2016)

Educação política no Brasil: reflexões, iniciativas e desafios (n. 1, 2016)

O global e o local (n. 4, 2015)

Internet e sociedade (n. 3, 2015)

Cidades resilientes (n. 2, 2015)

Juventudes no Brasil (n. 1, 2015)

Cibersegurança (n. 4, 2014)

Eficiência energética (n. 3, 2014)

Governança e sustentabilidade nas cidades (n. 2, 2014)

Justiça Eleitoral (n. 1, 2014)

Relações Brasil-Alemanha / Deutsch-Brasilianische Beziehungen (caderno especial, 2013)

Novas perspectivas de gênero no século XXI (n. 3, 2013)

Candidatos, Partidos e Coligações nas Eleições Municipais de 2012 (n. 2, 2013)

Perspectivas para o futuro da União Europeia (n. 1, 2013)

Democracia Virtual (n. 3, 2012)

Potências emergentes e desafios globais (n. 2, 2012)

Economia verde (n. 1, 2012)

Caminhos para a sustentabilidade (edição especial, 2012)

Municípios e Estados: experiências com arranjos cooperativos (n. 4, 2011)

Ética pública e controle da corrupção (n. 3, 2011)

O Congresso e o presidencialismo de coalizão (n. 2, 2011)

Infraestrutura e desenvolvimento (n. 1, 2011)

O Brasil no contexto político regional (n. 4, 2010)

Educação política: reflexões e práticas democráticas (n. 3, 2010)

Informalidade laboral na América Latina (n. 2, 2010)

Reforma do Estado brasileiro: perspectivas e desafios (n. 1, 2010)

Amazônia e desenvolvimento sustentável (n. 4, 2009)

Sair da crise: Economia Social de Mercado e justiça social (n. 3, 2009)

O mundo 20 anos após a queda do Muro (n. 2, 2009)

Migração e políticas sociais (n.1, 2009)

Segurança pública (n. 4, 2008)

Governança global (n. 3, 2008)

Política local e as eleições de 2008 (n. 2, 2008)

20 anos da Constituição Cidadã (n. 1, 2008)

A mídia entre regulamentação e concentração (n. 4, 2007)

Partidos políticos: quatro continentes (n. 3, 2007)

Geração futuro (n. 2, 2007)

União Europeia e Mercosul: dois momentos especiais da integração regional (n. 1, 2007)

Promessas e esperanças: Eleições na América Latina 2006 (n. 4, 2006)

Brasil: o que resta fazer? (n. 3, 2006)

Educação e pobreza na América Latina (n. 2, 2006)

China por toda parte (n. 1, 2006)

Energia: da crise aos conflitos? (n. 4, 2005)

Desarmamento, segurança pública e cultura da paz (n. 3, 2005)

Reforma política: agora vai? (n. 2, 2005)

Reformas na Onu (n. 1, 2005)

Liberdade Religiosa em questão (n. 4, 2004)

Revolução no Campo (n. 3, 2004)

Neopopulismo na América Latina (n. 2, 2004)

Avanços nas Prefeituras: novos caminhos da democracia (n. 1, 2004)

Mundo virtual (n. 6, 2003)

Os intelectuais e a política na América Latina (n. 5, 2003)

Experiências asiáticas: modelo para o Brasil? (n. 4, 2003)

Segurança cidadã e polícia na democracia (n. 3, 2003)

Reformas das políticas econômicas: experiências e alternativas (n. 2, 2003)

Eleições e partidos (n. 1, 2003)

O Terceiro Poder em crise: impasses e saídas (n. 6, 2002)

O Nordeste à procura da sustentabilidade (n. 5, 2002)

Dilemas da Dívida (n. 4, 2002)

Ano eleitoral: tempo para balanço (n. 3, 2002)

Sindicalismo e relações trabalhistas (n. 2, 2002)

Bioética (n. 1, 2002)

As caras da juventude (n. 6, 2001)

Segurança e soberania (n. 5, 2001)

Amazônia: avança o Brasil? (n. 4, 2001)

Burocracia e Reforma do Estado (n. 3, 2001)

União Europeia: transtornos e alcance da integração regional (n. 2, 2001)

A violência do cotidiano (n. 1, 2001)

Os custos da corrupção (n. 10, 2000)

Fé, vida e participação (n. 9, 2000)

Biotecnologia em discussão (n. 8, 2000)

Política externa na América do Sul (n. 7, 2000)

Universidade: panorama e perspectivas (n. 6, 2000)

A Rússia no início da era Putin (n. 5, 2000)

Os municípios e as eleições de 2000 (n. 4, 2000)

Acesso à justica e cidadania (n. 3, 2000)

O Brasil no cenário internacional (n. 2, 2000)

Pobreza e política social (n. 1, 2000)

Este livro foi composto por
Claudia Mendes em Adobe Garamond c.11/14
e impresso pela Stamppa em papel pólen 80g/m²
para a Fundação Konrad Adenauer
em outubro de 2019.