

COORDENAÇÃO

CÍNTIA ROSA PEREIRA DE LIMA

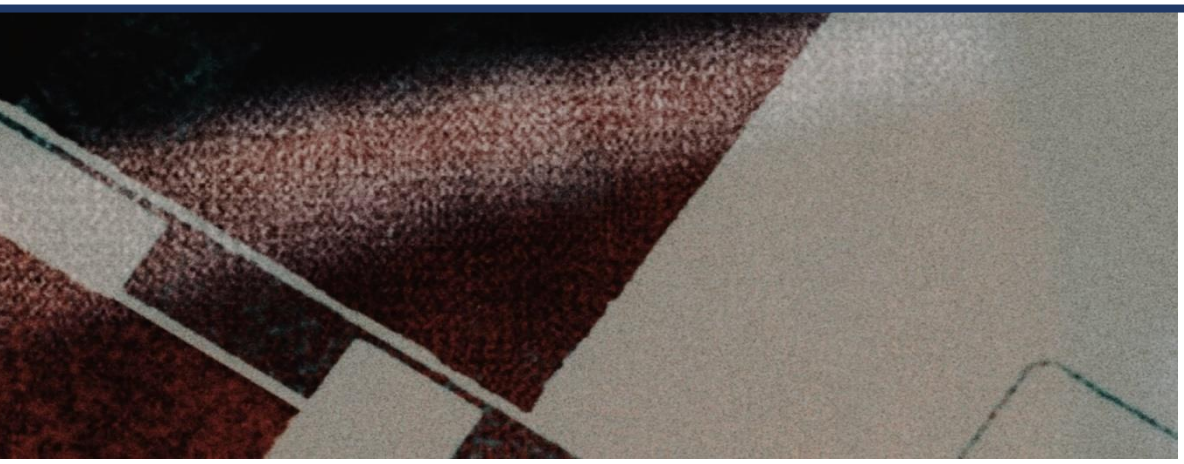
EVANDRO EDUARDO SERON RUIZ

MARTA RODRIGUES MAFFEIS

ANAIS DO CONGRESSO INTERNACIONAL

DESAFIOS E PERSPECTIVAS DAS AUTORIDADES DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

07 a 09 de novembro de 2019



UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
DE RIBEIRÃO PRETO

Universidade de São Paulo



Coordenação

Cíntia Rosa Pereira de Lima

Evandro Eduardo Seron Ruiz

Marta Rodrigues Maffeis

Anais do Congresso Internacional

Desafios e Perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade

Ficha Catalográfica

Congresso Internacional Desafios e Perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade (1. : 2019 : Ribeirão Preto, SP).

Anais [recurso eletrônico] / Congresso Internacional Desafios e Perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade. / Coordenação: Cíntia Rosa Pereira de Lima, Evandro Eduardo Seron Ruiz, Marta Rodrigues Maffeis Moreira. — Ribeirão Preto, SP: Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (FDRP/USP), 2020.

Modo de acesso: Internet.

ISBN: 978-65-86465-00-6

1. Proteção de dados. 2. Dados pessoais. 3. Direito à privacidade. I. Lima, Cíntia Rosa Pereira de. II. Ruiz, Evandro Eduardo Seron. III. Moreira, Marta Rodrigues Maffeis. IV. Faculdade de Direito de Ribeirão Preto.

Coordenação

Cíntia Rosa Pereira de Lima

Evandro Eduardo Seron Ruiz

Marta Rodrigues Maffeis

Patrocinadores

DPP (DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL)
DA FACULDADE DE RIBEIRÃO PRETO – FDRP

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

FAPESP

Comitê Científico

Adalberto Simão Filho
Adriana Cardoso de Moraes Cansian
Alessandro Hirata
Cíntia Rosa Pereira de Lima
Cristina Godoy Bernardo de Oliveira
Eliana Franco Neme
Emanuele Pezati Franco de Moraes
Evandro Eduardo Seron Ruiz
Gabriel Loretto Lochagin
Gustavo Assed Ferreira
Marta Rodrigues Maffeis
Renata Mota Maciel
Roberto Augusto Castellanos Pfeiffer
Rodrigo de Lima Vaz Sampaio
Rubens Beçak

Outros patrocinadores

IAPD
Instituto Avançado de Proteção de Dados

GRUPO DE PESQUISA – PROFA. DRA CINTIA ROSA (USP)
- Observatório do Marco Civil da Internet
- Tutela Jurídica dos Dados Pessoais da Internet

CESA Centro de Estudos das Sociedades de Advogados

OAB CAASP

MESTRADO FDRP

FADEP

ALMEDINA

VILAGE MARCAS E PATENTES

Kasznar Leonardos 1919

AIRES VIGO ADVOGADOS

SANCHEZ & SANCHEZ

ICAMP MARCAS E PATENTES

Podium tecnologia

vox2you

Apresentação

Um dos grandes impasses na tramitação da Lei Geral de Proteção de Dados Pessoais foi a criação de um órgão independente para a fiscalização do correto cumprimento da lei. De fato, em alguns projetos de lei este órgão foi previsto; mas, em outros, não. O temor em se criar um novo órgão para tal finalidade seria de várias ordens: uma questão de orçamento público, pois tal criação representaria aumento de gastos públicos; outra questão econômica, em que o tal órgão pudesse engessar o mercado informacional, regulamentando em demasia as condutas relacionadas ao tratamento de dados pessoais. Por fim, o grande receio está na punição que o órgão pudesse impor ao constatar violação à lei de proteção de dados.

Assim, a Lei Geral de Proteção de Dados Pessoais, Lei n. 13.709, de 14 de agosto de 2018, foi aprovada na Câmara dos Deputados e no Senado Federal, com a previsão da criação da Autoridade Nacional de Proteção de Dados – ANPD. Todavia, temendo um vício de forma, em que somente o Poder Executivo poderia propor a criação de um órgão de tal natureza, todos os artigos que faziam referência à ANPD foram vetados. Posteriormente, eles foram reinseridos pela Medida Provisória n. 869, de 27 de dezembro de 2018, ato do Presidente da República, sanando a exigência constitucional prevista no art. 61, § 1o, inc. II, "e", cumulado com art. 37, inc. XIX da CF/88.

Esta Medida Provisória foi convertida na Lei n. 13.853, de 08 de julho de 2019, criando efetivamente a Autoridade Nacional de Proteção de Dados – ANPD como órgão vinculado à Administração Pública direta.

A experiência internacional demonstra a importância deste órgão para a efetividade do sistema de proteção de dados pessoais. Por isso, o Congresso Internacional "Desafios e Perspectivas da Autoridade Nacional de Proteção de Dados" dedicou-se ao tema atual e relevante haja vista a entrada em vigor da LGPD, em agosto de 2020. O evento contou com a participação de renomados juristas nacionais e internacionais, todos dedicados ao tema. Além disso, os participantes puderam apresentar artigos científicos que foram revisados por dois dos professores integrantes do Comitê Científico, e após terem feito as revisões solicitadas, encaminharam a versão final dos respectivos artigos que compõem estes Anais.

Trata-se de obra fundamental para compreender o sistema brasileiro de proteção de dados pessoais, bem como vislumbrar o que esperar da Autoridade Nacional de Proteção de Dados.

Ribeirão Preto, 21 de fevereiro de 2020.

Cíntia Rosa Pereira de Lima, Evandro Eduardo Seron Ruiz & Marta Rodrigues Maffeis

Organizadores do Congresso Internacional

"Desafios e Perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade"

Sumário

Capítulo 1 9

1. ANPD e modelos internacionais de autoridades de proteção de dados 9

1.1. A Autoridade Nacional de Proteção de Dados brasileira e seus equivalentes nos Estados Unidos e na Europa – *Marcelo Trevilato Dorascienzi & Luciana Romano Morilas* 9

1.2. Os problemas das transferências internacionais de dados: Comarca, nacionalidade e origem – *Felipe Otávio Moraes Alves* 17

1.3. La aplicación del Reglamento Europeo de Protección de Datos a las Entidades no Europeas – *Raquel Guillén Catalán* 27

1.4. A institucionalização das Autoridades de Proteção de Dados Pessoais na América Latina: estudo dos modelos regulatórios da Argentina e do Uruguai – *Amanda Nunes Lopes Espiñeira Lemos* 30

Capítulo 2 38

2. Independência, autonomia e funções das autoridades de proteção de dados 38

2.1. Desafios, funções e referências internacionais para a Autoridade Nacional de Proteção de Dados – *Henrique Rocha* 38

2.2. Reflexos regulatórios da Lei da Liberdade Econômica no contexto da LGPD: uma perspectiva do artigo 5° da Lei n° 13.874/2019 – *Luiz Salles Giannellini, Renato Barros Cabral, Ylka Beltrão & Renata Mota Maciel* 48

2.3. A ANPD e a regulação da Lei 13.709/18 para a proteção de dados pessoais: da gestão de riscos à necessidade de reforçar a privacidade digital – *João Paulo Zanin Júnior* 56

2.4. A função da Autoridade Nacional de Proteção de Dados – ANPD a partir das garantias de livre iniciativa previstas no artigo 4° da Lei n° 13.874/2019 (Lei da Liberdade Econômica) – *Heloísa Corrêa Meneses, Suelen Bianca de Oliveira Sales & Renata Mota Maciel* 63

Capítulo 3 72

3. Proteção de dados e o uso de inteligência artificial (IA) 72

3.1. A inteligência artificial e a proteção de dados pessoais à luz dos direitos da personalidade – *Maria Vital da Rocha & Larissa Rocha de Paula Pessoa* 72

3.2. Inteligência artificial no raciocínio jurídico – *Guilherme Marconatto Modelli & Lorenzo Marino Domingues* 80

3.3. Artificial Intelligence and Liability in the Health System: International mapping of regulations and comparative analysis – *Gabriela A. S. Monteiro, Geneviéve David, Jean-Louis Denis & Catherine Regis*.....91

3.4. Desafios da proteção de dados frente aos avanços tecnológicos no âmbito dos municípios e o papel das procuradorias municipais – *Richard Bassan, Cláudio Lázaro Aparecido Junior, Renato Passos Ornelas & Bruno Bastos de Oliveira* 101

Capítulo 4 111

4. Tratamento de dados pessoais pelas pessoas jurídicas de direito público e de direito privado e formas de controle 111

4.1. Anonimização de dados genéticos: (in)suficiente na nova Lei Geral de Proteção de Dados? – *Fernando Luís Barroso da Silva Filho, João Paulo Sanchez de Rezende Goulart & Cristina Godoy Bernardo de Oliveira*.....111

4.2. O tratamento de dados pessoais pelas empresas públicas e sociedades de economia mista e a realização de licitações como operacionalização de políticas públicas – *Rafael Rizzi & Yago Funchal de Godoy*.....119

4.3. A crise do controle na era da informação: o direito à portabilidade de dados como instrumento de efetivação da autodeterminação do homem no ambiente digital – *Gabriel de Aguiar Tajra & Cíntia Rosa Pereira de Lima* 123

4.4. *Accountability* no tratamento de dados no Brasil – *Felipe Otávio Moraes Alves* 139

4.5. A disciplina jurídica do tratamento de dados pelo governo federal do Brasil – *Óthon Castrequini Piccini*.....149

4.6. Segurança pública no Brasil: desafios à luz do tratamento de dados pessoais – *Maria Eduarda Sampaio de Sousa, Matheus José Chiaramonte de Castro & Cíntia Rosa Pereira de Lima*...158

4.7. Meios eletrônicos de comunicação dos atos processuais: uma análise do processo judicial eletrônico no Brasil – *Márcio Martins Marano & Larissa Freitas Okamoto*.....167

4.8. A aplicabilidade da Lei Geral de Proteção de Dados aos condomínios edilícios: Lei n° 13.874/2019 – *Margarida Isabella Malena Macini, Natália Matos Santana Lourenço & Tatiana Pereira Chelest Miras Diniz* 184

4.9. Desafios da proteção de dados pessoais: o compartilhamento de dados entre Poder Público e setor privado – *Vitória Mattos Gonçalves & Verônica do Nascimento Marques*.....195

4.10. Aspectos controvertidos sobre a edição de leis municipais em face da proteção de dados pessoais – *Richard Bassan, Cláudio Lázaro Aparecido Junior, Renato Passos Ornelas & Bruno Bastos de Oliveira* 205

4.11. Análise da proteção de dados na América Latina e a possibilidade de aplicação do sistema multinível como garantidor dos direitos fundamentais digitais – *Leonardo de Andrade Alberto & Moacir Henrique Júnior* 213

Capítulo 5 222

5. Perspectivas multissetoriais da regulação em proteção de dados pessoais e privacidade 222

5.1. Os desafios da ANPD diante das bases de dados pessoais legadas – *Lucas Del Vecchio Soares* 222

5.2. Autoridade Nacional e sua efetividade na preservação da privacidade – *Bárbara de Sordi Faria & Iara Pereira Ribeiro* 230

Capítulo 6 237

6. Utilização econômica dos dados pessoais: os limites e as tendências face a monetização dos dados pessoais 237

6.1. Fluxo informacional e autodeterminação informativa: o dilema do consentimento informado – *Afonso Fratti Penna Rispoli & Hebert Fabrício Tortorelli Quadrado* 237

6.2. Valor patrimonial dos dados pessoais em mercados de preço zero – *Pietra Daneluzzi Quinelato* 252

6.3. Propaganda comportamental, consentimento para coleta de dados e a proteção consumerista – *Victor Sader Oliveira, Bruno Otávio Simozako Sadano & Caio César Domingues de Almeida* 267

6.4. A LGPD aplicada ao *marketing*: desafios e perspectivas – *Mariana Martins Ferreira* 273

6.5. Internet das Coisas e privacidade: o tratamento e a comercialização de dados pessoais no ciberespaço – *Bruna Bastos, Eduardo Missau Ruviaro & Rafael Santos de Oliveira* 282

6.6. Violação da privacidade de dados pessoais para fins econômicos, de acordo com a Lei 13.709/2018 – *Guilherme Lourenço da Silva Menezes Cunha & Joseane Isabel Becker* 292

6.7. A economia de dados pessoais no contexto da LGPD: há necessidade de regulação dos modelos de negócios pela Autoridade Nacional de Proteção de Dados? – *Renato Barros Cabral & Alexandre Multini Mihich* 299

6.8. Violação do livre consentimento: um estudo de caso da Ação Civil Pública movida pelo IDEC – em face da VIAQUATRO – *Rafaela Rabelo Daun, André Lucas Fontana, Jaqueline Yurie Miura & Vinicíus Silva Luiz* 308

6.9. Da livre publicidade ao dever de respeito pelos dados pessoais – *Gabriel Oliveira de Aguiar Borges, Luciano Nunes Marques & Arthur Pinheiro Basan* 315

6.10. O impacto da Lei Geral de Proteção de Dados nos contratos de prestação de serviços educacionais – *Luiz Fernando Salles Giannellini & Renata Mota Maciel* 325

6.11. Personal Data Protection and multi-side Internet market regulation: an analysis on the limits of profiling – *José Luiz de Moura Faleiros Júnior & Pietra Daneluzzi Quinelato* 340

Capítulo 1

1. ANPD e modelos internacionais de autoridades de proteção de dados

1.1. A Autoridade Nacional de Proteção de Dados brasileira e seus equivalentes nos Estados Unidos e na Europa – *Marcelo Trevilato Dorascienzi*[1] *& Luciana Romano Morilas*[2]

Resumo

A reflexão sobre os potenciais campos de atuação da Autoridade Nacional de Proteção de Dados aproveita o momento tardio da regulamentação brasileira sobre direito de dados a partir da análise comparativa de seus equivalentes nos Estados Unidos e na União Europeia na elaboração de proposições.

Palavras-chave: Autoridade Nacional de Proteção de Dados; dados; Estados Unidos; União Europeia.

Abstract

Reflecting on the potential fields of action of the National Data Protection Authority takes advantage of the late moment of Brazilian data law regulation on the comparative analysis of its counterparts in the United States and the European Union in the elaboration of propositions.

Keywords: National Data Protection Authority. Data. United States. European Union.

[1] FEARP-USP.

[2] Orientadora – FEARP-USP.

Introdução

Não é de hoje que a preocupação com a privacidade e o uso indevido de dados pessoais existe. A Declaração Universal dos Direitos Humanos (ONU, 1948), em seu artigo XII, estabelece, já na década de 40, o direito à vida privada. Essa proteção, no que diz respeito à vida pessoal do indivíduo, traz à tona o fundamento básico de dignidade da pessoa humana proposto pela Constituição da República Federativa do Brasil de 1988, uma vez que leva em consideração o direito de escolha e de omissão do indivíduo.

No entanto, mesmo com a interpretação desse direito como algo básico e de caráter fundamental à vida humana, a realidade mercadológica vai de encontro à essa concepção. O avanço tecnológico moderno e o foco das empresas para uma visão cada vez mais pautada em uma "orientação para marketing" (KOTLER, 2012) trouxe o uso irrestrito de técnicas de *data mining*, coleta e tratamento de dados para a compreensão cada vez mais precisa do comportamento do consumidor.

Nesse contexto, a lógica que reina é a da maior coleta de dados possível dos clientes para a elaboração de um CRM (*Costumer Relationship Management*) robusto e carregado de informações (SILVA, 2002). Com isso em mãos, as empresas são capazes de gerenciar com maior qualidade sua evolução no mercado e de compreender as demandas de seu público-alvo. Essa é uma prática que já faz parte do cotidiano de pequenas, médias e grandes empresas.

O desenvolvimento dessa realidade, por mais interessante que seja para o público, escancara uma preocupação muito válida: "qual o limite do uso desses dados?" Essa tem sido a pergunta que transformou a maneira de encarar essa lógica mercantil para com os dados. Grandes escândalos de vazamento de dados, como o caso do Facebook (540 MILHÕES, 2019), e seu uso indevido são os principais responsáveis por trazer à tona essa preocupação e elencar como urgente uma política de regulamentação à proteção de dados.

Surge, então, em meio a esse contexto, uma regulamentação que freia a arbitrariedade e o uso indevido desses dados. A exemplo dessa preocupação com o poderio das empresas com esses dados em mãos pode-se tomar o caso da jornalista Sarah Lacy (UBER, 2014), a qual, em uma coluna jornalística, criticou o posicionamento da empresa Uber sobre os casos de discriminação de gênero entre motoristas e passageiros. O vice-presidente da empresa Emil G. Michael, sabendo disso, ameaçou expor informações da vida privada de Lacy numa clara tentativa de vingança por suas críticas no jornal. Casos como esses, que evidenciam uma postura alheia às responsabilidades na proteção desses dados, ocorrem a todo instante com grandes organizações que detêm enorme volume de dados. Seja no uso indevido para controle da opinião pública, como no caso do Facebook em conjunto com a empresa inglesa

Cambridge Analytica (CASO, 2019), seja nos constantes vazamentos de dados da brasileira *Dataprev* no território nacional (INSTITUTO, 2019).

Este artigo pretende analisar a estruturação da regulamentação brasileira, que entra em vigor em 2020, em comparação com as regras já existentes nos Estados Unidos e na União Europeia, onde ocorreram os casos supracitados. Apesar de países como o Uruguai e a Coreia do Sul (CONFEDERAÇÃO, 2017) também já contarem com suas agências, essa escolha de análise comparativa se deve à relevância desses agentes na economia global e devido ao fato de se integrarem como hegemônicos na adoção de políticas voltadas para a proteção de dados.

Desse modo, a pesquisa tem caráter documental e propositivo. Documental porque leva em consideração os estudos já existentes na intenção de trazer uma análise profunda sobre a atuação de modelos regulatórios em outras nações e, propositivo, porque, com base neste estudo, visa propor potenciais planos de ação para a ANPD.

Desenvolvimento

1. Proteção de dados na União Europeia

Preocupada com os acontecimentos e escândalos mencionados, a União Europeia se voltou para o desenvolvimento da atual General Data Protection Regulation – GDPR (UNIÃO EUROPEIA, 2018) na intenção de trazer à luz do direito a inidoneidade das atitudes das gigantes dos dados[3]. Tal regulamentação se volta para os direitos dos titulares na intenção de garantir o princípio fundamental de dignidade, segurança e escolha. Nessa ótica, as empresas passam então a ter o dever de se organizar de acordo com o que está definido na GDPR. Outro fator que demonstrou tamanho valor em relação às novas diretrizes da lei foi a internacionalização da atuação legal. O regramento europeu se aplica às empresas que possuam qualquer relação com dados de nacionalidade europeia, mesmo que sua sede não seja no continente europeu. Isso implica, por exemplo, que empresas sediadas no Brasil sejam obrigadas a se submeter ao regramento europeu.

2. Proteção de dados nos Estados Unidos

Em um momento concomitante à criação da GDPR, o estado da Califórnia, nos Estados Unidos, lançou o *California Consumer's Privacy Act* (CALIFORNIA, 2018), projeto de lei aprovado e que entra em vigor em 1º de janeiro de 2020. Sua similaridade legal com a GDPR é notável. No entanto, se diferencia em algumas questões de governança pública, em questões de caráter contábil, na extensão de

[3] São consideradas gigantes aqueles integrantes da "Internet Association", conforme disponível em: https://internetassociation.org/our-members/. Acesso em: 13 out. 2019.

atuação e nas limitações legais do processamento de dados. Ainda assim, de acordo com o *Future of Privacy Forum* (2018), a similaridade com a GDPR trará grandes impactos para os Estados Unidos.

Percebe-se isso no crescente interesse em nacionalizar a política de proteção de dados, (McCABE, 2019) algo que já vem acontecendo com o *New York's Privacy Bill* (STATE OF NY, 2019), projeto de lei em discussão no estado de Nova York e que vai ao encontro da definição da política estadunidense de proteção de dados como seguindo um modelo regulatório setorizado com inclinação político-liberal (GUIDI, 201). Algo que é contrário aos interesses das empresas associadas à *Internet Association*, daí sua recente inquietação sobre a temática (McCABE; SWANSON, 2017).

3. Proteção de dados no Brasil

Acompanhando esse movimento mundial de regulamentação de proteção de dados, o Brasil aprovou, em 2019, a Lei nº 13.853/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2019). A lei evidencia clara relação com o descrito na GDPR, desde a preocupação com os titulares dos dados, a centralização nacional da regulamentação, até a previsão de um órgão regulamentador de caráter autárquico, a Autoridade Nacional de Proteção de Dados, um tanto quanto similar à *Data Protection Comission* – DPC (DATA, 2018), da Irlanda e ao *Information Commissioner's Office* – ICO (INFORMATION, 1994), do Reino Unido.

Vale ressaltar que, em matéria de direito de dados, os países europeus, em especial a Inglaterra, possuem longa trajetória de debates e vivência. O Reino Unido tem um primeiro Data Protection Act 1998 emitido em 1998. O mais recente é o *Data Protection Act 2018*, o responsável pela conclusão da GDPR. Tendo em vista todo esse contexto próximo com os dados, não é surpresa o nível de descrição legal da GDPR no território europeu, deixando claro as diretrizes centrais do bloco, ao mesmo tempo que evidencia clareza e autonomia para os Estados membros definirem suas próprias políticas de regulamentação acessória e fiscalização. Daí a existência de diferentes modelos regulatórios autárquicos com atuação territorial distantes (vide *Data Protection Comission e Information Commissioner's Office*).

A necessidade da criação dessas autoridades independentes se faz necessária como um planejamento de Estado, uma vez que garantem uma melhor administração pública sobre o tema à qual tem vínculo legal. Não só isso, mas também independência decisória e orçamentária para a realização de suas ações a elas designadas. Levando em consideração o caso da ANPD, seu caráter autárquico se faz relevante para que o acompanhamento das inovações tecnológicas seja mais eficiente, a tomada de decisão mais rápida, com menos retardamentos burocráticos, e mais alinhada com a realidade de cada caso fiscalizado, e para que a realização de políticas públicas partem diretamente de especialistas e administradores envolvidos inteiramente com a temática.

4. Da atuação da ANPD

Quando se pensa em transações comerciais internacionais, a existência de agências autárquicas que se relacionam entre si, torna-se de fácil compreensão a necessidade de alinhamento internacional em direito de proteção de dados. As organizações seguem um modelo pautado na Nova Divisão Internacional do Trabalho (ALBUQUERQUE, 1987). Essa lógica traz como consequência fluidez nas relações político-comerciais entre grandes empresas, sendo do direito privado ou público. Desse modo, o ideal seria que agências de cada país sintonizassem suas estruturas de governança pública pautadas numa legislação internacional similar, facilitariam a adequação legal dessas organizações transnacionais, assim como tornariam mais coesa a regulamentação de proteção de dados aos titulares.

Com o recente interesse no acordo UE-Mercosul (MENDONÇA, 2019) a ANPD (que passará a existir em agosto de 2020) será uma peça fundamental para as empresas brasileiras que lidam com o mercado europeu e se regulam de acordo com o imposto pela GDPR, fiscalizado e gerido pelas autarquias como o ICO e o DPC. Uma previsão promissora para empresas que conseguirem se adequar aos arquétipos da LGPD.

No Brasil, a ANPD passou por um veto presidencial no governo de Michel Temer no momento de elaboração do texto base da Lei, a qual, com uma Medida Provisória em dezembro do mesmo ano retornou com uma característica um tanto quanto questionável. A lei prevê um caráter transitório de dois anos para a existência da ANPD. Além disso, diferentemente das outras agências reguladoras do país, ela possui vínculo administrativo direto com a Presidência da República, o que, por sua vez, lhe confere, um posicionamento político (Art. 55-A, da Lei 12.853/19, BRASIL, 2019).

Dentre suas atribuições estão o papel normativo, o fiscalizador e o sancionatório. Em um primeiro momento, uma discussão sobre o papel educativo foi realizada (FERNANDES, 2019). Com a dificuldade das pequenas e médias empresas se enquadrarem no modelo regulatório proposto pela Autoridade, a elaboração de políticas públicas para o cumprimento legal das medidas em lei propostas viria a ser uma das primeiras tarefas essenciais da legislação e da atuação da ANPD.

Algo parecido tem sido realizado com a *Data Protection Comission* nos países europeus, vide site com a temática educativa em relação aos direitos dos titulares e aos deveres das organizações (DATA, 2018). Em um primeiro momento, uma postura mais flexível e mais voltada para a educação corporativa e em compliance seria a melhor estratégia para a ANPD. No entanto, seu caráter transitório é um potencial empecilho para a resolução dessas questões com as empresas brasileiras. Sua existência se faz necessária, e isso será levado em consideração no julgamento de sua trajetória até agosto de 2022 (quando encerra sua existência prevista em lei e sua discussão é retomada no Congresso Nacional).

Conclusão

Levando em consideração o momento atual dos Estados Unidos sobre sua nova regulamentação a respeito do direito de dados, percebe-se que uma postura mais mercantil e um tanto quanto fragmentada (quando se volta para a autonomia estatal e não centralização dos direitos e deveres aqui discutidos) que trazem certos riscos ao cidadão, vide recorrentes acontecimentos que ultrapassam certos limites éticos e morais.

Por outro lado, quando analisa-se a postura da União Europeia, percebe-se que a centralização de diretrizes e a preocupação com a regulamentação do direito de dados trouxe aos cidadãos a oportunidade da escolha e o direito à proteção. Desse modo, dificilmente a privacidade é afetada por qualquer tratamento de dados.

Tendo em vista a situação desses dois panoramas internacionais, o que pode-se inferir é que uma possível alternativa para o funcionamento da Agência Nacional de Proteção de Dados Pessoais é a associação do que há no exterior para melhor aproveitamento interno. Nesse sentido, uma postura mais mercantil (próxima a dos Estados Unidos) associada a uma centralização de ação, com diretrizes e normas bem definidas e fiscalizadas (exatamente como os órgãos europeus sobre a GDPR), possa ser uma postura a ser pensada.

Respeitando o V fundamento elencado no artigo 2º da Lei Geral de Proteção de Dados Pessoais: "o desenvolvimento econômico e tecnológico e a inovação", a ANPD surge com o dever de compreender a realidade brasileira encarando a regularização empresarial como uma ação que priorize o desenvolvimento econômico. Tal reflexão é levantada devido a dois importantes fatores: o escopo da lei atinge diretamente qualquer dado já tratado pelas empresas brasileiras, seja ele físico ou digital, todo o legado empresarial; o segundo fator é a realidade econômica do país, a qual se compõe majoritariamente por empresas de pequeno porte.

A combinação desses dois fatores dificulta a efetividade desse fundamento, isso porque a situação financeira de empresas de pequeno porte não é compatível com o que é exigido pela lei. Ressalta-se então a necessidade de uma postura educacional e mais amena para com essas organizações no intuito de incentivar a regularização legal e promover o desenvolvimento. Além disso, a centralização administrativa proposta pela existência autárquica da Autoridade Nacional de Proteção de Dados Pessoais tem sua validade nas experiências da União Europeia. As adequações legais e a fiscalização pública sobre as empresas que ferem qualquer norma elencada pela GDPR são muito bem realizadas pelas ações promovidas pelas autarquias existentes nos países do continente.

É evidente a necessidade de adequação e regularização legal quanto ao direito de dados pessoais. O Brasil mostrou essa preocupação de maneira bem integrada aos acontecimentos do continente europeu. No entanto, por mais que a Lei Geral de Proteção de Dados Pessoais tenha grande proximidade com o descrito na Europa, a realidade brasileira exige um olhar mais cuidadoso para o que cidadãos e

organizações vivenciam. Acreditar em uma proposta de adequação legal que tenha o mesmo nível de exigência que a legislação europeia é ignorar a situação brasileira. Desse modo, a flexibilidade e a demonstração de certa compreensão comercial faz-se necessária. O único modo da Lei Geral de Proteção de Dados Pessoais surtir real efeito é com a inclusão coorporativa nessa discussão e com uma atuação da ANPD sintonizada com o que é o Brasil.

Referências bibliográficas

540 MILHÕES de dados de usuários do Facebook ficam expostos em servidores da Amazon. **G1**, Rio de Janeiro, 04 abr.2019. Seção de Economia e Tecnologia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/04/04/dados-de-540-milhoes-deusuarios-do-facebook-ficam-expostos-em-servidor.ghtml. Acesso em: 13 out. 2019.

ALBUQUERQUE, Marcos Cintra Cavalcanti de. Divisão Internacional do Trabalho. **Lua Nova: Revista de Cultura e Política**, n.13. São Paulo: Centro de Estudos de Cultura Contemporânea, set. 1987, p. 95-103.

BRASIL. Lei nº 13.709, de 14 de agosto de 2019. Lei Geral De Proteção De Dados Pessoais (LGPD). Brasília: **Diário Oficial da União**, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 out.2019.

CALIFORNIA (EUA). **Assembly Bill N°. 375, California Consumer's Privacy Act.** Sacramento, EUA: California Legislative Information, 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Acesso em: 13 out. 2019.

CASO Cambridge Analytica. **El País.** Madrid: Prisa, 19 mar.2018 – 13 jul. 2019. Caso Cambridge Analytica. Disponível em: https://brasil.elpais.com/tag/caso_cambridge_analytica. Acesso em: 12 out. 2019.

CONFEDERAÇÃO Nacional da Indústria. Em busca de soluções: atributos de autoridades de proteção de dados eficazes. **Confederação Nacional da Indústria.** Brasília: CNI, 2017.

DATA PROTECTION COMISSION. **Mission Statement.** Dublin/Irlanda: Data Protection Comission, 2018. Disponível em: https://www.dataprotection.ie/en/about/background. Acesso em: 13 out.2019.

FERNANDES, André. O papel educativo da Autoridade Nacional de Proteção de Dados. Crypto-id. São Paulo: **Crypto-id**, 25 jun. 2019. Disponível em: https://cryptoid.com.br/protecao-de-dados/o-papel-educativo-da-autoridade-nacional-deprotecao-de-dados/. Acesso em: 13 out. 2019.

FUTURE OF PRIVACY FORUM; DATAGUIDANCE. **Comparing privacy laws: GDPR v. CCPA.** Washington, EUA: Future of Privacy Forum, 2018. Disponível em: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf. Acesso em: 13 out.2019. 10

GUIDI, Guilherme Berti dos Campos. **Modelos Regulatórios para Proteção de Dados Pessoais.** Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em: 13 out.2019.

INFORMATION COMMISSIONER'S OFFICE. Wilmslow, Cheshire, Reino Unido: Information Commissioner's Office, 1994. Disponível em: https://ico.org.uk. Acesso em: 13 out.2019.

INSTITUTO notifica Dataprev e aponta vazamento de dados do INSS. **UOL.** São Paulo: UOL, 03 set. 2019. Seção Economia. Disponível em: https://economia.uol.com.br/noticias/redacao/2019/09/03/idec-notifica-dataprev-licitacaoreconhecimento-facial-beneficiarios-inss.htm. Acesso em: 13 out.2019.

KOTLER, P. **Administração de Marketing.** 14. ed. São Paulo: Pearson Brazil, 2012.

McCABE, David. Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight. **The New York Times.** Tecnology. New York: The New York Times, 01 out.2019. Disponível em: https://www.nytimes.com/2019/10/01/technology/national-privacylaw.html. Acesso em: 13 out.2019.

_____; SWANSON, Ana. U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators. **The New York Times.** Business. New York: The New York Times, 07 out.2019. Disponível em: https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html. Acesso em: 13 out.2019.

MENDONÇA, Heloísa. Mercosul e União Europeia selam esperado acordo após 20 anos de negociações. **El País.** Economia. Madrid: Prisa, 28 de junho de 2019. Disponível em: https://brasil.elpais.com/brasil/2019/06/28/economia/1561741745_016799.html. Acesso em: 13 out.2019.

ONU, Assembleia Geral. **Declaração Universal dos Direitos Humanos.** Paris: ONU, 1948. Disponível em: http://www.un.org/en/universal-declaration-human-rights/ Acesso em: 12 out.2019.

REINO UNIDO. **Data Protection Act 1998**, C. 29. Londres, Reino Unido: The Stationery Office, 2005. Disponível em: 11 http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf. Acesso em: 13 out.2019.

_____. **Data Protection Act 2018**, C. 12. Londres, Reino Unido: The Stationery Office, 2018. Disponível em: http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf. Acesso em: 13 out.2019.

SILVA, Roberto Pessoa Madruga. **Implementação de CRM para viabilização de marketing de relacionamento:** um estudo de caso. 2002. Dissertação (Mestrado em Gestão Empresarial) - Escola Brasileira de Administração Pública e de Empresas da Fundação Getúlio Vargas. Rio de Janeiro, 2002. Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/8645/000320652.pdf;jsessionid=B152B266ED966F65A5FA435D87B98DC7?sequence=1. Acesso em: 12 out. 2019.

STATE OF NEW YORK. **New York's Privacy Bill.** New York's Senate: New York, 2019. Disponível em: https://legislation.nysenate.gov/pdf/bills/2019/S5642. Acesso em: 13 out.2019.
UBER executive apologises after suggesting the firm dig dirt on hostile journalists. **The Guardian,** Londres/Reino Unido, 19 nov. 2014. Disponível em: https://www.theguardian.com/technology/2014/nov/18/uber-exec-apologises-emil-michaeljournalist-sarah-lacy. Acesso em: 12 out. 2019.

UNIÃO EUROPEIA. General Data Protection Regulation. **EU data protection rules.** Bélgica: European Commission, 2018. Disponível em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/dataprotection/2018-reform-eu-data-protection-rules_en. Acesso em: 13 out. 2019.

1.2. Os problemas das transferências internacionais de dados: Comarca, nacionalidade e origem – *Felipe Otávio Moraes Alves*[4]

Resumo

[4] Professor de Direito na Faculdade de Ciências Humanas e Sociais da UNESP da disciplina "Teoria do Estado". Advogado na área de Direito Digital. Mestrando em Direito na UNESP, Universidade Estadual Paulista "Júlio de Mesquita Filho", se especializando na área de Direito Digital (correlacionando Direito à Tecnologia, principalmente a Internet), sob orientação do prof. Dr. Jorge David Barrientos-Parra. Graduado em Direito na Universidade Federal de Goiás. Tem experiência na área de Direito, com ênfase em Teoria do Direito, Direitos Fundamentais, Filosofia de Direito e Direito Digital, atuando principalmente nos seguintes temas: justiça, privacidade, liberdade, direitos humanos, informática, democracia, constituição e subjetividade. Integrante do Grupo de Estudos e Pesquisa em Propriedade Intelectual e Desenvolvimento Econômico-Social (GEPPIDES).

Este artigo busca comparar as eficiências das sanções sobre tratamento de dados no Brasil e no mundo, tratando dos problemas de comarca, nacionalidade e origem do aplicativo e de seus criadores. Com o uso do método indutivo, do direito comparado, da lógica, costumes, bom senso e a moderação fático-lógica, deve-se alcançar conclusões.
Palavras-chaves: tratamento de dados; Direito Internacional; Direito Comparado.

Abstract

This article seeks to compare the efficiencies of data processing sanctions in Brazil and around the world, addressing the problems of county, nationality and origin of the application and its creators. With the use of inductive method, comparative law, logic, customs, common sense, and phatic-logical moderation, conclusions must be reached.
Keywords: data processing. International Law. Comparative law.

Introdução

O objetivo da LGPD é de regulamentar o tratamento dos dados pessoais a fim de proteger direitos de liberdade, de privacidade e o de livre desenvolvimento da pessoa. Seus princípios (art. 6.º) são: Finalidade (propósitos legítimos); Adequação (compatibilidade com a finalidade); Livre Acesso (garantia aos titulares de consulta de como é o tratamento de seus dados); Qualidade dos Dados (garantia, clareza, exatidão, relevância e atualização dos dados); Transparência (garantia de informações acessíveis claras e precisas); Segurança (medidas de segurança para evitar extravios); Prevenção (Adoção de Medidas de Prevenção); Não-Discriminação (não pode servir para discriminar); e Responsabilização (*accountability*).

A título de exemplo, a "privacidade americana" difere da europeia, pois se desvincula do sentido físico do *right to privacy*, assim protege os aspectos socializados da personalidade e preocupa-se com os dados e o controle sobre eles. Na UE, existe uma relação mais vertical – contra o Estado – e nos EUA é contra abuso de particulares – horizontal – enxergando a privacidade como liberdade com aspectos espontâneos, independentes e unicamente individuais da personalidade. Ora, são tanto ordenamentos diferentes, com direitos diferentes, como fica a punição dos violadores do tratamento de dados pessoais no mundo?

1. A LGPD

Regular a transferência internacional de dados é questão de: Soberania, Segurança Nacional, Inovação, Competitividade, Transparência, Manutenção de uma rede aberta e descentralizada, Proteção de Direitos Fundamentais e de Colonialismo Digital (VARON, 2016).

A LGPD (2018) diz que:

> Art. 3 Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;
>
> II - 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;
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Ou seja, há a possiblidade de se punir um estrangeiro, que tratou dados de brasileiros, em um local estrangeiro, o que traz uma gama de problemas a serem observados e solucionados e este é o objetivo do presente trabalho. Outros conceitos-chave para pensar transferência internacional de dados são: Jurisdição nacional deve ser aplicável, Nível de proteção equiparável como pré-requisito, Princípios de Proteção de dados, Direitos do titular, Consentimento forte, Aprovação da Autoridade, Transparência, Responsabilização e Remédios e Sanções (DONEDA, 2017). E o estudo se preocupa justamente com este último.

2. Exemplo da OMPI (ONU)

Um exemplo a ser seguido é o da OMPI e do TRIPS. Com o aparecimento das organizações internacionais, não era mais possível manter as Uniões com as suas estruturas e características originárias. Assim, a Convenção de Estocolmo (1967) criou a Organização Mundial da Propriedade Intelectual (OMPI/WIPO) com status de Organismo Especializado da ONU, servindo para estimular a atividade de criação dos países membros, facilitando a aquisição de obras e o acesso à informação científica das patentes. A WIPO é o principal organismo internacional de proteção dos direitos de propriedade intelectual, juntamente com o TRIPS (Inclusão Acordo Sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio) no GATT (Acordo Geral de Tarifas e Comércio). Todavia, restringe-se mais aos aspectos técnicos porque inexistem mecanismos de fiscalização do adimplemento das obrigações estatais e de resolução de controvérsias – negociação, mediação, conciliação e arbitragem) (BASSO, 2004. p. 290).

No TRIPS, há alguns exemplos de Direito de Autor (Obras intelectuais e artísticas / Programas de Computador), Direito Conexos (Interpretações), Marcas (Marca de Serviço), Patentes (Invenções e Modelos de Utilidade), Indicações Geográficas (Vale dos Vinhedos) Desenho Industrial (Embalagem),

Proteção de Novas Variedades de Plantas (Planta geneticamente modificada) e Topografia de Circuito Integrado (Desenho do Circuito Integrado).

Em particular, a OMC é um acordo maior que se compõe de quatro Anexos e o TRIPS é o Anexo 1C. O TRIPS integra o "Acordo Constitutivo da Organização Mundial do Comércio – OMC", também conhecido como "Ata Final da Rodada do Uruguai". Em alguns países se discute a natureza do "Acordo Constitutivo da OMC", em seus respectivos ordenamentos internos. Para alguns, esse Acordo implica um *executive agrément*, para outros, um tratado de comércio - *trade agreement*.

O "Acordo Constitutivo da OMC" é um tratado-contrato, porque os Estados membros podem determinar como implementar suas regras. Os destinatários das normas do TRIPS são os Estados membros da OMC. Nenhum direito subjetivo resulta para a parte privada. As disposições do TRIPS constituem padrões mínimos de proteção que devem ser adotados pelos Estados partes, em suas legislações nacionais. Qualquer controvérsia deve ser submetida ao procedimento de solução de controvérsias da OMC. A "Rodada do Uruguai" intermediou três concepções sobre PI: a dos EUA, com proteção da PI como favorecimento da inovação e transferência de tecnologia, independente dos níveis econômicos dos países; a dos países em desenvolvimento, cujo objetivo principal era de assegurar difusão da tecnologia mediante mecanismos de transferência; e a de países desenvolvidos como Japão e a EU, que buscam assegurar a proteção dos direitos de PI, evitando abusos e impedimento ao comércio legítimo. As partes se comprometem a buscar "benefícios recíprocos", "bem-estar social e econômico" e, sobretudo, o "equilíbrio de direitos e obrigações". O reconhecimento e a observância dos direitos de propriedade intelectual dependem de valores sociais relevantes e, em particular, do equilíbrio entre os usuários de conhecimento tecnológico. (DEL'OLMO, et. al., 2013)

Os princípios gerais do TRIPS são o *Single Undertaking*: unidade do sistema sem reservas; Tratamento Nacional: cada Membro concederá aos nacionais dos demais Membros tratamento não menos favorável que o outorgado a seus próprios nacionais com relação à proteção da PI; Nação Mais Favorecida: todas as vantagens, favorecimentos, privilégios e imunidades que um Estado parte conceda aos nacionais de outro Estado parte serão automática e incondicionalmente estendidas aos nacionais dos demais Estados partes; Esgotamento Internacional dos Direitos (Exaustão): direito de exclusão comercial do titular do direito de propriedade intelectual se esgota no momento em que ele introduz o produto patenteado no comércio (possibilidade de importar legalmente um produto protegido por direitos de propriedade intelectual, desde que tenha sido introduzido, no mercado de qualquer outro país, pelo seu titular, ou com o seu consentimento); Transparência: os Estados partes se comprometem a tornar públicos as leis de aplicação relativos à matéria objeto do Acordo; Cooperação Internacional: promoção do interesse comum por meio de normas de cooperação mútua, a cooperação "interna" se realiza no âmbito da OMC entre seus membros e a cooperação internacional ou "externa" é a que se estabelece entre o TRIPS e a

OMPI e outras organizações internacionais relevantes na proteção dos direitos de propriedade intelectual; Interação entre os Tratados Internacionais sobre a Matéria: o TRIPS é dirigido aos direitos de propriedade intelectual relacionados ao comércio internacional, enquanto a Convenção de Paris não tem essa pretensão; Interpretação Evolutiva: a interpretação das suas cláusulas pode mudar de acordo com a evolução do tema e, para evitar diferentes interpretações, cada Estado incorpora as regras do TRIPS com base no seu próprio sistema e realidade observando os princípios básicos do Acordo (ou seja, ele não é auto-executável) (CORRÊA, 2004). E estes princípios poderiam ser o mesmo de uma suposta organização internacional sobre tratamento de dados.

Na OMC, há um mecanismo de solução de conflitos, o Órgão de Solução de Controvérsias" (OSC), composto por todos Membros da OMC. No Brasil, temos dois efeitos: o externo, com obrigações assumidas na OMC e aos seus Estados membros; e o interno, com o vigor no direito brasileiro e executoriedade no Brasil (Decreto Legislativo n.º 30/ 1994).

Hoje, transcorrido o período de transição, se houver discrepâncias entre a legislação nacional e o TRIPS, caberá ao legislador nacional dar corpo às disposições do Acordo (o que já vem fazendo), adaptar o direito interno aos padrões fixados pelo TRIPS, sob pena de, não o fazendo, o Brasil violar o Acordo e, consequentemente, ficar sujeito a responder perante o Órgão de Solução de Controvérsias da OMC. O que também poderia ter neste suposto órgão.

Um caso interessante envolvendo o Brasil foi o *DS199 Brazil - Measures Affecting Patent Protection*, a reclamante foram os Estados Unidos que, em 2000 através do OSC, pediu que se ponderasse a possibilidade e as causas de relativização da propriedade intelectual e as relações de PI entre Estados do Norte e do Sul global, onde o Brasil aceitou pedir permissão para os EUA toda vez que for quebrar uma patente deles. Ou seja, estes organismos internacionais podem ter eficácia.

De fato, esta comparação pode ser um pouco complicada pois os agentes destas ações quase sempre são os Estados, enquanto o ideal seria a criação de algum órgão internacional que acolhesse agentes privados para gerar soluções mais céleres.

3. Ação Declaratória de Constitucionalidade 51

Dia 16 de dezembro de 2019 haverá uma audiência pública para "depoimentos que possam contribuir com esclarecimentos técnicos e jurídicos sobre a aplicabilidade dos procedimentos de cooperação internacional para a obtenção de conteúdos de comunicações privadas sob controle de provedores de aplicativos de internet estabelecidos no exterior" (SUPREMO TRIBUNAL FEDERAL, 2019), sobre a Ação Declaratória de Constitucionalidade 51 (ADC 51), que trata sobre o assentamento da constitucionalidade de normas de cooperação jurídica internacional entre autoridades judiciárias brasileiras e estrangeiras, especialmente o do Decreto Executivo nº 3.8104/2001 que internalizou no

Direito brasileiro o Acordo de Assistência Judiciária em Matéria Penal entre o Brasil e os Estados Unidos, acordo também chamado de MLAT (*Mutual Legal Assistance Treaty*).

Este acordo é um ótimo exemplo já que as companhias mais prováveis e que mais atingem direitos de brasileiros no que diz respeito a dados são as companhias americanas Facebook e Google, além de outras, e estes acordos podem facilitar outros casos que nossa lei não abrange, especialmente no que se diz os litígios extraterritoriais. Assim, para a Assespro Nacional, não é cabível para a obtenção do conteúdo de comunicações privadas sob controle de provedor estabelecido fora do território nacional ("declaração branca de inconstitucionalidade" das normas).

Inicialmente, é válido lembrar as leis que abrangem este assunto: Lei nº 9.472/97 (arts. 3º, V e IX, e 72), 12.965/14 (art. 7º - garantem os direitos ao sigilo das comunicações e à privacidade no uso de telefonia e Internet), 9.296/96 (art. 10 e mediante ordem judicial, de ofício ou por requerimento de autoridade policial ou do Ministério Público, quando há indícios razoáveis de autoria ou participação em infração penal punida com pena de reclusão e indisponibilidade de outros meios de produção de prova - arts. 1º e 2º), CPC (art. 6º, III, recolher todas provas, e "objetos necessários à prova de infração ou à defesa do réu" e "cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato" - art. 240, §2º), 12.830/13 (art. 2º, § 2º, delegado de polícia deve requerer dados que interessem), 13.344/2016 (em casos de sequestro e cárcere privado, redução à condição de escravo, tráfico de pessoas, extorsão mediante restrição de liberdade da vítima e extorsão mediante sequestro, membro do Ministério Público ou delegado de polícia a "requisitar a quaisquer órgãos do poder público ou de empresas da iniciativa privada dados e informações cadastrais da vítima ou de suspeitos", ADI 4642) e tráfico internacional de criança ou adolescente); do RE 418.416-8/ SC, julgado pelo STF, mandado de busca e apreensão legitima acesso a dados armazenados em computadores; e do Acordo de Assistência Judiciária em Matéria Penal (MLAT), relativo à obtenção de conteúdo de comunicação privada sob controle de provedores de aplicativos de internet sediados no exterior.

Ora, o problema é a prática e a efetividade do tratado internacional para a obtenção e a interceptação do conteúdo de comunicações eletrônicas, a possibilidade de aplicação da legislação brasileira e de outros instrumentos para acesso a comunicações intermediadas por empresas norte-americanas ou estrangeiras contra a possível diminuição do nível de proteção da privacidade dos usuários de serviços de internet.

É válido notar as singularidades Jurídicas da Internet, pois elas intervêm na regulamentação da internet e das políticas públicas, sendo cruciais ao justificar a diferenciação da internet com outros meios do mundo "real". A característica basilar para uma regulamentação da internet é a dificuldade de identificação pelo anonimato dos usuários. É a Polícia Federal que pericia majoritariamente os casos, em algumas dezenas para milhares de casos. Empresas privadas raramente identificam o usuário,

tampouco cooperam em investigações e, muito menos, os denunciam ou sancionam. Ora, se não há uma maneira de saber quem alguém é, o sistema jurídico, que é depende dessas informações, perde sua efetividade. O anonimato na rede torna cibercriminosos mais suscetíveis a praticar violações da privacidade. A segunda característica é a irreversibilidade espaço-temporal, já que a violação a honra e da privacidade na internet tornam-se irreversíveis visto que as informações ficam permanentemente lá gravadas e alcançam inúmeros cidadãos. Há exceções, como o uso inapropriado de marca com a remoção da empresa plagiadora. Todavia, em redes sociais e ações cibercriminosas, a irreversibilidade é plenamente identificável. Qualquer ato é registrado e mesmo com remoção conteúdo, há a possibilidade de salvamento do conteúdo em algum hardware inacessível, permanecendo no servidor do provedor, além da incontável reprodução do mesmo. Ou seja, o dano causado pela violação da privacidade é imensuravelmente mais perigoso no ciberespaço.

A terceira característica é a permanência eterna da informação e do dano, pois uma vez inserida no mundo virtual, ela lá permanecerá até que alguém a retire. Para tanto, a violação de direitos na internet deveria ser tratada com mais severidade e celeridade. Esta singularidade restringe lato sensu a própria liberdade de expressão, pois os usuários, receosos das consequências eternas da rede, limitar-se-ão em comunicar no ciberespaço. A perecibilidade das provas contra cibercriminosos é a quarta característica. As possíveis provas contra cibercriminosos são submetidas a mecanismos de criptografia pelo próprio e que, habitualmente, só podem ser averiguadas quando o equipamento está ligado. São necessários pouquíssimos segundos para que o cibercriminoso possa apagar todos seus rastros digitais ou submetê-los a rigorosos mecanismos de criptografia. Por isso, uma perícia rápida se faz mister. E a última é a internacionalização das condutas. Os casos de litígios transnacionais englobando pessoas, físicas e jurídicas, de diferentes países ou de múltiplas jurisdições são bastante frequentes. Neste âmbito, houve o emblemático caso Garcia vs. Panasonic, em que o autor ganhou a ação pois era uma empresa grande contendo a venda dos dois produtos em ambos países, um caso bastante específico. A maioria dos casos permanece sem solução: empresas com sede em um só país, compra e venda de produtos em – e de – outros países, disponibilização do produto num só país etc. Hoje, usuários podem difamar e discriminar cidadãos de outros países sem sansão legal, elucidando a seriedade deste problema, tampouco incidindo responsabilidades trabalhistas, ambientais, tributárias etc.

Esta última característica é importantíssima para a análise do nosso caso em questão.

Assim, apesar de a Constituição proteger o sigilo das comunicações e a privacidade, cabem interpretações sobre o grau de proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações. Ora, as empresas internacionais devem satisfação ao Brasil e aos brasileiros ao tratar seus dados. Em princípio, não tem a ver com Quebra de Sigilo ou Interceptação do fluxo das comunicações (pelas supostas deficiências estruturais nas capacidades investigativas da

polícia judiciária, fazendo com que esta seja fortemente dependente desse meio agressivo de instrução probatória, recorrendo a medidas de interceptação e de quebra de sigilo como prima ratio), tampouco com uma suposta vigilância abusiva do Estado ou questões de quando o acesso se dá diretamente no aparelho apreendido (aplicam-se os dispositivos relativos à busca e apreensão).

Nesta solução do problema central da extraterritorialidade, temos alguns problemas agravantes. O primeiro é a necessidade de mandados judiciais (especialmente na questão de sigilos de comunicações), onde há o problema de se querer o conteúdo das informações comunicadas ou do mero fluxo dessas informações (conteúdos e registros de comunicações armazenadas em dispositivos pessoais, desde que "proporcionais", quando se fundamentarem em direito fundamental conflitante ou em interesse público, também para interceptações de comunicações eletrônicas – MCI). Um segundo problema agravante parece ser o acesso diretamente no aparelho apreendido; De acordo com os referidos dispositivos, fica autorizada a busca domiciliar e/ ou pessoal quando há "fundada suspeita de que alguém oculte consigo" "objetos necessários à prova de infração ou à defesa do réu" (art. 240, §2º). E em 2012, o STF decidiu que a análise de registros telefônicos (metadados) de celular apreendido após prisão em flagrante não caracteriza violação ao sigilo das comunicações (art. 5, inciso XII), porque sua proteção abarcaria "comunicações de dados e não dados em si" e porque "comunicação telefônica e registros telefônicos recebem proteção jurídica distinta". Em 2016, por outro lado, agora lidando com um smartphone e demonstrando-se ciente da enorme quantidade de dados que um celular moderno produz e armazena, o STJ decidiu que a verificação de histórico de conversas do WhatsApp (conteúdo) em celular apreendido após flagrante constitui quebra de sigilo, isto é, é ilegal sem a existência de ordem judicial autorizadora. Em tribunais estaduais, a apreciação do tema permanece casuística. E isto está estreitamente correlacionado com a proteção de dados pois em que medida deve o Brasil ter o direito de solicitar estes dados, o quão rápido precisa nossos órgãos fiscalizatórios de acessar estas informações de quebra de dados e para isso precisa ter leis e políticas públicas às vezes mais intrusivas em empresas e pessoas físicas.

Uma outra questão fora quando a Oficina Antivigilância identificou, em julho de 2015, a celebração de acordo entre o Departamento de Segurança Nacional dos Estados Unidos, pela Agência de Fiscalização de Aduana e Proteção de Fronteiras, e o Ministério da Fazenda do Brasil, por meio da Secretaria da Receita Federal, para "reconhecimento mútuo" dos Programas de "Parceria Aduana-Empresa contra o Terrorismo" da agência americana e de "Operador Econômico Autorizado" da Receita Federal, o que envolveria transferência de

infraestrutura de processamento de dados e desenvolvimento e uso de tecnologia da informação em comum. Considerando que a Receita Federal tem acesso a informações sobre comunicações de brasileiros, essa cooperação pode significar ampliação da vigilância a nível internacional.

Um quarto problema é a quebra de sigilo de conteúdo de comunicações eletrônicas em posse de provedores de aplicações de Internet (tais como Google e Facebook): está também prevista no Marco Civil da Internet, nos arts. 7º, III e 10, § 2º, os quais explicitam a necessidade de ordem judicial para tanto. Um quinto ponto são as comparações com a Manifestação da PGR na ADI 4642 sobre a Lei nº 13.344/2016, onde a celeridade ao procedimento investigatório de crimes que demandam atuação, sob pena da ineficácia do Estado, deve perseverar. Ora, a necessidade de mandado judicial dificulta a salvaguarda da vítima e deve ocorrer no caso concreto a fim de resguardar outros direitos fundamentais, assim como os demais direitos pessoais, também o direito à privacidade não se revela ilimitado e imune a intervenções restritivas: uma restrição apenas se justifica quando necessária a assegurar a proteção de outros direitos fundamentais ou bens constitucionais.

Um dos principais problemas desses MLATs são o fato de serem muito burocráticos e demorados e intrinsicamente pensados na territorialidade física. O Brasil faz parte de mais de 30 acordos bilaterais e multilaterais de assistência judicial recíproca em matéria penal, que só funciona para situações raras e excepcionais e porque a identificação dos limites da jurisdição e da necessidade de se recorrer a meios de cooperação é simples. Mas com a Internet: a necessidade de coleta de provas é cotidiana e "documentos digitais" estão em um servidor físico, mas podem ser acessados virtualmente em vários lugares do mundo e ainda os provedores de aplicações de Internet estão presentes multinacionalmente nem que apenas virtualmente.

Um sétimo problema é a frequência com a qual isso acontece entre estes países, já que a legislação americana aplicável ao fornecimento de dados de usuários a autoridades proíbe provedores de entregar conteúdo de comunicações sem a apresentação de um warrant emanado por um juiz americano. Uma saída para remediar esta situação é reformular o atual modelo de cooperação judiciária internacional em matéria penal e repensar os fatores definidores de jurisdição sobre dados digitais como elementos de prova, atendendo às necessidades de autoridades de segurança pública ao redor do mundo e respeitando direitos humanos. Enquanto isso não ocorre, ameaças de multas, prisões, bloqueios, além de inúmeros acordos "informais" entre empresas e autoridades serão frequentes. Exemplos: Inquérito nº 784/CF, de 2013, Google impetrou MS contra ofício da Polícia Federal pelo qual se requisitou a quebra de sigilo telemático de contas do Gmail onde o STJ rejeitou afirmando que "o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados". A Microsoft também já desafiou ordens de quebra de sigilo de e-mails Hotmail com mesma derrota pelo STJ. Em 2014, a Yahoo! foi alvo de ação civil pública proposta pelo MPF em razão dos alegados "reiterados descumprimentos de ordens judiciais" determinando o fornecimento de dados de usuários, porém a Justiça Federal estabeleceu o dever de fornecer somente dados de usuários que efetivamente se cadastraram na versão brasileira do serviço (@yahoo.com.br). E em 2016, a Justiça Federal do Rio

Grande do Sul decidiu que o MPF deve obter conteúdo de comunicações privadas transmitidas na rede social Facebook pela via diplomática, uma vez que tais dados são controlados pela Facebook Inc. mas alega que "apenas presta serviços relacionados a publicidade, não detendo informações relativas a usuários", ou seja, por falta de interesse de agir e impossibilidade do pedido.

Assim, conclui-se que os acordos internacionais de cooperação mútua em matéria penal são instrumentos que podem servir como uma via mais diplomática para o equacionamento dessas tensões, porém hoje é uma solução ineficiente. É necessário o aprimoramento desses mecanismos para tornar mais céleres e eficientes as investigações destes casos. Para este aprimoramento, deve-se permitir a possibilidade de requerimento e resposta rápida de pedidos do Brasil a empresas brasileiras (sem a necessidade de um warrant lá) e vice-versa, o que resolveria o problema de os MLATs serem burocráticos e demorados e resolveria as alegações das empresas de que o conteúdo está em servidores nos EUA Além disto, a realização de estudos empíricos acerca das práticas de autoridades policiais e do Ministério Público de requisição de dados cadastrais e pedidos de quebra de sigilo de metadados são necessários além da necessidade de se elaborar estatísticas acerca da quebra de sigilo de metadados e estender e dar publicidade às informações recolhidas pelo Sistema Nacional de Controle de Interceptações.

Conclusão

Há a necessidade de harmonia dos padrões internacionais e criação de um Órgão Internacional, assim como, para a propriedade industrial, a OMPI e o TRIPS, para facilitar sansões quando envolver tratamento de dados em âmbito internacional. Deve-se notar também que a ADC 51 também impactará significativamente como os dados serão tratados internacionalmente, em que estas cooperações mútuas internacionais tem uma importância fundamental e devem ser encorajadas.

Referências bibliográficas

BASSO, Maristela. **A proteção da propriedade intelectual e o direito internacional atual.** a. 44 n. 126 abr./jun. 2004. Brasília: Revista de Informação legislativa, 2004.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 2018.

CORRÊA, Charlene Maria de Ávila. **O direito internacional frente ao Instituto da Propriedade Intelectual:** OMC/Trips (Trade Related Aspects of Intellectual Property Rights). 17ª ed. Ribeirão Preto: Revista Paradigma, 2004.

DEL'OLMO, Florisbal; ROSADO, Olivério de Vargas; ARAÚJO, Thiago Luiz Rigon de. **Propriedade intelectual no cenário internacional:** organismos de proteção e o acordo TRIPS. Santa Maria: Revista Eletrônica de Direito UFSM, 2013.

DONEDA, Danilo. **Transferência Internacional de dados pessoais.** Audiência Pública - Comissão Especial de Tratamento e Proteção de Dados Pessoais, Brasília, DF, 2017. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/espe ciais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audien cias-e-eventos/danilo-doneda>. Acesso em: 14 out. 2019.

SUPREMO TRIBUNAL FEDERAL. **Audiências Públicas.** 2019. Disponível em: <http://www.stf.jus.br/portal/audienciaPublica/audienciaPublica.asp?tipo=prevista>. Acesso em: 09 dez. 2019.

VARON, Joana. **Transferência Internacional de Dados Pessoais.** Comissão Especial Câmara dos Deputados, Junho/2016, 2016. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-e-eventos/joana-varon>. Acesso em: 14 out. 2019.

1.3. La aplicación del Reglamento Europeo de Protección de Datos a las Entidades no Europeas[5] – *Raquel Guillén Catalán*[6]

El derecho fundamental de la «protección de datos» es el derecho que nos permite acceder, rectificar y cancelar la información almacenada y disponer de los propios datos personales, es decir, es el derecho de controlar la veracidad o exactitud de dichos datos, de impedir la difusión de los mismos si se trata de datos sensibles y de verificar su utilización para el fin autorizado[7]. La Constitución española, en su artículo 18 CE, apartado cuarto, establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

[5] Este trabajo se ha realizado en el marco del Proyecto «Contratos, Transparencia y protección de datos en el mercado digital», (RTI2018-097354-B-I00), financiado por el Ministerio de Ciencia, Innovación y Universidades.

[6] Profesora Titular de Derecho Civil de la Universitat de València.

[7] PEREZ LUÑO, A., *Derechos Humanos*, Estado de Derecho y Constitución: Madrid, Tecnos, 1984, pp. 316-375.

Inicialmente se discutía sobre si era un derecho autónomo o una rama del derecho a la intimidad[8] . Al respecto, la Sentencia del Tribunal Constitucional, núm. 292/2000, de 30 de noviembre de 2000 reconoce el Derecho a la Protección de Datos, como un derecho fundamental absolutamente independiente del Derecho al Honor, Intimidad y Propia Imagen, otorgando así a la protección de datos de carácter personal, una entidad absolutamente independiente del resto de derechos[9] . Así mismo, junto con el reconocimiento constitucional, se debe acudir, según lo establece el propio Tribunal Constitucional[10] , al Convenio nº 108 del Consejo, de 28 de enero de 1981, de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[11].

En la citada Sentencia también se hace referencia a la aplicación del párrafo segundo del artículo 8 del Convenio Europeo para la protección de los Derechos Humanos de Roma de 1950 que establece los límites al derecho a la intimidad[12].

El reconocimiento constitucional a la protección de datos fue desarrollado por la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), posteriormente por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, (en adelante LOPD), que trasponía a nuestro ordenamiento jurídico la Directiva de protección de datos (Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) y por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, (en adelante RLOPD).

En la actualidad, la protección de datos se regula por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que

[8] Sobre la necesaria configuración o no de un nuevo derecho fundamental, véase ORTI VALLEJO, A., *Derecho a la intimidad e informática:* Granada, Comares, 1994, p. 56 y ss.

[9] MARTÍNEZ VÁZQUEZ, F., «La tramitación parlamentaria de la Ley Orgánica de protección de datos», en RALLO LOMBARTE, A., *Tratado de protección de datos:* Valencia, Tirant Lo Blanch, 2019, p. 54.

[10] Vid. la Sentencia del Tribunal Constitucional 254/1993, de 20 de Julio, (RTC 1993\254).

[11] En particular, se debe prestar atención a los principios que reconoce el citado Convenio. En particular, a la calidad de los datos de carácter personal reconocido en el artículo 5, las categorías particulares de los datos establecidas en el artículo 6, las distintas medidas de seguridad aplicables a los mismos contenidas en el artículo 7, las garantías complementarias para la persona titular de los datos que se encuentran en el artículo 8, entre otros.

[12] Concretamente, el citado precepto hace alusión a la seguridad nacional, la seguridad pública y el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o la moral, la protección de los derechos y libertades de los demás. Este criterio también se halla previsto en el párrafo segundo del artículo 9 del Convenio 108 del Consejo de Europa para la protección de las personas com respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981.

respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD)[13].

El citado Reglamento es aplicable en todos los Estados de la Unión Europea y pretende homogeneizar[14] la normativa en materia de protección de datos[15], impidiendo que exista disparidad de regulaciones en cada Estado miembro[16].

No obstante, el legislador nacional promulgó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDDG)[17], ya no sólo integrando las normas establecidas en el RGPD[18], sino complementando la misma, atendiendo a que, como se verá más adelante, los Estados miembros debían precisar algunos aspectos que quedaban sin concretar en la normativa europea[19].

[13] Debe tenerse en cuenta que junto el Reglamento existen otra normativa europea que regula aspectos específicos en relación a la privacidad, como, por ejemplo, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) que, se prevé que, en breve, sea sustituía por el Reglamento del Parlamento europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónica. En relación a las dudas de conciliación entre las diversas normativas, véase LÓPEZ CALVO, J., *Comentarios al Reglamento Europeo de Protección de Datos:* Madrid, Sepín, 2017, pp. 60 y 77.

[14] Téngase en cuenta que mientras los reglamentos son normas vinculantes, las directivas únicamente establecen unos objetivos para todos los Estados miembros que deben trasponer a través de su propio ordenamiento jurídico. Vid. LÓPEZ CALVO, J., Comentarios al Reglamento Europeo de Protección de Datos, op. cit., p. 63.

[15] Uno de los objetivos del Reglamento era «evitar la fragmentación de los ordenamientos jurídicos de los Estados miembros en materia de protección de datos personales, especialmente en lo relativo al régimen sancionador». Vid. MARTÍNEZ VÁZQUEZ, F., «La tramitación parlamentaria de la Ley Orgánica de protección de datos», op. cit., pp. 55-56.

[16] Al respecto se debe tener en cuenta que una de las críticas a la Directiva 95/46/CE relativa a la protección de las personas físicas en lo respectivo al tratamiento de datos personales se refería a «la excesiva libertad con la que contaban los Estados miembros a la hora de establecer el correspondiente régimen sancionador». CORRAL SASTRE, A., «El régimen sancionador en materia de protección de datos en el Reglamento general de la Unión Europea», en PIÑAR MAÑAS, J.L., *Reglamento General de protección de datos. Hacia un nuevo modelo europeo de privacidad*: Madrid, Reus, 2016.

[17] Para mayor información sobre el iter parlamentario de la norma. Véase, MARTÍNEZ VÁZQUEZ, F., «La tramitación parlamentaria de la Ley Orgánica de protección de datos», *op. cit.* pp. 56-77.

[18] Vid. GARCÍA MEXÍA, P., «La singular naturaleza jurídica del Reglamento General de protección de datos de la UE. Sus efectos en el acervo nacional sobre protección de datos», en PIÑAR MAÑAS, J.L., *Reglamento General de protección de datos. Hacia un nuevo modelo europeo de privacidad*: Madrid, Reus, 2016, pp. 25-26.

[19] Junto con el objetivo mencionado, se debe señalar que la promulgación de la LOPDDG también supuso completar el RGPD con medidas más eficaces y clarificar la normativa aplicable al derogar expresamente la

La protección que se dispensa a través de la normativa señalada sería inútil si, a la vez, no se estableciera un régimen disciplinario que garantizase el cumplimiento de la legislación y, más, teniendo en cuenta, el impacto que tienen las tecnologías en cualquier ámbito de la sociedad, ya no sólo por las innumerables ventajas que ofrecen, como la contratación de un modo global o el desarrollo de nuevas formas de comunicación, como las plataformas de comunicación en línea[20], sino también por los nuevos retos a los que hacer frente, si se realiza de un modo masivo la recogida de nuestros datos personales, especialmente en relación a los menores, usuarios más desprotegidos[21].

Por todo ello, en este trabajo se quiere resaltar la importancia de la aplicación del Reglamento Europeo a las entidades de fuera de la Unión Europea que deben conocer sus disposiciones para no incurrir en las infracciones y describir brevemente el régimen de infracciones que se recogen para la protección del derecho y las cuantiosas multas económicas.

1.4. A institucionalização das Autoridades de Proteção de Dados Pessoais na América Latina: estudo dos modelos regulatórios da Argentina e do Uruguai – *Amanda Nunes Lopes Espiñeira Lemos*[22]

Resumo

O presente artigo tem como objetivo analisar os modelos regulatórios da Argentina e do Uruguai, países com legislação mais antiga de proteção de dados da América Latina, que possui Autoridade no tema, a fim de perceber se há a expansão do modelo europeu de controle administrativo para a América Latina.
Palavras-chave: Proteção de Dados Pessoais; Autoridade; Modelo Regulatório; Institucionalização; Argentina; Uruguai.

Abstract

LOPD. Vid. AMÉRIGO ALONSO, J., «Objeto y ámbito de aplicación», en RALLO LOMBARTE, A., *Tratado de protección de datos:* Valencia, Tirant Lo Blanch, 2019, p. 80.

[20] GIL ANTÓN, A. M., «La privacidad del menor en internet». REDS. *Revista de Derecho, Empresa y Sociedad*, núm.3, septiembre-diciembre, p.79. 2013.

[21] En este sentido señala el Prof. Vázquez de Castro que «el menor es un usuario más débil y menos consciente de sus derechos». VÁZQUEZ DE CASTRO, E., «Protección de datos personales, redes sociales y menores». *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 29, p. 53. 2012.

[22] Doutoranda pelo Programa de Pós-Graduação em Direito na Universidade de Brasília.

This paper aims to analyze the regulatory models of Argentina and Uruguay, countries with the oldest data protection legislation in Latin America, which has Data Protection Authority, in order to understand if there is an expansion of the European model of administrative control to Latin America.
Keywords: Data Protection. Authority. Regulatory Model. Institutionalization. Argentina. Uruguay.

Introdução

Vários países da América Latina possuem legislações nacionais sobre a proteção de dados pessoais, apenas sete deles possuem autoridades já instituídas que asseguram essa proteção. A Argentina possui a legislação mais antiga, de 2000, seguida do Uruguai, em 2008. O Brasil aprovou a Lei n. 13.709/2018, que entra em vigor em agosto de 2020, recém aprovou o Conselho que comporá a Autoridade e necessita implementar a sua autoridade, a fim de garantir a aplicabilidade da lei e a fiscalização da sua observância. Há um modelo regulatório previsto e passível de críticas pelos pesquisadores do tema, contudo, este será revisto, segundo previsão legal em 2 anos, o que abre espaço para atualização e aperfeiçoamento desse modelo.

Assim, o presente projeto propõe fazer um levantamento bibliográfico que subsidie uma pesquisa empírica realizada no âmbito de um projeto FAPESP, que possui o intuito de compreender como essas autoridades atuam nos países vizinhos, Dos 20 países da América Latina, propõe-se realizar visitas de campo em sete deles, quais sejam: Argentina, México, Uruguai, Colômbia, Costa Rica, Panamá e Peru, os quais possuem leis e autoridades de proteção implementadas.

PAÍS	LEI DE PROTEÇÃO DE DADOS	AUTORIDADE DE PROTEÇÃO DE DADOS
Argentina	Lei n. 25.326/2000	Dirección Nacional de Protección de Datos Personales
Uruguai	Lei n. 18.331/ 2008	Unidad Reguladora y de Control de Datos Personales
México	Lei Federal de Proteção de Dados e Proteção Individual de 2010	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Inai)

Peru	Lei n. 29.733/ 2011	Autoridad Nacional de Protección de Datos Personales
Colômbia	Lei n.1.581/2012	Superintendência de Indústria e Comércio (SIC)
Costa Rica	Lei Federal de Proteção de Dados 2016	Agencia de Protección de Datos de los Habitantes (PRODHAB)
Panamá	Lei n. 81/2019	Autoridad Nacional de Transparencia y Acceso a la Información (Antai)

Busca-se, para tanto, mapear dados que ainda não são compilados e compreender modelos regulatórios. Realiza-se nesse artigo um recorte com os dois países com a legislação mais antigas: Argentina e Uruguai. Serão usados os seguintes métodos de coleta e de análise das informações: (1) levantamento documental das autoridades de proteção de dados; (2) análise jurídica das legislações nacionais.

O problema teórico se biparte em duas questões. A primeira questão se refere às diferenças institucionais entre os vários países, nos modos de organizar seus sistemas de proteção de dados. Será aferido se existe influência do modelo europeu e se existe influência mútua entre os países latino-americanos. O modelo europeu é consolidado pela Diretiva 95/46/CE, de 24 out. 1995, atualmente substituída pelo Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679, de 27 abr. 2016).

A segunda questão se refere às práticas culturais e sua relação com as ações de proteção de dados. Será inquirido se existe uma cultura de proteção de dados pessoais na América Latina e se existem diferenças no significado social de privacidade entre os países da região.

Realiza-se uma comparação jurídica e institucional das legislações e das autoridades nacionais visitadas em uma breve comparação das instituições analisadas em relação ao modelo europeu.

Trata-se da europeização dos modelos de autoridade de proteção de dados ante o pioneirismo do Regulamento Geral de Proteção de Dados da União Europeia (GDPR)?

Existe nos países latino-americanos: (1) a formação de um sistema "civil law" de proteção de dados?; (2) a importação de modelos europeus?; ou (3) o ineditismo / inovação na América Latina? Qual o modelo adotado pelas Autoridades de Dados Pessoais na Proteção da Privacidade nas modulações jurídicas dos países

latino-americanos? E da União Europeia? Quais as semelhanças e diferenças entre eles? Quais papeis esses órgãos desempenham no contexto de proteção à privacidade? Essas competências na prática institucional correspondem ao que a legislação pátria própria determina?

A discussão gira em torno da existência de um modelo ideal de proteção de dados. Trata-se, ainda, da compatibilidade internacional das regras de proteção de dados pessoais e privacidade.

1. Modelos regulatórios de proteção de dados e a autoridade de proteção

1.1. O caso da Argentina

A Argentina sancionou desde 2000 a Lei nº 25.326[23] que trata em seu artigo 29 do órgão administrativo de controle dos dados. O conteúdo da lei se baseou bastante na Lei francesa 78-17, de 6 de janeiro de 1978 e surgiu como resposta à recomendação feita pelo então Conselho para a Consolidação da Democracia que sinalizava a conveniência de consagrar o direito à privacidade, principalmente com o objetivo de evitar que ela fosse afetada pelos avanços da tecnologia da informação. de registro de dados.

O debate no país era ainda mais antigo, já em 1968, a Lei 17.622, que estabeleceu a criação do INDEC, estabeleceu o sigilo dos dados coletados pelo Sistema Estatístico Nacional. No entanto, nenhum projeto sobre o assunto havia sido apresentado desde então. O longo caminho iniciado em 1986 teve vários projetos como protagonistas frustrados e, após um período de estagnação, tomou novo ímpeto no contexto da reforma constitucional de 1994 (TANÚS, 2001)

A autoridade de proteção de dados do país é a *Agencia de Acceso a la Información Pública*[24], que congrega tanto a competência de tratar de acesso à informação, quanto proteção de dados.

1.2. O modelo do Uruguai

Já o Uruguai aprovou em 2008 a Lei n° 18.331[25], cujos artigos 31 a 36 trata da criação da Autoridade de Proteção de Dados e no Art. 32 existe também a previsão de um Conselho Consultivo. A Declaração de Adequação do modelo europeu veio em 2012 e em 2013 a Lei 19030, de Ratificação ao Conselho 108. Constituiu o primeiro país fora da Europa a aderir à essa Convenção.

A Autoridade que trata do tema é a *Unidad Reguladora y de Control de Datos Personales* (URCDP)[26]. O órgão é desconcentrado, de segundo nível, e possui dependência do Poder Executivo, já que não possui em aspectos financeiros um fundo de arrecadação próprio. Falta, assim, independência financeira.

[23] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[24] https://www.argentina.gob.ar/aaip/autoridades

[25] https://legislativo.parlamento.gub.uy/temporales/leytemp6809155.htm

[26] https://www.gub.uy/unidad-reguladora-control-datos-personales.

A Autoridade, entre 2009 e 2012, publicou estatísticas dos dados extraídos sobre sua atuação[27], no tratamento de dados, inclusive em relação ao fluxo transfronteiriço, que de acordo com o art.23 da lei uruguaia merece atenção especial. Apesar de os dados estarem um pouco desatualizados, cerca de 7 anos atrás, o cenário apresenta-se semelhante, já que a Argentina, além do próprio Uruguai, é o único país com proteção adequada dentro das normativas europeias.

Puesto	País
1	Argentina
2	EEUU
3	Brasil
4	España
5	Suiza

(URCDP, 2012, p. 7).

Há ainda a *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*, que trata de transformações digitais no poder público uruguaio.

1.3. Atuação das autoridades de proteção de dados no fluxo transfronteiriço: influência da GDPR nos modelos da Argentina e do Uruguai

Os países fazem parte da *Red Iberoamerica de Datos Personales*, que surgiu em 2003, e constitui um espaço integrador de atores público de privados que tem como objetivos:

> desenvolver iniciativas e projetos relacionados à proteção de dados pessoais na América Latina, com o objetivo de promover, manter e fortalecer um intercâmbio próximo e permanente de informações, experiências e conhecimentos entre eles, bem como promover os desenvolvimentos regulatórios necessários para garantir a regulamentação avançada do direito à proteção de dados pessoais em um contexto democrático, levando em conta a necessidade do fluxo contínuo de dados entre países que têm laços comuns em comum e a preocupação por esse direito.[28] [29]

A comparação entre modelos nacionais regulatório com o intuito de predizer mecanismos de políticas públicas locais, antes do desenvolvimento de um método jurídico próprio de análise comparativa que contemple indicadores comensuráveis para a realizar a análise proposta. Essa metodologia busca abranger

[27] https://www.gub.uy/unidad-reguladora-control-datos-personales/datos-y-estadisticas/estadisticas

[28] http://www.redipd.es/la_red/Historia/index-idpt-idphp.php

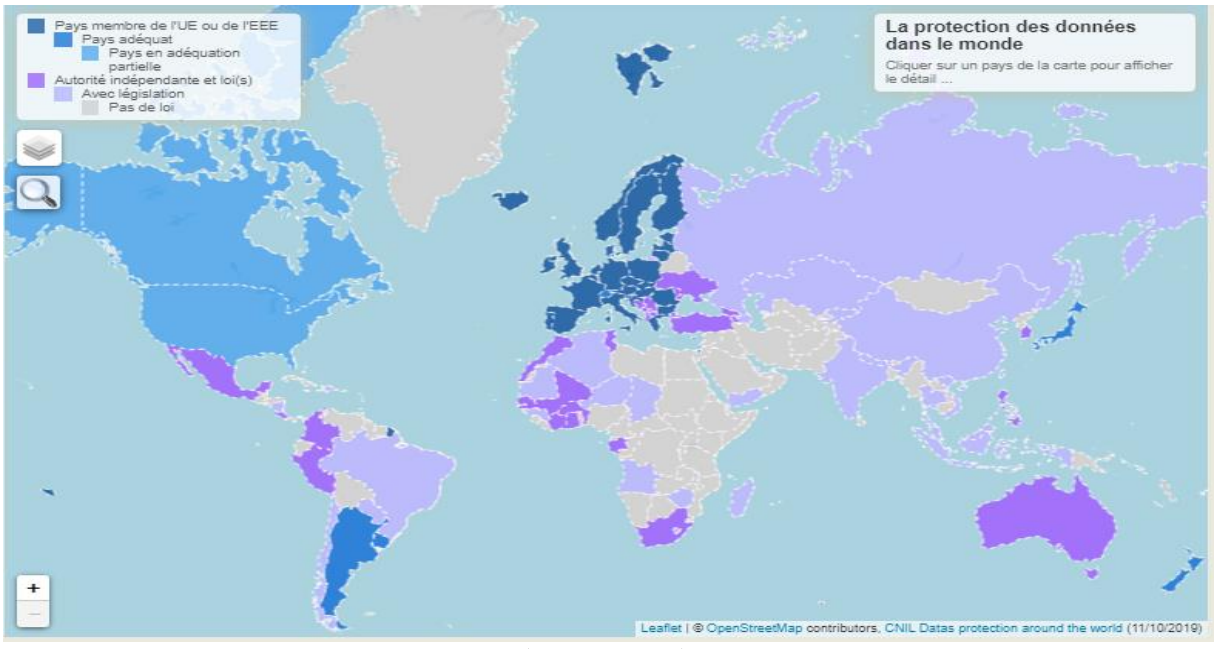
[29] "desarrollar iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho". (Tradução nossa)

uma "rede conceitual de atributos jurídicos, cuja realidade depende de indicadores de ordem normativa (base legal), de ordem concreta (implantação da legislação), de ordem institucional (papel dos atores envolvidos) e de ordem prospectiva (tendência para o futuro)" (ARANHA, 2011a, p. 17).

Há, nesse sentido, a preocupação com a dificuldade de desmembramento dos institutos jurídicos em seus efeitos práticos e de sua necessária contextualização nacional, isto é, a preocupação com o "transplante de práticas regulatórias nacionais para corpos políticos dotados de modelos socioeconômicos, políticos e jurídicos distintos" (ARANHA, 2011b, p. 4). Choudhry (2006, p. 29) aponta que "os transplantes legais só poderiam ocorrer se tanto a regra como seu contexto pudessem ser transferidos entre sistemas legais."[30].

Assim, existem algumas semelhanças entre o estatuto argentino e o uruguaio. Ambos os países atingiram um nível de adequação de acordo com os requisitos da Diretiva 95/46/CE. No momento, os dois países estão tentando se adequar aos padrões do RGPD (Regulamento UE 2016/679).

A Autoridade de Proteção de dados francesa (*Commission nationale de l'informatique et des libertés* - CNIL) apresenta um mapeamento[31] que que apontam a adequação da Argentina e Uruguai como únicos países da região adequados à EU, no tom azul. Representam uma referência para o tema, não apenas da América Latina, mas em todo mundo após análise do gráfico.



(CNIL, 2019).

Ambos os países acima analisados assinaram a Convenção 108+ do Conselho da Europa. Este tratado cobre questões de proteção de dados e também fornece padrões mínimos para o uso de dados pessoais,

[30] Legal transplants could only occur if both the rule and its context could be transferred between legal systems. (Tradução nossa)

[31] Disponível em: <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>.

como modelo de adequação para realização de transações comerciais e fluxo de dados entre outros países. A Convenção de 1980, de Strasbourg, é "resultado do movimento promovido pela OCDE para facilitar a harmonização das legislações de proteção de dados pessoais" (BIONI, 2019, p.122).

Bioni (2019) aponta que a própria Convenção associa a proteção de dados ao livre fluxo informacional e possui um capítulo sobre o fluxo de dados transfronteiriço. "Para além da coincidência terminológica, há, sobretudo, uma carga ideológica que foi posta em curso não só pelo organismo internacional multilateral, mas, também, pelo bloco continental europeu, o que rege, até hoje, o seu quadro normativo de proteção de dados" (p.122).

Conclusão

Há influência do Modelo Regulatório Europeu de Controle Administrativo de Proteção de Dados Pessoais e Privacidade nos casos latino-americanos. Contudo, não se trata de fato de uma expansão, já que os países da América Latina possuem aplicações sociais e econômicas dos dados distintas. As legislações, tanto argentina, quanto uruguaia, são anteriores à GDPR, apesar de posteriores e Diretiva 95/46.

Pontua-se, ainda, que as Autoridades de Proteção de Dados Pessoais possuem papel central na aplicação das regras de proteção da privacidade e de resolução de conflitos em temas pertinentes à Internet: regulação de aplicativos; gestão criptográfica e de segurança; formação e gestão dinâmica de bases de dados por meio de algoritmos. E que as Autoridades de Proteção de Dados colaboram de fato na redução de casos judicializados no contexto da Regulação da Internet, além de colaborarem na resolução de conflitos mesmo no Judiciário, como o pedido de desindexação de conteúdo nos sites de busca, conhecido como direito ao esquecimento, no paradigmático caso da Corte Europeia de Justiça *Mário Costeja González vs. Google Spain.*

Ademais, as competências que esses órgãos desempenham destoam em parte do que a legislação pátria própria determina, já que as ações sociais e econômicas, principalmente no contexto da Internet, pressupõem certa plasticidade, pois a regulamentação prévia pode gerar uma rápida obsolescência da norma jurídica em relação à facticidade do fenômeno que busca regular, bem como pode servir como um grave empecilho para a inovação institucional.

Depreende-se que os contornos de proteção à privacidade adotados na Lei nº 13.709/2018 decorrem da garantia de princípios e direitos conexos à personalidade, o que leva a um modelo regulatório centrado no Poder Público e nas previsões legais para a proteção dos dados pessoais no Brasil, tal qual ocorre na UE. A figura do Estado como garantidor de proteção dos dados pessoais remonta também um modelo regulatório baseado em critérios territoriais e geográficos, principalmente diante da matéria de transferência internacional de dados. Questiona-se se esse modelo não se tornaria obsoleto diante das novas tecnologias e dos negócios. Contudo, não obstante ser uma regulação voltada para o Estado, o órgão proposto para tratar do tema e resolver conflitos, o Conselho Nacional de Proteção de Dados Pessoais deveria composto de forma

multistakeholder com representantes não apenas do governo, mas da academia, do setor privado, da comunidade técnica e da sociedade civil.

O estímulo à uma cultura de proteção à privacidade, amparada na inovação e na competitividade de modelos de negócios que protejam os dados pessoais é essencial nesse cenário. Corre-se o risco de que o órgão competente criado seja extremamente burocrático e centralizado e que a lógica de compartilhamento de responsabilidades, onde participem ativamente empresas, terceiro setor, cidadãos e governo, todos interessados por um modelo regulatório adequado de tratamento de dados seja obstado, considerando que o modelo a ser construído no Brasil necessita da presença um órgão com expertise para tratar da proteção de dados pessoais, específico e autônomo administrativa e financeiramente.

Anualmente, as APDs existentes reúnem-se na "*Internacional Conference os Data Protection and Privacy Comissers*", o que demonstra a importância do órgão em um contexto mundial e a possibilidade de deliberação e trocas de experiências que o encontro possibilita, a fim de implementar melhores práticas e maximizar a eficiência da atuação das APDs diante das suas competências.

Referências bibliográficas

ARANHA, M. I. Diálogo político-jurídico na comparação de modelos regulatórios de comunicação. **Revista Brasileira de Políticas de Comunicação**, v.1, p. 1-20, 2011.

_____. Telecommunications Law Indicators for Comparative Studies (TLICS) Model: A Hermeneutical Approach. **The Proceedings of the Americas Information and Communications Research Network**. Lima (Perú), 2011b, v.3, p. 283-294.

ARGENTINA. **Leye n. 25.326, de 2000**. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

BIONI, Bruno R. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

CHOUDHRY, Sujit. **The Migration of Constitucional Ideas**. Cambridge University Press, 2006.

FRANÇA. CNIL. **La protection des données dans le monde**, 2019. Disponível: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

TANÚS, Gustavo Daniel. **El artículo 24 de la Ley 25.326 de protección de los datos personales.** Jornadas Argentinas de Informática e Investigación Operativa (JAIIO) organizadas por la Sociedad de Informática Operativa (SADIO). Buenos Aires, 2001.

URUGUAI. **Ley n. 18331, 11 ago. 2008**. Disponible en: https://www.agesic.gub.uy/innovaportal/v/302/ 1/agesic/ley-n°-18331-de-11-de-agosto-de-2008.html. Aceso em: 1 nov. 2018.

Capítulo 2

2.Independência, autonomia e funções das autoridades de proteção de dados

2.1. Desafios, funções e referências internacionais para a Autoridade Nacional de Proteção de Dados – *Henrique Rocha*[32]

Resumo

A Lei nº 13.709/2018, conhecida como LGPD, apresentou inovação legislativa para o melhor tratamento de dados pessoais no Brasil. A fim de garantir força executiva à nova legislação, determinou-se a criação de uma Autoridade Nacional de Proteção de Dados, responsável pela fiscalização, conscientização e aplicação de sanções no caso de descumprimento legislativo. Em um cenário de crise fiscal, desprovida de orçamento próprio e vinculada ao Poder Executivo, os desafios para efetivação do papel da ANPD serão grandes e, neste ensaio, buscar-se-á breves referências internacionais como modelo ao funcionamento da ANPD.

Abstract

Law No. 13.709 / 2018, known as LGPD, introduced legislative innovation for better processing of personal data in Brazil. In order to ensure enforcement of the new legislation, it was determined that a National Data Protection Authority was created to oversee, raise awareness and enforce sanctions in the event of legislative non-compliance. In a scenario of fiscal crisis, devoid of its own budget and linked to

[32] Advogado, especialista em Direito Digital, mestrando em direito pela Universidade Nove de Julho, São Paulo – SP.

the Executive Branch, the challenges to fulfill the role of the ANPD will be great and, in this essay, brief international references will be sought as a model for the functioning of the ANPD.

Introdução

Depois de a Medida Provisória nº 869/2018 ter sido aprovada pelo Senado Federal em 29 de maio de 2019 e sancionada pela Presidência da República, foi publicada em 9 de julho de 2019 a Lei nº 13.853/2019, inserindo o Brasil em seleto grupo que, num futuro breve, contará com uma Autoridade Nacional de Proteção de Dados, ou apenas ANPD como preferem os fãs de acrônimos.

Mas qual a razão de se festejar o nascimento de mais um órgão estatal num país já tão burocrático quanto o Brasil? Quais as finalidades da ANPD? Há efetiva necessidade de mais uma autoridade reguladora no país? Esses são alguns dos desafios que se ousa enfrentar nesse breve ensaio.

Por meio do método comparativo e finalista, tendo como referenciais teóricos Newton de Lucca, Cíntia Rosa Pereira de Lima e Bruno Ricardo Bioni, desafiamo-nos a enfrentar o tema. Porém, antes de refletir sobre a problemática exposta acima, cremos que é importante tecer considerações sobre o cenário existente antes da aprovação da medida e, ainda, o complexo existente antes da promulgação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, a popular LGPD.

Desenvolvimento

A primeira constatação que deve ser trazida à luz caminha no sentido de que embora a nova legislação seja de louvável realização, a tutela dos direitos relativos à proteção de dados pessoais não estava à margem da ordenação[33] jurídico brasileira.

Diz-se isso pois mesmo antes da promulgação da LGPD e da respectiva Autoridade Nacional de Proteção de Dados, o Brasil já contava com leis e entidades que tutelavam a matéria em certa medida.

Neste sentido, a Constituição da República promulgada em 05 de outubro de 1988 já previa em seu art. 5º, X, a inviolabilidade de da intimidade e da vida privada como garantias fundamentais do texto constitucional brasileiro.

[33] Filiamo-nos neste artigo à corrente do professor Newton de Lucca que faz uso do vocábulo ordenação ao invés de ordenamento, referindo-se ao fato histórico de o conjunto primeiro de normas brasileiras decorrerem das Ordenações filipinas, manuelinas e afonsinas.

Também o Código de Defesa do Consumidor, publicado em 11 de setembro de 1990 já previa em seu artigo 43 que o consumidor gozaria, entre outros direitos, o poder acessar cadastros de dados pessoais armazenados por terceiros, requerendo as retificações cabíveis inclusive.

Da mesma forma o Marco Civil da Internet – Lei nº 12.965/2014, festejada legislação levada a publicação em 23 de abril daquele ano, também já prevê como um de seus princípios a proteção da privacidade e dos dados pessoais na forma da lei, conforme art. 3º, II e III do referido diploma.

O próprio Marco Civil da Internet desde a sua publicação já previa, por exemplo, que o tratamento de dados pessoais somente poderia ser realizado após a exposição de finalidades claras e completas sobre o referido tratamento, como descrito no art. 7º, VIII do MCI. Aqui já se prenunciava um novo conceito de privacidade na prática jurídica brasileira (SCHERTEL MENDES, p.128).

Esclarecido, pois, o fato de que, no país, a LGPD não é a primeira e única legislação a versar sobre o tratamento de dados pessoais e a ANPD igualmente não é a única autoridade que será a responsável pela fiscalização dos referidos temas, avança-se aos desafios implícitos ao cenário de regulação de dados pessoais no Brasil, como será visto mais à frente.

Ainda que não seja a primeira legislação a tratar do tema, é fato que inexistia no Brasil, até a publicação da LGPD, um conjunto de regras que vinculasse o tratamento de dados pessoais de forma específica, principiológica e moderna como é o caso da Lei nº 13.709/18. Desde a década de 70 já se alertava para a necessidade de uma lei específica para viabilização de negócios no Brasil (DE LUCCA, SIMÃO FILHO, PEREIRA DE LIMA e MACIEL, p.39).

Nitidamente influenciada pelo *General Data Protection Regulation* Europeu, ou GDPR, a Lei Geral de Proteção de Dados do Brasil é, além de necessária, digna de elogios em relação à sua construção, pois mesmo sendo fortemente influenciada por legislação estrangeira, manteve-se atenta aos anseios e necessidades de um país com economia, história e dinâmica de negócios como o Brasil.

Além de trazer em seu bojo princípios relevantes para o tratamento de dados pessoais, como transparência, segurança, prevenção entre outros, a LGPD apresenta importantes ferramentas para apoio ao uso adequado de dados pessoais, bem como oferece instrumentos visando a conscientização, orientação e, obviamente, penalização no caso de condutas graves envolvendo os incidentes no trato de dados pessoais.

Atualmente com 10 (dez) capítulos, a LGPD conta com 65 (sessenta e cinco) artigos bem distribuídos que permeiam e regem a forma de tratamento dos dados pessoais de milhões de brasileiros.

Diante da relevância e complexidade do tema, não se tem a pretensão de discorrer sobre todo o conjunto legal previsto na LGPD nas estreitas linhas deste artigo, porém, é de bom grado discorrer sobre os

principais aspectos da lei, notadamente quanto às características e funções da Autoridade Nacional de Proteção de Dados Pessoais - ANDP, prevista no art. 55-A da Lei.

Dentre os 7 (sete) fundamentos principais que norteiam a LGPD, em relação ao tema em comento, talvez os que mais façam sentido sejam os dispostos no art. 2º, II e VI, que tratam da autodeterminação informativa e defesa do consumidor, respectivamente. Norteado por esses dois principais fundamentos, a nosso ver, deve ser pautada a atuação da ANPD.

Criada sem aumento de despesa em razão do cenário de crise fiscal em que o Brasil vive, a ANPD enfrentará grandes desafios e precisará contar com criatividade para garantir sua efetiva atuação no cenário que envolve o tratamento de dados pessoais no país. Em que pese a vinculação inicial à presidência da República, a ANDP gozará de autonomia técnica e decisória, conforme disposto no art. 55-B da LGPD.

Liderada por um Conselho Diretor dotado de 5 (cinco) integrantes, dentre eles o Diretor Presidente, a ANPD contará com membros dotados de mandato de 4 (quatro) anos. Todos deverão ser sabatinados pelo Senado Federal e, na primeira composição, contarão com prazos de nomeação distintos, justamente para garantir continuidade regular da atuação da autoridade.

As atribuições da ANPD estão delimitadas no art. 55-J[34] da LGPD, mas destaca-se, ainda, o fato de, em matéria de proteção de dados, as sanções proferidas pela Autoridade Nacional gozarem de prevalência[35] em relação a outras atuações de órgãos administrativos, como o PROCON por exemplo.

[34] Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - 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 do art. 2º desta Lei;

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV - 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;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - 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;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI - 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 desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

Os instrumentos que garantirão a efetivação das decisões tomadas pela ANPD deverão passar por acompanhamento quando a Autoridade estiver em pleno funcionamento, no entanto, a capacidade de emitir recomendações e padrões para serviços e produtos, a viabilidade de editar regulamentos e procedimentos sobre proteção de dados pessoais e, claro, a realização de auditorias e aplicação, cobrança e recolhimento de sanções pecuniárias em face dos infratores de dados pessoais parecem despontar como principais ferramentas de afirmação do órgão.

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei.

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada.

[35] Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Considerando a inegável necessidade de conscientização da população sobre a nova e necessária revisão do fluxo de tratamento de dados pessoais, torna-se inegável a importância da ANPD no âmbito da vida dos brasileiros, que, sem prejuízo do Ministério Público, PROCON e SENACON, passarão a contar com mais um órgão para zelar, especificamente, pelo uso saudável de dados pessoais.

Como última contribuição, é importante que a ANPD brasileira observe os acertos e erros praticados por outras Autoridades no decorrer dos últimos anos. A título de exemplo, apresentam-se a seguir três entidades que se mostram como importantes referências para os modelos de atuação a ser aplicados no Brasil.

É certo que outras tantas autoridades internacionais poderiam ser consultadas para realização de um melhor *benchmark* sobre o tema, contudo, como alertado acima, em razão das estreitas linhas deste trabalho, foca-se o esforço nas autoridades que mais são mencionadas nas pesquisas realizadas para este trabalho, conforme visto a seguir.

A ***Information Commissioner's Office*** ou ICO[36], autoridade independente britânica conta com sítio eletrônico na rede permeado de informações sobre informações educacionais, espaço para abertura de reclamações e até mesmo uma espécie de prestação de conta das ações tomadas, gozando de transparência em sua atuação e servindo de ótimo referencial para a Autoridade Brasileira de Proteção de Dados. A estruturação da ICO é segmentada em 5 (cinco) departamentos, a saber Time Executivo, Diretoria Executiva de Operações, Diretoria Executiva de Estratégia e Planejamento, Diretoria Executiva de Políticas Estratégicas e Diretoria Executiva de Políticas de Tecnologia e Inovação.

A autoridade britânica é custeada primordialmente por meio do recolhimento de taxas de notificações e, ainda, pelo pagamento anual de contribuição pelo Departamento de Cultura, Mídia e Esportes, há o custeio do escritório central da referida autoridade. Tais receitas são calculadas e publicidazadas mensalmente no próprio site da ICO[37]. Estima-se que a ICO conte com cerca de 700 colaboradores, enquanto que a ANPD deverá gozar de, no máximo, 30 agentes no início de suas atividades, o que já representa grande desafio para o país.

Temida após multar a Google em no importe de 50 (cinquenta) milhões de Euros em razão de ter identificado falha em princípios de transparência para coleta do consentimento de seus usuários, a CNIL – ***Commission Nationale de l'informatique et des libertés***, autoridade administrativa autônoma francesa, fundada em 1978, já é reconhecida pela contundência e firmeza de suas posições.

[36] Disponível em: https://ico.org.uk/about-the-ico. Acesso em 25 de setembro de 2019.

[37] Disponível em: https://ico.org.uk/about-the-ico/our-information/income-and-expenditure. Acesso em 02 de outubro de 2019.

A CNIL destaca-se pelo papel orientador da autoridade, que tem como uma de suas missões informar e os cidadãos sobre os direitos decorrentes da legislação de proteção de dados pessoais. Em 2018 o órgão realizou 310 (trezentos e dez) investigações e recebeu quase 200.000 (duzentas mil) chamadas para informação. Contudo, as sanções aplicadas, sob a ótica da quantidade, não são expressivas:

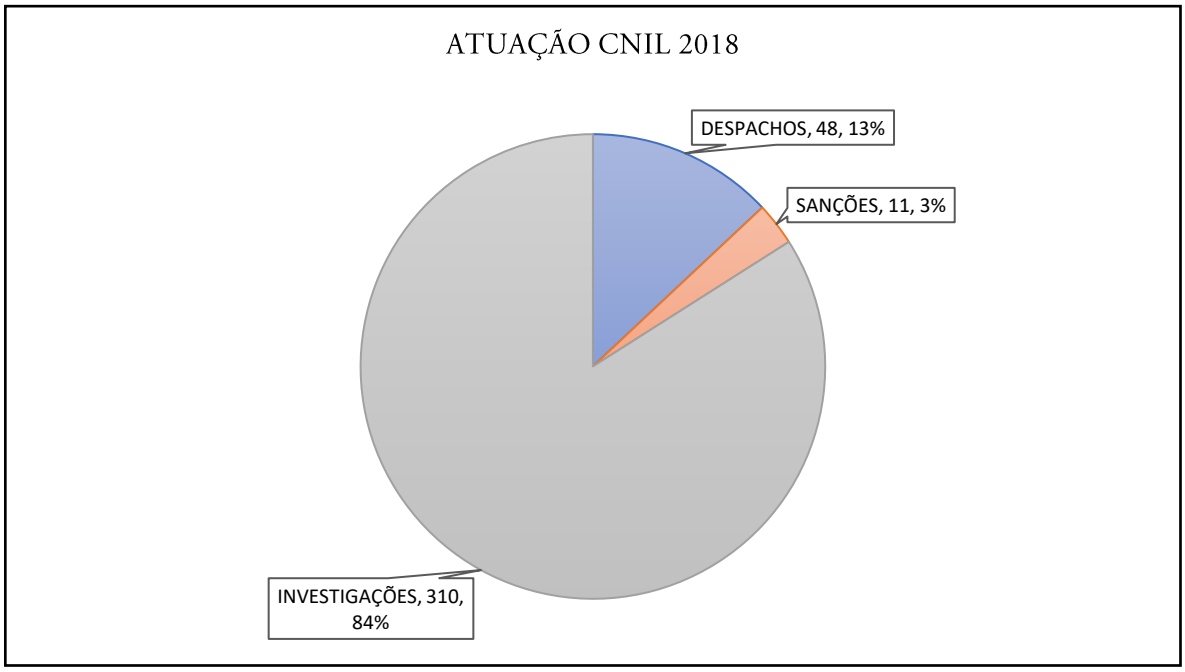


Tabela 1: Síntese de ordens e sanções aplicadas pela CNIL. Disponível em https://www.cnil.fr/en/cnils-facts-and-figures. Acesso em 19/09/2019.

A Autoridade Francesa é composta por 17 (dezessete) membros, com mandatos de 5 (cinco) anos ou, até o término da atividade legislativa para os que assim se enquadrarem, com a seguinte composição: 2 (dois) membros da assembleia legislativa; 2 (dois) Senadores; 2 (dois) Membros do Conselho Econômico, Social e Ambiental; 6 (seis) Membros das cortes superiores e; 5 (cinco) Figuras públicas indicadas pelo presidente do Senado (1), Presidente da Assembleia Nacional (1) e pelo Gabinete Presidencial (3).

Gozando de autonomia administrativa e operacional, os membros reúnem-se semanalmente em agenda pré-estabelecida pelo presidente eleito. Como tarefas principais, além de atender reclamações, orientar e aplicar sanções quando necessário, é a CNIL que autoriza o tratamento de dados sensíveis, como é o caso da biometria.

Já em Portugal, a autoridade recebe o nome de ***Comissão Nacional de Protecção de Dados***[38], órgão administrativo igualmente independente, mas com funcionamento em sintonia com a Assembleia da República daquele país.

[38] Disponível em: https://www.cnpd.pt/bin/cnpd/acnpd.htm. Acesso em: 02 de outubro de 2019.

A CNPD portuguesa é composta por 7 (sete) membros, sendo 1 (um) presidente e 2 (dois) vogais eleitos pela Assembleia Nacional, 2 (dois) membros designados pelo governo central, 1 (um) magistrado com mais de 10 (dez) anos de carreira eleito pelo Conselho Superior da Magistratura e 1 (um) membro do Ministério Público igualmente com mais de 10 (dez) anos de carreira eleito pelo Conselho Superior do Ministério Público.

A autoridade portuguesa também conta com interessante canal para acesso a outras autoridades na Europa e, ainda, com portal para pesquisa de jurisprudência sobre o tema em que atua, permitindo rápidas e pertinentes consultas sobre decisões, orientações e recursos tratados pela referida autoridade. Trata-se de interessante ferramental a ser utilizado pela Autoridade Nacional Brasileira, quando esta passar a vigorar.

A autoridade de proteção dos dados pessoais no Canadá é a OPC ou ***Privacy Commissioner of Canada***[39], fundada em **1983**, e embora seja autoridade independente em relação ao governo executivo, tem dever de reporte diretamente ao Parlamento daquele país.

Com atribuições para investigar reclamações e realizar auditorias, a OPC pauta sua atuação visando o atendimento de duas legislações principais no Canadá, a saber, o ***Privacy Act*** e o ***Personal Information Protection and Eletronic Documents Act*** (PIPEDA)[40].

A OPC também tem como funções publicar relatórios sobre pesquisas e campanhas públicas de conscientização relacionadas aos aspectos da privacidade, boas práticas e ao próprio tratamento de dados pessoais[41], igualmente servindo de referência para a autoridade brasileira vindoura.

Conclusão

Com efeito, observando os desafios que esperam a ANPD, é relevante trazer à baila a importância de se aproveitar as boas práticas já aplicadas pelas Autoridades Nacionais ao redor do mundo para, na medida do possível, garantir que a ANPD seja, efetivamente, um órgão capaz de regular o tema e evite ser, à frente, mais uma agência reguladora ineficaz e frustrante no país.

Disponibilização de canais rápidos de pesquisa de decisões como o oferecido pela autoridade portuguesa, transparência de valores e robustez no número de agentes como a ICO e direcionamento sancionatório

[39] Disponível em https://www.priv.gc.ca/en/about-the-opc. Acesso em: 25 de setembro de 2019.

[40] Disponível em https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda. Acesso em: 25 de setembro de 2019.

[41] Disponível em https://www.priv.gc.ca/en/about-the-opc/what-we-do. Acesso em: 25 de setembro de 2019.

visando grandes ofensores como realizado pela CNIL servem de bons referenciais para a execução das atividades da ANPD no Brasil.

É importante ponderar que a existência de uma agência reguladora sobre o tratamento de dados pessoais, em uma economia digital e globalizada, é essencial, especialmente em um cenário que o titular do dado é hipervulnerável, orientando, educando e trazendo o *enforcement* necessário para não tornar a LGPD letra morta.

Forçoso concordar com a necessidade de fiscalização e pressão da sociedade civil, como já alertado pela doutrina (DE LUCCA, SIMÃO FILHO, PEREIRA DE LIMA e MACIEL, p.468), para que a ANPD goze de eficiência e seja um órgão fiscalizador esperado para atender os desafios exigidos pela lei e pela nova cultura acerca da privacidade.

Parece-nos, portanto, que a autoridade de dados não deverá voltar sua atividade para aplicação de sanções de forma desenfreada, mas sim como escopo a educação e mudança de cultura no tratamento de dados pessoais no país.

Imperioso reconhecer, contudo e ao final, que a ANDP não servirá, nem poderia ser classificada como bala de prata para solver todos os problemas do ambiente de negócios da 4ª Revolução Industrial, mas sim para garantir um amplo acesso ao conhecimento econômico, de forma prudente adequadamente regulada, como já descrito pela boa doutrina sobre o tema (SALOMÃO FILHO, p.54).

Referências bibliográficas

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro. Editora GEN. 2019.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cintia Rosa; MACIEL, Renata Rosa. **Direito & Internet IV:** Sistema de proteção de dados pessoais. São Paulo. Quartier Latin, 2019.

SALOMÃO FILHO, Calixto. **Regulação da atividade econômica** (princípios e fundamentos jurídicos), 2ª edição. Editora Malheiros, 2008.

SCHERTEL MENDES, Laura. **Privacidade, proteção de dados e defesa do consumidor:** Linhas gerais de um direito fundamental. 1ª edição. São Paulo. Saraiva, 2014.

2.2. Reflexos regulatórios da Lei da Liberdade Econômica no contexto da LGPD: uma perspectiva do artigo 5° da Lei n° 13.874/2019 – *Luiz Salles Giannellini*[42], *Renato Barros Cabral*[43], *Ylka Beltrão*[44] *& Renata Mota Maciel*[45]

Resumo

A Lei n. 13.874/19 instituiu a chamada Declaração de Direitos de Liberdade Econômica e estabeleceu garantias de livre mercado. O artigo 5º da referida Lei trouxe a previsão de realização de análise de impacto regulatório, precedente à edição ou alteração de atos normativos de interesse geral de agentes econômicos ou de usuários dos serviços prestados. O problema formulado neste estudo é o de que este procedimento prévio de análise de impacto regulatório traria reflexos à atividade regulatória da Autoridade Nacional de Proteção de Dados – ANPD, prevista na Lei Geral de Proteção de Dados – LGPD (Lei n. 13.709/18). As hipóteses são a de que haveria conflito evidente entre o "interesse geral de agentes econômicos" e o "interesse geral de usuários dos serviços prestados", especificamente em matéria de proteção de dados; a conformação da estrutura da ANPD deveria levar em conta o nível de independência para o exercício de suas atividades e o referido artigo 5º da Lei n. 13.874/19 apresentaria potencial restritivo, sobretudo se pensado a partir do poder econômico das empresas de tecnologia; e a análise da "razoabilidade do impacto econômico" da regulação da proteção de dados deveria levar em conta vetores abrangentes e não apenas o interesse econômico dos agentes do mercado de tecnologia, sob pena de neutralizar a 2 atividade da ANPD a ponto de torná-la inócua e apenas formal, com consequências graves para o desenvolvimento nacional. A investigação está em curso e pretende-se apresentar as suas conclusões no Congresso Internacional "Desafios e perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade".

Palavras-chave: Liberdade econômica; livre mercado; regulação da atividade empresarial; poder econômico; proteção de dados pessoais; Autoridade Nacional de Proteção de Dados; tecnologia.

Abstract

Law n. 13.874/19 instituted the so-called Declaration of Rights of Economic Freedom and established free market guarantees. Article 5 of the aforementioned Law provided for the provision of regulatory

[42] Mestrando em Direito pela Universidade Nove de Julho – UNINOVE.

[43] Mestrando em Direito pela Universidade Nove de Julho – UNINOVE.

[44] Mestranda em Direito pela Universidade Nove de Julho – UNINOVE.

[45] Professora Permanente do Programa de pós-graduação stricto sensu em Direito da Universidade Nove de Julho – UNINOVE.

impact analysis, preceding the edition or amendment of normative acts of general interest of economic agents or users of the services provided. The problem formulated in this research is that this prior regulatory impact analysis procedure would reflect the regulatory activity of the National Data Protection Authority (ANPD), provided for in the Brazilian General Data Protection Act (LGPD) – Law n. 13.709/18). The hypothesis is that there would be a clear conflict between the "general interest of economic agents" and the "general interest of users of the services provided", specifically regarding data protection; the structure of the ANPD should take into account the level of independence for the exercise of its activities and the referred article 5 of Law n. 13.874/19 would present restrictive potential, especially if thought from the economic power of technology companies; and the analysis of the "reasonableness of the economic impact" of data protection regulation should take into account comprehensive vectors and not just the economic interest of technology market players, otherwise it would neutralize the ANPD's activity to the point of rendering it innocuous and only formal, with serious consequences for national development. The investigation is ongoing, and it is intended to present its findings at the International Congress "Challenges and Perspectives of Data Protection Authorities".

Keywords: Economic freedom. Free market. Regulation of business activity. Economic power. Personal data protection. National Data Protection Authority. Technology.

Introdução

A Lei n. 13.874/19, ao instituir a Declaração de Direitos de Liberdade Econômica e estabelecer garantias de livre mercado, previu em seu artigo 5º a realização de análise de impacto regulatório, precedente à edição ou alteração de atos normativos de interesse geral de agentes econômicos ou de usuários dos serviços prestados, editadas por órgão ou entidade da administração pública federal, incluídas as autarquias e as fundações públicas.

O problema formulado neste estudo é o de que este procedimento prévio de análise de impacto regulatório trará reflexos à atividade regulatória da Autoridade Nacional de Proteção de Dados – ANPD, prevista na Lei Geral de Proteção de Dados – LGPD (Lei n. 13.709/18).

A partir dele, foram formuladas as seguintes hipóteses: a) haveria conflito evidente entre o "interesse geral de agentes econômicos" e o "interesse geral de usuários dos serviços prestados", especificamente em matéria de proteção de dados; b) a análise da "razoabilidade do impacto econômico" da regulação da proteção de dados deve levar em conta vetores abrangentes e não apenas o interesse econômico dos agentes do mercado de tecnologia, sob pena de neutralizar a atividade da ANPD a ponto de torná-la inócua e apenas formal, com consequências graves para o desenvolvimento nacional.

O método utilizado será o hipotético-dedutivo indutivo; a partir das normas que regulam a chamada Declaração de Direitos de Liberdade Econômica e a Lei Geral de Proteção de Dados, mediante

hipóteses, busca-se investigar as consequências para a regulação da atividade empresarial voltada à coleta, uso e tratamento de dados, advindas da aplicação desse novo marco legal em cotejo com a LGPD.

A proteção de dados pessoais é, sem nenhuma dúvida, um dos pilares mais importantes do Estado Democrático de Direito, cujo principal fundamento é a dignidade da pessoa humana. 4 Por outro lado, a ordem econômica constitucional apresenta fundamentos e princípios que impõem à atividade empresarial, para além do lucro, a busca pelo desenvolvimento integral, o que inclui aspectos econômicos, sociais e ambientais.

Portanto, ainda que a Lei n. 13.874/19 institua a chamada Declaração de Direitos de Liberdade Econômica e as garantias de livre mercado, é preciso refletir acerca dos seus limites constitucionais e, sobretudo, a extensão de normas como o artigo 5º, que prevê procedimento prévio de análise de impacto regulatório.

A propósito, indaga-se até mesmo se teria referida Lei apresentado um novo paradigma regulatório para o Brasil, dado que eventual flexibilização da ordenação em matéria de regulação, para além de aspectos políticos e de direcionamento econômico, com vistas à formular indicadores para o mercado interno e externo, têm potencial para a geração de consequências ainda mais complexas, como em matéria de proteção de dados, recorte proposto no presente estudo.

Nesse contexto é que se apresentará o papel da Autoridade Nacional de Proteção de Dados – ANPD e os reflexos do procedimento prévio de análise de impacto regulatório previsto no artigo 5º da Lei n. 13.874/19 em sua atividade regulatória.

Embora a pesquisa esteja em curso, a revisão de bibliografia inicial, a partir do problema e das hipóteses formuladas permitiu, como primeira conclusão, afirmar que o procedimento de análise prévia de impacto regulatório deveria estabelecer critérios puramente técnicos, a fim de garantir a regulação da atividade econômica, nos moldes constitucionais e da própria regulamentação prevista na LGPD, a partir da instituição da Autoridade Nacional de Proteção de Dados.

1. A Declaração de Direitos de Liberdade Econômica e as garantias de livre mercado previstas na Lei n. 13.874/19: novo paradigma regulatório?

A resposta do questionamento acima, numa primeira análise, não nos parece permitir considerar que a Declaração de Direitos de Liberdade Econômica possa se caracterizar como sendo um novo paradigma regulatório, mas sim um importante avanço na desburocratização das atividades regulatórias.

Primeiramente, é necessário observar que o próprio estudo prévio de impacto regulatório, nem mesmo do ponto de vista normativo, se trata de uma novidade. Veja-se, a 5 título de exemplo, que o próprio inciso IV, § 1º do artigo 225 da Constituição Federal/88 já previa que para instalação de obra ou

atividade potencialmente causadora de significativa degradação do meio ambiente, estudo prévio de impacto ambiental, a que se dará publicidade.

Isso significa que, há muito tempo, os agentes econômicos e o Estado têm se valido de estudo prévio de impacto, a fim de conciliar, ao mesmo tempo, o fomento da atividade econômica – proporcionado por obras ou atividades que, em geral, podem causar danos ao meio ambiente ao mesmo tempo em que podem gerar empregos – e a proteção de interesses que se relacionem, por exemplo, (i) à função social da propriedade, (ii) à defesa do consumidor e do meio ambiente e (iii) à redução das desigualdades sociais.

Em segundo lugar, convém salientar, que a Administração Pública, em alguns casos, já tem se valido de estudo prévio de impacto regulatório, como ocorre, por exemplo, através da disciplina normativa produzida pelas agências reguladoras, (v.g., ANEEL, ANATEL, ANS, ANVISA, ANTT, entre outras,) e por meio da qual, tanto os agentes públicos, no cumprimento do desiderato fiscalizatório, quanto os agentes econômicos privados, para planejamento estratégico de exploração da atividade empresarial, podem se basear como referência para cumprimento legislativo. Mesmo que sua aplicação não seja homogênea e sistemática.

Inobstante, prima facie, não se possa atribuir à Declaração de Direitos de Liberdade Econômica um status de Novo Paradigma Regulatório, é necessário ressaltar a sua importância. Pois, com efeito, altera uma realidade premente da exploração da atividade empresarial: o receio de investimentos por parte dos agentes econômicos na exploração de novos negócios em razão da ineficiência e dos entraves burocráticos criados pela Administração.

2. A Autoridade Nacional de Proteção de Dados – ANPD na LGPD: conformação de sua atuação a partir dos fundamentos e princípios constitucionais da ordem econômica brasileira

Embora a proteção à privacidade sempre tenha recebido tratamento jurídico no Brasil, fato é que sua importância foi exponencialmente aumentada em razão de 02 (dois) fatores principais: (i) *o da globalização*, processo de integração entres as várias partes do mundo, especialmente nos campos político, econômico, social e cultural, com vistas a formar 6 um espaço internacional comum, dentro do qual bens, serviços e pessoas circulem da maneira mais desimpedida possível, conforme assinala Paulo Portela[46] e (ii) do *incremento do avanço tecnológico*, em especial da internet e suas aplicações, e dos ferramentais de veiculação de informações (smartphones, tablets e outros dispositivos).

Nesse contexto, é certo que a LGPD tem como escopo garantir a *"autodeterminação informativa"* e, ao mesmo, tempo escalar o desenvolvimento da atividade econômica e da tecnologia em um ambiente de

[46] PORTELA, Paulo Henrique Gonçalves. Direito Internacional Público e Privado, 8ª edição, p. 35.

regulação, assegurando os interesses de todas as pessoas envolvidas na chamada *"data driven economy"* (economia baseada em dados/informações)[47].

Considerando-se que a informação (entendida esta, como dados pessoais objeto de proteção da LGPD) é o principal ativo imaterial para a celebração de negócios e, consequentemente, para o desenvolvimento de novos modelos de atividades empresariais, bem como a proteção constitucional desses dados, forçosamente se vislumbra que atuação da Autoridade Nacional de Proteção de Dados – ANPD, prevista na LGPD, deverá assumir um viés jurídico-empresarial.

Essa atuação, como se acredita que não poderá deixar de ser, será informada tanto pelo aspecto econômico – e, nesse aspecto, é inegável que a atuação da ANPD deverá ater-se aos preceitos trazidos pela Declaração de Direitos de Liberdade Econômica e dos objetivos por ela delineados – quanto pelo aspecto técnico jurídico, justamente, com o fim de atender às competências preconizadas no artigo 55-J, com a redação dada pela Lei n.º 13.853, de 08 de julho de 2019.

Releva dizer que, qualquer que seja o prisma enfocado, a atuação da Autoridade Nacional de Proteção de Dados – ANPD jamais deverá deixar de se orientar pelos princípios específicos previstos no artigo 174 da Constituição Federal, tanto quanto pelos fundamentos preconizados no seu artigo 1º, em especial pelos incisos III e IV que contemplam, respectivamente, a dignidade da pessoa humana e os valores sociais do trabalho e da livre iniciativa.

A partir de uma comparação entre a atuação da Autoridade Nacional de Proteção de Dados (ANPD) com a enumeração das hipóteses legais caracterizadoras do abuso de poder regulatório, tem-se que a Declaração de Direitos de Liberdade Econômica, além de desestimular a produção de regulação desnecessária, terá o condão de balizar o Poder Judiciário para estabelecer e criar freios ao regulador, caso não fiquem demonstrados, por exemplo, a necessidade técnica e os efeitos positivos esperados com a edição de determinada norma regulatória.

Um dos objetivos deste artigo é estabelecer um diálogo entre a Lei Geral de Proteção de Dados (Lei nº 13.709/18) e a Lei da Liberdade Econômica (Lei nº 13.874/19) de modo a garantir que a regulação da privacidade e da proteção dos dados pessoais no ambiente virtual não se transforme em instrumento de limitação da atividade empresarial. Para tanto, uma interpretação sistemática à luz do diálogo das fontes permitirá extrair o direito básico dos titulares à proteção de dados pessoais veiculados na internet.

[47] BIONI, Ricardo Bruno. Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, regulação dos bancos de dados eletrônicos e arquitetura da internet. 2016. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2016.

Não se está a tratar apenas e tão somente de um conflito entre legislações, a ser resolvido pelas regras de conflitos de leis no tempo, mas da aplicação simultânea de ambas as leis.

Por isso, a utilização da expressão "diálogo das fontes", que constitui um modelo de aplicação simultânea de fontes normativas diversas, adequando-as aos atuais fenômenos jurídicos complexos, não mais passíveis de serem resolvidos à luz dos conceitos de abrogação, derrogação e revogação.

Conforme explicado por Claudia Lima Marques, o diálogo das fontes é *"a atual aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o Código de Defesa do Consumidor, a lei de seguro-saúde) e gerais (como o CC/2002), com campos de aplicação convergentes, mas não mais iguais"*[48].

Bem por isso, a relação entre a LGPD e demais normas deve pautar-se pela busca de um sistema harmônico de proteção de dados. Nesse sentido, a LGPD é apenas um "pontapé inicial" na busca por uma regulamentação do assunto. É certo que 132 países já adotaram algum tipo de lei de proteção de dados, e muitos têm elementos harmônicos entre si e, vale lembrar, a lei brasileira surgiu com as tendo como norte as experiências internacionais.

Nesse panorama há que destacar, ainda, a importância da Autoridade Nacional de Proteção de Dados (ANPD) como organismo responsável para efetivar a lei que, em função da pluralidade de implicações legais entre vários ramos do direito, não pode estar conectada a apenas um órgão governamental. A implementação da lei, conforme anteriormente afirmado, é uma questão complexa devido ao conflito de normas.

E, o Legislador andou bem ao estabelecer um regime jurídico de proteção de dados pessoais que pressupõe a aplicação de outros diplomas legais, dentre os quais em lista exemplificativa, o Marco Civil da Internet, o Código de Defesa do Consumidor, o Código Civil e a própria Constituição Federal.

Tendo em vista que a internet constitui um ambiente de exercício de diversos direitos fundamentais – como, por exemplo, o direito à liberdade de expressão, associação, informação, comunicação e profissão – a proteção da privacidade e dos dados pessoais apresenta-se como um pressuposto para o exercício desses direitos e, é nesse sentido, que a ANPD deverá atuar, qual seja, para garantir ao titular dos dados a sua autogestão informacional.

O "diálogo das fontes" deve servir justamente para garantir a coesão da Lei Geral de Proteção de Dados com a Declaração de Direito da Liberdade Econômica e, ao mesmo, para garantir que em função da necessidade de regulação, pela Autoridade Nacional de Proteção de Dados, a atividade empresarial não seja ceifada e/ou impedida por inconsistências e/ou falhas interpretativas.

[48] MARQUES, Cláudia Lima (coord.). Diálogo das Fontes: do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012.

Afinal, se o titular acreditar que seus dados e informações poderão ser utilizados para fins alheios às suas expectativas ou de forma a prejudicá-lo no futuro, ele certamente não agirá livremente no ambiente virtual e, inclusive, não compartilhará as suas ideias com liberdade.

Nessa ordem de ideias e, para concluir, a harmonização da Lei Geral de Proteção de Dados e da Declaração de Direito da Liberdade Econômica está ligada à constituição de uma autoridade que possa de maneira eficiente garantir autonomia e assegurar o diálogo com os outros ramos do direito, sem impedir e sem criar obstáculos à atividade empresarial baseada nos modelos de negócios que envolvam tecnologia, ambiente virtual e dados pessoais.

3. Reflexos do procedimento prévio de Análise de Impacto Regulatório previsto no artigo 5º da Lei n. 13.874/19 na atividade regulatória da Autoridade Nacional de Proteção de Dados – ANPD

A análise de impacto regulatório – AIR, sem qualquer dúvida, é uma prática regulatória reconhecida internacionalmente e que, em larga escala, somente apresenta benefícios.

Além de destinar-se a garantir uma melhora da própria atividade normativa regulatória, uma vez que pautada pela transparência, robustez técnica e analítica ao processo decisório, conferindo segurança ao ambiente de investimentos, trata-se de importante instrumento de participação dos próprios agentes econômicos no processo de regulação, circunstância que lhe garante alto grau de legitimidade.

Com maior participação social e dos próprios agentes econômicos no processo de regulação, acredita-se que o grau de discricionariedade da Administração será cada vez menor, garantindo-se com isso, uma atuação regulatória estatal técnica e equidistante de influências políticas, tudo com o objetivo de garantir previsibilidade, planejamento, efetividade e, sobretudo, segurança jurídica. Como corolário, tende-se a evitar, a um só tempo, (i) possíveis gargalos de corrupção e (ii) o risco de ativismo judicial, que ainda poderia ser agravado pelo desconhecimento técnico decorrente da velocidade da transformação dos novos modelos de negócios que envolvem tecnologia.

Outro importante benefício do estudo prévio também é o de servir como norte para o julgamento de casos judiciais, evitando, repita-se, o ativismo judicial com decisões desencontradas, uma vez que haverá um aprofundamento detalhado nos motivos que ensejaram a criação normativa e os impactos que ela trará na atividade empresarial, ajudando de forma significativa na elaboração de decisões judiciais coesas, inclusive, servindo de instrumento para a eventual aplicação das multas a serem impostas pela ANPD, de forma a não inviabilizar a atividade empresarial, mas, ao mesmo tempo para impedir que a mesma seja leviana.

Nessa toada, a exigência de análise de impacto regulatório pode ser considerada como uma garantia à livre iniciativa e, no mínimo, reforça o mandamento de razoabilidade de eventuais restrições à atividade

econômica. Nesse sentido, a liberdade para o exercício das atividades econômicas é o norte da Lei nº 13.874/19 e a restrição é a exceção que, bem por isso, deve ser comprovadamente mínima e aplicada quando necessária. A título de uma primeira conclusão acerca da AIR sem a cabal demonstração da necessidade, a imposição de alguma restrição regulatória deverá ser considerada como uma inconstitucional limitação da liberdade econômica.

Conclusão

A redação do artigo 5º da Lei nº 13.874/19, nos limites do que foi aprovado pelo Congresso Nacional, contém relevante diretriz que determinará a redução da ampla discricionariedade da administração pública em implantar normas regulatórias. Por outro lado, 10 não se pode desconsiderar a necessidade da regulação da atividade econômica e, por consequência, empresarial.

Assim, a atuação regulatória estatal precisa manter-se técnica e equidistante de influência políticas, a fim de garantir previsibilidade, planejamento, efetividade e, sobretudo, segurança jurídica, evitando o perigo de da discricionariedade excessiva da administração pública e o risco do próprio ativismo judicial, em caso de judicialização das questões, agravado pelo desconhecimento técnico decorrente da velocidade da transformação dos novos modelos de negócios que envolvem tecnologia.

No contexto de evitar soluções distantes de aspectos técnicos e dos próprios objetivos da regulação, faz-se necessário identificar critérios a enformar o procedimento prévio de análise de impacto regulatório, que possibilitará a edição e alteração de atos normativos regulatórios tendentes a disciplinar interesses econômicos, como no caso da atividade econômica voltada à coleta, uso e tratamento de dados, sem descurar do regime recém estabelecido para a proteção dos dados pessoais, por meio da Lei n. 13.709/18 – LGPD e, em especial, à atividade da Autoridade Nacional de Proteção de Dados – ANPD.

A chamada Lei da Liberdade Econômica apresenta diversos dispositivos principiológicos, de modo que ainda se pode considerá-la um indicativo do caminho a ser trilhado. Caberá à administração e ao regulador estabelecer o efetivo direcionamento a ser implementado a partir de sua edição. Ainda que por um lado seja indiscutível que não se pode postergar ou desperdiçar a oportunidade de aprimorar regras ultrapassadas, com o objetivo de desburocratizar os tantos entraves à atividade econômica, também é evidente que burocratização não se confunde com regulação.

Por isso, superado o discurso inicial, voltado à redução da excessiva e desnecessária burocracia envolvida desde a constituição das sociedades empresárias e do seu registro, passando pelas exigências em âmbito municipal, estadual e federal para a efetiva implementação da atividade empresarial, mostra-se premente a necessidade de análise cuidadosa dos reflexos da Lei nº 13.874/19 no plano regulatório da atividade

econômica e, para o enfoque desta pesquisa, na atividade empresarial relacionada à coleta, ao uso e ao tratamento de dados pessoais.

Referências bibliográficas

ARAÚJO, Nicete Lacerda; GUERRA, Bráulio Madureira; et al. **Marco Legal da Inovação:** breves comentários. Rio de Janeiro: Lumen Juris, 2018.

BIONI, Ricardo Bruno. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, regulação dos bancos de dados eletrônicos e arquitetura da internet. 2016. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2016.

_____. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

DE LUCCA, Newton; DEZEM, Renata Mota Maciel Madeira. A proteção de dados pessoais no Brasil a partir da Lei nº 13.709/2018. *In:* JORGE LEMOS, André Guilherme et al. (Coord.). **Direito Empresarial:** estruturas e regulação. Volume 2. São Paulo: UNINOVE. 2018, p 255-276.

LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção de dados pessoais no cenário futuro do Brasil.** Tese de Livre-Docência apresentada à Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. Ribeirão Preto: Universidade de São Paulo, 2015.

MARQUES, Cláudia Lima (coord.). **Diálogo das Fontes:** do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012.

PINTO, Renata Ávila. Digital Sovereignty Or Digital Colonialism. **Sur – International Journal on Human Rights**, v. 15, n.27, 2018, p. 15-27. Disponível em HeinOnline. Acesso em 10.7.2019.

PORTELA, Paulo Henrique Gonçalves. **Direito Internacional Público e Privado**, 8ª edição, p. 35.

SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016.

2.3. A ANPD e a regulação da Lei 13.709/18 para a proteção de dados pessoais: da gestão de riscos à necessidade de reforçar a privacidade digital – *João Paulo Zanin Júnior*[49]

[49] Graduado em Direito pela Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo (FDRP/USP).

Resumo

A questão da proteção de dados pessoais e da privacidade vem ganhando destaque nas duas últimas décadas, em face de escândalos de vazamento de dados. Diversos países já possuem leis consolidadas sobre esse tema, sendo que no Brasil tal legislação ainda é recente e está em fase de implementação. A Lei Geral de Proteção de Dados (lei 13.709/18) tem o direito fundamental à privacidade como base e se preocupa com a gestão de riscos no meio digital. E para concretizar a proteção à privacidade, a Lei 13.853/19 criou a Autoridade Nacional de Proteção de Dados (ANPD), a fim de promover o enforcement do modelo regulatório que tutela dados pessoais; este órgão ainda tem competências para deliberar, elaborar normas, fiscalizar e sancionar, e possui autonomia técnica e decisória. Prevista para funcionar a partir de 2020, os membros da ANPD têm a perspectiva enfrentar desafios como regular o mercado de dados pessoais, para proteger a privacidade de consumidores; enfrentar uma possível judicialização excessiva de medidas regulatórias e administrativas, que podem "imobilizar" a agência; o distanciamento da sociedade civil quanto às deliberações e medidas técnicas da ANPD; e a vigilância e espionagem estrangeira e invasões de *hackers* aos dispositivos eletrônicos de autoridades políticas e cidadãos comuns. Ao final, conclui-se que a proteção aos dados pessoais e a privacidade apenas pode ser efetivada se houver, na ANPD, um funcionamento sério e técnico, e precisa estar longe de ingerências políticas e econômicas.

Palavras-chave: Proteção de Dados Pessoais, Privacidade, Lei Geral de Proteção de Dados, Autoridade Nacional de Proteção de Dados, Gestão de Riscos, Regulação.

Abstract

The issue about data protection and privacy has been coming to prominence on the two last decades, due to scandals of data breach. Several countries already have consolidated laws about this issue, but in Brazil this special law is recent and it is in the implementation phase. The General Law of Data Protection (Law nº 13.709/18) has the fundamental right to privacy as the basis and it is worried about the risk management on the digital space. And in order to materialize the protection of privacy, the Law nº 13.853/19 created National Data Protection Authority (ANPD), to make enforcement of regulatory model that safeguard personal data; this agency also has competence to deliberate, create rules, make inspection and to sanction, and moreover, this agency has technical and decision-making autonomy. Provided to work starting 2020, the ANPD members have the perspective to face challenges as regulate the personal data market, in order to protect consumers' privacy; face a potential judicialization of its administrative and regulatory measures, that may "immobilize" the agency, the apartness of civil society from deliberations and technical measures of ANPD; and the stranger surveillance and espionage and hacker invasions to electronic gadgets belonging to political authorities or common citizens. In the end, the conclusion is that Data Protection and Privacy Protection can only be effective if there is, in ANPD, a serious and technical work, and it needs to be far from political and economical interferences.

Keywords: Personal Data Protection, Privacy, General Law of Data Protection, National Authority of Data Protection, Risk Management, Regulation.

Introdução

A informática, há mais de duas décadas, se tornou uma área de suma importância para qualquer país que se pretenda inserir no cenário internacional, principalmente em um contexto de interconexão entre as redes computadorizadas de informações e dados de toda espécie, com destaque para os dados pessoais. Existe hoje uma facilidade para acessar dados pessoais, disponibilizados em perfis de redes sociais e sites de empresas ou órgãos públicos. Dado o fluxo informacional gigantesco, ainda mais quando a privacidade é, por vezes, difícil de ser protegida, torna-se fundamental uma regulação nesse fluxo e no armazenamento de dados pessoais. Ainda mais para evitar vazamento de informações, que, mesmo estando, em tese, protegidas, podem sofrer "invasões" por hackers ou serviços de espionagem. Estas informações requerem uma maior proteção, uma vez que há o risco de serem utilizadas para fins ilícitos, como fraudes e estelionatos. E, mesmo que usada para fins lícitos, como o cruzamento de dados por empresas visando a traçar um perfil dos consumidores ou a elaboração de pesquisas e análises estatísticas, outros direitos como a privacidade podem estar sendo violados, uma vez que esta área não possui regulamentação suficiente. O presente artigo visa a analisar a LGPD conjuntamente com a ANPD, destacando seus principais aspectos e mecanismos de funcionamento para a tutela da privacidade. Em seguida, serão apontados possíveis problemas que as autoridades deste órgão enfrentarão em suas atribuições, de modo que a conclusão a que se chega é a da necessidade de um trabalho sério e altamente técnico e sem interferências de agentes políticos e econômicos. A metodologia utilizada será a pesquisa bibliográfica, por meio da busca de textos acadêmicos ou de valor científico relevante em revistas, bibliotecas, textos oficiais e legislação. Levanta-se a hipótese de o modelo regulatório de gestão de riscos em meio digital ser mais eficiente à medida que as autoridades de proteção de dados têm garantida autonomia técnica e decisória. Será usado o método indutivo, uma vez que a partir da análise de circunstâncias específicas e de leis separadamente, será extraída uma conclusão geral.

1. A sistemática jurídica da proteção de dados pessoais e da privacidade

1.1. Da Lei 13.709/18 – a Lei Geral de Proteção de Dados

Em agosto de 2018, foi sancionada a Lei 13.709/18, que teve posteriormente sua redação alterada para Lei Geral de Proteção de Dados (LGPD), que promoveu alterações no Marco Civil da Internet.

A LGPD acompanha a tendência de diversos países pelo mundo, que é a de elaborar legislação com a finalidade de proteger dados pessoais e a privacidade dos usuários de meios digitais. Vale ressaltar que mais de 120 países já têm lei específica visando a proteger dados pessoais (com destaque para a General Data Protection Regulation - GDPR - da União Europeia), de modo que na maioria destes há uma

autoridade nacional independente encarregada do assunto, enquanto em cerca de 20% destes países, não há independência administrativa para esta autoridade ou não há ente governamental especializado (CAMARGO C., 2019, p. 6).

Como objetivos da LGPD, um dos principais é a garantia da privacidade que os dados pessoais devem ter. Assim, a LGPD estabelece normas para que tais informações sejam coletadas e processadas, bem como normas para seu compartilhamento. A Lei 13.709/18 é aplicada de forma extraterritorial, conforme o art. 3º, sendo que inclusive empresas estrangeiras que tiverem negócios no Brasil devem se adaptar à LGPD.

No tocante à proteção de dados pessoais, a LGPD se baseia na gestão de riscos em meio digital, conforme é notável em seu art. 5º, XVII, que considera:

> 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**. (grifos próprios)

Desta forma, as empresas devem adotar medidas que diminuam o risco de dados pessoais serem expostos, podendo ser medidas de segurança, técnica ou administrativa que não deixe os ativos de informação se perderem, se indisponibilizarem ou minimizem esse risco (CAMARGO, G., 2018).

No âmbito da fiscalização, para que seja promovido um enforcement na segurança dos dados pessoais, a Lei Geral de Proteção de Dados traz, em seu art. 52, sanções administrativas contra os agentes de tratamento de dados que descumprirem suas normativas.

Dentre as punições previstas, estão: advertência, indicando prazo para que medidas corretivas sejam adotadas (inc. I); multa de até 2% do faturamento da empresa, grupo ou conglomerado no país em seu último exercício, com o limite de cinquenta milhões por infração (inc. II); multa diária (inc. III); publicização da infração após devidamente apurada e confirmada sua ocorrência (inc. IV); bloqueio dos dados pessoais a que se refere a infração até sua regularização (inc. V) e eliminação dos dados pessoais a que se refere a infração (VI).

1.2. Da Lei 13.853/19 – Autoridade Nacional de Proteção de Dados

No primeiro semestre de 2019, foi sancionada uma nova lei, versando sobre dados pessoais e a privacidade em meio digital. Inicialmente, estava prevista a criação da ANPD já na Lei 13.709/18, contudo, houve o veto do dispositivo legal que a criava. Assim, houve a edição da Medida Provisória de nº 869/18, que instituía a ANPD, sendo que posteriormente, esta MP foi convertida na Lei 13.853/19.

Deve-se mencionar, ainda, que a proteção de dados pessoais é decorrente da tutela constitucional à privacidade, adjunto à intimidade, previstos no art. 5º, inc. X da Carta Magna e no art. 2º, inc. I da LGPD; assim sendo, a autoridade nacional de proteção de dados materializa a tutela específica do direito à privacidade (MACHADO, 2015, p. 50).

Deve-se ter em conta que a proteção dos dados pessoais não se trata apenas de restringir o acesso a estes dados pelas instituições, mas também tal proteção se refere a assegurar que este fluxo de informações ocorra de modo apropriado, respeitando a integridade contextual (NISSEMBAUM, 2010, p. 2).

Uma vez que segundo o art. 55-J, inc. I da Lei 13.853/19, é competência da ANPD zelar pela proteção dos dados pessoais, cabe ressaltar que estão abrangidos nesta categoria os dados sensíveis, cuja exposição pode acarretar severos danos na vida pessoal e/ou profissional. Além disso, pode haver prejuízos no tocante ao direito da personalidade, uma vez que o manuseio indevido de dados sensíveis pode aumentar as chances de o indivíduo ser discriminado (DONEDA, 2006, p.163).

A ANPD possui competências de cunho deliberativo, normativo, fiscalizador e sancionador, sendo ainda, conforme o art. 55-B da Lei 13.709/18, dotada de autonomia técnica e decisória. Desta forma, a ANPD é um dos mecanismos institucionais para proteger dados pessoais (RIBEIRO, 2019 p. 11). Assim, a ideia por trás da criação da ANPD é a do modelo teórico da regulação de risco, segundo a qual os riscos constituem o elemento central de normas jurídicas com o intuito de salvaguardar liberdades e direitos de cunho coletivo. Assim, para minimizar os riscos da exposição de dados pessoais e atingir efetividade, a LGPD coloca em uma agência reguladora (ANPD) o *enforcement* de seu modelo regulatório (ZANATTA, 2017, pp.181-88).

2. Os membros da ANPD e os encargos pela frente

Diversos e trabalhosos serão os desafios e as perspectivas dos membros da ANPD e seus maiores órgãos, o Conselho Diretor (art. 55-C, I LGPD) e Conselho Nacional de proteção de dados pessoais e da privacidade (art. 55-C, II LGPD). Ainda mais ao considerar o contexto brasileiro, no qual há alta vulnerabilidade do Brasil em termos de segurança digital.

Um dos desafios será impor limites ao mercado de dados pessoais, que pode ser entendido como "as interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente. O mercado de dados pessoais se baseia nas necessidades de informação das empresas, instituições públicas e usuários finais" (SILVEIRA et al., p. 219).

O mercado de dados pessoais, que inclui a venda de dados pessoais para a confecção de anúncios e serviços direcionados, já representa a maior fonte de receitas para várias grandes corporações da

economia informacional (SILVEIRA et al., p. 228), o que pode levar a discriminações de usuários por circunstâncias particulares.

A eficiência do modelo brasileiro de regulação de risco, contudo, pode ser prejudicada se houver uma volumosa judicialização de medidas regulatórias e administrativas, de modo que fosse usada a estratégia de refreamento do processo de regulação por parte de determinados interesses econômicos (ZANATTA, 2017, p.190). Ainda segundo o mesmo autor, há o risco de ocorrer um distanciamento da população em relação aos temas regulatórios da proteção de dados pessoais e da privacidade, uma vez que há muito conteúdo técnico atinente ao campo de informática e tecnologia da informação, de modo que os conflitos e negociações coletivas desta área só fiquem restritos às autoridades 9 reguladoras, empresas do setor de tecnologia e entidades civis especializadas (ZANATTA 2017, p. 190).

Transpondo a questão da proteção de dados pessoais ao contexto internacional, é preciso enfatizar o fenômeno da vigilância global e da espionagem. Na última década, houve notórios vazamentos de informações sobre agências de segurança, dentre eles o *Wikileaks* e o Caso *Snowden*. Antes mesmo de ser criado um órgão encarregado de proteger dados pessoais, o Brasil sofreu desde espionagem até invasão de hackers, cujos alvos mais notáveis foram desde Presidente da República até Ministros de Estado.

Assim, um dos desafios da ANPD será construir mecanismos para evitar esse tipo de ingerência, de modo a proteger desde as autoridades políticas mais altas até os cidadãos comuns da vigilância exógena ao país. A tarefa se mostra um tanto quanto trabalhosa ao se levar em conta que os Estados que mais promovem essa vigilância têm recursos tecnológicos mais sofisticados que o Brasil, além de maiores condições econômicas e financeiras.

Conclusão

A Lei 13.709/18 a Lei 13.853/19 podem ser interpretadas sistematicamente, formando um microssistema legal de segurança digital. A LGPD, desta maneira, acompanha as inovações legislativas de outros ordenamentos jurídicos, tais como o GPDR da União Europeia, tem como fundamento o direito à privacidade, baseando-se na gestão de riscos no meio digital. A ANPD ainda tem competências para deliberar, elaborar normas, fiscalizar e sancionar, sendo dotada de autonomia técnica e decisória. Desta forma, a ANPD constitui um dos mecanismos institucionais previstos na Lei 13.709/18 para proteger dados pessoais.

Ao entrar em funcionamento a partir de 2020, a ANPD já tem a perspectiva de enfrentar desafios como promover a regulação do mercado de dados pessoais, afim de proteger a privacidade de consumidores, a judicialização excessiva de medidas regulatórias e administrativas que podem emperrar seu

funcionamento, o alheamento da população civil quanto às deliberações e medidas da ANPD, e a vigilância e espionagem estrangeira e invasões de hackers aos dispositivos eletrônicos de autoridades políticas e cidadãos comuns, sendo estes mais vulneráveis do que aqueles.

A proteção aos dados pessoais e a privacidade apenas pode ser efetivada se houver, na ANPD, um funcionamento sério e técnico, independente o tanto quanto possível de 10 ingerências partidárias e também de interesses econômicos de grupos interessados na mínima regulamentação do fluxo, armazenamento e compartilhamento de dados pessoais.

As ingerências a que a ANPD fica suscetível, assim, podem tornar ineficaz a proteção de dados pessoais, uma vez que interesses diversos da privacidade em meio digital podem prevalecer dentro deste órgão. O modelo regulatório de gestão de riscos digitais, desta forma, tende a ser mais eficiente à medida que as autoridades de proteção de dados têm garantida autonomia técnica e decisória.

Referências bibliográficas

CAMARGO, Coriolano. **Criação da Autoridade Nacional de Proteção de Dados.** FIESP e CIESP, 2019.

CAMARGO, Gabriel. LGPD: **10 pontos para entender a nova lei de proteção de dados no Brasil.** Disponível em: https://computerworld.com.br/2018/09/19/lgpd-10-pontos-paraentender-a nova-lei-de-protecao-de-dados-no-brasil/. Acesso em: 26/08/2019 às 19:37.

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

MACHADO, Joana de Moraes Souza. **A Tutela da Privacidade o Controle de Dados Pessoais no Direito Brasileiro,** v. 2, n. 2, Arquivo Jurídico: Teresina, 2015. pp. 43-65.

NISSEMBAUM, Helen. **Privacy in context:** technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010.

RIBEIRO, Yasmin Sousa. **A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/18.** Centro Universitário de Brasília – UniCEUB; Brasília, 2019.

SILVEIRA, Sergio Amadeu da. et al. **A privacidade e o mercado de dados pessoais.** Rio de Janeiro: LIINC em Revista, Instituto Brasileiro de Informação em Ciência e tecnologia, 2016.

ZANATTA, Rafael Augusto Ferreira. **Proteção de dados pessoais como regulação de risco:** uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017.

2.4. A função da Autoridade Nacional de Proteção de Dados – ANPD a partir das garantias de livre iniciativa previstas no artigo 4° da Lei n° 13.874/2019 (Lei da Liberdade Econômica) – *Heloísa Corrêa Meneses*[50], *Suelen Bianca de Oliveira Sales*[51] & *Renata Mota Maciel*[52]

Resumo

A função da autoridade nacional de proteção de dados – ANPD é analisada a partir das garantias da livre iniciativa previstas no artigo 4º da Lei n. 13.874/2019, sobretudo em face da atividade regulatória, típica deste órgão nos termos da LGPD. O problema formulado neste estudo é o de que as garantias de livre iniciativa previstas no artigo 4º da Lei n. 13.874/2019 podem ser vistos como entrave à atividade da autoridade nacional de proteção de dados. As hipóteses são analisar até que ponto é suficiente regular a atividade da ANPD por meio da LGPD e, ao mesmo tempo, assegurar autonomia técnica e decisória, conforme disposto no artigo 55-B (redação dada pela Lei n. 13.853/2019); vislumbrar como a competência da ANPD, prevista no artigo 55-J da LGPD (redação dada pela Lei n. 13.853/2019) poderia afrontar, e em que medida, o disposto no artigo 4º da Lei n. 13.874/2019; analisar os incisos do artigo 4º, a partir da atividade empresarial voltada à coleta, ao uso e ao tratamento de dados e verificar os potenciais reflexos na função da ANPD. A investigação do presente tema foi debatida no Congresso Internacional "Desafios e perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade".

Palavras-chave: livre iniciativa; proteção de dados; liberdade econômica; regulação da atividade empresarial; Autoridade Nacional de Proteção de Dados; tecnologia.

[50] Mestranda em Direito pela Universidade Nove de Julho (UNINOVE/SP). Pós-graduada em Direito Societário e Contratos Empresarias pela Universidade Federal de Uberlândia. Pós-graduada em Direito Processual Civil pela Faculdade Damásio de Jesus. Graduada em Direito pela Universidade Federal de Uberlândia. Advogada, inscrita na OAB/MG sob o nº 153.705, com escritório situado na Rua Rio de Janeiro, 353, Sala 108, Edifício Neo Office, Bairro Brasil, CEP: 38.400-658, Uberlândia/Mg. heloisameneses@hotmail.com (34) 99158-3581.

[51] Mestranda em Direito pela Universidade Nove de Julho (UNINOVE/SP). Pós-graduada em Direito Constitucional pela Anhanguera. Graduada em Direito pelo Instituto de Educação Superior de Brasília/IESB. Advogada, inscrita na OAB/DF sob nº 31.256, adv.sbianca@gmail.com, (61)991710304.

[52] Professora do Programa de Mestrado em Direito da Universidade Nove de Julho (UNINOVE/SP). Professora na Escola Paulista da Magistratura (EPM). Juíza de Direito do Tribunal de Justiça do Estado de São Paulo. Doutorado em Direito Comercial pela Universidade de São Paulo.

Abstract

The function of the national data protection authority - ANPD is analyzed based on the guarantees of free initiative provided for in article 4 of Law n. 13.874/2019, especially in light of the regulatory activity typical of this body under LGPD. The problem formulated in this study is that the guarantees of free initiative provided for in article 4 of Law n. 13.874/2019 can be seen as a barrier to the activity of the national data protection authority. The hypotheses are to analyze to what extent it is sufficient to regulate the activity of the ANPD through the LGPD and, at the same time, to ensure technical and decision-making autonomy, as provided for in article 55-B (wording given by Law N. 13.853/2019); glimpse how the competence of the ANPD, as provided for in article 55-J of the LGPD (wording given by Law n. 13.853/2019) could confront, and to what extent, the provisions of article 4 of Law n. 13.874/2019; analyze the items of article 4, from the business activity focused on data collection, use and processing and verify the potential reflexes in the function of the ANPD. The investigation of this topic was debated at the International Congress "Challenges and Prospects of Personal Data Protection and Privacy Authorities".

Keywords: Free enterprise. Data protection. Economic freedom. Regulation of business activity. National Data Protection Authority. Technology.

Introdução

A Lei nº 13.874/2019, ao instituir a Declaração de Direitos de Liberdade Econômica, estabeleceu garantias de livre iniciativa no seu artigo 4º e o objetivo desse estudo é analisá-la a luz da regulação da atividade empresarial destinada às empresas que atuam com a coleta, o uso e o tratamento de dados, nos moldes da ordenação trazida pela Lei Geral de Proteção de Dados – LGPD, em especial a partir das funções da Autoridade Nacional de Proteção de Dados - ANPD.

O problema formulado neste estudo é o de que as garantias de livre iniciativa previstas no artigo 4º da Lei n. 13.874/2019 poderiam constituir entrave à atividade da Autoridade Nacional de Proteção de Dados – ANPD, na medida em que tem potencial limitador do poder regulatório daquele órgão.

A partir dele, foram formuladas as seguintes hipóteses: a) A LGPD, ao regular a atividade da ANPD, assegurou autonomia técnica e decisória no artigo 55-B (redação dada pela Lei n. 13.853/2019). Seria suficiente? b) A competência da ANPD, prevista no artigo 55-J da LGPD (redação dada pela Lei n. 13.853/2019) poderia afrontar, e em que medida, o disposto no artigo 4º da Lei n. 13.874/2019? c) Como analisar os incisos do artigo 4º a partir da atividade empresarial voltada à coleta, ao uso e ao tratamento de dados e verificar os potenciais reflexos na função da ANPD? No discorrer do texto os questionamentos acima serão pontualmente apreciados.

A importância do tema está exatamente em demonstrar a necessidade de coordenação entre as ordenações voltadas à proteção de dados e à garantia da liberdade econômica, sem prejuízo dos fundamentos regulatórios da atividade empresarial no Brasil.

A livre iniciativa, como fundamento da ordem econômica constitucional brasileira, por certo, teria carga normativa suficiente para garantir a liberdade econômica com base na Carta Magna, visto que já é uma garantia constitucional.

No entanto, com a edição da Lei n. 13.874/2019, na esfera infraconstitucional verifica-se a necessidade de regulação por meio do ente estatal no âmbito legislativo no que tange à atividade de coleta, tratamento e uso de dados pessoais no exercício da atividade empresarial e ao poder econômico decorrente dessa atividade.

O presente trabalho parte das posições capitaneadas pela Prof.ª Dr.ª Cíntia Rosa Pereira de Lima, pelo Prof. Dr. Roberto Augusto Castellanos Pfeiffer e pelo Prof. Dr. Bernardo Strobel Guimarães, como referenciais teóricos, para abordar a economia da privacidade a partir da previsão de uma autoridade responsável pela regulação da proteção de dados, conforme a LGPD, com as inclusões trazidas pela Lei n. 13.853/2019, analisando os reflexos das garantias de livre iniciativa previstas no artigo 4º da Lei n. 13.874/2019 à atividade da Autoridade Nacional de Proteção de Dados – ANPD.

O método utilizado será o hipotético-dedutivo; a partir das normas que regulam a chamada Declaração de Direitos de Liberdade Econômica e a Lei Geral de Proteção de Dados, mediante hipóteses, busca-se investigar as consequências das garantias de livre iniciativa, previstas no artigo 4º da Lei, para a regulação da atividade empresarial voltada à coleta, uso e tratamento de dados por meio de um intenso estudo bibliográfico para alcançar diretrizes iniciais ao problema levantado com a análise criteriosa dos conceitos trazidos acima.

1. Livre iniciativa como fundamento da ordem econômica constitucional brasileira: necessidade de garantia por norma infraconstitucional?

A Constituição Federal de 1988 consagra o princípio da livre iniciativa com um dos fundamentos tanto da República Federativa do Brasil (art.1º, V), como da ordem econômica (art.170) demonstrando a necessidade de garantia do equilíbrio da econômica com estímulo ao setor empresarial.

O princípio da livre iniciativa está correlacionado com o princípio da livre concorrência (Art.170, IV), pois, é a manifestação da liberdade de iniciativa e, para garanti-la, a Constituição estatui que a lei reprimirá o abuso de poder econômico que vise a dominação dos mercados. (SILVA, 1998, p.876).

Neste diapasão, a liberdade também deve ser vista no contexto da preservação da privacidade de dados pessoais por meio do princípio da personalidade e da dignidade da pessoa humana.

De outra sorte, pode-se perceber que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) também trouxe como um de seus fundamentos a garantia da livre iniciativa: *"Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: VI - a livre iniciativa, a livre concorrência e a defesa do consumidor"*.

Nesta esteira, temos que a Lei da Liberdade Econômica (Lei nº13.874/2019) enuncia em seu art. 4º os deveres de abstenção do poder público para garantir a livre iniciativa do setor econômico, ou seja o intuito do legislador é estabelecer parâmetros para auferir a existência de abuso regulatórios por parte da administração pública, no exercício de do poder regulamentar.

Com isto, pode-se perceber que o direito a livre iniciativa além de estar consagrado na constituição como um princípio da ordem econômica é também disposto nas duas leis mencionadas acima, fazendo com que este princípio reverbere por todo ordenamento infraconstitucional.

Ora, a liberdade caminha nas esferas individual, social e econômica, com foco na conduta e resultado de uma empresa. Contudo, não existe uma liberdade absoluta, a implementação da LGPD nada mais é do que um marco para atividade regulatória da proteção de dados.

2. A livre iniciativa na atividade empresarial voltada à coleta, ao uso e ao tratamento de dados: a necessária regulação do poder econômico

A legislação infraconstitucional ao regular a atividade econômica com a Autoridade Nacional de Proteção de Dados, seja da forma punitiva, por meio de multas punitivas, seja por meio de diretrizes estruturantes da gestão de dados, busca estruturar o mercado econômico nesta seara do direito digital.

Na visão de Floriano de Azevedo, a regulação tida numa perspectiva mais restritiva, teria como função apenas a garantia do equilíbrio de mercado, coibindo práticas distorcidas dos agentes econômicos. Assim, a regulação teria o objetivo de corrigir as falhas de mercado, perpetuando o equilíbrio interno do sistema regulado. (CAMPOS, 2008, p.283)

Todavia, a função regulatória deveria ser abordada numa perspectiva mais completa, devendo atuar na manutenção do funcionamento do mercado, bem assim, buscando introduzir objetivos de ordem geral que não seriam alcançados exclusivamente pela iniciativa privada.(CAMPOS, 2008, p.283)

Numa perspectiva atual na sociedade de informação surge um novo olhar para o sistema regulatório frente à perspectiva de responsabilidade dos agentes de tratamento de dados dentre eles a forma de gestão de dados compartilhados.

A regulação é conciliar os interesses econômicos, públicos e sociais. Assim, uma legislação sobre proteção de dados não pretende limitar o desenvolvimento econômico. Ao contrário, assim como outras leis setoriais, denominadas de microssistemas jurídicos, uma Lei Geral de Proteção de Dados Pessoais pretende consolidar um sistema de proteção de dados ao necessário equilíbrio entre proteção humana da pessoa humana e o desenvolvimento social. (LIMA; PEROLI, 2019, p. 423)

Dessa forma, insta salientar que a LGPD ao normatizar a proteção da privacidade, define o que são os dados de ordem pessoal e os dados pessoais sensíveis. (art. 5ª da LGPD). Os dados pessoais sensíveis diante de seu elevado potencial discriminatório, devem ser objetos de maior proteção, devendo sua coleta ter a finalidade especificada. Para tanto, a chave primordial do tratamento de dados está no consentimento explícito de seu titular, sendo exceção a sua utilização sem o consentimento (art.11, II, LGPD).

Tratamento de dados refere-se a todo processo em que se utilizam os dados pessoais, sendo estes: 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, X, LDPD).

Com o escopo de propiciar um ambiente de efetiva proteção no processo de tratamento de dados, o princípio da livre iniciativa dentro do regramento de proteção de dados deve estar em consonância com a boa-fé, além dos demais princípios trazidos no art.6º da LGPD, a saber; (i) finalidade; (ii) adequação; (iii) limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades; (iv) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (v) qualidade dos dados (garantia de exatidão, clareza, relevância e atualização dos dados); (vi) transparência; (vii) segurança; (viii) adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (ix) impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (x) responsabilização e prestação de contas.

Desta feita, todos os princípios acima de forma holística são responsáveis para direcionar o comportamento das empresas que atuam no uso, coleta e tratamento de dados.

Para Paolo Lazzara, as autoridades são divididas em reguladoras e de garantia, sendo que a primeira costuma estar vinculada a determinado serviço público, com funções próprias da administração pública. Ao passo que, a autoridade de garantia tem o escopo de proteger os direitos ou situações subjetivas específicas para os quais tenha sido constituída, nos mesmos termos da ANPD, um organismo criado para proteção do direito a dados pessoais. (DONEDA, 2019, p.476)

De outra sorte, a ANPD além do poder de garante e regulador, também possui dentre suas atribuições o poder regulamentador, ou seja, de impor restrições e limitações por meios de normas e padrões aos agentes e empresas que desempenham a função estatal. O Estado assume a responsabilidade pela prestação do serviço e transfere para iniciativa privada a gestão e operação dos serviços, atuando como regulador.

Para melhor entendimento das funções da ANPD, seu microssistema regulatório, prevê a obrigatoriedade do relatório de impacto de proteção de dados, documento que contém todo o acervo de banco de dados do respectivo empreendimento, conforme dispõe o artigo 5º da LGPD. Este documento

poderá ser solicitado pela ANPD e deve ser emitido pelo controlador de dados da empresa e pode vir a ser solicitado em virtude de verificação de interesse legítimo.

Assim, a ANPD como órgão regulador, possui tanto a função de impor restrições haja vista a aplicação de multa para as empresas que não se enquadrarem na legislação relativa à coleta e tratamento de dados, como no âmbito regulamentar de criar normas para gestão e operação das empresas que atuam com dados sensíveis.

3. Reflexos das garantias de livre iniciativa previstas no artigo 4° da Lei n. 13.874/2019 à atividade da Autoridade Nacional de Proteção de Dados – ANPD

A ANPD surge como um importante instrumento de regulação na era da sociedade de informação, assim, é salutar entender os meandros dos desdobramentos até a efetiva definição de sua função como órgão regulamentador e demais competências.

A autoridade regulamentada inicialmente pela MP 869/2018 e posteriormente pela Lei nº 13.853/2019, foi normatizada como sendo um órgão da administração pública federal integrante da Presidência da República, com autonomia técnica e decisória nos termos do Art. 55-B da LGPD, o que se mostra insuficiente na conjuntura da economia brasileira e faz com que paire uma preocupação no ambiente jurídico, pois, diante do caráter meramente técnico atribuído ao órgão, o caráter político prevalece e consequentemente isto enfraquece a referida entidade.

A expressão "decisória" é uma forma de afastar o risco de possível recurso hierárquico para o poder Executivo, pois, a ANPD faz parte da administração direta, subordinada à Presidência da República, devendo em tese ensejar a aplicação do art.56 da Lei nº 9.787/99, o qual dispõe o direito de recurso contra todas as decisões administrativas no âmbito federal. No entanto, ao instituir expressamente a autonomia decisória, faz que se afaste qualquer interpretação neste sentido, dando a efetiva autonomia desta autoridade para decidir sobre matérias de sua atribuição. (PEIFFER, 2019, p.458)

Todavia, em que pese à autonomia ser apenas no âmbito técnico, à luz do artigo 55-J, a estrutura organizacional da ANPD pode contar com dezesseis competências para coordenar os dados pessoais em território nacional, sendo estas agrupadas em preventivas, fiscalizatórias e regulatórias, sancionatórias e reparatórias, estabelecendo normas e diretrizes para sua implementação, devendo esta entidade ser pensada como o instrumento de política pública para tutelar a privacidade.

Insta salientar que as sanções só poderão ser aplicadas pela autoridade nacional após o efetivo procedimento administrativo, devendo ser garantido a ampla defesa e seus respectivos critérios, tais como a gravidade e natureza das infrações, a reincidência, o grau do dano, condição econômica do infrator, entre outros. Entretanto, o princípio da livre iniciativa disposto no artigo 4º da Lei de Liberdade Econômica, ao estabelecer garantias para coibir o abuso do poder regulatório pode ser tido como mais um limitador ao poder regulatório da ANPD, visto que seu caráter técnico já diminui o seu caráter impositivo.

Todavia, o artigo 55-J, faz ainda remissão ao artigo 170 da Constituição Federal, impondo a ANPD uma atuação harmônica face os interesses dos agentes econômicos – atuantes no segmento de tratamento de dados – e os consumidores – titulares dos dados protegidos pela lei, sendo a sua baliza para aferir a conformidade dos atos normativos, a adequação aos ditames da Lei nº 13.709/2018. (PEIFFER, 2019, p.461)

Neste diapasão, importante salientar que a ANPD é um órgão da administração pública direta, vinculada à Presidência da República, mas que segundo os §§1º e 2º do art. 55-A da LGPD, foi previsto uma revisão desta estrutura em dois anos, para analisar a viabilidade desta entidade ser transformada em órgão da administração pública federal indireta, em regime autárquico especial e vinculado à Presidência da República, garantindo assim sua maior autonomia. (LIMA; PEROLI, 2019, p.442)

A Lei de Liberdade Econômica tem o viés da desburocratização pautada no princípio da intervenção mínima do Estado, criada para ser uma lei mais inteligível ao empresário, para que o mesmo cumpra de forma voluntaria seus enunciados, inibindo qualquer abuso regulatório pelo poder público.

De outro ponto a ANPD instituída para regulamentar diretrizes estruturantes da gestão de dados e regular o mercado econômico na seara do direito digital, a sua atuação no mercado econômico e social não deve ser encarada como um obstáculo para o exercício da atividade econômica.

Assim, para que a Autoridade Nacional de Proteção de Dados de fato exerça o seu poderio de equilibrar a relação de liberdade com regulação, seja na aplicação de multa ou por meio da criação de regras para adequação das empresas, é preciso repensar a privacidade como um direito realmente essencial.

A privacidade encontra-se no campo das garantias constitucionais, e encontra previsão legal no inciso X do art. 5º da CF/88. A liberdade, intimidade e dignidade da pessoa humana, traduzindo-se em direito fundamental a personalidade e dessa forma, o seu respeito se faz fundamental para que exista uma eficiente e eficaz segurança das informações pessoais.

Conclusão

A reflexão trazida sobre a regulação econômica teve o intuito de analisar o direito empresarial na esfera da proteção de dados pessoais, perpassando toda esfera de garantias de livre iniciativa versus regulação econômica da Autoridade Nacional de Proteção de Dados, analisando a proteção de dados frente à ordem econômica.

Ademais, cumpre salientar que a normatização trazida pela Lei Geral de Proteção de Dados é extremamente extensa e complexa, para tanto, as empresas devem se adequar no prazo da *vacatio legis* para posteriormente não sofrer as sanções legislativas.

Nessa esteira, é notável a transformação no ordenamento jurídico brasileiro que é vivenciada com a aplicação da Lei de Liberdade Econômica e da Lei Geral de Proteção de Dados.

Para tanto foi analisado que a autonomia técnica e decisória da ANPD em que pese sua limitação na sua atuação de fato, deverá ser revista em até dois anos da implementação da LGPD, o que pode alterar substancialmente a sua regulamentação.

Assim, para que haja uma regulação efetiva da atividade econômica embasada por conceitos constitucionais e também pela regulamentação prevista na LGPD, a Autoridade Nacional de Proteção de Dados deverá, dentro da sua competência prevista no artigo 55-J, equalizar as garantias da livre iniciativa com os ditames regulatórios do mercado econômico por meio de uma regulação econômica social.

Em epítome, para que haja um equilíbrio na ordem econômica constitucional é preciso garantir a função social da atividade empresarial, devendo ser vista como um mecanismo que propicia o desenvolvimento integral da economia, tanto em seus aspectos econômicos, sociais e política.

Referências bibliográficas

CAMPOS, Humberto Alves de. **Falhas de mercado e falhas de governo:** uma revisão da literatura sobre regulação econômica. Brasília – Ed. Prismas: Dir., Pol. Publ. e Mundial, v.5, n.2, p. 281-303, jul./dez.2008.

DONEDA, Danilo. Rumo à Autoridade Nacional de Proteção de Dados. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA; Cintia R.Pereira de. (Coord). **Direito & Internet IV**: Sistema de proteção de Dados Pessoais. São Paulo: Quartier Latin, p. 471-482, 2019.

GUIMARÃES, Bernardo Strobel. Abuso do "Poder Regulador" (o que é e como se controla). *In:* GOERGEN, Jerônimo (Coord.). **Liberdade Econômica:** O Brasil livre para crescer. Coletânea de artigos jurídicos, p.68-85, 2019. Disponível em: <https://aquanticacontabilidade.com.br/webfiles/uploads/arquivo/site/1beb05f3260626831375b1dae21477cb.pdf> Acesso em 26 nov. 2019.

GUIMARÃES, Bernardo Strobel. **Da regulação como função de direito administrativo.** 2007. Dissertação (Mestrado em Direito do Estado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2007. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2134/tde-25022008-155225/pt-br.php. Acesso em 26 nov. 2019.

GONÇALVES, Tânia C. N. Machado. Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei – Brasília, 2019. Dissertação (Mestrado em Direito) – Uniceub, 2019.

LIMA, Cíntia Rosa Pereira de. PEROLI, Kelvin. Desafios para a atuação independente da Autoridade Nacional de Proteção de Dados Pessoais Brasileira à luz das exigências internacionais para a adequada proteção dos dados pessoais. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA; Cintia R.Pereira de. (Coord). **Direito & Internet IV**: Sistema de proteção de Dados Pessoais. São Paulo: Quartier Latin, p. 419-443, 2019.

LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.** Tese de Livre Docência apresentada à faculdade de Direito de Ribeirão Preto, Universidade de São Paulo. Ribeirão Preto, 2015.

PFEIFFER, Roberto A. Castellanos. A saga da Autoridade Nacional de Proteção de Dados: do veto à Lei nº 13.853/2019. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA; Cintia R. Pereira de. (Coord). **Direito & Internet IV**: Sistema de proteção de Dados Pessoais. São Paulo: Quartier Latin, p. 447-469, 2019.

SALOMÃO FILHO, Calixto. **Regulação da atividade econômica** (princípios e fundamentos jurídicos). São Paulo – 2º ed., atual. e ampl. – Malheiros Editores, 2008.

SILVA, José Afonso. **Curso de Direito Constitucional Positivo**. 15 ed. São Paulo: Malheiros, 1998.

Capítulo 3

3. Proteção de dados e o uso de inteligência artificial (IA)

3.1. A inteligência artificial e a proteção de dados pessoais à luz dos direitos da personalidade – *Maria Vital da Rocha*[53] *& Larissa Rocha de Paula Pessoa*[54]

Sumário

Os avanços tecnológicos na sociedade da informação, principalmente relacionados ao uso da inteligência artificial, que apresenta capacidade de aprendizagem e percepção, vêm provocando mudanças sociais, sendo necessário discutir sobre essa expansão tecnológica. Assim, faz-se uma reflexão sobre esse assunto que envolve as implicações da utilização de dados e seu cruzamento como forma de antecipar, mapear

[53] Pós Doutoranda em Direito, na Faculdade de Direito da Universidade de Lisboa (clássica), sob a supervisão do Professor Doutor Eduardo Vera-Cruz Pinto. Possui Doutorado em Direito Civil pela Universidade de São Paulo; "Perfezionamento" em Direito Romano na Universidade de Roma La Sapienza, graduação em Direito pela Universidade Federal do Ceará e graduação em Letras pela Universidade Estadual do Ceará. Atualmente é Professora Adjunta de Direito Civil, na Faculdade de Direito da Universidade Federal do Ceará, lecionando na graduação e no programa de pós-graduação stricto sensu, é Professora Titular do Curso de Direito do Centro Universitário 7 de Setembro - UNI7, lecionando na graduação e no mestrado. Procuradora Federal aposentada.

[54] Mestranda em Direito pela Universidade Federal do Ceará – UFC. Pós-Graduanda em Direito Processual Civil pela Universidade de Fortaleza – UNIFOR. Graduada em Direito pela Universidade Sete de setembro. Email: larissarch@globo.com

ou manipular atributos da personalidade dos indivíduos, além da fragilidade e riscos de vazamento de informações dos dados pessoais. Por conseguinte, o presente trabalho visa discutir e problematizar o fenômeno da utilização da inteligência artificial e os desafios da proteção de dados sob a perspectiva dos direitos de personalidade. Portanto, utiliza-se como metodologia uma pesquisa qualitativa, através de levantamento bibliográfico como livros, legislações, revistas cientificas especializadas, artigos, nacionais e estrangeiros, buscando uma abordagem interdisciplinar sobre o tema. Por fim, evidencia-se que a proteção de dados deve ser vista como um novo direito da personalidade.

Palavras-chaves: Inteligência Artificial; Proteção de Dados; Direitos da Personalidade.

Abstract

The technological advances in the information society, mainly, related to the intelligence artificial usage, represents the learning and perception capacity that are provocating social changes, being necessary to discuss that technological expansion. Thus, we do a reflection about that complex subject involves implications over the data crossing in order to anticipate, mapping or handling personality attributes of individuals, besides exists the fragility and risks of personal information leaking. Consequently, the present paper discusses and problematizes the phenomenon of artificial intelligence usage and data security challenges under the perspective of personality rights. Although, the methodology used is qualitative research, through bibliography revision as books, legislations, specialized scientific magazines, international and national papers, seeking an interdisciplinary approach about the theme. Finally, we highlight the data protection must be seen as a new personality right.

Keywords: Artificial intelligence. Data Protection. Personality Rights.

Introdução

A evolução tecnológica está promovendo profundas mudanças sociais, seja nas relações sociais, ou na própria forma de organização social. Vive-se em uma sociedade da informação, onde todo o desenvolvimento socioeconômico tem sido pautado na informação. Nesse contexto, a expansão da tecnologia da informação precisa ser vista com cautela, pois apesar dos inúmeros benefícios, é preciso resguardar os direitos da personalidade, principalmente, a intimidade e a privacidade. Atualmente, observa-se que muito se discute sobre o futuro da inteligência artificial e os seus impactos na empregabilidade e na possibilidade de várias formas de trabalho passarem a não existir, apesar de ser relevante, essa não será a abordagem dada nessa pesquisa. Nesse aspecto, trata-se de um assunto complexo e interdisciplinar, envolvendo o direito, ciência da computação, neurociência entre outros ramos relacionados ao desenvolvimento tecnológico, sendo necessária a reflexão sobre essa realidade.

Assim, o presente trabalho visa discutir e problematizar o fenômeno da utilização da inteligência artificial e os desafios da proteção de dados sob a perspectiva dos direitos de personalidade. Dessa forma,

as inovações tecnológicas decorrentes da inteligência artificial impulsionam a necessidade da proteção de dados como um novo direito da personalidade e não como uma releitura ou evolução dos direitos já existentes. Por fim, a metodologia utilizada é de uma pesquisa qualitativa, através de levantamento bibliográfico como livros, legislações, revistas cientificas especializadas, artigos, nacionais e estrangeiros, buscando uma abordagem interdisciplinar sobre o tema.

1. Inteligência Artificial

A inteligência artificial (IA) é relevante para qualquer tarefa intelectual e abrange uma ampla variedade de subcampos, seja de forma geral, pela aprendizagem e percepção, seja de forma específica, como jogos de xadrez, demonstração de teoremas matemáticos, criação de poesia, direção de um carro e diagnóstico de doenças. (RUSSELL; NORVIG, 2013, p.3)

Atualmente, a IA faz parte da sociedade da informação, participando no modo das pessoas se relacionarem, trabalharem e se locomoverem. A sua extensão é tão ampla, que até o Judiciário tem buscado utilizá-la a seu favor, com o desenvolvimento do robô Victor do Supremo Tribunal Federal (STF, 2018, online) e o robô Ju do Tribunal de Roraima (TJRR, online), são exemplos disso. Dessa forma, é necessário compreender no que consiste a IA, que faz parte da realidade de inúmeras pessoas, empresas, órgãos e Estados.

Observa-se que surgimento da IA encontra-se relacionado, ou mesmo é comparado, com a inteligência humana. Para Russell; Norvig (2013, p.3) a inteligência humana é capaz de perceber, compreender, prever e manipular um mundo maior e mais complexo do que ela própria, já a inteligência artificial vai além da inteligência humana, pois não apenas é capaz de compreender, mas também de construir entidades inteligentes.

A inteligência artificial na perspectiva de Santos, Camilo e Mello (2018, p.51-52) é que deve ser vista como um processo de solução para o êxito da gestão Big Data, bem como uma ferramenta que incrementa a padronização, gerenciamento e estruturação dos dados da vida das pessoas no contexto organizacional onde estão inseridas.

Existem algumas definições sobre a inteligência artificial, as que se relacionam a processos de pensamentos e raciocínio, as definições que se referem ao comportamento, bem como as definições que compara a um conceito ideal de inteligência, a racionalidade, pois um sistema é racional quando "faz a coisa certa", dado o que ele sabe. (RUSSELL; NORVIG, 2013, p.3). Por isso, a importância de conhecer as referidas abordagens, pois, como já foi dito, ambas coexistem e são utilizadas, não havendo uma única abordagem quando se trata de inteligência artificial.

Além disso, de acordo com os autores Russell; Norvig (2013) a inteligência artificial tem fundamentos na filosofia, matemática, economia, neurociência, psicologia, engenharia de computadores, teoria de controle e cibernética, linguística, sendo, portanto, um campo interdisciplinar.

A partir disso, pode-se dizer que a inteligência através de processos de pensamentos e raciocínio, comportamento, ou mesmo um ideal de inteligência, a própria racionalidade, é capaz de perceber, compreender, prever, manipular e construir entidades inteligentes, se diferenciando apenas pelas peculiaridades da abordagem adotada. Assim, compreendido no que consiste a inteligência artificial, será analisada no próximo tópico, a utilização e seus impactos nos dados pessoais e direitos da personalidade.

2. Os desafios da proteção de dados

Atualmente, vive-se numa sociedade da informação (ou sociedade em rede), que é uma sociedade global, baseada em redes globais, pois a sua lógica alcança todos os países e difunde-se por meio do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia. (CASTELLS, 2005, p.18)

Nessa lógica da sociedade, informação e tecnologia, Boff, Fortes e Freitas (2018, p.16) destacam que o conhecimento deve ser utilizado para gerar conhecimento, uma ferramenta a ser aplicada num processo de integração, controle e internet, relacionado a informação que é gerada, armazenada, recuperada, processada e transmitida. Ressalta-se, na sociedade da informação, o aspecto informacional dos dados com o avanço tecnológico que refletem nos direitos da personalidade dos indivíduos, principalmente, relacionados a intimidade e privacidade das pessoas.

É que na sociedade da informação os dados pessoais "[...] são as informações que podem ser coletadas e tratadas por meios eletrônicos. São utilizadas por empresas ou órgãos públicos para determinado fim comercial, como o uso para uma publicidade, ou para análise de políticas públicas." (SILVA, 2017, p.11)

Nesse aspecto, chama-se atenção para os desafios da proteção de dados, que surgem com o fenômeno da IA, uma vez que, a utilização do algoritmo não deverá ocasionar discriminação. Sendo assim, a proteção dos dados, apesar da fragilidade e possibilidade de vazamento de dados, divulgação indevida de conversas, envio de dados para o exterior, comercialização ilegal de dados, manipulação das informações, que acarretam uma vulnerabilidade na segurança da informação, resguarda-se ao titular do direito da personalidade que tem o direito ameaçado ou lesado, a possibilidade de alcançar a tutela civil dos referidos direitos.

Sobre a utilização e cruzamento de dados, observa-se o famoso caso da "previsão de gravidez" da Target, em que o Andrew Pole estatístico da empresa, em 2002, foi desafiado pela equipe de marketing a

descobrir se uma cliente estava grávida, antes mesmo dela. Desse modo, a empresa começou a coletar informações e mapear os dados dos seus clientes, por muitos anos. Então, começou a aplicar vários testes, analisando-se os dados e, em pouco tempo, surgiram alguns padrões úteis, que possibilitaram uma atribuição a cada cliente uma pontuação de "previsão de gravidez". Aproximadamente, um ano depois da utilização do modelo de "previsão de gravidez", um senhor procurou o gerente, segurando cupons de produtos para bebês que a empresa havia enviado para sua filha, que era apenas uma estudante, o gerente pediu desculpas e depois de alguns dias entrou em contato, novamente, para pedir desculpas, quando foi surpreendido com a informação de que a filha realmente estava grávida. (DUHIGG, 2012, online)

Nesse sentido, Kosinski, Stillwell e Graepel (2013, online) realizaram um estudo sobre como as características e atributos privados são previsíveis a partir de registros digitais do comportamento humano. O estudo demonstra que uma grande variedade de atributos pessoais das pessoas, da orientação sexual à inteligência, pode ser extraída de forma automática e precisa através dos likes do Facebook. Dessa forma, a previsão dos atributos e preferências individuais das pessoas podem ser utilizadas para melhorar vários produtos e serviços. Contudo, a previsibilidade de atributos individuais através de registros digitais de comportamento pode ter implicações negativas consideráveis, uma vez que existe a possibilidade e a facilidade de ser aplicada a um grande número de pessoas sem que haja o consentimento individual, ou mesmo sem que elas percebam. Dessa forma, empresas, instituições governamentais, amigos do Facebook entre outros, "[...] podem usar software para inferir atributos como inteligência, orientação sexual ou opiniões políticas que um indivíduo pode não ter a intenção de compartilhar."

Nesse aspecto, evidencia-se o escândalo envolvendo a Cambridge Analytica, que trabalhou com a equipe eleitoral do atual presidente dos Estados Unidos da América- EUA, Donald Trump, e a campanha vencedora do Brexit, a empresa coletou milhões de perfis de eleitores dos EUA no Facebook e os usou para criar um programa de software capaz de prever e influenciar escolhas nas eleições, foi considerada uma das maiores violações de dados. (CADWALLADR; GRAHAM-HARRISON, 2018, online)

A neurociência evidencia que apesar dos humanos não serem irracionais, necessitam de ajuda para realizarem julgamentos mais precisos e tomadas de decisões melhores, visto que são capazes de tomar decisões rápidas e equivocadas, sobretudo, quando a intuição é influenciada por estereótipos, vieses e diversos outros fatores. (KAHNEMAN, 2019, p.514- 522)

Diante da possibilidade de utilização de dados das pessoas para auferir informações sobre os atributos da sua personalidade, que no contexto da sociedade da informação, é perceptível a elevada produção de dados pelos indivíduos, torna-se até imensurável saber quais informações sobre a personalidade podem ou são reveladas por meio da tecnologia.

Dessa forma, o acesso à informação consiste no desafio dos tempos atuais, uma vez que a informação é uma ferramenta de ação, pois através de uma simples conexão na rede mundial de computadores, tem-se acesso a registros de acontecimentos e outros, com facilidade e baixo custo em pesquisa. (BOFF; FORTES; FREITAS, 2018, p.15)

Além disso, problematiza-se o desconhecimento pelo individuo da destinação da sua imagem no reconhecimento facial seja pelo Estado em abordagens policiais seja por empresas privadas, bem como os riscos de vazamento e manipulação das informações. Assim, outro caso é o da empresa Google, em que um desenvolvedor de software, em 2015, afirmou que o Google, no seu serviço de fotos da empresa rotulou fotos dele com um amigo afrodescendente como "gorilas".

Desse modo, o Google declarou-se "horrorizado e genuinamente arrependido", afirmando que o rótulo gorila não seria mais aplicado a grupos de imagens e que empresa estava trabalhando em correções de longo prazo. Cerca de dois anos depois, uma das correções adotadas foi excluir os gorilas e alguns outros primatas do serviço de reconhecimento de imagem. Verifica-se que a solução foi improvisada e ilustra as dificuldades relacionadas ao avanço da tecnologia de reconhecimento de imagem, que as empresas visam utilizar em carros autônomos, assistentes pessoais e outros produtos. (SIMONITE, 2018, online)

Observa-se que Google, Telegram, Whatsapp, Instagram, Twitter, Facebook, YouTube, Amazon, Ifood, Uber, Smartphone, GPS, Waze, Lawtech entre tantos outros, que são presentes na rotina das pessoas, utilizam a inteligência artificial. Trata-se da economia informacional e global, conforme Boff, Fortes e Freitas (2018, p.16), que "[...] dependente da capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos, e o consumo e a circulação estão organizados em escala global diretamente ou mediante uma rede de conexões entre agentes econômicos."

Sendo assim, notório os benefícios da utilização da inteligência artificial, na forma de comunicação, nas relações sociais, nas práticas comerciais, no modo de locomoção, nos métodos de pesquisa e inúmeros outros. Contudo, é necessária cautela com relação aos dados que são obtidos, utilizados e tratados, para resguardar os direitos da personalidade dos indivíduos.

3. Reflexões sobre os direitos da personalidade

A liberdade, intimidade, privacidade, integridade são direitos da personalidade resguardados pelo ordenamento jurídico. Na sociedade da informação, os dados pessoais são englobados pelo direito da personalidade, por refletirem diretamente na personalidade das pessoas.

Nesse sentido, Bioni (2019, p.84) afirma que os dados pessoais não apenas se caracterizam como prolongamento da pessoa, no que diz respeito a subjetividade, mas, também, influenciam essa perspectiva relacional da pessoa, ou seja, a intersubjetividade dentro da sociedade. Sendo assim, a

proteção dos dados pessoais é um instrumento necessário para que a pessoa possa desenvolver a sua personalidade livremente.

Dessa forma, a Lei Geral de Proteção de Dados estabelece no "art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei." (LGPD, online). Verifica-se, assim, que "a proteção de dados pessoais situa-se entre os direitos da personalidade, pois, também, interfere na dimensão relacional e social do ser humano." (BIONI, 2019, p.84).

Além disso, a LGPD estabelece no art. 21, que "os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.". Isso referese a tutela jurídica que visa assegurar que o "titular dos dados pessoais possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto." (BIONI, 2019, p.86)

A proteção de dados é importante frente ao desenvolvimento tecnológico, pois alertam Santos, Camillo e Mello (2018, p.58) que as pessoas são utilizadas como base para o desenvolvimento e ascensão da inteligência artificial com a expansão do uso do Big Data, bem como as comunidades cientificas possibilitaram reflexões entorno dos métodos de rastrear preferências humanas visando auxiliar setores empresariais, não englobando a dimensão ética nesse uso.

Nesse sentido, ressalta-se a importância da efetividade da Lei Geral de Proteção de Dados, para que o titular dos dados pessoais tenha seu direito protegido contra violações por particulares e estado, bem como busca disciplinar a utilização dos dados pelas empresas.

Portanto, conforme Bioni (2019, p.92) o direito à proteção de dados deve ser encarado como um novo direito da personalidade, pois relaciona-se dentre outras liberdades e garantias fundamentais, a liberdade de expressão, acesso à informação e não discriminação, tratando-se da própria capacidade de autodeterminação.

Conclusão

A evolução tecnológica está provocando mudanças sociais, momento em que se vive na sociedade da informação, que força discutir a expansão tecnológica, principalmente, sobre a utilização da inteligência artificial relacionada a dados pessoais.

Nesse aspecto, trata-se de um assunto complexo, pois há várias implicações referentes a utilização de dados e seu cruzamento como forma de descobrir ou até mesmo mapear atributos da personalidade dos indivíduos, apresentando, possibilidades de riscos de vazamento de informações, discriminação e manipulação desses dados.

Por isso, um dos grandes desafios da Lei Geral de Proteção de Dados é a efetividade na proteção dos direitos da personalidade, para garantir que o indivíduo possa desenvolver livremente a sua personalidade, evitando violações e explorações que influenciem ou manipulem as escolhas afetando, assim, a autodeterminação do indivíduo, bem como coloquem em risco a própria dignidade da pessoa humana. Portanto, a proteção de dados deve ser vista como um novo direito da personalidade.

Referências bibliográficas

BRASIL. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 13.out.2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** A função e os limites do consentimento. Forense, 2019. BOFF, Salete Oro. Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação/ Salete Oro Boff, Vinícius Borges Fortes, Cinthia Obladen de Almendra Freitas. – Rio de Janeiro: Lumen Juris, 2018.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian.** Disponível em: Acesso em: 24.nov.2019.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede:** do conhecimento à ação política; Conferência. Belém (Por): Imprensa Nacional, 2005. DUHIGG, Charles. How Companies Learn Your Secrets. New York Times. Disponível em: Acesso em: 14.out.2019.

KAHNEMAN, Daniel. **Rápido e devagar:** duas formas de pensar. Daniel Kahneman; Tradução Cássio de Arantes Leite. 1ª ed. Rio de Janeiro: Objetiva [2012], 26ª reimpressão, 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior.** Disponível em: Acesso em: 12.out.2019.

RUSSELL, Stuart J.; NORVIG, Peter, 1962. **Inteligência Artificial.** Stuart Russell, Peter Norvig. Tradução Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

SANTOS, Beatriz Rosa Pinheiro dos; CAMILO, Everton da Silva; MELLO, Mariana Rodrigues Gomes. **Big Data e Inteligência Artificial:** Aspectos Éticos e Legais Mediante Teoria Crítica. Complexitas - Rev. Fil. Tem., Belém, v. 3, n. 1 , p. 50-60, jan./jun. 2018 – ISSN: 2525- 4154.

SILVA, Alexandre Ribeiro da. **A Proteção de Dados no Brasil: a tutela do direito à privacidade na sociedade de informação.** Dissertação. Faculdade de Direito da Universidade 10 Federal de Juiz de Fora.

SIMONITE, Tom. When It Comes to Gorillas, Google Photos Remains Blind. **WIRED.** Disponível em: Acesso em: 13.out.2019 STF, Supremo Tribunal Federal. Inteligência artificial vai agilizar a tramitação de processos no STF. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038> Acesso em: 15.out.2019.

TJRR, Tribunal de Justiça de Roraima. **JUSTIÇA 4.0** - Robô humanoide apresenta sistemas com Inteligência Artificial e outras soluções tecnológicas do Poder Judiciário de Roraima nesta terça-feira. Disponível em: <http://www.tjrr.jus.br/index.php/noticias/noticias/3894-justica-4-0-robo-humanoideapresenta-sistemas-com-inteligencia-artificial-e-outras-solucoes-tecnologicas-do-poderjudiciario-de-roraima-nesta-terca-feira> Acesso em: 15.out.2019.

3.2. Inteligência artificial no raciocínio jurídico – *Guilherme Marconatto Modelli*[55] *& Lorenzo Marino Domingues*[56]

Sumário

Não se dúvida que as novas tecnologias são o presente do mundo jurídico. Ocorre que atualmente o assunto se tornou viral no dia-a-dia dos operadores do direito, entretanto, a o presente trabalho se valeu de buscar a resposta se a inteligência artificial realmente se impõe como raciocínio jurídico.

Palavras-chave: Inteligência Artificial; Raciocínio Jurídico; Tecnologias.

Abstract

There is no doubt that new technologies are the gift of the legal world. It turns out that nowadays the subject has gone viral in the day-to-day life of the legal operators, however, the present work used to seek the answer if artificial intelligence really imposes itself as legal reasoning.

Keywords: Artificial Intelligence; Legal reasoning; Technologies.

Introdução

[55] Mestrando em Direito pelo Centro Universitário Eurípedes de Marília; Advogado; gmarconattomodelli@hotmail.com

[56] Graduando em Direito pelo Centro Universitário Eurípedes de Marília; lorenzo_domingues@hotmail.com

O tema se demonstra relevante, uma vez que as condições de emergência, existência e transformação da atualidade encontram-se indissociavelmente interligadas à tese da colonialidade como uma exterioridade constitutiva. (OLIVEIRA, 2018)

Não é de hoje que a Inteligência Artificial (IA) vem se comunicando com diversas áreas de conhecimento e permitindo o desenvolvimento destas, utilizando de suas ferramentas, como por exemplo, da *machine learning*, para efetivação de afazeres repetitivos, intrincadas, que requisitaria maior tempo, com grandes esforços humanos.

Nesse sentido, Russel (2018) realizou um detalhamento histórico, dividindo a história em período gestacional (1943-1955); período de nascimento (1956); período de entusiasmo (1953-1969); período do realismo (1966-1973); período dos sistemas baseados em conhecimento (1969-1979) e, por fim, o período industrial da IA (1980 até hoje). (RUSSEL, 2018)

Nesta linha, Shabbir e Anwer (2015), atribuem a origem da Inteligência Artificial para Alan Turing, durante a Segunda Guerra Mundial e o serviço de decodificação de mensagens. Segundo eles, a denominação fora utilizada por Turing, em meados dos anos 50, no artigo *Computational Machinery and Intelligence.* Ressalta-se que o alumbramento da Inteligência Artificial se deu década passa, principalmente pela evolução dos microprocessadores e da internet, diminuição de custos com o *Cloud Computing*[57] , novos algoritmos e outras inovações. (SHABBIR; ANWER, 2015)

De acordo com Peixoto e Silva, ainda houve outra fase, quando assim mencionam:

Após Turing, John Von Neumann, nos Estados Unidos, contribuiu com a ideia central de que os computadores podem ser desenhados usando-se o cérebro humano como modelo, e iniciou uma concepção antropomórfica da computação, com linguagem, memória e termos típicos ao funcionamento das redes neurais humanas. Ainda na década de 50, um pressuposto básico para o desenvolvimento da IA surgiu com o estabelecimento de teorias que reconheceram a possibilidade de pensamento fora do cérebro humano. (PEIXOTO; SILVA, 2019)

Entretanto, foi apenas em 1958 que surgiu o primeiro programa inteligente com base em modelos de processamento de informação. (SHABBIR; ANWER, 2015)

Houve em 2015 um experimento realizado pelo Google com IA, em que arquitetou um agente de IA com capacidade de interação com humanos, inclusive apto a promover discussões sobre moralidade, com opinião própria e respostas condizentes com esta. (MAINI; SABRI, 2017)

[57] *Cloud computing* ou computação em nuvem é a entrega da computação como um serviço ao invés de um produto, onde recursos compartilhados, *software* e informações são fornecidas, permitindo o acesso através de qualquer computador, tablet ou celular conectado à Internet.

Nessa toada, o Facebook desenvolveu uma aplicação bem-sucedida para negociação em 2017. Já o Google, ativou um aplicativo de tradução com tratamento de imagem para escrita. Nessa linha, existiria vários depoimentos de aplicação em diagnóstico médico, pesquisas de fármaco, pesquisa aeroespacial. (MAINI; SABRI, 2017)

Desenvolvimento

1. A Inteligência Artificial no Direito

O nome impactante da Inteligência Artificial parece que veio a causar mais prejuízos do que benefícios.

Isso porque, por mais que a Inteligência Artificial tenha como objetivo a modelagem do raciocínio humano e a execução de tarefas inteligentes, a inteligência "da máquina" e a humana são incomparáveis.

Shabbir e Anwer mencionam que a Inteligência Artificial tenha como referência o potencial de uma máquina[58] realizar tarefas que reproduzam a inteligência humana. (SHABBIR, ANWER. 2015)

Em outras palavras, a Inteligência Artificial passaria a prover características humanas ao robô. Deste modo, os comportamentos seriam reflexos do humano, seria viável inclusive o aprendizado com experiências passadas (clássico exemplo do robô que está aprendendo a andar e, após repetidas quedas, passa a ir aperfeiçoando suas passadas).

Assim, embora a Inteligência Artificial possua a competência de imitar o comportamento humano em algumas medidas, ela se torna limitado diante da diferença entre o cérebro humano e os computadores. Ressalta-se que esta é perfeita para casos específicos, em que envolvam atividades repetidas, que necessitem de alto grau de atenção e memória.

A Inteligência Artificial, ao buscar formas para simulação da inteligência humana, precisa do desenvolvimento de algumas habilidades. (SHABBIR; ANWER, 2015)

Estas habilidades, são, necessariamente a possibilidade de a Inteligência Artificial reconhecer objetos, converter sons em palavras e vice-versa, extrair sentido da linguagem e transmitir significado por meio de sentenças geradas, ordenar informações de uma forma prática, combinar pedaços de informações para alcançar conclusões e programar uma sequência de ações para cumprir determinado objetivo e ter certeza de que ela foi bem executada. (SHABBIR; ANWER, 2015)

Isso porque, não faria sentido algum a Inteligência Artificial ser utilizada, no direito por exemplo, como aplicadora do raciocínio baseado em casos, se ao menos não conseguisse realizar as habilidades acima elencadas.

[58] Um computador.

Nesse sentido, o desafio que se faz em tal aplicação é em relação à possibilidade de valores morais serem corretamente compreendidos e aplicados pela máquina.

Três grandes campos da IA despertaram interesse na área do Direito: raciocínio baseado em casos; sistemas especialistas e redes neurais.

Sobre a primeira área, a qual será objeto do presente trabalho, Peixoto e Silva afirmam que:

A primeira área, muito adequada à operação do Direito, utiliza os precedentes no raciocínio jurídico. Nesse sentido, Mcjonh (1998) relata programas utilizados na busca de distinguir hard cases na área jurídica de contratos; de modelar diferentes pesos para diferentes fatores que poderiam influenciar na aplicação de normas; bem como programa para comparação de precedentes, exame de similaridades e atribuição de fatores.

Sendo assim, o objeto do presente estudo será baseado na primeira área, qual seja, o raciocínio baseado em casos e com que paridade humana a IA pode atuar no raciocínio jurídico.

Em recente estudo orquestrado pelo *Massachussets Institute os Technology* (MIT), foi feito um experimento no sentido de testar a capacidade de verificação da caracterização de um moral individual ou valores morais de determinado grupo inferidos na máquina.

O estudo detectou uma realidade posta à utilização de *deep learning*, que normalmente utiliza grande volume de dados e exemplos para treinamento e a possibilidade de achar dilemas morais com maior grau de singularidade. Não se deve ignorar também, que a cognição humana é capaz de aprender e fazer antecipações, mesmo com referenciais imperfeitos e escassos. (PEIXOTO; SILVA, 2019)

Os humanos também possuem a capacidade de racionalizar suas decisões morais e articular razões. (KIM, 2018) O que se pode dizer, portanto, é que a Inteligência Artificial e a espontânea, podem ter grande similaridade. (PEIXOTO; SILVA, 2019)

Peixoto e Silva muito bem leciona que:

A importância das reflexões está justamente nas suas diferenças, posto não associadas a uma personalidade jurídica definida/definível. Embora, por razões óbvias, a Inteligência Artificial e a Inteligência Espontânea não se confundam, as características de autonomia desta última são muito mais próximas das personalidades jurídicas atribuídas aos humanos que a discussão/regulamentação sobre personalidade da Inteligência Artificial. O que se deve afirmar é que não se pode teorizar todos os mecanismos de inteligências não humanos como idênticos.

O que se deve afirmar é que não se pode teorizar todos os mecanismos de inteligências não humanos como idênticos.

2. Os limites da Inteligência Artificial dentre as principais áreas do Direito

De plano, de acordo com o que até então fora exposto no presente artigo, já se pode concluir que possuímos pensamentos divergentes no que tange à conhecida expressão "a Inteligência artificial substituirá os profissionais do Direito" que tanto se ouve no âmbito profissional.

A priori, em atenção ao contexto fático cotidiano em que vivem os aplicadores do Direito, resta mais que cristalino o quão complexa e multifacetada se mostra a atividade jurídica. Assim, não se pode afirmar que uma máquina terá capacidade suficiente para não somente adentrar ao campo em que a inteligência comum atua, mas, também, para competir – e por competir entenda vencer – os seres humanos, tomando cada vez mais seus espaços.

A respeito do tema, o autor Wolfgang Hoffmann-Riemm, escreve que:

Tanto para o estado quanto para o setor privado existem, nas zonas de risco, principalmente, um problema de conhecimento e, em especial, o problema da falta de conhecimento. Na verdade, estamos a falar da sociedade do conhecimento, no entanto, talvez a falta de conhecimento seja maior do que o conhecimento. Isso se aplica ao conhecimento do risco, bem como ao conhecimento do benefício. Embora a sociedade moderna esteja comprometida com o princípio da ação racional, voltada para uma contínua aquisição de conhecimento, ela cai em uma situação paradoxal: novos e maiores conhecimentos revelam amiúde novo e maior desconhecimento. O sociólogo Ulrich Beck pondera que não estamos lidando com a sociedade do conhecimento, mas com a falta da sociedade do conhecimento. No entanto, segue sendo o intento promover o conhecimento para gerar um objetivo irrenunciável, inclusive quando se observa, como consequência, um novo desconhecimento. Porque o uso do conhecimento disponível cria um grau de segurança de orientação. Sobre a utilização de conhecimento especializados, mas também (apenas) do conhecimento geral, não há alternativa convincente. De outro modo, a decisão a ser tomada ocorre desde considerações não intersubjetivas, questionáveis m termos de que não se basearam em premissas e acertos eventuais, reversíveis, e certamente não em casa de falha na revisão.

Neste sentido, trazendo a discussão para o âmbito dos advogados, é cediço que este não se presta, ao contrário do que muitos pensam, apenas em elaborar petições e participar de audiência. Caso assim o fosse, sob a minha ótica, a IA teria muito mais chances de alcançar tudo o que acima fora dito ser impossível de acontecer. Entretanto, como anteriormente exposto, dentre tais atividades, existem inúmeras outras em que a Inteligência Artificial não consegue – e não conseguirá – nunca alcançar.

Para começar a explicação, imperioso destacar que o primeiro obstáculo, ou limite, que a Inteligência Artificial encontra seria justamente no primeiro contato entre o advogado e seu cliente. Apenas de forma a corroborar o que acima fora explanado, tamanha as multiplicidades de faces que se encontra na

atividade jurídica que esta, muitas das vezes não se prestam a qualquer questão jurídica, mas apenas e tão somente tratar do sentimento de cada indivíduo que ao nobre advogado, busca.

Isto por que, se analisar o dia a dia dos advogados, a cada 10 (dez) reuniões com novos clientes (ou seja, o primeiro contato entre eles, no qual se expõe, por parte do cliente, todo o seu imbróglio) baixíssima porcentagem deste número será de indivíduos expondo apenas seu percalço, mas, *a contrario sensu*, altíssima será a probabilidade de estes estarem em busca de alguém que os ouça, sem os julgar, e sempre no escopo principal de os proteger.

Neste sentido, muito se equivoca os que explanam a expressão que inicialmente fora exposta pois atualmente as máquinas capazes de proferirem os seus pensamentos, ainda que extremamente desenvolvidas ao ponto de receberem informações, as processarem e chegarem sozinhas a uma conclusão lógica, em nenhuma dessas etapas terá a influência do sentimento que abarca o âmago de cada ser humano.

Inobstante a isso, dentre outras atividades, em que pese a virtualização dos processos, inclusive à margem da extinção dos processos físicos, atividades corriqueiras como idas ao fórum, ligações ao cartório, despachar com os Magistrados, dentre outras inúmeras que, se realmente as foram listar despenderá muito tempo para, são exemplos dos quais não consigo, e penso que nunca conseguirei, vislumbrar uma máquina realizar.

Por outro lado, na carreira dos Magistrados, melhor sorte não encontram os robôs detentores da inteligência artificial, como restará demonstrado a seguir.

É cediço que a invocação do sistema precedentalista no ordenamento jurídico brasileiro, caminhando, portanto, não para este propriamente dito, mas, sim, sob a nossa visão para um sistema misto, caminha em consonância a inclusão da Inteligência Artificial em nosso ordenamento jurídico brasileiro, por intermédio da função nomofilácica, a qual garante uma uniformização de interpretações e aplicabilidade do Direito, de modo a ser previsível tal entendimento no caso concreto, fundamentado no núcleo da decisão de outro análogo.

Neste sentido, caberia sim a inclusão de forma mais efetiva da inteligência artificial na atividade exercida pelos Magistrados. Um belo exemplo de espaço em que poderia adentrar a IA seria nos despachos de mero expediente ou até nos juízos de admissibilidade da petição inicial, caso possuam capacidade para tanto.

Contudo, fundamentado nas mesmas razões, limites, ou barreiras que a Inteligência Artificial encontra no que tange às atividades exercidas pelos Advogados, estas se mostram evidentes também na carreira dos advogados. Isto pois, não é sequer crível que haveria a possibilidade de uma máquina conduzir, por

exemplo, uma audiência de instrução e julgamento, sobretudo tendo em vista as partes exporem sua versão *in casu* para um computador.

Destarte, em análise ao que até então vos fora exposto, temos que, de forma sintética, não há que se falar na substituição dos que exercem a atividade jurídica por uma máquina, mas que nada impede, de forma a evoluir o sistema judiciário, que esta (Inteligência Artificial), sirva como mais uma ferramenta para contribuir, ou então facilitar, o labor diário dos nobres aplicadores do Direito.

3. Futuro da Inteligência Artificial ante ao Direito atual (contemporâneo)

Que as novas tecnologias já fazem – e farão cada vez mais - parte do dia a dia dos advogados, Magistrado, Promotor de Justiça, Delegado e de todas as outras carreiras possíveis de se cursar dentro do universo do Direito não é nenhuma surpresa ou novidade. Contudo, pôr em pauta a forma em que será inclusa ou em quais áreas mais carece da mão amiga (e não adversária) que é a Inteligência Artificial são o cerne e escopo deste artigo.

Neste sentido, Cessna (2015, p.1-2) expôs sua visão e, aqui, na tradução de Hartmann Peixoto, Fabiano e Zumblick Martins da Silva, Roberta: *"a ascensão da e-discovery e o aumento drástico nos documentos que a acompanham criaram mais trabalho para os advogados. Também levaram ao surgimento de soluções tecnológicas para lidar com a e-discovery."*

Em síntese, o que o autor acima expressou, de forma simples, é que atividades que requereriam menos esforço psíquico e antes seria realizado por algum funcionário, hoje, já se pode transpassar tal serviço para a máquina que, por meio de sua inteligência artificial, conseguirá o realizar.

Ressalta-se que nestes casos em que há a possibilidade de transferência de serviço do funcionário comum à máquina, como se verifica inclusive de algumas pesquisas realizada, em todas a máquina se destaca, posto que realiza os mesmos trabalhos de forma demasiadamente mais célere que os funcionários, bem como com excelência em sobeja.

Tanto é verdade que, segundo pesquisa realizada pela Lawgeex, startup da tecnologia jurídica, como se em um ringue jurídico existisse de um lado máquina (IA) versus humanos.

No "time" dos humanos existiam diretores jurídicos de grandes empresas, tais como Goldman Sachs, Cisco e Alston & Bird, entre outras. De acordo com o site do Fórum Econômico Mundial (FEM), o trabalho seria examinar riscos contidos em cinco contratos de confidencialidade (*NDAs – non-disclosure agreements*).

Ao final, verificou-se que um dos 20 (vinte) advogados conseguiu empatar com a inteligência artificial. Ambos atingiram 94% de precisão na respectiva tarefa. Ao analisar o grupo como um todo, a inteligência artificial ganhou, pois o grupo de advogados atingiu a média de 85%.

Entretanto, o que nos causa espécie é que enquanto os humanos demoraram 92 (noventa e dois) minutos, em média, para concluir a tarefa, a Inteligência Artificial revisou todos os cinco contratos de confidencialidade em apenas 26 (vinte e seis) segundos.

Neste panorama, há a identificação de um modelo conhecido como *predictive coding*, sendo este, um exemplo de aplicação da Inteligência Artificial no contexto do mercado jurídico, o qual, inclusive, pode se submeter a diversas configurações para melhor se adequar à solução de cada caso concreto. Vejamos a forma em que se é habitualmente explicado:

1) Uma amostra inicial de um conjunto de dados filtrados/estruturados é revisada e categorizada por relevância por uma pessoa ou um conjunto de especialistas;

2) Uma análise dos documentos estruturados, pelos especialistas, é feita a fim de identificar os principais conceitos e temas;

3) A máquina aplica os conceitos a um conjunto maior de dados, destacando as que ela mesmo considera relevantes;

4) Há uma espécie de revisão humana em que a relevância identificada pelo revisor é enviada ao sistema;

5) Este processo é repetido até se chegar à uma precisão aceitável.

Ressalta-se que na última etapa, o método labora no campo do considerável, justamente por este lidar com linguagens, interpretações, valorações, que, independentemente de ser manuseada pela mão humana ou inteligência artificial, obterá um coeficiente de imprecisão.

De forma a corroborar a plausividade de todo o aqui exposto, Hartmann Peixoto, Fabiano e Zumblick Martins da Silva, Roberta, na já citada obra "Inteligência Artificial e Direito" bem expuseram que "a Inteligência só existe em razão de desafios". Destarte, elencam 03 (três) leis da Inteligência Artificial, as quais resta imperioso destacar.

A primeira lei da IA, de acordo com Bentley (2018), elenca que "desafio gera inteligência". De forma simples, o que vos fora posto é que são os problemas, os responsáveis pelo desenvolvimento da inteligência; segundo Bentley, a inteligência não seria condição, mas sim, consequência da existência de desafios originados em problemas. No mesmo sentido, sem novos desafios a serem vencidos pela força da inteligência, esta, se estagnaria, não evoluiria, afirmando, para tanto, que "sem uma necessidade urgente, a inteligência é simplesmente um desperdício de tempo e esforço".

No mesmo diapasão, Bentley (2018) finaliza suas pontuações acerca da primeira lei informando que não há, até então, evidências de que o motor propulsor de uma superinteligência seria movido pelo objetivo ou interesse em prejudicar a humanidade, alegando, inclusive que, tal suposição pode ser decorrente de

uma constatação da tamanha violência do comportamento humana existente no âmago de cada um deles.

No que tange à segunda lei da Inteligência Artificial, esta se baseia justamente na equivocada percepção de que a quantidade de redes neurais está submetida à lógica do "quanto mais, melhor". Destarte, é cediço que a IA possui uma quantidade de redes neurais muito superior às do cérebro humano, de forma que, consequentemente, traria a ideia de que esta primeira, teria desempenho superior à segunda. Esta percepção, para Bentley, como já dito, é equivocada. Tanto que a segunda lei trata justamente da inexistência desta lógica de quantidade, posto que, sob sua visão, o grande – e verdadeiro – desafio está em justamente definir os algoritmos apropriados para a solução de cada desafio, sendo, esta, a essência da 2ª (segunda) lei.

Para o autor, cabe salientar a necessidade de termos a exata noção de que não se produz Inteligência Artificial de uma só vez. Sob sua ótica, quando se incrementa os mecanismos de IA, sempre surgem e surgirão novos problemas (1ª lei); assim, temos que não há possibilidade de existência de condições matemáticas para prever e projetar tantas possibilidades de futuras e eventuais intercorrências que possam vir a surgir, de forma a afastar uma necessidade de complementação, ou, em suas exatas palavras, que não dependam de uma abordagem incremental; mas a verdadeira evolução se fundamenta na sistemática "de tentativas e testes e de construção baseada em estruturas e sobre-estruturas que não se interrompem, mas que se constroem cuidadosamente levando-se em conta a estrutura anterior".

Por fim, e não menos importante, a 3ª lei da IA determina que a inteligência e o tempo necessário para os testes (2ª lei) aumentam gradativa e proporcionalmente, na medida em que se torna mais difícil ir mais rápido quanto mais próximo da velocidade da luz, torna-se mais difícil aumentar a inteligência à medida que construímos "cérebros" mais inteligentes.

Em vias de conclusão, Bentley (2018) observa e salienta que, tendo em vista o desenvolvimento da inteligência artificial ocorrer em camadas, cada tentativa de melhorá-la, 12 põe em risco todas as capacidades anteriores, reforçando, para tanto, que tal desenvolvimento requer um conjunto de testes completos, em que os problemas existentes serão resolvidos. Reitera que, em seus exatos termos (traduzidos), "para fazer uma IA é necessário treiná-la e testá-la em todas as suas capacidades de forma abrangente, em seu ambiente de atuação, e observando todas as etapas de seu projeto". Daí, portanto, se extrai a interface do Direito com a Inteligência Artificial, uma vez que é preciso identificar que o fundamento das pesquisas em IA está em busca de soluções inteligentes para problemas específicos, relevantes e complexos que podem ser encaminhados com o auxílio da Inteligência Artificial.

Outro ponto que merece destaque, é o fato da neutralidade da rede na internet:

A discussão em torno do conceito de neutralidade da rede mostra-se momentaneamente com intensidade significativa na rede de comunicação da Internet. Neutralidade da rede significa, nesse contexto, acima de tudo, a igualdade de tratamento dos pacotes de dados, independentemente da sua origem, do seu destinatário e de seu conteúdo. Até agora o acesso às redes globais, que formam a internet, ainda é garantida a todos sem distinção. O desenvolvimento tecnológico, no entanto torna possível não apenas identificar a fonte – o computador do qual o pacote de dados é enviado – como descobrir o conteúdo dos pacotes de dados (*Deep Packet Inspection*). Isso permite, por um lado, um tratamento preferencial tanto qualitativo, quanto quantitativo na transmissão de dados, por outro lado, permite a afetação de interesse de terceiros, mediante a filtragem ou mesmo o bloqueio de pacotes de dados indesejados.

Isso significa dizer, por tanto, que podemos mensurar uma outra linha problemática, estranha àquelas já elevadas, qual seja, a neutralidade dos serviços.

Isso porque, as condições técnicas permitem, portanto, que os provedores restrinjam a neutralidade da Internet.

Conclusão

Embora existam semelhanças fragmentárias, os computadores não funcionam como cérebro humano, especialmente em relação às habilidades comportamentais, como por exemplo o senso de humor, opiniões morais complexas e atitudes especificas humanas, como a intuição[59].

Tais limitações fazem com que a Inteligência Artificial padeça a transferir aprendizagem para cenários om combinações mais complexas de problemas não previstos, de forma que, casos como estes permitiriam que a Inteligência Humana agisse com grande facilidade e com arranjos cognitivos diversos, atrelando de forma complexa a lógica, a criatividade, engenho e razão.

Não é demasiado afirmar que a Inteligência Artificial, seu evolutivo aperfeiçoamento e sua difusão de usos e aplicações, trazem a possibilidade de produzirem severas mudanças em nosso ambiente político e social, com consequências revolucionárias similares a outros fenômenos indutores de viradas paradigmáticas.

A Inteligência Artificial tende a buscar descobertas por meio de uso dos computadores para execução de tarefas impossíveis a capacidade e resistência humana, além do aperfeiçoamento das tarefas que já são executadas pela inteligência humana.

[59] Tudo isso em uma dimensão mais global.

Em sede de conclusão, verifica-se que a inteligência artificial tem muito a nos oferecer com sua inclusão no mundo jurídico. Como já exposto, esta, que possui o escopo de servir como uma mão amiga, se insere em um contexto onde os aplicadores do direito gastam dias em serviços maçantes e repetitivos, como revisões, análises e pesquisas de documentos.

Deste modo, inolvidável que inserir a Inteligência Artificial no contexto retro descrito, de modo a otimizar o tempo e deixá-los livres para focar naquilo que realmente importa trará inúmeros benefícios, tanto para os próprios funcionários, como, principalmente, aos patronos (nos casos de escritórios de advocacia), uma vez que, além do desenvolvimento de seus funcionários, obterá, certamente, uma demasiada elevação na qualidade de seus serviços e desenvolvimento de sua produtividade.

Assim, por intermédio das máquinas que possuem capacidade de aprenderem sozinhas, como, por exemplo, as *machines learnings*, estas, permitirão que advogados, realizem pesquisas e consultas de informações jurídicas com muito mais agilidade e eficiência.

Por estes exemplos, entre inúmeros outros possíveis de se exemplificar, podemos concluir que o foco da Inteligência Artificial, no campo da advocacia é maximizar a produtividade do nobre advogado, deixando os seres humanos com enfoque direcionado em tarefas que só nós somos capazes de realizar, como aquelas que envolvem análise crítica, criatividade e competências sociais. A Inteligência Artificial e suas soluções, como já explanado, não vão tirar o emprego de ninguém; muito pelo contrário, elas nos ajudarão a nos tornarmos ainda melhores profissionais e a melhorar a gestão dos escritórios de advocacia.

Ante a todo o exposto, se mostra de fundamental importância a necessidade de atualização dos profissionais na área da Inteligência Artificial inserida na área jurídica, não para os ter como adversários no escopo de tentar vencê-los, mas sim para poder extrair o máximo do auxílio que esta tecnologia pode – e poderá – nos oferecer.

O presente trabalho buscou da melhor forma possível demonstrar o contexto histórico em que a Inteligência Artificial veio se desenvolvimento, desde o momento de seu surgimento, passando pelas épocas de aperfeiçoamento, e aterrissando no momento de seu maior impulsionamento, o qual creditamos às pesquisas e desenvolvimentos recentes das redes de internet, bem como de empresas conceituadas, como Facebook e Google.

Adiante, esclarecemos o momento que se atrelou a Inteligência Artificial ao Direito e sua aplicação, demonstrando assim, sua forma de "pensar" e se esta, realmente está em sintonia com a Inteligência Humana.

Referências bibliográficas

ANDREAS, Vobkuhle, Expertise und Verwalltng, em: Hans-Heinrich Trute; Thomas Grub; Hans-Christian Rohl; Christoph Mollers (Hrsg.). **Allgemeines Verwaltungsrecht** – zur Tragfahigkeit eine Konzepts, 2008, pp. 637 e 633.

EDWINA, Rissland L. **Artifical intelligence and law:** Stepping stones to a modelo f legal reasoning. 99 Yale L. J., 1990.

HARTMANN PEIXOTO, Fabiano; SILVA, Roberta Zumblick Martins da. **Inteligência artificial e direito,** 1. ed. Curitiba: Alteridade Editora, 2019.

HOFFMANN-RIEMM, Wolfgang. **Direito, inovação e tecnologia.** Coordenadores Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015 (Série Direito, inovação e tecnologia, v. 1).

KLOEPFER, Michael. **Direito, inovação e tecnologia.** Coordenadores Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho. São Paulo: Saraiva, 2015 (Série Direito, inovação e tecnologia, v. 1), pp. 146 e 147.

MAINI, Vishal; SABRI, Samer. Machine Learning for Humans. **Every Thing Computer Science,** 2017.

OLIVEIRA, Wagner Vinícius de. Epistemologias do sul aplicadas no controle concentrado de constitucionalidade brasileiro. **Revista Em Tempo.** Centro Universitário Eurípedes de Marília – UNIVEM. Revista de Direito do UNIVEM. Marília: Letras Jurídicas, v. 17, 2018.

RUSSEL, Stuart; DEWEY, Daniel; TEGMARK, Max. **Research Priorities for Robust and Beneficial Artificial Intelligence.** Cornell University. Al Magazine, 36n. 4 (2015).

SHABBIR, Jahanzaib; ANWER, Tarique. Artificial Intelligence and its Role in Near Future**. Journal Of Latex Class Files**, v. 14, n. 8, 2015.

BECK, Urich. **Weltrisikogesellschaft:** Auf der Suche nach der verlorenen Sicherheit. 2007.

3.3. Artificial Intelligence and Liability in the Health System: International mapping of regulations and comparative analysis

– Gabriela A. S. Monteiro, Geneviéve David, Jean-Louis Denis & Catherine Regis[60]

Abstract

Artificial Intelligence (AI) is being used on health broadly and the its development has increased considerably since the late 2000s (Liao, Chu, & Hsiao, 2012; Michael, Bowman, Jones, & Pringle, 2018; Nebeker, Torous, & Bartlett Ellis, 2019; Pagallo, 2018; Pesapane, Volonté, Codari, & Sardanelli, 2018), arising new legal issues during the last decade. With that in mind, this research was divided in two major parts: the first one to do a international mapping of regulation or regulatory efforts on AI use in the health sector; and the second one to analyze liability and responsibility over data protection for medical AI in both USA and Brazil, in a legal comparative perspective.

Keywords: Artificial Intelligence. Accountability. Liability. Data protection. Health.

Introduction

For the first part of this work, we used as criteria the twenty most developed economies in the world (G20), observing for each of them if there was any governmental efforts towards regulating AI in the health system, and analysed some specific scenarios. Although that technology is greatly advanced (Michael et al., 2018; Nebeker et al., 2019; Pesapane et al., 2018; W. N. I. Price, 2017), it brought many issues that shouldn't be ignored.

The AI evolution in health made it more complex (Matthias, 2004; O'Sullivan et al., 2019). Some of the important concerns brought out of this are data protection and liability (Cellan-Jones, 2016; Michael et al., 2018; Pesapane et al., 2018), and how those concerns have been regulated around the world was our main objective during this research.

The development of technology in the health sector includes robots capable of doing surgery, diagnosis, rehabilitation, prosthetics and more (O'Sullivan et al., 2019). Even though only some of them are yet considered AI, one may worry if people will "trust these machines to make decisions that are actually beyond the machines' capabilities, and this reliance on machines will effectively reduce human agency in ethically important domains" (O'Sullivan et al., 2019)

[60] Ribeirão Preto Law School of University of São Paulo, Brazil. Faculty of Law of University of Montréal, Canada. The project was developed at the Faculty of Law of University of Montréal with coordination and supervision by the H-POD research group, with fundings of MITACS Globalink Research Internship Program, from June 26th to September 18th of 2019.

Results

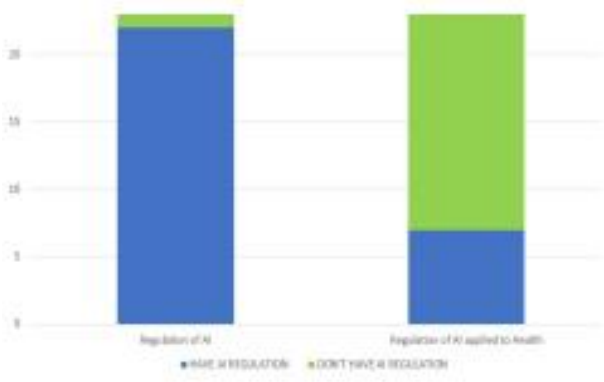


FIGURE 1: TABLE OF RESULTS FROM EFFORTS TOWARDS REGULATING A.I.

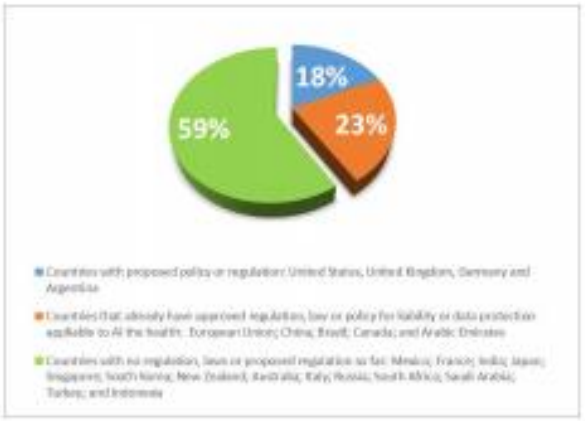


FIGURE 2: INTERNATIONAL ARTIFICIAL INTELLIGENCE REGULATION MAPPING

In the search for the G20 nations, some information about other countries came up, and were added to the research's results. So, the total of countries included is 23. We observed if they have regulatory efforts for AI, hereby meaning any government policy, campaign, or public-private partnerships for AI. The first column of the graphic (FIGURE 1) shows countries that have regulation, proposed regulation or any other kind of private-public cooperation into regulating A.I., and 22 out of 23 countries were positively included in it (Bnamericas, 2019; Cabral, 2018; Daws, 2019; G7 Research Group, 2018; Government of Canada, 2018; Konnangath, 2019; Ortiz Freuler et al., 2018; W. N. Price, 2019; Team, [s.d.]; Tschider, 2018; YİNANÇ, 2019; Anggraeni, 2018). However, in the second column (FIGURE 1) we show that we found so far only six, out of those 23 countries, with the same kind of effort towards regulating AI specifically for the health sector (Srivastava, 2018; Gameiro, Arasaki, Lira, Neto, & Stachuk, 2019).

In sequence, the results collected for the first column were divided in a second, more specified chart (FIGURE 2). As we show, the results were divided in three sub-criterias, that being (i) countries that have regulation and/or policies for liability and/or data protection for AI, which can be applied to the use within the health sector (Government of Canada, 2018; Konnangath, 2019; Forbes, 2019; Tschider, 2018); (ii) countries that have proposed regulations or policies as same as (i), but not yet approved or efficient (Bnamericas, 2019; W. N. Price, 2019; Forbes, 2019); (iii) countries that have no regulation or policy, whether proposed or approved (Anggraeni, 2018; Daws, 2019; Forbes, 2019; YİNANÇ, 2019).

Besides that, we also found that 3 of 23 countries have a specific Ministry or Council for AI established in the government to deal only with A.I. development and regulation or innovative technologies

protection legal framework (Bnamericas, 2019; Konnangath, 2019; Ortiz Freuler et al., 2018; Forbes, 2019); and 3 of 23 countries have a fully functioning agency to regulate and fiscalize data protection (Konnangath, 2019; Forbes, 2019).

Discussion

The clipping of this research was to analyse how liability takes place in the regulation of AI in the health sector, being for medical AI devices mistakes, malpractice or torts caused by the misuse or malfunction, such as releasing personal sensitive data. The development and the use of AI in health, the injury caused can be very serious. Usually it needs to be determined whether the doctor is responsible, but when the conflict involves the use of AI, or robots with machine learning capacity per say, that analysis becomes more complex: Should the developer and operator, or the facility, be held responsible? (O'Sullivan et al., 2019).

The problem in those situations is that not always the robot is entirely under the control of the operator wishes or programming (Matthias, 2004). And, in a classical legal approach, the one to hold responsible is the developer of the technology, if it is not the operator's fault (J.M. Fischer and M.S.J. Ravizza Responsibility and Control, 1998).

> [...] under current law, the robot, even if autonomous, may not be held liable for its actions or its inactions in case of damage. It cannot therefore be ordered to compensate the victim. In this case, the damage caused to the patient by a surgical robot is imputed, either (1) to the manufacturer (if the robot has a manufacturing defect), or (2) to the operator (if the robot is implicated or if it has made a medical error), or (3) to the person responsible for performing the maintenance of the robot's adjustments if the damage results from irs failure" (O'Sullivan et al., 2019).

Originally, the advances towards robotical use in medicine relate to the need of medical performances in urgent situations where the human efforts cannot achieve the results, such as the case of the surgical robot used first by militaries to operate in places where the doctors could not reach (Nebeker et al., 2019; O'Sullivan et al., 2019). However, the situation becomes more complicated when that emergency service is extended to the civilian casualties context, in which scenario would be possible to prosecute for manslaughter if an autonomous surgery robot's action leaded to the death of the patiente (O'Sullivan et al., 2019).

O'Sullivan (2019) points out that AI use in the health sector can have two different responsibility levels to concern about: accountability and liability (O'Sullivan et al., 2019). Of course the law rationale

diverges in each country but these protection principles should be mainly equivalent in both USA and Brazil. However, neither of the nations hereby analysed had such advanced protection in the regulatory level so far.

Regarding accountability for the robot, it should be the machine's capacity to explain the reasons why it took some decision, if it's autonomous (O'Sullivan et al., 2019). That could mean that if the robot was autonomous in the decision making, regardless of what the operator or the manufacturer predicted for it to do, it should be able to explain the reasons for such decision and therefore be held responsible itself for that (Matthias, 2004).

Usually having a system for recording the input, internal state and output would solve the accountability gap in these cases (O'Sullivan et al., 2019), but there is the concern that robots can evolve bias and discriminatory decision making criterias (Wachter, Mittelstadt, & Floridi, 2017), making that statement uncertain. However, the accountability should be the easiest part of robot responsibility, considering that the practical solution should be enough.

As maintains O'Sullivan (2019), one solution for accountability could be a technology such as the used in the aircraft's black boxes recorder to be workable for sufficiently complex autonomous surgical systems (O'Sullivan et al., 2019).

The liability aspect can be more tricky to solve, due to the unexplored field of robotics and algorithms in the health sector in a legal perspective (Matthias, 2004; Nebeker et al., 2019; W. N. I. Price, 2017; Wachter, Mittelstadt, & Floridi, 2017). For Matthias (2004), the operator may be less or not at all liable for damages when he had reduced control over the system. In that matter, the classic legal rationale of liability are not suitable for machines that act independently of the human operator and make decision on their own (Matthias, 2004).

The question for O'Sullivan (2019) is if the development of such complex robotics - the systems, methods and reasoning of it - and autonomy really makes it harder to establish and to determine liability. He continues: "[t]he operation of an autonomous robot, capable of learning new things for itself [...] could lead to unpredictable behaviour. It could therefore cause damage that would not be the result of its programming" (O'Sullivan et al., 2019). In that sense, not only it can be ineffective to hold the robot's operator or manufacturer responsible for its decisions, but also would be unjust to do so:

> If we want to avoid the injustice of holding men responsible for actions of machines over which they could not have sufficient control, we must find a way to address the responsibility gap in moral practice and legislation. The increasing use of autonomously learning and acting machines in all areas of modern life will not permit us to ignore this gap any longer (Matthias, 2004).

That gap could get even bigger if we consider the health sector in which a damage caused by an autonomous decision making robot would be very serious. However, medical robots technology acting autonomously is not a reality yet, specially for the healthcare field. Medical robots do not have really unpredictable behaviour yet, due to the limitation of its learning abilities to the its purpose and its software (O'Sullivan et al., 2019).

Even though the machine learning existing development is necessarily within the specified framework by the designers (O'Sullivan et al., 2019), it is probably not so bold to risk saying that in the next years we will have that kind of autonomy for medical AI devices, with robots that learn broadly then its programmed objectives. So a regulation in that matter would still be a questionable situation, as it already is now. As explained by O'Sullivan (2019):

> Court sanctions are likely to drive the development of the insurance market for autonomous surgical robots. The way that humans in modern societies deal with liability is via insurance (such as for a doctor when he/she practices medicine). In the current state of the law, as the robot is not liable, it is up to humans to incur liability by design, manufacture, or use of the robot to take insurance. The solution is identical in surgical robotics (O'Sullivan et al., 2019)

On 2017, the European Union have manifested over the possibility of providing robots with legal personhood, making them responsible for the torts caused by their autonomous decisions and to compensate victims (UNESCO, 2017). In the recommendations of EU, it is clearly considered creating an specific legal status for robots as a legislative instrument to solve those implications. But, even though it is not legally mandatory to follow those recommendations, not for EU member nor any other country, it may be a start on the framework for robotics regulation on liability worldwide (O'Sullivan et al., 2019).

In the opposite way, "[...] these physically impressive machines still lack common sense, basic communication skills, and emotional intelligence" (Michael et al., 2018). The same report above referred from the European Parliament also describes some problematic aspects of giving robots personhood, calling counterintuitive to call them persons because they wouldn't have typical human qualities (UNESCO, 2017). The breaking point between a robot that can have legal personhood and one that can't is a very difficult criteria to establish for being a philosophical unsolvable issue the humanity criteria.

An interesting thing to also consider is that even if the AI used in the health system gets legal personhood and therefore start to be held responsible for its own decision-making, it might not be so

effective. That because behind any attributed legal personhood there is a natural person. So the dilemma on who to be responsibilized objectively remains, even if the robot or algorithm can be directly processed.

Usually, the intent of attributing legal personhood is facilitate holding accountable and liable the human, ultimately the natural person behind the legal one. But that is not the case when involving autonomous robots, "even if the aim of the legal personhood of the robot is to set up a specific legal regime [...] the most serious risk is that of disempowering the manufacturer in the event of damage caused by the machine" (O'Sullivan et al., 2019).

> [E]thical challenges arise from the combination of new, rapidly evolving technologies[...] and a lack of regulatory controls or common standards to guide this convergence in the health ecosystem (Nebeker et al., 2019).

On the other way, for Datteri (2013) the legal framework now existing regarding responsibility for medical robots settle most a retrospective approach of the liability, holding problems raised in the connection with the injuries caused by the robot behaviour. As retrospective responsibility he refers to the determination of who is responsible for the injury caused, after it is already damaged, and for which there is already an extant legal framework for liability issues. He addresses "no legal gap has emerged so far in connection with actual cases of injuries caused by autonomous (medical) robot behaviours" (Datteri, 2013).

In that meaning, for retrospective perspective the regulation is fullfing enough, or at least the legal rationale over responsibility is. That not necessarily exclude the upcoming need for regulatory efforts to cover the advances on AI applied to the health system. However, as the referred author says, there is no obvious answer for such dilemma (Datteri, 2013). Considering the unsolved scenario on ethically appropriate responses for the use of AI and machine learning on the health sector, it is important not only for the jurists to worry about it, but also for the robots designers to try developing an ethical framework as part of the creation process (O'Sullivan et al., 2019). That applies both for the non-mistakes and liability aspect and for the data privacy sense of ethical framework.

Engagement from AI developers is needed in a bigger baseline because the main biomedical and behavioral research is still carried out by the academical field, with the interest of technology giants and start-up companies (Nebeker et al., 2019), but not in the extant that it should be as a main technological concern. For Pagallo (2018), policy makers should establish new accountability and liability forms of legal agenthood for complex cases involving AI for distributing responsibility. Nonetheless, there is no denying the foreseeable future scenario where robots may be "human" enough to have legal personhood (Matthias, 2004; Pagallo, 2018).

Final observations

If we consider medical errors, it sets an unsolved question: is a surgery robot, even though not considered AI properly, actually less propense to mistakes then a human, and how does it really affect the legal standards for malpractice? That question is becoming frequent within the literature, just like the problem of how to hold robots accountable in those situations (O'Sullivan et al., 2019; Pagallo, 2018).

For Tschider (2018), USA and EU have not "effectively developed a standardized approach to regulation AI in traditional medical devices, and consumer health devices receive considerably less attention". In what regards health mobile applications (apps), it has become more popular, but yet non-regulated with a standard regulatory requirement for manufacturers or operators (W. N. Price, 2019; Tschider, 2018), specially around liability, accountability or responsibility over data protection.

Price (2017) suggests that a different and new path of governance should be taken to pursue an appropriate regulatory approach, with requirement sufficient for developers to disclose information underlying their algorithms or robots. There's being a big development of AI algorithms in health (Matthias, 2004; Pagallo, 2018; Pesapane et al., 2018; Tschider, 2018), such as "Mobile Health", or "m-Health", which use is complicating protection of personal data (W. N. I. Price, 2017). Algorithmic medicine needs to be regulated in the proper way, due to the default for new technologies, at least in the "free-market-based United States" where there are no major impediditives: if a producer wants to produce and a buyer wants to buy, that is all it takes to establish a commercial transaction, and "regulation in the form of premarket approval is especially rare" (W. N. I. Price, 2017).

As highlights Tschider (2018), AI use in medical sector have being technologically improved to the point of revolutionizing health care. Therefore, the need for appropriate regulation grow along in the same speed. The main concerns here are accountability, liability and data protection within the use of big data, algorithms and medical apps (Matthias, 2004; W. N. I. Price, 2017; Tschider, 2018).

Big data collection includes algorithmic decision-making: "1) ubiquitous data collection, data breach, and identity theft; 2) unrestrained collection of sensitive, personal data; and 3) the use of algorithmic decision-making to make consequential decisions" (Tschider, 2018). However, regulation must be able to accompany the technological fast improvement, and therefore to be not so strict when deploying AI and autonomous surgical robots or other medical devices of that sort (O'Sullivan et al., 2019).

This context can lead to the questioning of whether this same rationale may be applicable for developing countries with fewer healthcare resources (O'Sullivan et al., 2019). And in that context we can insert Brazilian regulatory situation, and understand it comparing to the U.S. reality hereby explored so far.

Of course, that developing of technology in that way strongly rely on the country's funding for such. It may not be the case for Brazil yet (Barbosa, 2017), but the increase of AI as discussed is worldwide, and has got to a point of having global consequences (Cabral, 2018). The regulation regarding data protection and liability should consider the specificity that this type of development brings along, in order to maintain a safety level for both users and operators of medical devices. That picture becomes even more critical when we consider that autonomous decision-making AI devices are no longer sci-fi, and are not far from being applied also to the health sector.

References

BARBOSA, M. M. **Inteligência Artificial, *e-persons* e Direito:** Desafios e perspectivas, 2017.

BNAMERICAS. **Argentina advances national AI plan.** Julho, 2019. Available: <https://www.bnamericas.com/en/news/argentina-advances-national-ai-plan> Access August 4th, 2019.

CABRAL, I. **Tudo sobre inteligência artificial:** 10 fatos que você precisa saber. 2018. Available: <https://www.techtudo.com.br/listas/2018/05/tudo-sobre-inteligencia-artificial-10-fatos-que-voce-precisa-saber.ghtml.> Access July 30th, 2019

CANADA. Government of Canada. **Prime Minister announces investment in artificial intelligence to create over 16,000 jobs for Canadians.** Prime Minister of Canada. 2018, June 12. Available: <https://pm.gc.ca/en/news/news-releases/2018/12/06/prime-minister-announces-investment-artificial-intelligence-create>. Access August 10th, 2019.

CELLAN-JONES, R. C.-J., Rory. Stephen Hawking—Will AI kill or save? **BBC News.** 2016, October 20. Available: <https://www.bbc.com/news/technology-37713629>. Access July 30th, 2019.

DATTERI, E. (2013). **Predicting the Long-Term Effects of Human-Robot Interaction:** A Reflection on Responsibility in Medical Robotics. Science and Engineering Ethics, 19(1), 139–160. https://doi.org/10.1007/s11948-011-9301-3

DAWS, R. **Putin outlines Russia's national AI strategy priorities.** 2019, May 31th. Available: <https://artificialintelligence-news.com/2019/05/31/putin-russia-national-ai-strategy-priorities/> Access August 4th, 2019.

GAMEIRO, G. R., Arasaki, A. M., Lira, C. C. D., Neto, S. K., & Stachuk, M. R. (2019). Inteligência Artificial a Serviço da Medicina Brasileira. **Revista de Medicina**, 98(1), i–iii. https://doi.org/10.11606/issn.1679-9836.v98i1pi-iii

FISCHER, J.M.; RAVIZZA, M.S.J. **Responsibility and Control.** Theory of Moral Responsibility. Cambridge University Press, Cambridge, 1998. In: O'Sullivan, S. et al. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. The International Journal of Medical Robotics and Computer Assisted Surgery, 15(1), e1968. https://doi.org/10.1002/rcs.1968

FORBES, (2019). **Wrestling With AI Governance Around The World.** Available: <https://www.forbes.com/sites/insights-intelai/2019/03/27/wrestling-with-ai-governance-around-theworld/> Acess July 29th, 2019.

KONNANGATH, S. (2019). **Abu Dhabi's New Policy on the Use of Artificial Intelligence in the Healthcare Sector.** Court Uncourt, (1), 17–20.

LIAO, S.-H., Chu, P.-H., & Hsiao, P.-Y. (2012). **Data mining techniques and applications** – A decade review from 2000 to 2011. Expert Systems with Applications, 39(12), 11303–11311. https://doi.org/10.1016/j.eswa.2012.02.063.

MAKARY, M. A., & Daniel, M. (2016). **Medical error**—The third leading cause of death in the US. BMJ, i2139. https://doi.org/10.1136/bmj.i2139

MATTHIAS, A. (2004). **The responsibility gap:** Ascribing responsibility for the actions of learning automata. Ethics and Information Technology, 6(3), 175–183. https://doi.org/10.1007/s10676-004-3422-1.

MICHAEL, K., Bowman, D., Jones, M. L., & Pringle, R. (2018). **Robots and Socio-Ethical Implications** [Guest Editorial]. IEEE Technology and Society Magazine, 37(1), 19–21. https://doi.org/10.1109/MTS.2018.2795094

NEBEKER, C., Torous, J., & Bartlett Ellis, R. J. (2019). **Building the case for actionable ethics in digital health research supported by artificial intelligence.** BMC Medicine, 17(1), 137. https://doi.org/10.1186/s12916-019-1377-7

ORTIZ FREULER, J.; IGLESIAS, C. (2018). **Algorithms and Artificial Intelligence in Latin America:** A Study of Implementation by Governments in Argentina and Uruguay, World Wide Web Foundation. Access on August 4th, 2019. Available on: http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Screen_AW.pdf.

O'SULLIVAN, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., … Ashrafian, H. (2019). **Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery.** The International Journal of Medical Robotics and Computer Assisted Surgery, 15(1), e1968. https://doi.org/10.1002/rcs.1968

PAGALLO, U. **Vital, Sophia, and Co.** —The Quest for the Legal Personhood of Robots. 2018. Information, 9(9), 230. https://doi.org/10.3390/info9090230

PESAPANE, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). **Artificial intelligence as a medical device in radiology:** Ethical and regulatory issues in Europe and the United States. Insights into Imaging, 9(5), 745–753. https://doi.org/10.1007/s13244-018-0645-y

PRICE, W. N. (2019, fevereiro 11). **Forbes Insights: Can You Sue An Algorithm For Malpractice?** Available: <https://www.forbes.com/sites/insights-intelai/2019/02/11/can-you-sue-an-algorithm-for-malpractice/#319c53067013>. Access in August 17th, 2019.

PRICE, W. N. I. (2017). Regulating Black-Box Medicine. **Michigan Law Review**, (3), 421–474.

UNESCO. **REPORT with recommendations to the Commission on Civil Law Rules on Robotics** — Digital Library UNESCO. (2017). Available: <https://unesdoc.unesco.org/ark:/48223/pf0000253952>. Access August 20th, 2019.

SRIVASTAVA, S. K. (2018). **Artificial Intelligence:** Way forward for India. Journal of Information Systems and Technology Management, 15(0). https://doi.org/10.4301/S1807-1775201815004

TSCHIDER, C. A. (2018). **Deus Ex Machina:** Regulating Cybersecurity and Artificial Intelligence for Patients of the Future. Savannah Law Review, (1), 177–210.

UNIVERSITY OF TORONTO. G7 Research Group. **Annex B: G7 Innovation Ministers' Statement on Artificial Intelligence.** 2018, March 28th. Available: <http://www.g8.utoronto.ca/employment/2018-labour-annex-b-en.html>. Access July 23 th, 2019.

WACHTER, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. **Science Robotics**, 2(6), eaan6080. https://doi.org/10.1126/scirobotics.aan6080

YİNANÇ, B. Artificial Intelligence era 'opportunity for Turkey'—**Turkey News**, 2019, July 15. Available: <http://www.hurriyetdailynews.com/artificial-intelligence-era-opportunity-for-turkey-144960>. Access August 6th, 2019.

3.4. Desafios da proteção de dados frente aos avanços tecnológicos no âmbito dos municípios e o papel das procuradorias

municipais – *Richard Bassan*[61], *Cláudio Lázaro Aparecido Junior*[62], *Renato Passos Ornelas*[63] *& Bruno Bastos de Oliveira*[64]

Resumo

O presente trabalho propõe a análise do papel das Procuradorias face aos desafios para proteção de dados no âmbito da administração pública municipal. Objetiva propor mecanismos e orientações jurídicas a fim de que haja adequação à Lei Geral de Proteção de Dados. Utilizou-se o método dedutivo, pesquisa bibliográfica e legislação nacional.

Palavras-chave: Avanços tecnológicos; Procuradorias municipais; proteção de dados pessoais.

Abstract

This paper proposes an analysis of the role of prosecutors in the face of data protection challenges within the municipal public administration. It aims to propose mechanisms and legal guidelines in order to comply with the General Data Protection Law. The deductive method, bibliographic research and national legislation were used.

Keywords: Technological advancements. Municipal Attorneys. Protection of personal data.

Introdução

Cuida-se a pesquisa da análise dos desafios enfrentados pelos municípios para adequação à Lei de Proteção de Dados Pessoais no âmbito dos municípios, assim como o papel das Procuradorias, como órgãos consultivos, em orientar o Poder executivo e demais órgãos da estrutura local para que tenham a conduta adequada diante desse regramento.

Os ditames previstos na LGPD poderão ser adequados a cada realidade, de modo que se encaixem nas atividades desempenhadas por cada setor, de modo características sejam atendidas de acordo com suas peculiaridades. Já existe na doutrina afirmação que contém o afastamento de normas municipais regendo cláusulas gerais acerca da proteção de dados pessoais, competência relegada apenas à União, por serem de natureza civil.

[61] Universidade de Marília – UNIMAR

[62] Universidade de Marília - UNIMAR

[63] Procurador no Município de Amparo, São Paulo, Brasil.

[64] Universidade de Marília - UNIMAR

Entretanto, os municípios poderão legislar acerca dos procedimentos internos, ou seja, normas adjacentes e derivadas da LGPD, a fim de orientar os servidores para a condução do trabalho e tratamento dos dados que vierem a ser colhidos, armazenados e utilizados pela administração pública.

Assim, para que essas normas sejam devidamente dotadas de constitucionalidade, relevante a orientação, acompanhamento e indicação do modo como esse regramento deve ser executo nos diversos órgãos que compõem a município, para evitar que haja excessos ou práticas dissonantes do objetivo da LGPD.

Além disso, caberá às Procuradorias a devida responsabilidade por parte do acautelamento de dados judiciais, de ordem fiscal e civil que estiverem sob sua tutela, compreendendo a guarda de informações judiciais e dos bancos de dados fiscais que alimentam as execuções do município. Essas informações já possuíam regramentos próprios de salvaguarda das informações fiscais, sendo a partir da entrada em vigor do regramento geral apenas um reforço para que esses dados pessoais sejam devidamente protegidos.

O trabalho, portanto, delineia o entendimento atual da doutrina no que tange as adequações a serem feitas no município, sendo de extrema importância o alinhamento dos entendimentos acerca das implicações do não cumprimento dos ditames éticos e legais da LGPD. A pesquisa desenvolveu-se por meio do método dedutivo, pesquisa bibliográfica e legislação nacional.

Pretende-se demonstrar a importância das Procuradorias, como órgão consultivo e interventivo diante dos desafios enfrentados para adequação dos municípios na proteção dos dados pessoais, que possuem diversos desníveis em face do avanço expressivo da tecnologia. Em outras palavras, a proteção de dados contra malversação que pode ocorrer e as consequências jurídicas para o município e para o titular das informações precisam ser constantemente analisadas, a fim de que mecanismos e técnicas sejam aperfeiçoadas e assim possam contribui para a sua preservação.

1. Desafios frente aos avanços tecnológicos no âmbito dos Municípios

Os avanços tecnológicos mostram-se reveladores em todas as áreas do desenvolvimento humano, da comunicação, das ciências exatas, biológicas, sociais, humanas, promovendo em suas interfaces o aumento de capacitação de coleta, armazenamento e processamento de uma infinidade de dados e informações que permitem para o campo do direito uma maior e melhor prestação jurisdicional e é neste contexto da era tecnológica da sociedade da informação, que se mostra imperioso o dever de zelar pela privacidade de dados dos cidadãos e usuários no âmbito da Administração Pública, especialmente no plano municipal.

Observa-se que no âmbito da Constituição Federal, a proteção de dados ganha relevo na garantia da inviolabilidade, como também no direito ao acesso à informação, tal como ensina Adalberto Simão Filho, citado por Alexandre Pires Vieira e Cláudio Ralves, 2019:

> Adalberto Simão Filho entende que a Sociedade da Informação estrutura-se na premissa estabelecida pelo art. 5º da Constituição Federal no sentido de que todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo aos brasileiros e aos estrangeiros residentes no País a inviolabilidade de direito à vida, à liberdade, à igualdade, à segurança e à propriedade e se completa no inciso XIV do art. 5º da Constituição Federal, que assegura a todos o acesso à informação.

Entende-se que o princípio constitucional preconizado é fornecedor de garantias reais com consequências positivas e negativas, o entendimento de sociedade da informação alicerçada ao desenvolvimento tecnológico requer novas potencialidades técnicas e legislativas para que se detenham os abusos privilegiados de quem detêm os meios de telecomunicações e os órgãos governamentais que se utilizam da tecnologia da informação por meio de redes interligadas, onde se espera a predominância de todas as áreas do direito na busca da igualdade e da proteção voltadas para a sociedade digital e sua privacidade. (VIEIRA; RALVES, 2019).

Destaque-se neste caminho o entendimento de Alexandre de Moraes sobre o tema:

> O preceito que garante o sigilo de dados engloba o uso de informações decorrentes da informática (...); necessária em virtude da existência de uma nova forma de armazenamento e transmissão de informações deve coadunar-se com as garantias de intimidade, honra e dignidade humanas, de forma que se impeçam interceptações ou divulgações por meios ilícitos. (MORAES, 2014, p. 54).

Observa-se que a legislação brasileira de fato estabeleceu novo marco civil para regulamentar o uso da Internet e o fornecimento dos serviços por meio da Lei nº 13.853/19, preconizando diretrizes e princípios, definindo direitos e deveres, contudo, o tema tem demonstrado a necessidade de reflexões, como também vem gerando questionamentos e insegurança relacionada à proteção de dados pessoais. (BRASIL, 2019). Alessandro Hirata, citado por Rose Talamone, ao retratar os avanços e retrocessos trazidos por essa legislação destaca:

> É sempre muito complicado fazer um documento legislativo dessa forma, porque há muitos interesses envolvidos, dos provedores, empresas de conteúdo, jornalísticas, então chegar a um senso comum, um documento único, não é uma tarefa simples. De certa forma, é normal que se tenha

> retrocessos, porque na hora de fazer uma lei como essa é preciso abrir mão de um pedaço para se chegar a outro. É difícil chegar a um ponto ideal. Em relação à proteção de dados dos usuários, de acordo com os docentes, o Marco ainda não chegou a um modelo adequado, o que traz prejuízos inclusive nas relações internacionais. Isso traz efeitos também nas nossas relações com outros países, principalmente da Europa. A preferência é por um sistema que nós ainda não temos, o notice and take down, que é o sistema europeu. Nele, a pessoa que se sente lesada notifica o provedor, que retira imediatamente o conteúdo do ar. (TALAMONE, 2019).

No âmbito do poder público, notadamente no plano municipal, o desafio é ainda mais revelador quando se pauta, por exemplo, questões relacionadas a utilização das tecnologias e também no cumprimento da lei de proteção de dados, ao se permitir por exemplo, a edição de leis complementares municipais visando abranger pontos não evidenciados na norma federal a pretexto de legislar para alcançar interesses locais, o que pode provocar conflitos com a norma federal.

Ademais, as dificuldades enfrentadas pelos Municípios para concretizar a lei em comento transcende para além da antinomia jurídica, questões de naturezas diversas, tais como, orçamentos menores, estrutura tecnológica deficitária, falta de mão de obra capacitada, contratações, mudanças de gestores e ainda o prazo para se adequar à complexidade trazida pela norma, frente às realidades locais.

Evidenciam-se ainda outros desafios, como se extrai da recente matéria divulgada na Agência Brasil, assim difundidos:

> O desafio maior a ser enfrentado vai ser montar estrutura interna que demonstre funcionalidade. Pessoas capazes de produzir a parte burocrática, estrutura de recebimento de denúncias, investigações externas, processo administrativo, cooperação internacional. Mesmo com possibilidade de supervisão pela Casa Civil, a autoridade deve ter autonomia de fato, diz. Caso isso não ocorra, o vácuo pode ser ocupado por outros entes, como na fiscalização e punição pelo Ministério Público. (AGÊNCIA BRASIL, 2019).

Diante do exposto corrobora-se que regular, normatizar e controlar juridicamente as ferramentas tecnológicas é tarefa imprescindível para assegurar, de que as mesmas, serão utilizadas adequadamente, com responsabilidade primando pela autonomia e direitos constitucionais dos indivíduos de ter a salvo a privacidade de seus dados, contudo, mostra-se premente a estruturação dos Municípios para o enfrentamento dos avanços legislativos e tecnológicos trazidos pela norma, especialmente diante de um cenário em que milhares de Municípios sequer disponibilizam de departamentos estruturados de informática e de pessoal capacitado para o manuseio das novas tecnologias.

2. A importância das Procuradorias Municipais na fiscalização, controle e cumprimento da norma

Traços marcantes de uma evolução digital e comportamental fizeram com que olhares sensíveis fossem lançados para quantidade massiva de informações que circulavam a cada instante na rede mundial de computadores, assim como a destinação que estava sendo dada a elas. Pessoas comuns, detentoras de suas informações cediam – como até então cedem – gratuitamente e voluntariamente seus dados, desconhecem as implicações da malversação desses conteúdos e as implicações jurídicas decorrentes.

Perfazem poucas décadas a expansão do acesso à internet, e nesse meio tempo foi possível verificar que existem poderosas ferramentas de captação e armazenamento de dados cada vez mais sofisticadas dentro de organismos governamentais. Pelo recorte material deste trabalho, a análise se restringirá ao contexto inserido no âmbito dos municípios, cuja atuação das procuradorias, como órgãos consultivos-preventivos, também podem passar a exercer o caráter fiscalizatório de controle e cumprimento da norma.

Os municípios padecem de algumas chagas, consoante aponta Meirelles (2008, p. 783):

> Os mesmos defeitos apontados na administração federal e na estadual são encontrados no âmbito municipal: ausência de racionalização dos serviços, agravada pela falta de planejamento e de pessoal técnico para a execução de empreendimentos públicos reclamados pela comunidade. Urge reformulação de profundidade na administração municipal brasileira para a modernização dos métodos, sistemas e técnicas vigentes nas Prefeituras [...]

As normas referidas são a Lei Geral de Proteção de Dados, como corolário do enfoque ao tratamento dos dados e do fluxo de informações, como também aquelas que forem afetas ao assunto, como o marco civil da internet. As implicações constitucionais civis e penais são consequência de condutas inoportunas e irresponsáveis, que podem ser praticadas no âmbito da administração pública municipal.

Assim, as procuradorias passaram a acumular funções de salvaguarda do cumprimento da LGPD, ainda em período de *vacatio legis* mas que implica no lapso dado à sociedade para que passe a ter conhecimento da lei e também para que aqueles que lidam com fluxos de informações promovam as devidas adequações. Não obstante, a lei tem eficácia *erga omnis* e, portanto, se vale para todos e contra todos, tendo em vista o viés de norma de ordem pública. Meirelles (2008, p. 89) explica:

> As leis administrativas são, normalmente, de *ordem pública* e seus preceitos não podem ser descumpridos, nem mesmo por acordo ou vontade conjunta de seus aplicadores e destinatários, uma vez que contém verdadeiros poderes-deveres, irrelegáveis pelos agentes públicos. Por outras palavras, a natureza da função pública e a finalidade do Estado impedem que seus agentes deixem de

> exercitar os poderes e de cumprir os deveres que a lei lhes impõe (grifos do autor).

Essa adequação prescinde inicialmente de conscientização acerca do alcance e das implicações da lei para os municípios. Servidores públicos e sistemas de captação e armazenamento de dados tem que estar adequadamente postos a cumprir o regramento que emergiu no ordenamento jurídico, malgrado já fazia parte dos preceitos éticos que permeiam a função social da empresa (que inclui também a administração pública).

Nesta senda, os princípios éticos que norteiam a atividade pública, quando condensados, compõem a moralidade administrativa, e por esta razão, é necessário que conheça a fronteira entre o lícito e o ilícito. Meirelles (2008, p. 92) lembra que *"o inegável é que a moralidade administrativa integra o Direito como elemento indissociável na sua aplicação e na sua finalidade, erigindo-se em fator de legalidade."*

Nesse ínterim, também as Procuradorias precisaram se adequar, tomando por base cursos de atualização jurídica no contexto da LGPD, cujo panorama expansionista se espraia por todo o ordenamento jurídico. As regras de ordem pública aplicadas às administrações municipais precisaram ser adequadas, a fim de que as ações necessárias fossem feitas no contexto do que for determinado por lei, consoante o princípio da legalidade que compõe os cinco pilares da atividade administrativa.

É dizer que, consoante aponta Meirelles (2008, p. 89):

> A legalidade, como princípio da administração (CF, art. 37, caput), significa que o administrador público está, em toda a sua atividade funcional, sujeita aos mandamentos da lei e às exigências do bem comum, e deles não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se a responsabilidade disciplinar, civil e criminal, conforme o caso.

Este princípio, de acordo com Di Pietro (2010, p. 63) "[...] juntamente com o de controle da Administração pelo Poder Judiciário nasceu com o Estado de Direito e constitui uma das principais garantias de respeito aos direitos individuais,". Assim, é possível compreender que as ações pautadas na legalidade e cumprimento da LGPD se destinam aos munícipes, e por isso são tão importantes.

Não se mostra viável que somente a Procuradoria, como órgão jurídico máximo na administração pública, acumule todas as funções afetas aos ajustes que devem ser realizados para cumprimento da LGPD. Por esta razão, consoante aduz Limberger Neto (2016, p. 10):

> Os Advogados Públicos são procuradores de Estado e não de governo, cabendo a eles emanar orientações jurídicas e normativas que regulem a atuação do gestor público. Ademais, o primeiro controle de legalidade dentro das administrações municipais é feito pelas procuradorias, por advogados

> públicos concursados que defendem o ente público e a coisa pública como um todo.

Veja-se que além dessas atribuições, ainda se movimenta um contencioso expressivo, principalmente na seara executória fiscal. Não seria de bom alvitre permitir que um órgão com tantas atribuições cumulasse sozinho função de tamanha importância na administração pública municipal. O adensamento de funções municipais é colocado por Oliveira e Bolonha (2018, p. 274) nos seguintes termos:

> O problema da questão municipal não é, conforme foi demonstrado acima, de índole normativa. Para além de compreensões ortodoxas sobre o Estado Federal, o fato é que o Constituinte não foi econômico ao outorgar competências, metas e objetivos aos municípios brasileiros. Além disso, diplomas legais explicitadores de normas jurídicas constitucionais são pródigos em atribuir às municipalidades toda sorte de encargos.

Implica ainda na noção de que a Administração Pública toma decisões todos os dias. Note-se que "o plexo de competências que ela reúne e as demandas que lhe são formuladas exigem interpretação da legislação vigente por parte dos inúmeros agentes incumbidos da gestão pública." (OLIVEIRA; BOLONHA, 2018, p. 297). Ainda assim, a Constituição de 1988 não delimitou a moldura das atribuições dos procuradores, no esquadro da hierarquia institucional.

Apesar disso, defende-se que os órgãos de advocacia pública podem ocupar maior papel nesse cenário. Oliveira e Bolonha (2018, p. 298) sustentam que "aposta decorre do fato de que eles possuem proximidade com a realidade e, portanto, ostentam melhor posição institucional para avaliar situações concretas, as quais outros profissionais ad hoc da advocacia não teriam.". E arrematam concluindo que "a advocacia pública local poderia promover maior consistência e credibilidade na interpretação interna do direito pelas municipalidades." (OLIVEIRA; BOLONHA, 2018, p. 298).

Desse modo, a proposta formulada neste trabalho é que as procuradorias municipais tenham maior autonomia para praticar os atos dentro dos princípios constitucionais e que norteiam a administração pública, a fim de cumpri-los de acordo com o deslinde de suas atribuições. Amarras políticas e institucionais não são saudáveis ao serviço público, que deve ser realizado com a maior heterogeneidade possível, respeitada a hierarquia institucional.

Conclusão

Viu-se ao longo da pesquisa que a LGPD significou um passo importante para o contexto jurídico brasileiro, cujos reflexos atingiram todas as esferas sociais sem distinção. Não obstante, as mudanças requeridas para o cumprimento dos seus ditames representaram desafios no âmbito dos municípios, que historicamente não possuem a estrutura necessária para grandes mudanças.

Certo é que os ditames previstos na LGPD deverão ser cumpridos, respeitado o prazo para que todos possam promover as respectivas e necessárias modificações e adequações, ao passo em que os municípios, peças fundamentais na composição da estrutura federativa, devem promover o encaixe impreterível ao cumprimento do princípio de legalidade.

Como visto, a esteira das atribuições das procuradorias municipais se encarrega de diversas especificidades, e dentre elas assegurar o cumprimento dos ditames legais acerca da proteção de dados em toda a estrutura que forma os municípios. Apesar de concentrar tantas atribuições, é dela a maior capacidade técnica para desempenhar a função, de modo que a finalidade seja atingida.

A seara dos aspectos normativos de atribuições e da repartição de poderes da esfera municipal padece de algumas inconsistências constitucionais, conforme ventilado na pesquisa. Entretanto, apesar de sua peculiaridade, por estar mais próximo do munícipe e dele comungar o maior número de informações, os municípios estão, assim como Estados e a União, dotados das mesmas atribuições em decorrência do tratamento de dados sensíveis, pois possuem a mesma responsabilidade sobre eles.

A importância do trabalho realizado pelas Procuradorias municipais, portanto, se mostrou axiomático, e, embora se tenha apontado que são o órgão que mais agrega condições técnicas para tal mister, a ausência de autonomia, guardadas as proporções hierárquicas, ainda impossibilitam que se faça um trabalho mais completo e mais harmonioso com a sociedade.

Referências bibliográficas

AGÊNCIA BRASIL. **Lei de Proteção de dados traz desafios a empresas, cidadãos e governo:** Novas regras entrarão em vigor em agosto de 2020. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo. Acesso em: 07 out. 2019.

BRASIL. **Lei nº 13.853, de 8 de Julho 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>. Acesso em: 06 out. 2019.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** São Paulo: Atlas, 2010.

CORRÊA, Danilo Maia. **Informatização e violação de privacidade: novas tecnologias e a (in)segurança quanto aos direitos fundamentais.** Disponível em: <https://cepein.femanet.com.br/BDigital/arqTccs/1111400280.pdf.>. Acesso em: 06 out. 2019.

LIMBERGER NETO, Jacob. **Procuradorias municipais no contexto hodierno.** Trabalho de conclusão apresentado ao Curso de Especialização Gestão Pública Municipal da Universidade Federal de Santa Maria. Santa Maria: UFSM, 2016.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro.** São Paulo: Malheiros, 2008.

MORAES, Alexandre de. **Direito Constitucional.** São Paulo: Atlas, 2014.

OLIVEIRA, Daniel Mitidieri Fernandes; BOLONHA, Carlos Alberto Pereira das Neves. A contribuição da advocacia pública local para a superação da baixa dimensão institucional dos municípios brasileiros. **Revista Opinião Jurídica.** Fortaleza, ano 16, n. 23, p.290-309, jul./dez. 2018. Disponível em: <https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/1602/718>. Acesso em: 17 out. 2019.

TALAMONE, Rose. Marco Civil da Internet é destaque no "USP Analisa": Programa debate avanços e retrocessos da legislação e problemas relacionados à proteção de dados dos usuários. **Jornal da USP**, 29 nov. 2017. Disponível em: <https://jornal.usp.br/radiousp/radioagencia-usp/marco-civil-da-internet-e-destaque-no-usp-analisa/.>. Acesso em: 07 out. 2019.

VIEIRA, Alexandre Pires; RALVES, Cláudio. O direito à privacidade frente aos avanços tecnológicos na sociedade da informação. **Revista Jus Navigandi.** Teresina, ano 19, n. 3979, 24 maio 2014. Disponível em: <https://jus.com.br/artigos/27972.>. Acesso em: 05 out. 2019.

Capítulo 4

4. Tratamento de dados pessoais pelas pessoas jurídicas de direito público e de direito privado e formas de controle

4.1. Anonimização de dados genéticos: (in)suficiente na nova Lei Geral de Proteção de Dados? – *Fernando Luís Barroso da Silva Filho*[65], *João Paulo Sanchez de Rezende Goulart*[66] *& Cristina Godoy Bernardo de Oliveira*[67]

Resumo

O presente artigo busca analisar a Lei Geral de Proteção de Dados no que tange à anonimização de dados genéticos. Assim, faz-se necessário abordar as categorias de dados trazidas pela própria lei e desenvolvida por alguns autores, bem como as especificidades dos dados genéticos e técnicas de anonimização, suas particularidades e limitações. A metodologia utilizada foi a pesquisa bibliográfica

[65] Graduando em Direito pela Faculdade de Direito de Ribeirão Preto - USP. E-mail: flbfilho@usp.br

[66] Graduando em Direito pela Faculdade de Direito de Ribeirão Preto - USP. E-mail: joaosrg@usp.br

[67] Professora de Graduação e Pós-Graduação da FDRP-USP. Bacharel e doutora em Direito pela Universidade de São Paulo. Membro de corpo editorial da Frontiers of Legal Research. E-mail: cristinagodoy@usp.br

de livros, periódicos e outras publicações jurídicas e não-jurídicas. As conclusões do trabalho reiteram a insuficiência das técnicas de anonimização e a necessidade de tratamento distinto aos diferentes tipos de dados genéticos, assim como possíveis soluções, tal qual os dados minimizado e regulamentações específicas da ANPD.

Palavras-chave: Anonimização; dados pessoais sensíveis; dados genéticos; Lei Geral de Proteção de Dados.

Abstract

The present paper aims to analyse the General Data Protection Law in reference of the anonymization of genetic data. Thus, it is necessary to address the categories of data brought by the law itself and developed by some authors, as well as the specificities of genetic data and anonymization techniques, their particularities and limitations. The methodology used was the bibliographic research of books, journals and other legal and non-legal publications. The conclusions of the study reiterate the insufficiency of anonymization techniques and the need for different treatment of different types of genetic data, as well as possible solutions, such as minimized data and specific regulations of the Supervisory Authority.

Keywords: Anonymization. Sensitive personal data. Genetic data. General Data Protection Law.

Introdução

A Lei Geral de Proteção de Dados, que entra em vigência no ano de 2020, traz diversas definições acerca dos dados[68] a serem protegidos. Define, por exemplo, dado 4 anonimizado como aquele que, por meio de técnicas, não pode ser identificado (art. 5º, III). O dado anonimizado, portanto, contrapõe-se ao dado pessoal (art. 5º, I), aquele que se pode identificar a pessoa natural (BIONI, 2019, p. 105) — tendo a lei adotado a teoria expansionista.

Segundo BIONI (2019, p. 94), o conceito expansionista, diferentemente do reducionista, é a equivalência da identificabilidade entre um dado e uma informação, direta ou indiretamente, em relação ao sujeito. Tal conceituação, nesse sentido, abarca mesmo aquelas informações em têm a possibilidade, ainda que pequena (identificável), de distinguir alguém. Com isso, poder-se-ia afirmar que todo dado anonimizado seria passível de se transformar em um dado pessoal — o que geraria uma redundância

[68] Entende-se, para os fins do presente artigo, "dado" conforme definido por Russel Ackoff (1989, p. 170): entidade crua que simplesmente existe, sem significado algum além de sua simples existência. No entanto, adiante, o conceito de "dado" misturar-se-á com o conceito de "informação", isto é, dados que possuem significado por conta de relações com outros dados.

normativa entre dado anônimo e dado pessoal —, no sentido de que haveria a viabilidade, como se verá a seguir, de reverter o processo de anonimização, ainda que de forma mais ou menos dificultosa.

Porém, para eliminar essa possível redundância, a lei brasileira, sabidamente, reconhece que a anonimização é falível, que não é perfeita, posto que, no seu artigo 5º, XI[69], dispõe que, para se chegar à anonimização, deverá haver o emprego "de meios técnicos razoáveis e disponíveis no momento do tratamento", e, no artigo 18, § 1º, determina o critério de razoabilidade[70] — BIONI chama isso de filtro da razoabilidade (2019, pp. 96-97), ou seja, o 6 termo identificável não está ligado ao fato da potencialidade de se chegar ao dado pessoal por meio da desanonimização de um dado anonimizado, mas sim de um esforço considerável, isto é, razoável para se chegar àquele. Passemos, então, à definição de dados pessoais.

Dentro da categoria de dados pessoais, merecem maior destaque os dados pessoas sensíveis, visto que podem, com maior facilidade, levar a discriminação de seu titular (VOIGT et al., 2017, p. 111).

A legislação brasileira considera diversos tipos de dados sensíveis, inclusive os biométricos e os genéticos. No entanto, esquece-se os biomédicos (não genéticos), isto é, aqueles relativos à prática de exercícios físicios e à saúde coletados, por exemplo, por meio de *smartwatches* e *smartphones* (AZENCOTT, 2018, p. 3). E, também, dos dados que permitem traçar o perfil comportamental, sendo estes considerados apenas como pessoais, quando, na verdade, deveriam receber tratamento de dados pessoais *sensíveis*, visto que podem levar à completa identificação da pessoa, bem como sua discriminação.

Buscando proteger os dados pessoais, especialmente os sensíveis, surgem as técnicas de anonimização, que, como já mencionado, criam os dados anonimizados. Com tais dados, é, teoricamente, impossível chegar à pessoa física originariamente titular deles. Por isso, para alguns ordenamentos jurídicos, tal qual o europeu, são irrelevantes (EUROPEAN UNION AGENCY, 2018, p. 94), posto que não possuem titular, isto é, não pertencem à esfera jurídica de ninguém.

No âmbito dessa esfera, faz-se essencial a compreensão do direito à privacidade que, com toda certeza, está inserido na categoria de direitos da personalidade, visto que a privacidade é característica intrínseca da personalidade (JUNIOR, 1995). Assim, atrelado à proteção de dados em geral — e, em especial, o genético — encontra-se o direito à privacidade.

[69] Segundo a LGPD, "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".

[70] Nas palavras do autor: "A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios" (BIONI, 2019, pp. 96-97).

Sua conceituação, no entanto, é complexa. Começa-se pela definição de privacidade, o que, para os fins deste artigo, entendemos como o controle sobre as próprias informações. Nas palavras de FRIED (1984, p. 209): *"Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves"*[71].

Desse modo, aos nossos olhos, esse direito — positivado no ordenamento constitucional pátrio no inciso X do artigo 5º — refere-se ao direito de manter o domínio ao nosso redor, o que inclui tudo que faz parte de nós, como corpo, lar, pensamentos, sentimentos, segredos e identidade. Esse direito dá autonomia aos indivíduos para controlar essas partes que lhes pertencem, bem como o poder de permitir quais delas, e em qual extensão, podem ser acessadas por outras pessoas, quais partes podem e querem divulgar (ONN et al, 2005, p. 12).

Tendo em vista esse panorama geral quanto aos dados sensíveis e o direito à privacidade, passa-se, agora, a um aprofundamento, com o objetivo de discutir as especificidades dos dados genéticos e os limites de sua anonimização.

1. Dados genéticos e suas especificidades

Os dados genéticos são, conforme disposto artigo 5º, inciso II, da LGPD, dados pessoais sensíveis. Tendo sido os termos e conceitos de dados pessoais e de dados sensíveis explanados na introdução acima, iniciemos com a delimitação do termo e a exposição das particularidades do conceito de dados genéticos.

Esses dados são sequências de Ácido Desoxirribonucleico (ADN ou, em inglês, DNA). Eles, no entanto, apresentam-se de diversas formas distintas — por exemplo, em trechos ou como sequências completas (FINNEGAN; HALL, 2017, p. 11); sendo possível categorizá-los de acordo com sua qualidade e utilidade, fatores intrinsecamente ligados.

Esses dados, em geral, não são tão sensíveis assim, isso porque, de um indivíduo para outro, cerca de 99% do genoma é simular (FINNEGAN; HALL, 2017, p. 11). Os dados genéticos sensíveis seriam, assim, aqueles capazes de serem relacionados à ancestralidade, a uma determinada população ou doença específica — isto é, *genomic variants*[72] (FINNEGAN; 8 HALL, 2017, p. 11).

Os referidos autores (2017, p. 12) elencam ao menos 4 características dos dados genéticos. Em primeiro lugar, os dados genéticos são fortemente identificáveis, mas isso não os faz "identificáveis por excelência", haja vista que a ligação desse dado ao seu titular depende do tipo de dado genético que se

[71] Em tradução livre dos autores: "A privacidade não é simplesmente uma ausência de informação sobre nós nas mentes dos outros; é antes o controle que temos sobre a informação que nos diz respeito."

[72] As *genomic variants* são justamente trechos diferenciados do DNA, isto é, que não são comuns a todos os indivíduos da espécie humana.

tem ao alcance das mãos. É diferente, portanto, ter acesso à sequência completa, às *genomic variants* ou aos trechos isolados.

Em segundo, esses dados são familiares, isto é, apesar de serem do titular, também é possível que se identifique seus parentes, a depender do contexto. Em terceiro lugar, os dados genéticos são considerados estáticos, visto que mantém sua relevância e importância ao longo do tempo. Caso haja redução de sua utilidade, ela é ínfima.

Em último lugar, não se pode negar que tais dados são especiais. Além de serem únicos para cada titular (salvo raríssimas exceções), ainda são dotados de incrível mística — no sentido de despertarem a curiosidade e, até mesmo, inquietação por parte da população quanto aos seus usos.

Essa mística não é injustificada. Cita-se aqui duas pesquisas impressionantes. Os pesquisadores LIPPERT et al (2017, pp. 10169-10170) conseguiram prever traços físicos — tais quais, altura, peso, cor da pele, estrutura facial, voz, cor dos olhos e mais — por meio do dado de *whole-genome sequencing*.

Em outras palavras, através da sequência completa do genoma, os pesquisadores conseguiram formar um perfil do titular, sem qualquer outra informação a mais, demonstrando o poder desse tipo de dado genético. As aplicações para essa pesquisa são infinitas, servindo, por exemplo, para uso forense de mais alto nível, como forma de identificar indivíduos que cometeram delitos da mais alta gravidade e que não tenham seu perfil cadastrado aos bancos de dados genéticos[73].

Outro grupo de pesquisadores, GYMREK et al. (2013, pp. 321-24), conseguiu feito impressionante valendo-se de trechos de DNA, utilizados em combinação com metadados[74] — tais quais o sobrenome, a idade e o estado de residência do indivíduo. Dessarte, com ferramentas computacionais simples, os pesquisadores foram capazes de desenvolver método eficaz para identificar os parentes dos titulares. Isso tudo feito por meio de bases de dados abertas que apresentam o trecho de DNA juntamente com o respectivo sobrenome ao qual ele está associado.

Com essa compreensão quanto aos dados genéticos, parte-se a analisar os limites da anonimização desse tipo específico de dado.

2. Os limites da anonimização

[73] Aos moldes do que se encontra disposto no artigo 9º-A e seus parágrafos da Lei 7.210/84 (Lei de Execução Penal). Sem questionar aqui outras implicações, inclusive as de cunho ético, visto que fugiria do escopo do presente artigo.

[74] Aqui entendidos literalmente, isto é, meta + dados: "dados transcendentes" ou "dados que trazem reflexão sobre si".

As técnicas utilizadas para anonimizar dados são classificadas de diversas formas, a depender do autor. Podemos sintetizá-las com a seguinte partição: algumas garantem a anonimização estatística, enquanto outras, por meio de criptografia (AZENCOTT, 2018, p. 9).

Como representantes da primeira técnica, pode-se citar a randomização, generalização (VOIGT et al., 2017, p. 13) e supressão (BIONI, 2018, p. 105); no segundo, chave simétrica, assimétrica e, como mencionado por AZENCOTT (2018, p. 8), o blockchain. Analisemos, então, cada uma dessas técnicas.

A randomização consiste em alterar a precisão de determinado dado, removendo a ligação entre este e o indivíduo. Com esse instrumental, quando os dados se tornam suficientemente não identificáveis, não se conseguirá vinculá-lo a um indivíduo específico (VOIGT et al., 2017, p. 13).

O problema, tanto aqui quanto na generalização, é a possibilidade de cruzar dados anonimizados com outro banco de dados públicos. AZENCOTT (2018, p. 5) cita o exemplo do governador de Massachusetts: seus registros médicos foram identificados por cruzamento de dados médicos anônimos com registros de recenseamento eleitoral. Além disso, diz a autora na mesma página, no caso de sequências genômicas em que o número de variáveis sensíveis é grande, corre-se o risco de perder toda a utilidade do armazenamento desses dados, pois, para anonimizar dados dessa natureza, há de se deletar a maioria dessas variáveis.

A generalização é generalizar ou diluir as características dos titulares dos dados, alterando, destes, a respectiva escala ou ordem — uma região em vez de uma cidade, um mês em vez de uma semana (VOIGT et al., 2017, p. 13).

Já a supressão, como o próprio nome diz, é o método pelo qual certos valores dos atributos são substituídos por um asterisco '*', isto é, suprimidos; todos ou alguns valores de uma coluna podem ser substituídos por '*'. Por exemplo, no caso do CPF de uma pessoa registrado num banco de dados, é mais interessante suprimi-lo todo, "por ser por ser um identificador capaz de diferenciar até mesmo pessoas homônimas" (BIONI, 2018, p. 105). Entretanto, é uma técnica a ser usada com cautela, haja vista a possibilidade de desvinculação por completo, o que traria uma inutilidade no armazenamento dos dados, porquanto, em um exemplo extremo, se se suprime todos os dados de uma pessoa de uma base de dados, sobrariam apenas asteriscos como "informações", não tendo sentido seu armazenamento. Dessa forma, caso a caso, deve-se analisar o que deverá, de forma equilibrada, ser suprimido.

Por fim, as chaves simétrica e assimétrica e o blockchain são técnicas de encriptação, isto é, meios pelos quais os dados se tornam inutilizáveis para aqueles que não detêm a chave para o acesso. Consideram-se seguros, com tais técnicas, os dados em que o custo para descriptografá-los seja maior do que os próprios dados, ou se, ao fazer a decriptação destes, não se chegasse a mais nenhum valor deles (FINNEGANN; HALL, 2017, p. 20). No que tange ao risco desses métodos, é que uma ou algumas

pessoas terão o acesso aos dados brutos dessas pessoas, porque serão o(s) guardião(ães) dessas chaves, correndo-se o risco de haver vazamentos por parte deles.

Vale mencionar, no entanto, que os dados que ainda possuem algum grau de identificabilidade quando se considera alguma informação adicional devem ser considerados pseudoanonimizados (VOIGT et al., 2017, p. 15). De forma paralela ao que foi dito sobre os dados anonimizados, tanto a legislação européia como a brasileira ainda atribuem a eles proteção legal, ainda os considerando como dados pessoais (EUROPEAN UNION AGENCY, 2018, p. 94).

O ideal seria que apenas os próprios titulares desses dados ou os órgãos autorizados tivessem acesso a essa informação — que pode ser vista como uma chave de encriptação, haja vista que, apenas por meio de algoritmos, pode-se chegar a informação original. No entanto, diversos são seus usos.

Em vários países, antes de serem analisados ou compartilhados, os dados sensíveis passam pela anonimização. E, por isso, com os dados genéticos não seria diferente. Nesse sentido, para ilustrar, peguemos um paciente que tenha participado de um estudo relacionado à AIDS em uma faculdade de medicina. Chamemo-lo de João. Se a entrevista dada à pesquisa fosse anonimizada, João não poderia ter registrada, em um banco de dados, sua identidade associada ao status da doença (ele tem AIDS), bem como a outras características sensíveis que pudessem identificá-lo (AZENCOTT, 2018, p. 3).

Porém, mesmo bem-sucedida, a anonimização não seria suficiente para evitar esse rastreio. Porquanto, por meio de outras técnicas de reversão, seria possível chegar ao paciente numa espécie de "desanonimização". Isso, nesse caso, é possível utilizando dados auxiliares que facilitariam a identificação (PORTER, 2008, p. 2).

Para exemplificar, voltemos ao João do exemplo anterior. Se, nessa mesma pesquisa, ele tivesse sido o único paciente idoso da amostra, ficaria praticamente evidente que se trataria do referido paciente.

Sendo assim, diversos estudos têm mostrado a limitação da anonimização. Em razão disso, alguns autores, como VOIGT et al. (2017, p. 14), recomendam que as empresas, os pesquisadores e outras entidades se valham dos "dados minimizados", isto é, a não requisição de certos dados pessoais para que, desde o início, eles sejam anonimizados. Tal proposição é reconhecida pela nossa lei por meio do princípio da necessidade, previsto em seu artigo 6º, inciso III, da LGPD. Ele estabelece que o tratamento da anonimização deve se limitar ao mínimo (de dados) necessários para a realização de suas finalidades.

Resta ver, no entanto, como se daria o dado genético minimizado. Uma provável hipótese seria trechos ao invés da sequência completa, reduzindo as chances de identificação para além das técnicas de anonimização utilizadas. Contudo, vale dizer que o problema não estaria solucionado, visto que, caso se

tratasse de uma *genomic variant* — situação em que, mesmo se utilizando de dados minimizados e de técnicas razoáveis de anonimização, ainda existiria clara possibilidade de reversão.

Conclusão

Buscou-se demonstrar as insuficiências da anonimização e do tratamento dos dados genéticos na referida lei, com destaque a alguns pontos.

Primeiramente, critica-se o tratamento homogêneo aos dados genéticos, haja vista suas especificidades e possibilidades de categorização.

Em segundo lugar, os termos adotados pela Lei Geral de Proteção de Dados e a incapacidade das técnicas de anonimização que podem levar à utilização de um dado, tecnicamente não anônimo, como anônimo.

Os pontos, contudo, não são de todos negativos. A lei, em alguns momentos, reconhece que as técnicas de anonimização não são suficientes, devendo os controladores se valerem de outros métodos que não a anonimização, tal qual ao mencionado "dado 8 minimizado". Dessa forma, apesar de a anonimização ser uma técnica falível — e, por isso, em algumas circunstâncias, insuficiente —, nossa lei garante a suficiência na medida do possível, conforme demonstrado na introdução deste trabalho.

Ademais, eventuais falhas quanto ao tratamento diferenciado dos dados genéticos não devem, no presente momento, gerar grandes problemas, visto que a lei ainda não está vigente e a Autoridade Nacional de Proteção de Dados (ANPD) não está em pleno funcionamento. Desse modo, é de se esperar que a diferenciação ocorra em regulamentação específica — seja por meio de lei stricto sensu, seja por meio de instruções normativas da ANPD.

Referências bibliográficas

ACKOFF, Russel L. From Data to Wisdom. In: _____. (org.) Ackoff's Best: His Classic Writings on Management. Nova York: John Wiley & Sons, 1999.

AZENCOTT, Chloe Agathe. Machine Learning and Genomics: Precision Medicine versus Patient Privacy. **Philosophical Transactions. Series A, Mathematical, physical and engineering sciences.** N. 13,376 set., 2018. Disponível em: https://www.ncbi.nlm.nih.gov/pubmed/30082298.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. **Handbook on European data protection law.** Luxemburgo: Publications Office of Europe Union, 2018.

FINNEGAN, Thomas; HALL, Alisson. **Identification and genomic data.** Cambridge: PHG Foundation, 2017.

FRIED, Charles. Privacy. In SCHOEMAN, Ferdinand D. (org.). **Philosophical dimensions of privacy.** New York: Cambridge University Press, 1984, pp. 203-22.

GYMREK, Melissa et al. Identifying Personal Genomes by Surname Inference. **Science.** vol. 339, pp. 321-24, 18. jan. 2013.

JUNIOR, Paulo José da Costa. **O Direito de Estar Só:** Tutela Penal da Intimidade. São Paulo, Revista dos Tribunais, 1995.

LIPPERT, Cristoph et al. Identification of Individuals by Trait Prediction Using Whole-Genome Sequencing Data. **PNAS**, vol. 144, n. 38, set. 2017, pp. 10166-10171. Disponível em: https://www.pnas.org/content/114/38/10166

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large sparse datasets:** a decade later, 2019.

ONN, Yael, et al. **Privacy in the Digital Environment.** Haifa: Haifa Center of Law & Technology, 2005.

PORTER, Christine. De-Identified Data and Third Party Data Mining: The Risk of ReIdentification of Personal Information, **5 Shidler J.L. Com. & Tech.** 3, sep. 23, 2008. Disponível em: http://www.lctjournal.washington.edu/Vol5/a03Porter.html

VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)** - A Practical Guide. Gewerbestrasse: Springer International Publishing, 2017.

4.2. O tratamento de dados pessoais pelas empresas públicas e sociedades de economia mista e a realização de licitações como

operacionalização de políticas públicas – *Rafael Rizzi*[75] *& Yago Funchal de Godoy*[76]

Resumo

O presente trabalho tem como objetivo analisar a possibilidade do tratamento e uso compartilhado de dados pessoais, previstos na Lei geral de proteção de dados, por empresas públicas e sociedades de economia mista na operacionalização de políticas públicas por meio da realização de licitações. **Palavras-chave:** Dados pessoais; Administração pública; políticas públicas.

Abstract

This paper aims to analyze the possibility of processing and shared use of personal data, based on the General Data Protection Law, by public companies and mixed economy companies in the operationalization of public policies through the execution of licitations.

Keywords: Personal data. Public administration. Public policies.

Introdução

No ordenamento jurídico brasileiro não é dado ao Estado a capacidade de criação de Empresas Públicas ou Sociedades de Economia Mista sem que haja prévia lei que expresse um relevante interesse coletivo ou imperativo de segurança nacional para tal intervenção econômica, conforme determinado no artigo 173 da Constituição federal.

Neste contexto é que se insere o dever de licitar destas empresas, sendo atualmente regulado pelas disposições da Lei 13.303/2016 que indica algumas finalidades a serem ser perseguidas pelos procedimentos licitatórios das Estatais, de forma à assegurar que as referidas entidades de Administração Indireta selecionem as propostas mais vantajosas.

A literatura acerca das licitações no âmbito das Empresas Públicas ou Sociedades de Economia Mista indica que estas podem ser um instrumento de consecução de políticas públicas, principalmente as

[75] Mestrando em Direito da Sociedade da Informação no Centro Universitário das Faculdades Metropolitanas Unidas. Pós-graduado em Direito Civil pela PUC Minas. Bacharel em Direito pela Faculdade de Direito de São Bernardo do Campo. Advogado.

[76] Pós-graduando em Direito Processual Civil pela Faculdade de Direito São Bernardo do Campo, Pós-graduando em Direito Administrativo e Constitucional na Escola Paulista de Direito, Bacharel em Direito pela Faculdade de Direito de São Bernardo do Campo, Advogado.

relacionadas a atuação do Estado em prol do desenvolvimento local, regional ou da promoção de práticas ecologicamente sustentáveis.

A Lei Geral de Proteção de Dados (LGPD) estabelece que a administração pública poderá realizar o tratamento de dados pessoais e utilizá-los de forma compartilhada quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Com relação as Empresas Públicas ou Sociedades de Economia Mista, a Lei Geral de Proteção de Dados prevê que quando tais entidades estiverem operacionalizando políticas públicas e no âmbito de sua execução, elas terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, desta forma, considerando que tais entes são obrigatoriamente criados por lei, que sua atuação no âmbito das contratações públicas se pauta por um contrato ou instrumento congênere, busca-se compreender, no presente trabalho, se as Empresas Públicas ou Sociedades de Economia Mista poderiam realizar o tratamento de dados pessoais e utilizá-los de forma compartilhada quando necessários nos processos licitatórios, dado que a elas é conferido o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público quando estiverem operacionalizando políticas públicas como por exemplo licitações que tenham como um de seus objetivos a promoção do desenvolvimento local, regional ou de práticas ecologicamente sustentáveis.

Desenvolvimento

A atuação do Estado considerada no âmbito das Empresas Públicas e Sociedades de Economia Mista demanda alinhamentos mínimos com vistas à compreensão da conformação constitucional que de um lado autoriza ao Estado a exploração da atividade econômica e por outro vincula esta atividade a uma série de situações próprias que se prestam a orientar esta atuação.

A ordem econômica brasileira prestigia o protagonismo do ambiente mercadológico à atores não estatais, consagrando de forma fundamental o sistema de economia capitalista, na medida em que se funda na propriedade dos meios de produção, na organização da empresa e na atividade do empresário (FERREIRA, 2019. p. 24), contudo, sem que exclua ou impeça a participação do Poder Público. De modo a proporcionar uma conformação da atuação do Estado, sujeita a limites e regramentos próprios, tendo em vista a busca pelo bem público e a consecução de valores previstos constitucional prevê (FERREIRA, 2019. p. 26).

As Empresas Públicas e Sociedades de Economia Mista servem como instrumentos para realização e materialização da participação do Estado na ordem econômica (FERRAZ, 2019. p.86), tal participação

pode se dar também pelo uso do grande poder de compra estatal, por meio das licitações, na busca pela realização dos objetivos constitucionais.

No caso das políticas de desenvolvimento regional e incentivo ao empreendedorismo.

> O uso de licitações pode ser uma opção viável, principalmente em se tratando ela de ser uma possibilidade interessante de acesso ao mercado para MPEs regionais. Mas, para tanto, ela precisa ser amparada por uma engenharia institucional, mormente no que tange a fazer a ligação entre o tratamento favorecido e diferenciado dado a MPEs em licitações e o estímulo a que as empresas regionais de tais portes participem e vençam certames ocorridos nas regiões em que as mesmas se encontram sediadas (BARADEL, 2011, p. 70)

O advento da Lei Geral de Proteção de Dados prevê requisitos para que as Empresas Públicas e Sociedades de Economia Mista possam realizar o tratamento de dados pessoais e utilizá-los de forma compartilhada, tal autorização tem o potencial de tornar mais eficiente a realização de tais procedimentos licitatórios e, consequentemente, impactar positivamente as políticas públicas operacionalizadas por meio das licitações.

Conclusão

Considerando que a revisão de literatura realizada acerca do uso de licitações para a operacionalização de políticas públicas, a partir da análise da Lei Geral de Proteção de Dados, especialmente dos seus artigos 7º e 24, conclui-se que é possível a utilização compartilhada e o tratamento de dados pessoais na realização de licitações que, na busca de satisfazer as necessidades de bens e serviços da administração pública, operacionalizem políticas públicas.

Referências bibliográficas

ARAGÃO, Alexandre Santos de. **Regime jurídico das empresas estatais.** Enciclopédia jurídica da PUC-SP. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em https://enciclopediajuridica.pucsp.br/verbete/44/edicao-1/regime-juridico-dasempresas-estatais. Acesso em 02 Out. 2019.

BARADEL, Evandro Meira. **Licitação como instrumento de política pública de desenvolvimento regional.** 2011. 91 p. Dissertação (MPGPP) - Escola de Administração de Empresas de São Paulo. Fundação Getúlio Vargas. 2011.

FERREIRA, Sérgio de Andréa. História e Regime Constitucional da Atividade Empresarial Estatal. *In:* FERRAZ, Sérgio (Organizador). **Comentários sobre a Lei das Estatais (13.303, de 30.06.2016).** São Paulo: Malheiros, 2019.

FERRAZ, Sérgio. Disposições Preliminares da Lei. *In:* FERRAZ, Sérgio (Organizador). **Comentários sobre a Lei das Estatais (13.303, de 30.06.2016).** São Paulo: Malheiros, 2019.

PEREIRA, Cesar A. Guimarães. Processo Licitatório das Empresas Estatais: Finalidades, Princípios e Disposições Gerais. *In:* JUSTEN FILHO, Marçal (Organizador). **Estatuto Jurídico das Empresas Estatais, Lei 13.303/2016** – "Lei das Estatais". 1. Ed. São Paulo: Revista dos Tribunais, 2016.

4.3. A crise do controle na era da informação: o direito à portabilidade de dados como instrumento de efetivação da autodeterminação do homem no ambiente digital – *Gabriel de Aguiar Tajra & Cíntia Rosa Pereira de Lima*

Resumo

Pretende-se, no decorrer deste artigo, desenvolver possibilidades normativas para efetivação do instituto da portabilidade de dados mediante potencialização dos atributos da titularidade, primordialmente acerca do controle dos dados pelo usuário, em consonância aos atos normativos formulados pela União Europeia, tais quais o Regulamento Geral sobre Proteção de Dados, as Directivas 2013/37/EU e 95/46/CE e estudos e pareceres expedidos pelos órgãos executivos europeus para fins de regulamentação de operabilidade da portabilidade de dados, tais quais os *Guidelines on the right to data portability*, dentre os quais nos interessa os Working Parties de nº 29 e 242, bem como em consonância ao *California Consumer Privacy Act of 2018 (Assembly Bill n. 375*), permitindo, assim, situar o ser como agente autodeterminado e senhor de sua significação no ecossistema digital.

Palavras-chave: Tratamento de dados pessoais; titularidade e controle; intersubjetividade humana.

Abstract

This article intends to develop nomartive possibilites to reach the effectiveness of the data portability right, upon the potentiation of its titularity attributes, especialy those concerned to data control. This, in consonance to the Europe Union standards, as the General Data Protection Regulation (GDPR), the Directives 2013/37/EU, 95/46/CE and the Guidelines on the right to data portability, in which includes, primordialy, the Working Parties of n. 29 and 242, as well as the California Consumer Privacy Act of 2018 (Assembly Bill n. 375), enabling to stablish the data subject as self-determined and self-possessed of its own meaning into the digital ecosystem.

Keywords: data treatment. Titularity and control. Human intersubjectivity.

Introdução

"Tudo que era diretamente vívido se afastou numa representação"

Guy Debord

1. A emergência da cacofonia digital: do contexto do *small* ao *Big Data*

O século XX experimentou uma determinada crise de visão de mundo promovida pela virada linguística, ante a percepção dos limites da dimensão do homem pela linguagem – não só por ela os fenômenos são expressos e significados, como por ela a significação e a expressão são possíveis, mediante ato e vigência que se faz sempre perante o social e ao outro, mas nunca per si[77].

O homem, em cada ação, produz uma representação no social, constituindo fenômeno dotado de significação, pois "é pela realidade humana que o valor aparece no mundo" (SARTRE, 2015, p. 14). Por conseguinte, aparecendo no mundo, é aparência sensível a ser compreendida. Isto significa dizer, de forma mais profunda e elementar, que o homem atribui valor à sua existência mediante a própria manifestação que assume.

Em concomitância, o desenvolvimento técnico contemporâneo, assentado primordialmente nas tecnologias da informação, viabilizaram a potencialização da realidade fática mediante o estabelecimento de uma rede comunicacional permanente, imediata e de dimensões globais (LÉVY, 1999, p. 15), permitindo uma desmaterialização do social[78] e uma respectiva digitalização, mediante produção de coleta de dados variáveis, volumosos e com respectivo armazenamento em data centers e análises e minerações de dados (*data mining*) em dimensões exponenciais, que se sucedem de forma tão acelerada, bem como concentrada e centralizada, de forma a inviabilizar o controle do homem de sua própria significação no mundo, posto que, no ambiente virtual – interrelacionado com a realidade material – a dimensão da quantificação e qualificação de sua representação por dados não é por ele próprio conhecida, valorada, manipulada ou comercializada[79], mas sim mediada pelas empresas,

[77] A percepção da linguística como atributo inerente ao homem, mas também como estrutura limitante de sua dimensão de existência e de compreensão, abre zona de análise antes obscura e ignorada, bem averiguada pelas análises de Sartre e Heidegger: "Mesmo que Deus não exista, há ao menos um ser cuja existência precede à essência, um ser que existe antes de poder ser definido por algum conceito, e que tal ser é o homem ou, como diz Heidegger, a realidade humana. Que significa, aqui, que a existência precede a essência? Significa que o homem existe primeiro, se encontra, surge no mundo, e se define em seguida" (SARTRE, 2014, p. 25).

[78] Por desmaterialização entende-se, simplificadamente, a "perda da forma material" (LEMOS, 2012, p. 38).

[79] A conceituação de *Big Data* permeia a análise dos atributos inerentes à sua qualidade, razão pela qual a 3 doutrina subdividiu seu significado consoante o estudo referente a seus atributos, arquitetura própria ou em

proprietárias do meio e da arquitetura digital, de forma a reestruturar a interação entre o homem e o social, ante o aprimoramento dos métodos de armazenamento, transformação e transmissão das representações simbólicas (LÉVY, 1999, p. 84-85).

Tal reestruturação é marcada por uma reconfiguração das formas de produção e comunicação da prática humana, decorrentes da revolução tecnológica hodierna (PONS, 2013, p. 27), impondo-se uma nova cultura e – por constituir a identidade pessoal o processo pelo qual um ator social reconhece a si perante o outro e constrói significados com base em uma dada cultura estruturada (CASTELLS, 2010, p. 22) –, respectivamente, uma nova estrutura de significação da intersubjetividade humana em meio a arquitetura e ao ambiente digital.

Com esta grande diversidade de informações "o ciberespaço tornou-se uma ágora eletrônica global em que a diversidade da divergência humana explode numa *cacofonia* de sotaques" (CASTELLS, 2003, p. 114-115 – grifo próprio), isto é, ampliou-se a viabilidade de produção da informação, potencializando, por um lado, a emergência de individualidades, mas ofuscadas pela dimensão das informações disponíveis dissonantes.

Neste ínterim, entre a percepção do valor como qualidade atribuída pelo próprio homem mediante sua aparição no mundo, mas em dimensão de volume sequer capaz de ser completamente analisada pela própria humanidade – tanto no ambiente físico, quanto no digital –, o homem encontra-se perdido[80].

Se o homem se põe no mundo e deve, por este meio, ser capaz de significá-lo por sua própria determinação, é fato que a utilização dos dados – invariavelmente uma extensão da significação do homem, usurpada, social e economicamente, pelos controladores dos dados – sem o respectivo controle

comparação perante outros conceitos. Não obstante, a doutrina bem alinhou qualidades e características próprias ao conceito quais sejam: volume, variedade e velocidade, ante a publicação de artigo intitulado "3D Data Management: Controlling Data Volume, Velocity, and Variety", por Doug Laney, publicado em fevereiro de 2001.

[80] O contexto sócio-histórico da revolução tecnológica pode ser analisada pela interessante metáfora proposta por Nicolau Sevcenko, iminente falecido professor da USP, que dispôs três partes da experiência tecnológica em correlação a uma experiência em montanha russa, perpassando a ascensão inicial com expectativas otimistas – pensado o período entre o século VI e meados do século XIX, quando o homem pode dominar conhecimentos especializados e forças naturais –, a queda decorrente da perda de referência espacial e temporal, ante processos tecnológicos capazes de facilitarem a intercomunicação em escala global e a última fase, consistente no loop, em que , contemporaneamente, a "aceleração das inovações tecnológicas se dá agora numa escala multiplicativa, uma autêntica reação em cadeia, de modo que em curtos intervalos de tempo o conjunto do aparato tecnológico vigente passa por saltos qualitativos em que a ampliação, a condensação e a miniaturização de seus potenciais reconfigura completamente o universo de possibilidades e expectativas, tornando-o cada vez mais imprevisível irresistível e incompreensível" (SEVCENKO, 2001, p. 14-7).

pelo titular resulta na perda de sua autodeterminação, bem como no processo por nós denominado de fragmentação do homem[81].

Entretanto, antes mesmo de se significar um sujeito ou existência no mundo, deve-se controlar o processo pelo qual se dá a significação. E, consoante se depreende da perda do controle pelo homem de seus próprios dados – e consequentemente de seu próprio significado, em sendo o dado uma extensão de si –, o homem não mais é capaz de determinar e dispor de sua extensão simbólica.

Em face do desenvolvimento tecnológico desenfreado, a realidade dotou-se de tantas e tamanhas significações, que se rompeu o mundo da lógica, da sequencialidade e linearidade (COELHO, 2012, p. 76), revertendo o quadro institucional pela transposição do small data ao contexto do big data, marcado pela otimização da velocidade, variedade e volume da informação (LANEY, 2001), em que a dominação ideológica opera por uma lógica técnicocientificista de ofuscamento da ação comunicativa por um programa compensatório mediatamente observável por disfunções da livre-troca comercial (HABERMAS, 2014, p. 105)[82], dificultando a estruturação de um sistema normativo adequado à nova dinâmica ou 6 mesmo um processo de reconfiguração dos conceitos jurídicos pela expansão metafórica, ante o abalo ao núcleo de sua constituição (MARANHÃO, 2016, p. 29).

Esta percepção da crise do controle traz à baila a real dimensão da era da informação. Para além do direito à privacidade, trata-se de uma questão de titularidade e controle referente à própria personalidade humana, vez que, mediante os atributos deste último instituto, o homem materializa sua dimensão axiológica.

[81] O que se pretende, ao expor a fragmentação do homem na era digital, é esclarecer determinada condição social 5 prévia à perda da identidade do homem analisada por Manuel Castells. Isto porque, consoante seu próprio entendimento: "By identiy, as it refers to social actors, I undestand the process of constructing meaning on the basis of a cultural attribut, or a related set of cultural attributes, that is given priority over the sources of meaning" (CASTELLS, Manuel. The power of identity. 2 ed. Singapore: Wiley-Blackwell, 2009, p. 6).

[82] Neste mesmo sentido: "Nesse cenário flutuante, a mais-valia relativa é somente uma metáfora obsoleta que não 6 resiste à prova da cultura empresarial ou da lógica digital. Alguns pesquisadores chegam a conslusoes segundo as quais capital e trabalho assalariado ter-se-iam tornado supérfluos há tempos. Todavia, após terem-se apercebido da morte terminal da mais-valia relativa, fazem-na ressurgir como mais-valia cognitiva. De acordo com ese enfoque de cunho cognitivo, o trabalho mental – somo saber necessário Às inovações tecnológicas – não seria aproveitável pelo capital como força produtiva, sendo o saber 'biologicamente' afixado na mente do operador. Essa posição percebe a importância do momento da invenção-cognição, mas o encerra num organicismo mentalista isolado das relações comunicaativas dominantes, para sobrepor o mistério da mais-valia: isso depende de sua incapacidade de ver a economia comunicacional como determinante dos novos fluxo globalizantes" (CANEVACCI, 2018, p. 34).

É nesta perspectiva que o instituto da portabilidade de dados – compreendido como o direito de receber cópia em formatação corrente, estruturada e de leitura automática de dados que lhe digam respeito, bem como transferi-lo sem obstruções pelo controlador, nos termos do art. 20 (1) do Regulamento 2016/679 (General Data Protection Regulation) – constitui verdadeiro direito da personalidade atinente ao desenvolvimento humano, de forma a permitir a reapropriação do homem de sua própria significação intersubjetiva e exteriorizada, mesmo porque afigura-se como instituto central de potencialização de outros direitos digitais, como o acesso, correção, eliminação ou consentimento ao tratamento dos dados.

Não obstante, a recepção do instituto pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018) como direito do titular em seu art. 18, V, é possível prever possíveis problemáticas inerentes à estruturação normativa adotada, tal qual o requisito implícito da viabilidade de operabilidade técnica entre controladores para efetiva transferência de dados pela exigência da formatação comum dos arquivos, bem como a desnecessidade de transmissão da cópia dos dados quando já anonimizados (art. 18, §7º).

Portanto, para efetivação da portabilidade de dados como instituto normativo apto a garantir a autodeterminação do usuário no ambiente digital, cumpre repensar estruturas normativas adotadas pela LGPD, objetivando sua operacionalização em consonância aos atributos da titularidade, notadamente quanto ao controle deste com seus respectivos dados, permitindo situá-lo como agente autônomo dentro da estrutura da rede.

2. Sociedade do descontrole

A sociedade contemporânea, ao estruturar-se para além do mundo analógico, mas também em uma nova dimensão de progressão espaço-temporal – qual seja o âmbito digital –, pressupôs-se desterritorializada de início, permitindo uma desregulamentação das ações e expectativas na seara da rede, seguida por evidente instabilidade em diferentes espectros da sociedade, tal qual o âmbito jurídico, econômico e mesmo comunicacional.

Por decorrência, observou-se uma determinada ocupação do digital por empresas de tecnologia – primordialmente aquelas centradas no estudo das tecnologias da informação (TICs) –, ante o poderio econômico capaz de enfrentar as adversidades econômicas e as instabilidades jurídicas pela formação e estabilização das expectativas na rede, estruturando a arquitetura e o ambiente digital segundo interesses de grandes corporações (CASTELLS, 2010, p. 397) e condicionando a apropriação da significação do ser pelos interesses sociais dominantes, em prejuízo da autodeterminação informacional do homem no ambiente digital.

Isto porque, como fruto material do desenvolvimento tecnológico do capital moderno, acompanhado da ocupação da rede pelos *players* econômicos de maior controle e relevância política, rompeu-se a

liberdade de representação social e simbólica no digital pela mediação tecnológica da ação social[83], abarcando invariavelmente a extensão de tais efeitos na formação do espírito autoconsciente, notadamente também pela relação entre a ação comunicativa e o processo de individuação do ser controlado pela socialização simbólica (HABERMAS, 2014, p. 42).

Assim, a potencialidade do acúmulo de mensagens pelo aprimoramento das tecnologias da informação – atinentes à produção, coleta e armazenamento da informação, expandindo-se, consequentemente, também a memória coletiva –, resultou numa constante *vigilância* dos indivíduos, viabilizada pela exposição massiva das informações particulares na rede, materializando uma nova espécie de controle.

Controle este que, diferentemente do das *sociedades disciplinares*, situadas por Foucault nos séculos XVIII e XIX e organizadas sobre o confinamento dos corpos por distribuição no espaço e ordenação no tempo voltados à produção, ora modulam a distribuição e o acesso à informação, convertendo-se a realidade social: "Não se está mais diante do par massa-indivíduo. Os indivíduos tornaram-se '*dividuais*', *divisíveis*, e as massas tornaram-se amostras, dados, mercados ou '*bancos*'" (DELEUZE, 2000, p. 2 – grifo próprio).

Por conta desta nova via do controle sobre os corpos e, ainda mais, sobre a mente do sujeito ou mesmo da coletividade constituída como memória que Deleuze aventurou-se em denominar a contemporaneidade de sociedade do controle.

Não obstante, uma filosofia que preze pelo aspecto antropológico não pode abandonar a dimensão do homem fundante de tais entidades da realidade. Isto é, não se pode esquivar de um fato: a sociedade é fruto da socialização do homem, que ora auto explora-se no seio social[84].

Assim por exemplo nos servem os ensaios de Byung-Chul Han, que ao estudar as transformações da espécie de controle existente no Panóptico de Bentham para a espécie de controle da sociedade digital, conclui que, como centralidade do conceito nas sociedades disciplinares tinha-se a não comunicabilidade dos prisioneiros, em contrapartida a hipercomunicação presente no digital que sustenta uma autoexploração[85].

[83] O conceito de ação social situa-se no campo das Ciências Sociais. Neste sentido: "ações sociais são sempre 7 parte de sistemas mais amplos e de processos de compreensão intersubjetiva, o que introduz a questão do papel do agente ('mediação humana') nos processos através dos quais as ações são coordenadas." (OUTHWAITE e BOTTOMORE, 1996, p. 03). Em análise para além da individualidade da ação, outra perspectiva: "considera a mediação um conjunto de práticas sociais, que se desenvolvem em setores institucionais variados e que visam construir um espaço determinado pelas relações que nele se manifestam" (CAUNE, 2014, p. 73).

[84] Ou seja, não se pretende olvidar o êxito dos estudos de Deleuze, mas complementá-lo com análises hodiernas.

[85] Vejamos: "O panóptico de Bentham consiste de células isoladas umas das outras. Os prisioneiros não podem se comunicar uns com os outros. As divisórias cuidam para que eles não possam ver uns aos outros. Tendo por

Neste sentido, a exposição do ser na rede perpetua um ciclo de apropriação de sua informação como via de afirmação social, pois a sua socialização é modulada pela positividade da rede. Positividade esta carente de sentido e direcionamento, ante a ausência do negativo como medida de imposição e diferenciação[86]. A hipercomunicação contemporânea, ao evitar ruídos, equilibra toda sociabilidade em uma falsa verdade, em um verdadeiro vazio existencial[87].

A estruturação do ambiente digital, neste contexto, fomentou a circulação da informação mediada pela tecnologia das instituições corporativas, não apenas moldando a arquitetura do ambiente, mas as conexões ali efetuadas. Conexões estas pautadas na transparência, pelo esfacelamento do público ao privado, e na positividade, pela ausência de negatividade em sua sociabilidade.

a) A representação social e simbólica dos dados

finalidade o melhoramento, eles são expostos à solidão. Os habitantes do panóptico digital, em contrapartida, se conectam e se comunicam intensamente uns com os outros. Não o isolamento espacial e comunicativo, mas sim a conexão e a hipercomunicação que tornam o controle total possível" (HAN, 2018, p. 1073). Interessante, portanto, ressaltar que um dos pontos centrais de Bentham no panóptico é buscar a constante vigilância dos prisioneiros por sua exposição ao olhar do vigilante. Assim, "sua essência consiste, pois, na centralidade da situação do inspetor, combinada com os dispositivos mais bem conhecidos e eficazes para ver sem ser visto" (2008, p. 28). "É obvio que, em todos esses casos, quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado. A perfeição ideal, se esse fosse o objetivo, exigiria que cada pessoa estivesse realmente nessa condição, durante cada momento do tempo. Sendo isso impossível, a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária, ele deveria pensar que está nessa condição" (BENTHAM, 2008, p. 20). Ocorre que, à época, Bentham não poderia prever a potencialidade do eletrônico e do digital, de forma a radicalizar as vias de vigilância, mas, talvez ainda mais que isto, radicalizar as vias de exposição do indivíduo, expondo-se constantemente na rede.

[86] A positividade da rede equilibra o sistema e remove os ruídos – tudo aquilo que venha desacelerar os fluxos da 10 informação, obstruir a livre circulação –, Entretanto: "A sociedade da positividade atual evita, todas as formas de resistência. Ela suprime, desse modo, ações. Nela dominam apenas diferentes estados do mesmo (posição 526)". Assim, impermeabiliza-se o social das individualidades do espirito, desfigurando as ações sociais. "Nela dominam apenas diferentes estados do mesmo (HAN, 2018, p. 526). A positividade que habita o digital reduz a possibilidade de uma tal experiência. Ela promove o igual" (HAN, 2018, p. 379).

[87] "Transparência e verdade não são idênticos. A verdade é uma nefatividade na medida em que se põe e impõe, 11 declarando tudo o mais como falso. Mais informação ou um acúmulo de informações, por si sós, não produzem qualquer verdade; faltam-lhes direção, saber e sentido. É precisamente em virtude da falta de negatividade do verdadeiro que se dá a proliferação e massificação do positivo. A hiperinformação e hipercomunicação gera precisamente a falta de verdade, sim, a falta de ser. Mais informação e mais comunicação não afastam a fundamental falta de precisão do todo. Pelo contrário, intensifica-a ainda mais" (p. 25).

As informações que circulam na rede como dados digitais fruto da manifestação do comportamento humano, notoriamente vinculam-se, cada qual, a um determinado corpo concreto – qual seja o corpo humano. Assim, tal vinculação permite qualificar o dado objeto de estudo como dado pessoal, nos termos do art. 5º, I, da LGPD[88], ampliando a significação e a representação simbólica contida em sua dimensão semântica, abrindo-se margem a um aprofundamento da análise dos sentidos manifestos e exteriorizados pela intersubjetividade dos usuários na rede.

Isto porque, consoante firmado no capítulo anterior, a cacofonia digital é a marca da atual qualidade do ambiente digital, dotado de diversas informações dissonantes que obstruem o bom funcionamento da rede, prejudicando a socialização do ser e, respectivamente, sua individuação como agente autônomo, livre , quanto mais pensada a dimensão do controle[89] sobre a significação do ser pela mediação tecnológica perpetrada por grandes corporações.

Portanto, o aprofundamento passível é, notadamente, atinente à dimensão simbólica da representação do ser como dado fático manifesto no mundo. Neste sentido, na filosofia de Cassirer encontramos, talvez, a melhor viabilidade teórica de complementação de tais estudos pela apropriação do significado simbólico e sua relação com o ser.

Segundo o autor, a própria marca distintiva do homem em relação aos outros animais é a sua dimensão simbólica[90], para além da dimensão racional classicamente assimilada pela filosofia (CASSIRER, 2005

[88] "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

[89] "Liberdade significa aqui a raiz única, irredutível a conceitos, do eu humano no palco de um mundo aberto, simultaneamente pre-dado e oferecido como tarefa, onde ela toma posição, se dá a si mesma forma, ao desempenhar o seu papel de actriz (personare). A liberdade real mostra-se, faz-se ouvir (sonat) no mundo a que pertence e onde ganha forma ou figura, como o actor antigo, que, ao falar através da máscara, desempenha o seu papel no mundo lúdico. Tal é provavelmente o significado original da palavra grega "prosopon", que foi traduzida em latim por "persona" no sentido de máscara, rosto ou aspecto pelo qual a unidade de acção de tina figura lúdica se faz ver e ouvir. A pessoa constitui-se mediante o aparecimento temporal da raiz originária, que é, no palco do mundo a que pertence. A dignidade inalienável da pessoa está precisamente no aparecimento da sua raiz profunda e única no mundo variável e multidimensional que habita" (PEREIRA, 2004, p. 4).

[90] "É obvio que esse mundo não é nenhuma exceção às regras biológicas que regem a vida de todos os demais organismos. No entanto, no mundo humano encontramos uma característica nova que parece ser a marca distintiva da vida humana. O círculo funcional do homem não é só quantitativamente maior; passou também por uma mudança qualitativa. O homem descobriu, por assim dizer, um novo método para adaptar-se ao seu ambiente. Entre o sistema receptor e o efetuador, que são encontrados em todas as espécies animais, observamos no homem um terceiro elo que podemos descrever como o sistema simbólico. Essa nova aquisição transforma o conjunto da vida humana" (CASSIRER, 2005, p. 47).

p. 50), ante a capacidade de sistematização da realidade em "variados fios que tecem a rede simbólica, o emaranhado da experiência humana" (CASSIRER, 2005, p. 48), afastando-a como representação[91].

Diferentemente do signo, que em uma relação representativa direta entre significante e significado16, o símbolo, em Cassirer, encerra a dimensão harmoniosa de contrários que se coincidem, tal qual a unidade humana, que é concebida como unidade funcional dialética, pela coexistência de multiformas que variam desde o sentimento ao pensamento (2005, p. 362-3).

Desta forma, é a dinamicidade que marca a essência da vida e cultura humana, ante a necessidade de equilíbrio entre as formas constituintes do ser. Como consequência, tal dinamicidade pode-se completar apenas pela recuperação da própria história do indivíduo e seu desenrolar no mundo.

Para tanto, resta apenas uma possibilidade: o exame das condições de controle dos dados pessoais, de forma a viabilizar a recuperação do sentido firmado pelo símbolo na sua experimentação no mundo. Sua trajetória, seus usos e os valores sociais que assume no cotidiano traduzem a representação que significa, no mundo, o usuário digital.

Entretanto, pela limitação do presente artigo e em vista de seu objetivo primordial – qual seja viabilizar a autodeterminação do ser no ambiente digital –, buscar-se-á apenas analisar os enclaves e obstruções ao controle dos dados pelo usuário, ante a relevância da dimensão do controle para garantia de autonomia da significação do indivíduo pelas liberdades de agir no meio e os sentidos firmados pelo símbolo na sua experimentação no mundo.

3. Estruturação normativa sobre portabilidade de dados

Consoante firmado anteriormente, o instituto da portabilidade de dados surge como instrumento capaz de operacionalizar o controle dos dados pelo próprio usuário, viabilizando a autodeterminação no ambiente digital. Assim, a portabilidade dos dados surge como instrumento de empoderamento do homem no mundo digital, pois tanto busca evitar a centralização dos dados pelos controladores ofertantes (efeito este denominado *lock in*), quanto facilitam os custos de troca (*switching costs*), operacionalizando os atributos da titularidade.

Ocorre que, se por um lado a percepção da necessidade de regulação do tema nos infere o objetivo de intervenção estatal para determinado fim – qual seja efetivar a autodeterminação individual do titular do dado em meio ao contexto digital do *Big Data* –, por outro é notório que a análise destes instrumentos

[91] "A linguagem, o mito, a arte e a religião são partes desse universo (...). Todo o progresso humano em 15 pensamento e experiência é refinado por essa rede, e a fortalece. O homem não pode mais confrontar-se com a realidade imediatamente; não pode vê-la, por assim dizer, frente a frente. A realidade física parece recuar em proporção ao avanço da atividade simbólica do homem" (CASSIRER, 2005, p. 48).

normativos já nos permite auferir problemáticas e obstruções decorrentes da usabilidade, custos, segurança e eficiência deste instituto, concretizado no direito à portabilidade de dados.

a. Problemáticas da estruturação normativa brasileira

Consoante se depreende do tratamento jurídico dado ao tema, a portabilidade dos dados é abarcada, no ordenamento pátrio, pela Lei Geral de Proteção de Dados, notadamente em seus artigos 11, 18 e 40. Em sendo a portabilidade um instituto voltado à concretização do domínio sobre os dados, deve buscar efetivar os atributos inerentes à essência deste mesmo instituto.

No entanto, tanto no Regulamento europeu – em seu art. 20 (2), quanto na normativa pátria – nos termos do art. 18, §4º, II –, o direito à portabilidade é exigível, tão somente, quando exista viabilidade técnica de operabilidade dos dados no mercado. Isto porque, enquanto a primeira dispensa a exigibilidade de transferência dos dados se não existir compatibilidade operacional entre os controladores, a segunda dispensa a obrigatoriedade de fornecimento da cópia quando inviável tecnicamente, mediante indicação das razões que a impossibilitem.

Frise-se que ambas normativas sequer abarcam o direito de escolha, pelo titular, da formatação a ser adotada pela empresa controladora. Ou seja, as normas abarcadas acabam por beneficiar as empresas que dispensem o desenvolvimento técnico de operabilidade padrão no mercado de dados.

Outra problemática suscetível de debate no ambiente jurídico surge do §7º do art. 18 da LGPD, que não inclui no direito à portabilidade os dados já anonimizados pelo controlador. Sem se alongar, por ora, acerca do direito a ser esquecido – vez que tal análise será aprofundada na pesquisa propriamente dita –, o dispositivo legal é obscuro também quanto ao momento de aviso do processamento dos dados, permitindo subterfúgios à aplicabilidade da lei.

Assim, é perceptível que, se por um lado, dos dados surge a extensão da significação do homem na era da informação, por outro, servem estes de ativo econômico às empresas, pois permitem, mediante a análise dos dados para produção de informação, o aprimoramento da tomada de decisões – ou seja, em síntese geram uma economia mais efetiva, ao permitir uma melhor alocação de recursos[92].

[92] O estudo da alocação dos dados como recurso econômico assume relevante posição na economia da era da 17 informação, vejamos: "Data has been acknowledged as an essential resource for economic growth, and it is estimated that by 2020 the size of the EU data economy may increase to C739 billion-or 4% of the overall EU GDP. 2 Against this background, the regulation of the allocation of and extent of control over data-by way of exclusive rights or possibilities of access-becomes increasingly important" (GRAEF, Inge; HUSOVEC, Martin; PURTOVA, Nadezhda, p. 1361).

É evidente, portanto, o conflito de interesses na sociedade da informação, embate este protagonizado pela autodeterminação do homem, e, em sua contraparte, pelo controle de dados exercido pelas empresas.

Desta forma, torna-se fundamental repensar o instituto da portabilidade dos dados como instrumento de efetivação do controle e, consequentemente, da autodeterminação do homem, mediante estudo dos atributos inerentes à titularidade, bem como em comparação para com legislações alienígenas, tais quais o Regulamento Geral sobre Proteção de Dados, as Diretivas 20213/37/EU e 95/46/CE, a Lei de Privacidade dos Consumidores da Califórnia – *California Consumer Privacy Act* (CCPA) e atos normativos expedidos pelos órgãos executivos europeus para fins de regulamentação de operabilidade da portabilidade de dados, tais quais os *Guidelines on the right to data portability*, dentre os quais nos interessa os *Working Parties* de n° 29 e 242.

b. Repensando a estruturação normativa de portabilidade de dados

Para superação das problemáticas observadas, foram analisadas, primordialmente, o *General Data Protection Regulation* (GDPR), os *Guidelines on the right to data portability* (WP242), o *Regulation on cross-border portability of online content services in the internet market* e o *California Consumer Privacy Act* (CCPA), ante o enfrentamento contemporâneo do tema no *Assembly Bill n. 375* de 2018.

Acerca do requisito de interoperabilidade entre softwares para transferência direta dos dados entre controladores, cumpre de início pensar a divisão clássica do direito à portabilidade em seus dois elementos constituintes: (i) a obtenção de cópia dos dados e (ii) o direito de transferi-los; para posteriormente analisarmos a efetivação dos objetivos centrais do instituto, quais sejam aprimorar o controle individual dos titulares de dados para viabilizar um desempenho ativo destes no ecossistema digital, mediante seu empoderamento pela facilitação das habilidades de interação entre o homem e a informação (WP242, 2017, p.4).

A divisão bipartite do instituto permite inferir que, a despeito da lesão ao direito de transferência dos dados, a obtenção da cópia resta salvaguardada, devendo proceder-se, na hipótese de processamento brasileiro, em atenção ao disposto no art. 9º da LGPD, que exige o "acesso facilitado às informações" pela disponibilização "de forma clara, adequada e ostensiva", acerca de sua finalidade, forma, duração e mesmo com menção explícitas aos direitos do titular, materializando os princípios previstos no art. 2º, da mesma normativa.

Para tanto, frise-se também as boas práticas de governança impostas pelo art. 50, dentre as quais figura a implementação de um programa em privacidade que, no mínimo: "tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular" (Art.50, §2º, I, da LGPD).

Assim, o direito de obtenção da cópia como elemento decorrente da portabilidade de dados deve ser analisado sistematicamente, de forma a materializar o acesso aos dados e facilitar a liquidez do controle dos dados pelo próprio usuário, mediante potencialização dos atributos decorrentes do instituto da titularidade.

Nas *Guidelines on the right to data portability*, emitida por instituições executivas da União Europeia, o enfrentamento do tema permitiu propor que os controladores não podem obstruir tecnicamente o usuário e deveriam sempre transmitir quando tecnicamente possível, valendo-se de dois caminhos para viabilizar a transmissão: um meio único para transmissão direta dos dados do usuário, captados por um instrumento automatizado de grande extração e captação dos dados reservados, para fins de garantia do rápido cumprimento da obrigação.

Frise-se que nos *Working Parties* 242, definiu-se que o dado estruturado em um meio de formatação legível comum, consoante o art. 20 (1) do GDPR deve coadunar-se ao sentido definido na Diretiva 2013/37/EU em seu recital 21, em que os sistemas não precisam ser compatíveis, mas interoperáveis, razão pela qual propõe-se a utilização de formatos comuns (XML, JSON, CSV).

Já no *California Consumer Privacy Act*, por sua vez, o instrumento normativo fez interessante proposta inovadora ao obrigar dois meios mínimos de solicitação, como via website ou telefonema gratuito, conforme a subdivisão (a) (1)1 da seção 1798.130, além de bem definir a subdivisão das categorias dos dados de forma clara e bem delineada – seção 1798.110, subdivisões (a) e (c), obrigatoriamente cedidos durante o momento de coleta das informações, nos termos da subdivisão (b) da seção (1798.100).

Frise-se também interessante normativa acerca do direito de *opt out*, isto é, requisitar ao controlador que não deseja a venda de seus dados pessoais a terceiros (1798.120) (a), devendo a empresa informar o consumidor da transmissão dos dados e de seus direitos (b) e, no caso da ausência de aviso prévio de informação, não poderá proceder à venda senão com autorização expressa do consumidor (c).

Acerca da desnecessidade de cópia de portabilidade de dados quando já anonimizados (art. 18, §7º, da LGPD), o dispositivo é obscuro quanto ao momento de aviso do processamento, possibilitando subterfúgios no entendimento do momento de solicitação de cópia, prejudicado ainda pelo sentido em aberto da razoabilidade na configuração do que seja anonimizado (ante possível esforço de reversão – art. 12, caput, da LGPD), requerendo critérios objetivo de tempo, custo e tecnologias (art. 18, §1º, da LGPD). Neste sentido, andou bem a LGPD ao classificar como dados pessoais aqueles que anonimizados são utilizados para formação de perfis comportamentais (art. 12, §2º, da LGPD).

A estruturação do tema caminhou em sentido similar ao do GDPR, que eximiu o controlador do cumprimento do direito de portabilidade dos dados quando comprovar que o usuário não era identificável, nos termos do art. 11 (2).

Tal disposição deverá ocorrer na aplicação jurisprudencial da normativa, uma vez que o Código de Defesa do Consumidor permitirá um diálogo de fontes apto a inverter o ônus da prova de veracidade e, respectivamente, o ônus processual da prova (arts. 38 e 6º, VIII, do CDC).

Pode-se, desde já, propor eventual expedição, pela Autoridade Nacional de Proteção de Dados, de pareceres técnicos que estabeleçam diálogo de fontes entre, o dano decorrente de tratamento de dados aos riscos que dele razoavelmente se espera (art. 44, II, da LGPD) e o prazo de comunicação da impossibilidade de cumprimento do fornecimento da cópia (art. 48, §1º, da LGPD), com os danos consumeristas e os entendimentos doutrinários em consonância à responsabilização objetiva, oportunizando um sistema coeso de maior integração da cadeia de valor.

Interessante ressaltar que o tema da anonimização pode ser analisado pela via de proteção do usuário, quando utilizado para fins de não identificação no banco de dados do controlador. Neste sentido, GDPR impôs tal mecanismo como via de preenchimento do princípio da minimização em seu art. 89 (1), diferentemente da LGPD, que nada dispôs acerca do tema.

Assim, é perceptível que, se por um lado, dos dados surge uma extensão da significação do ser na era da informação, por outro, servem estes de ativo econômico altamente sujeito a riscos e apropriado pelas empresas, que, mediante a análise para produção de informação, aprimora sua tomada de decisões – ou seja, em síntese estruturam uma economia mais efetiva no sentido de permitir uma melhor alocação de seus recursos. É evidente, portanto, o conflito de interesses na sociedade da informação, embate este protagonizado pela autodeterminação do homem, e, em sua contraparte, pelo controle de dados exercido pelas empresas.

Não obstante, a estruturação de um mecanismo de controle do usuário acerca de seus próprios dados permite viabilizar uma descentralização na alocação de tais ativos digitais, garantindo maior liquidez pela usabilidade tecnicamente operacionalizada no acesso e respectiva transmissão das informações, de forma também a estruturar um mercado digital mais competitivo e menos assimétrico na relação entre o indivíduo e as plataformas de mediação digital.

Conclusão

Acerca do tema, é possível situar a problemática do controle de dados pelos usuários como algo inerente à estruturação arquétipa da rede na contemporaneidade, potencializada pelos efeitos concorrenciais do mercado digital inicialmente desregulado (CASTELLS, 2010, p. 96), de forma a viabilizar verdadeira sistemática de apropriação da significação do homem no ambiente digital e respectiva busca pela reconstrução da intersubjetividade do ser no ambiente mediatizado pelas tecnologias da informação.

Dentre tais problemáticas, a portabilidade de dados figura como instituto cerne capaz de efetivar a materialização dos atributos da titularidade dos dados, notadamente o acesso à informação e respectiva viabilidade de facilitação de transferência das informações, a garantir maior liquidez no controle de tal ativo e maior interação do usuário com suas próprias informações, razão pela qual sua estruturação normativa configura possível campo de transformação do *medium* digital, que configura campo central de individuação do ser, ora afetada pela estruturação técnica, econômica e normativa assimétrica, ante a apropriação pelas instituições financeiras.

Neste sentido, a portabilidade de dados, tal qual estruturada na LGPD, permite inferir possíveis problemáticas já vivenciadas pela União Europeia, tanto porque o modelo normativo pátrio moldou-se em consonância ao europeu, quanto pelo lapso temporal de vigência de tal instrumento normativo acerca em vigor no território europeu, de sorte que se pode experimentar e propor soluções para efetivação da autodeterminação informacional mediante sua operacionalização técnica e estruturação normativa.

Conforme observado, a problemática atinente à operabilidade entre softwares dos controladores obstou a transferência direta dos dados na realidade europeia, razão pela qual o tema fora tópico central nos trabalhos formulados nos *Working Parties* n° 242 e 29, resultando na estruturação técnica mínima obrigatória de um meio único para transmissão direta dos dados do usuário, captados por um instrumento automatizado de grande extração e captação dos dados reservados, para fins de garantia do rápido cumprimento da obrigação, além do incentivo para modelos de arquivos comumente utilizados nas redes, posta a facilitação da interoperabilidade do arquivo para com o software do novo controlador, ainda que incompatível esta com o *software* do controlador anterior.

No caso do Estado da Califórnia, o *Consumer Privacy Act* de 2018 propôs uma estruturação técnica mínima imposta à empresa para agilizar a operacionalização do direito, como a fixação de duas vias mínimas de requisição (como telefonema e website), bem como especificar as subdivisões da cópia dos dados em estrutura legível e facilmente identificável, favorecendo a análise pelo próprio usuário.

Quanto ao tema da anonimização dos dados, notoriamente problemática se pensados os estudos recentes que demonstram a impossibilidade técnica de uma anonimização infalível, é certo que trará dificuldades para além do critério da razoabilidade como qualificador do status contrário ao de dado pessoal, resguardando ao operador o direito de não entregá-los ao usuário. Em verdade, a autodeterminação fica severamente em risco quanto as possibilidades de interferência em seu livre arbítrio pela análise de preferências, não obstante a previsão da LGPD em classificar como dados pessoais aqueles anonimizados que sejam utilizados para tais fins.

Acerca do tema, fez bem o *Consumer Privacy Act* da Califórnia em exigir a informação dos dados quando do momento de seu processamento, de forma a deixar ciente o usuário dos dados disponíveis ao

controlador. Do contrário, poderia os dados serem anonimizados, de forma a eximir os controladores de suas responsabilidades. Cumpre pensar que a anonimização é técnica viável também para a proteção do usuário, conforme o GDPR regulou a pseudoanonimização como mecanismo de proteção dos dados nos bancos de dados do controlador, nos termos do art. 89 (1).

Ainda, é certo que cumprirá à Autoridade Nacional de Proteção de Dados a expedição de normativas referentes a configuração da anonimização, bem como aprofundamento da ideia de razoabilidade, evitando que a zona cinzenta seja apropriada pelas instituições financeiras como espaço de disputa e favorecimento aos interesses próprios.

Por todo o exposto, tem-se a portabilidade de dados como instituto central para garantia do controle de dados pelo usuário, otimizando os atributos da titularidade pela estruturação normativa pensada em benefício da livre circulação de dados. Para tanto, a descentralização do controle dos dados pelo maior acesso à informação e respectiva facilitação da usabilidade e liquidez pelo usuário permite fomentar a alocação de tais ativos em consonância aos interesses dos próprios usuários.

Nesta seara, foram propostas possíveis reflexões acerca da estruturação normativa adotada pela Lei Geral de Proteção de Dados, decorrentes de problemáticas enfrentadas pelas legislações já em vigor da União Europeia e do Estado da Califórnia, em vista da reestruturação em prol da autodeterminação informacional dos usuários, situados como senhor de suas significações no ecossistema digital.

Referências bibliográficas

BENTHAM, Jeremy. **O Panóptico.** Trad. Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. 2. Ed. Belo Horizonte: Autêntica Editora, 2008.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei geral de proteção de dados. Brasília, **Diário Oficial da União**, 2018. Disponível em: http://planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01/12/2019.

CANEVACCI, Massimo. **Antropologia da comunicação visual:** explorações etnográficas por meio do fetichismo metodológico. 1. Ed. São Paulo: Perspectiva, 2018.

CASTELLS, Manuel. **The power of identity.** 2 ed. Singapore: Wiley-Blackwell, 2009.

_____. **The rise of the network society.** 2. Ed. Blackwell Publishing Ltd: Oxford, 2010.

CAUNE, Jean. **Cultura e comunicação:** convergências teóricas e lugares de mediação. São Paulo: Ed. UNESP, 2014.

DELEUZE, Gilles. Post-Scriptum sobre as Sociedades de Controle. *In:* **Conversações.** Trad. Peter Pál Pelbart. 1. Ed. Rio de Janeiro: Editora 34, 2000.

EUA. **California Consumer Privacy Act of 2018.** Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&fbclid=IwAR1Uaqgjty8v1Sc04YfgjTr81o99ro67UcXDy0kKnCNvY9su12TOvKkM7-0. Acesso em: 11/10/2019.

GRAEF, Inge; HUSOVEC, Martin; PURTOVA, Nadezhda. **Data Portability and Data Control:** Lessons for an Emerging Concept in EU Law, 19 German L.J.

GUIDELINES ON THE RIGHT TO DATA PORTABILITY. Wp242. Disponível em: https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611233&fbclid=IwAR3uD74WCq2Ygmv2VyNn7QZolFs8l7OFzuuf_0sB0zzDU Gq9c2HlPjo. Acesso em: 11/10/2019.

HABERMAS, Jurgen. **Técnica e ciência como ideologia.** Tradução de Felipe Gonçalves Silva. 1. Ed. São Paulo: Editora Uneso, 2014.

HAN, Byung-Chul. **No enxame:** perspectivas do digital. Trad. Lucas Machado. Ed. Digita. Petrópolis: Vozes, 2018.

LANEY, Doug. **3D data managment:** controlling data volume, velocity and variety. Meta group, Stamford, 2001. Disponível em: blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Managment-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso em: 01/12/2019.

LEMOS, Patrícia Faga Iglecias. Consumo sustentável e desmaterialização no âmbito do direito brasileiro. **Revista CEDOUA**, ano XV, Vol. I, n. 29. Universidade de Coimbra, 2012.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". **Communications of the ACM**, v. 53, n. 06, p. 24, June 2010. Disponível em: WWW.cs.utexas.edu/~shmat/shmat_cacm10.pdf

OUTHWAITE, William; BOTTOMORE, Tom (eds). **Dicionário do pensamento social do século XX.** Rio de Janeiro: Jorge Zahar, 1996.

PEREIRA, Miguel Baptista. Para uma filosofia do símbolo. *In:* **Revista filosófica de Coimbra,** n. 25. Coimbra, 2004.

PONS, Anaclet. **El desorden digital:** Guía para historiadores y humanistas. Siglo XXI. España: Madrid, 2013.

SARTRE, Jean-Paul. **O existencialismo é um humanismo.** Tradução de João Batista. Petrópolis: Vozes, p. 25, 2014.

_____. **O ser e o nada:** ensaio de ontologia fenomenológica. Tradução de Paulo Perdigão. Petrópolis: Vozes, 2015.

SEVCENKO, Nicolau. **A corrida para o século XXI:** no loop da montanha russa. Coordenação de Laura de Mello e Souza, Lilia Moritz Schwarcz. 1. Ed. São Paulo: Companhia das Letras, 2001.

UNIÃO EUROPEIA. **General Data Protection Regulation.** Disponível em: https://eurlex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679. Acesso em: 11/10/2019.

WITTGENSTEIN, Ludwig. **Investigações filosóficas.** Tradução de José Carlos Bruni. 1. Ed. São Paulo: Abril S.A., 1975.

4.4. *Accountability* no tratamento de dados no Brasil – *Felipe Otávio Moraes Alves*[93]

Resumo

[93] Professor de Direito na Faculdade de Ciências Humanas e Sociais da UNESP da disciplina "Teoria do Estado". Advogado na área de Direito Digital. Mestrando em Direito na UNESP, Universidade Estadual Paulista "Júlio de Mesquita Filho", se especializando na área de Direito Digital (correlacionando Direito à Tecnologia, principalmente a Internet), sob orientação do prof. Dr. Jorge David Barrientos-Parra. Graduado em Direito na Universidade Federal de Goiás. Tem experiência na área de Direito, com ênfase em Teoria do Direito, Direitos Fundamentais, Filosofia de Direito e Direito Digital, atuando principalmente nos seguintes temas: justiça, privacidade, liberdade, direitos humanos, informática, democracia, constituição e subjetividade. Integrante do Grupo de Estudos e Pesquisa em Propriedade Intelectual e Desenvolvimento Econômico-Social (GEPPIDES).

No presente trabalho, discute-se quais devem ser os desempenhos de aperfeiçoamento mecanismos de *accountability* na gestão pública em relação à atual institucionalização de sistemas de tratamento de dados, especialmente a ANPD. Foi adotado, como método de procedimento, a pesquisa bibliográfica e legislativa e, como método de abordagem, o teórico-dedutivo.

Palavras-chave: *Accountability*; políticas públicas; tratamento de dados.

Abstract

In the present work, it is discussed what should be the performance of improving accountability mechanisms in public management in relation to the current institutionalization of data processing systems, especially the ANPD. The bibliographical and legislative research was adopted as a method of procedure and the theoretical-deductive as method of approach.

Keywords: Accountability. Public policy. Data processing.

Introdução

Através do paradigma que enfrenta o estado hodierno, em tempos de pós-modernidade, com o cidadão carecendo de maiores eficácias estatais, a qualidade das ações dos governos depende em grande medida dos controles e incentivos, derivados do desenho institucional das políticas públicas (PRZEWORSKI, 1996). A introdução da *accountability* por meio da lógica de "privatização" dos conceitos e princípios privados – por uma inconsciente preferência por sua eficácia fática mais clara para a população – aparece como uma promessa de substituição da atual máquina morosa e burocrática por uma outra no qual a sociedade participa da definição de metas e dos índices de desempenho e que fiscaliza este Estado, com a implementação de políticas públicas pautadas pelos resultados (CENEVIVA, 2008). E aqui entra essa transparência e sua importância. Assim, a efetividade, eficiência, *accountability* e o desempenho da gestão pública serão aqui tratados.

E, por isso, a preocupação do atual trabalho é de criar sistemas de *accountability* nos quais os aplicativos brasileiros e a ANPD possam aderir para uma melhor compreensão e tutela dos direitos dos brasileiros. Aliás, serão propostas medidas justamente para que o país possa servir de exemplo.

Accountability é um termo inglês, sem tradução exata para o português, que trata da obrigação de membros de um órgão administrativo ou representativo de prestar contas a seus representados, representando o compromisso ético e legal de responder por uma responsabilidade delegada. Naves (2012, p. 34) diz que: "se os cidadãos são a fonte da autoridade dos governantes, eles têm o direito de ser informados das decisões deste poder, pelo que essas decisões devem ser públicas e os procedimentos que conduzem a essas decisões devem ser especificados em regras legais que também estejam

disponíveis". Então, daí vem a importância de divulgação dos resultados das auditorias operacionais aos cidadãos e à imprensa, pois atestam o desempenho das políticas públicas para que seja avaliado (CENEVIVA, 2008).

Neste trabalho utilizaremos a noção de *accountability* horizontal, em que, neste caso em específico, ocorre através da mútua fiscalização e controle existente entre Controladorias Gerais e agências fiscalizadora, já que pressupõe uma ação entre iguais ou autônomos, sempre preocupado com a transparência das ações da gestão pública em relação aos agentes que podem fiscalizá-las e puni-las. Assim, esta *accountability* exige que órgãos estatais com poder e capacidade para realizar ações, como o monitoramento de rotina assim como a ANPD, em relação a ações ou omissões ilegais exercidas por outros órgãos ou agentes do Estado. Lembrando que a ANPD tem um foco também, talvez até majoritário, nas relações privadas. Todavia, mesmo neste caso, existe a *accountability*, agora já vertical, em que o Estado deverá prestar contas para este cidadão que o Estado deve satisfação de justificar toda vez que atinge um direito seu ou o avalia, sempre fornecendo meios para o cidadão tenha capacidade e conhecimento de ser ressarcido em caso de má ação estatal.

Assim, no presente estudo, discute-se quais devem ser os desempenhos de aperfeiçoamento mecanismos de *accountability* na gestão pública em relação a atual institucionalização de sistemas de tratamento de dados, principalmente os pessoais. Mais especificamente, busca-se as relações entre o fortalecimento da função e da capacidade avaliadora do governo e a promoção de níveis crescentes de tratamento de dados pessoais. As considerações finais perquiriram concluir esta incidência como importantíssimas e potencialmente eficaz a fim de proteger o cidadão. Foi adotado, como método de procedimento, a pesquisa bibliográfica, legislativa e, como método de abordagem, o teórico-dedutivo.

1. No mundo

A *accountability*, como um conceito geral aplicável a qualquer entidade e há algumas definições elaboradas por alguns organismos internacionais. Para a *International Federation of Accountants* (IFAC) (2001), *accountability* é o processo em que entidades e indivíduos do setor público são responsáveis por decisões e ações (como a gerência dos recursos públicos) além do desempenho e de resultados. A *International Organization of Supreme Audit Institutions* (INTOSAI) (1998) considera *accountability* a obrigação imposta aos agentes e entidades públicos de responderem de "forma fiscal, gerencial e programática quanto aos recursos que lhes foram conferidos a quem lhes acometeram tais recursos". E, também, a *Organisation for Economic Co-operation and Development* (OECD) (2008) diz que *accountability* é "manter alguém responsável, usado como sinônimo do dever prestação de contas, com o intuito de melhorar a possibilidade de as pessoas mais vulneráveis na sociedade expressarem as necessidades".

Assim, nota-se que *accountability* está ligada a ideia de que o gestor tem o compromisso de demonstrar o resultado obtido em relação aos recursos recebidos, a quem lhes ofereceu.

2. No setor público do Brasil

Accountability é a solução para o combate à corrupção, exercendo um papel essencial na redução dessa mazela. Na visão atual da *accountability* dos recursos públicos o GAO (2005, p.31) estabelece a importância no processo de governo de um país, para mostrar se os recursos públicos estão sendo administrados adequadamente e legalmente, se os programas de governo estão alcançando os resultados previstos e se os programas de governo estão sendo administrados de forma eficiente, econômica e efetiva.

O Art. 1º, parágrafo único da Constituição Federal do Brasil, estabelece que o administrador público está representando os interesses de toda sociedade, uma vez que todo poder emana do povo e em nome dele será exercido, devendo sempre se pautar pelo fiel cumprimento do ordenamento jurídico; e num outro ponto específico, nos Art. 34 e 35, há a *accountability* como um princípio constitucional e, portanto, uma norma jurídica de observação obrigatória a todos os entes federativos:

> Art. 34. A União não intervirá nos Estados nem no Distrito Federal, exceto para: (...) VII - assegurar a observância dos seguintes princípios constitucionais: (...) d) prestação de contas da administração pública, direta e indireta. Art. 35. O Estado não intervirá em seus Municípios, nem a União nos Municípios localizados em Território Federal, exceto quando: (...) II - não forem prestadas contas devidas, na forma da lei.

Quanto aos aplicativos brasileiros, há problemas hodiernos a serem concertados, de acordo com a InternetLab (2018):

Permissões	FGTS	CAIXA	BOLSA FAMÍLIA	SEFAZ NF	MEU INSS	CNH DIGITAL	ANATEL
Acessar a localização aproximada	■		■		■		■
Acessar a localização precisa	■	■	■		■		■
Acessar as contas	■		■				■
Ler Memória Externa	■	■	■	■	■		■
Escreve memória externa	■	■	■	■	■		■
Ler estado do telefone	■	■	■				■
Realizar ligações							
Acessar a câmera		■		■			
Acessar a internet	■	■	■	■	■	■	■
Acessar o estado da rede	■	■	■	■		■	■
Acessar o estado do wifi	■	■	■	■			■
Receber informações do *boot*							

Requisitar instalação de pacotes				■			
Vibrar		■					■
Manter o aparelho ativo	■		■			■	■
Usar *hardware* de impressão digital		■		■			
Acessar a lanterna				■			
Acessar as tarefas							■
Criar Janelas		■					
Possui Política de Privacidade	■	■	■		■		

Permissões	SP SERVIÇOS	EMTU SP	METRÔ SP	CPTM SP	SNE DETRAN	MEU IR
Acessar a localização aproximada	■	■	■			
Acessar a localização precisa	■	■			■	
Acessar as contas	■	■				■
Ler Memória Externa	■	■		■	■	■
Escreve memória externa	■	■		■	■	■
Ler estado do telefone	■					■
Realizar ligações				■		
Acessar a câmera						
Acessar a internet	■	■	■	■	■	■
Acessar o estado da rede	■	■	■	■	■	■
Acessar o estado do *wifi*	■					
Receber informações do *boot*					■	
Requisitar instalação de pacotes						
Vibrar		■				■
Manter o aparelho ativo	■	■			■	■
Usar *hardware* de impressão digital						
Acessar a lanterna						
Acessar as tarefas						
Criar Janelas						
Possui Política de Privacidade	■			■		■

Tabela 01: Invasão de Privacidade de *apps* do governo.

Através da análise desta tabela, observamos, primeiramente, que vários aplicativos utilizam vários serviços que supostamente não precisavam. Qual seria a necessidade de terá localização exata ou aproximada para um aplicativo de cálculo de aposentadoria, por exemplo? Acessar as contas do celular, acessar câmera, internet? Até acessar a lanterna pelo SEFAZ NF. Todo direito que o aplicativo e, portanto, o Brasil se dá sobre o usuário, tem que ser feita de forma informada e consentida. Ou seja, deve se passar por dois processos de avaliação para que a transparência prevaleça no caso dos aplicativos do Brasil e que a ANPD, por exemplo, teria de avaliar e regular.

O primeiro passo é avaliar a real necessidade e sempre optar por abusar o mínimo possível dos direitos dos consumidores, até pelo benefício da própria federação, pois quanto menos direitos afetar, menos chances de errar ou ter de arcar com indenizações e reparações. O segundo passo é sempre informar da melhor maneira possível o usuário, sendo ideal informar até o motivo pelo qual precisa daquela permissão de uso daquela ferramenta no celular. Concomitante a esse segundo passo, depois de informar, deve fazer a parte do consentimento o mais claro possível.

3. Questão da cidadania

Quanto aos elementos essenciais do Estado, essencial por ser indispensáveis para a existência do Estado, existe uma grande diversidade de opiniões. A maioria dos autores indica três elementos, embora divirjam quanto a eles. De maneira geral, costuma-se mencionar a existência de dois elementos materiais, o território e o povo, havendo variedade de opiniões quanto ao terceiro elemento (formal e identificado com o poder). Dalmo Dallari (2011), por seu turno, ciente das variadas posições que entendem os diversos autores sobre os elementos essenciais do Estado, comenta sobre a soberania, o território, o povo e a finalidade.

O aspecto interessante é o da Cidadania que se trata de consciência coletiva que vai participar "bem". A cidadania é a pessoa estar de posse do direito civil e político, participando do Estado. Participação constante em todos os atos, mesmo quando se ache fora do território. Cada indivíduo integrante do povo participa também da natureza de sujeito, derivando-se daí duas situações, os indivíduos: a) enquanto objetos do poder do Estado, estão numa relação de subordinação e são, portanto, sujeitos de deveres (súdito). b) enquanto membros do Estado, os indivíduos se acham, quanto a ele e aos demais indivíduos, numa relação de coordenação, sendo, neste caso, sujeitos de direitos. É o direito político conferido ao indivíduo para que possa participar da vida política do país em que reside e pode ser: natural (decorre do nascimento) ou legal (através da naturalização). E aqui podemos ver elementos em que o Estado deve satisfação para o cidadão.

4. Questão da democracia

Tanto o conceito como a palavra Democracia foi originada na Grécia (Atenas). Entende-se como o poder exercido pelo povo. A democracia, em um sentido formal, pode ser definida como forma de governo (antiga), onde o povo governa a si mesmo. Consistindo em:

1) todo poder emana do povo, sendo exercido em seu nome e no seu interesse;
2) as funções de mando são temporárias e eletivas;
3) a ordem pública baseia-se em uma constituição escrita, respeitado o princípio da tripartição do poder de Estado;
4) é admitido o sistema de pluralidade de partidos políticos, com a garantia de livre crítica;

5) os direitos fundamentais do homem são reconhecidos e declarados em ato constitucional, proporcionando o Estado os meios a torná-los efetivos;
6) o princípio da igualdade se realiza no plano jurídico, tendo em mira conciliar as desigualdades humanas, especialmente as de ordem econômica;
7) é assegurada a supremacia da lei como expressão da soberania popular;
8) os atos dos governantes são submetidos permanentemente aos princípios da responsabilidade e do consenso geral como condição de validade.

Tem como berço a Inglaterra (1689), mas como marco principal a revolução francesa (1789), a troca do direito divino dos reis pela soberania popular. A expressão do regime representativo é o sistema constitucional no qual o povo se governa por intermédio de seus eleitos, opondo-se ao despotismo (sem ação sobre os governantes) e ao governo direto (cidadãos governam a si mesmos). A impossibilidade prática de utilização dos processos da democracia direta e semidireta tornou inevitável o recurso à Democracia Representativa. Na democracia representativa o povo concede um mandato (mandato político) a alguns cidadãos para, na condição de representantes, externarem a vontade popular e tomarem decisões em seu nome, como se o próprio povo estivesse governando, o mandato político.

Em relação à democracia direta, não existe país puramente assim. Povo exerce por si os poderes governamentais, fazendo leis, administrando e julgando. Ex.: Grécia Antiga e no Cantão de Glanus e no semicantão Appenzell Innerrhoden, na Suíça, há prática de democracia direta, com o povo se reunido para tomar decisões, ao ar livre. Para a existência de uma democracia direta, o homem precisava ocupar-se, tão-somente, dos negócios públicos, conservando sempre aceso o interesse pela cidadania e pela causa da democracia. Na verdade, o Estado, para exercer democracia direta, deve ser muito pequeno quanto ao número de cidadãos e extensão territorial - crítica feita por Dallari (2011).

Muitas vezes, as instituições de democracia direta são transformadas em um mero complemento das engrenagens da democracia representativa. Esse é o caso da maioria dos estados norte-americanos. Por exemplo, a Constituição da Califórnia prevê formas legais de iniciativas populares através das instituições de democracia representativa, de forma a permitir sua votação.

Talvez junto ao Plebiscito, Referendo, Iniciativa Popular, Veto Popular e *Recall* (estes dois últimos não existe em escala nacional no Brasil), devêssemos incluir a *accountability*, onde o povo iria averiguar diretamente todos as políticas públicas que não carecem de segredo. Princípio que será essencial quando Estado for averiguar as proteções públicas e privadas de dados.

5. Exemplo de caso a se incidir a *accountability* no Brasil

Com a aprovação do Marco Civil, a necessidade de ordem judicial foi incluída no ordenamento. O MCI trouxe uma regra específica acerca da necessidade de ordem judicial para o Estado obter quaisquer tipos

de informações privadas e o usuário ter conteúdo ofensivo retirado. Nisto contata-se que o cibercrime pode ser considerado um crime permanente pois o bem jurídico na maioria das vezes será algum bem imaterial da pessoa, ferirá sua liberdade e em muitas vezes também a sua privacidade. E observa-se, em muitos casos, também as duas fases, já que o crime se consolida em um momento através do da ação do *hacker*, e em momento permanente posterior há a ação de atuação permanente e ilícita pelo meio virtual até eventual descobrimento da invasão ou até o hacker tiver extraído todas informações ou benefícios de sua vítima.

Mas qual a relevância jurídica da incidência de cibercrime como crime permanente? A Busca e Apreensão sem este mandado judicial é possível em flagrante permanente pela preocupação jurídica de cessá-lo imediatamente, engendrando um acometimento mais célere. Nesse caso, não se pode falar em ilicitude das provas obtidas porque o momento consumativo do delito está sempre em execução. O flagrante digital realizar-se-ia, assim, quando se descobrisse, por investigação, a localização do suspeito pela identificação da localidade de perpetração do crime, bastando a evidência de que o conteúdo ou a ação delituosa ainda esteja disponível e em continuidade, de alguma forma, na internet. Logo, asseguraria suas vítimas em detrimento de certas garantias jurídicas do acusado. Ora, trata-se da mesma lógica dos cibercrimes, o momento consumativo da ilicitude de *hacking* ou divulgação de conteúdo indevido também está em contínua execução.

Em 2003, houve a propositura de um "método de verificação" para verificar qual direito, privacidade do suspeito e o direito de averiguação do Estado, tem peso maior em cada caso. Trata-se de uma decisão prolatada pelo STJ, em sede do Recurso Ordinário em Mandado de Segurança[94], interposto para contestar o acórdão o qual autorizou a quebra de sigilo bancário requerida pelo Ministério Público. Na época, tal decisão fora conturbada. O relator do acórdão, o ministro Luiz Fux, entendeu que a quebra para fins de investigação de suspeita de crime financeiro não viola a privacidade do impetrante, porque o sigilo bancário não é um direito absoluto. Noutras palavras, o colegiado do STJ sentenciou pela

[94] EMENTA. RECURSO ORDINÁRIO. MINISTÉRIO PÚBLICO. SIGILO BANCÁRIO. DIREITO RELATIVO. SUSPEITA DE CRIME FINANCEIRO. 1. **A suspeita de crime financeiro, calcado em prova de lesividade manifesta, autoriza a obtenção de informações preliminares acerca de movimentação bancária de pessoa física ou jurídica determinada por autoridade judicial com o escopo de instruir inquérito instaurado por órgão competente.** 2. A quebra de sigilo bancário encerra um procedimento administrativo investigatório de natureza inquisitiva, diverso da natureza do Processo, o que afasta a alegação de violação dos Princípios do Devido Processo Legal, do Contraditório, e da Ampla Defesa. 3. O sigilo bancário não é um direito absoluto, deparando-se ele com uma série de exceções previstas em lei ou impostas pela necessidade de defesa ou salvaguarda de interesses sociais mais relevantes (Vide §§ 3º e 4º do art. 1º e art. 7º da Lei Complementar 105/2001) 4. Recurso ordinário improvido. (STJ-SC, RMS 15146 SC 2002/0087609-7, Rel. Min. Luiz Fux, Data de Julgamento: 18/03/2003, Data de Publicação: DJ 07.04.2003, **JusBrasil** 2003) (grifo do autor).

sobreposição do direito à informação ao direito à privacidade, determinando a quebra do sigilo bancário do autor do mandato. O interesse público envolvido e a licitude dos meios de obtenção da informação são de monta essencial para a dissolução do embate. Em relação ao interesse público, a própria ementa regula a importância da fiscalização de suspeita de crime financeiro. Para o ministro relator, Luiz Fux, tal valor é digno per si de determinar a quebra do sigilo bancário. Averígua-se, isto posto, a legitimidade e necessidade pública do Estado utilizar seu direito de verificação da informação em detrimento da privacidade de alguns de seus cidadãos. Para isto, conta-se com a conformidade, a idoneidade, a necessidade, a exigibilidade e a proporcionalidade em sentido estrito.

Em síntese, há uma propensão lógica à consideração do princípio da liberdade de informação em preferência ao direito à privacidade do indivíduo suspeito de fraude. Essa inclinação ocorre porque as vantagens da supressão do direito à privacidade são maiores do que se o contrário acontecesse, como prega o princípio da ponderação de Alexy (2009, p. 91).

Destarte, cada órgão público deveria fornecer meios os quais o cidadão possa conferir tanto os acessos aos seus dados pessoais, como a motivação do ato administrativo materializado pelo agente público que os acessou, efetivando o princípio da publicidade como preceito geral e do sigilo como exceção, conforme o inciso I do artigo 3 da Lei de Acesso à Informação (Lei n.º 12.527/2011). Portanto, caso o cidadão discorde com a motivação do acesso e perceba distorções quanto aos seus fins, poderá contestá-lo através de um processo administrativo ou ação judicial, como a Ação de Indenização contra a Administração Pública, v.g. Em caso da comprovação dos fatos ilícitos, deve o suspeito ser autuado; no caso de inocência, deve o Estado "prestar contas" a este cidadão, apresentando documentos ao mesmo de como fora extraído e analisado seus dados. Essa *accountability* é de responsabilidade do Estado e das empresas com seus usuários-consumidores. Atualmente, os provedores ferem este direito do usuário ao utilizar seus dados – como localização, padrão de imagens etc. – sem prévia autorização; já o Estado, ao investigar estes delitos e não oferecer mecanismos para eludir excessos desse próprio Estado. E aqui entra o próximo capítulo.

6. Exemplo americano para se evitar

Para combater a pirataria, nos EUA, existem algumas leis interessantes sobre o assunto: Lei de Auxílio de Comunicações para Aplicação do Direito, que reforça com que os provedores de internet e telefonia tenham uma política de grampo – sem autorização judicial – sempre que for necessário; Lei de Vigilância Estrangeira, com grampo de grandes potências sem autorização e que o tribunal aceita as solicitações dos congressistas; Lei do Lobo Solitário, onde qualquer pessoa sob vigilância dos EUA tem todos seus dados digitais vigiados; Lei da Escuta sem Destino, que trata do controle contínuo de qualquer pessoa que seja um risco ou que já foi vigiado; Lei de Recolha de Objetos Relevantes, que é o direito dos EUA de recolher qualquer objeto pessoal de qualquer pessoa que mostre no ambiente digital ser um risco para

o Estado; Ato específico sobre a privacidade de dados online de crianças (menores de 13 anos e 364 dias), CIPA (Lei de Proteção à Criança da Internet), que obriga todos os sites pornográficos a usar a verificação da idade, proíbe a pornografia pública, exige que as escolas monitorem o uso da Internet por menores de idade e exige que conteúdos com material obsceno e pornográfico devam ser filtrados (menos restritivos para adultos); *Digital Millennium Copyright Act*, onde há a criminalização de difusão de tecnologias que contornam direitos autorais; Online Copyright *Infringement Liability Limitation Act*, que trata da limitação da responsabilidade do provedor; Lei Antipirataria das Coleções de Informações (CIAA), que torna ilegal o uso do conteúdo informativo dos bancos de dados e, assim, protegeria fatos não originais que não são protegidos pela lei de direitos autorais; e a U.C.C., no seu artigo 2B da disposição sobre licenças de mercado de massa, há a imposição de disposições contratuais referentes às informações, mesmo que concedam aos proprietários do produto informações muito mais amplos do que a lei de direitos autorais.

E há outras três propostas no Congresso do Senado Americano desde 2010 que poderiam trazer grandes mudanças: SOPA e PIPA, que garantem que o Dep. de Justiça e os Departamentos responsáveis pelos Direitos Autorais consigam ir à justiça para que violações sejam tiradas do ar ao bloquear conteúdo do exterior, suspender o pagamento direitos ou verbas, suspender totalmente a publicidade e responsabilizar os provedores; e SISPA, que busca combater cibercrimes, incluindo sobre atos cometidos no exterior (rebateria o direito ao anonimato e a questão da competência jurisdicional), ao criar Agência de Vigilância Mundial e uma Plataforma de Ciberinteligência com punições bem definidas, inclusive a empresas e governos (divulgando dados sigilosos).

Tudo isto justifica interceptações e violações de privacidade sem nunca o cidadão – de qualquer país – ter o conhecimento. A Regra 41 (2016) dos Procedimentos Especiais concede poderes ao FBI para interceptar qualquer computador suspeito sem reportar-se ao judiciário, isto é, "deram-se" permissão para invadir qualquer computador do mundo.

Conclusão

É a partir da articulação inteligente de políticas públicas, com a devida transparência, que se pode alcançar os melhores resultados, sobretudo, quando se trata de evolução cultural que deve permear as organizações do Estado e a própria cidadania, tendo em vista a utilização ética e eficiente dos recursos públicos. Assim, em relação ao tratamento de dados, deve o Brasil tomar medidas eficientes para seu cuidado.

Referências bibliográficas

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Viroílio Afonso da Silva da 5ª edição de "Theorie der Grundrechte" (2006). São Paulo: Malheiros Editores LTDA, 2009.

CENEVIVA, Ricardo. Avaliação e *Accountability* no Setor Público: um Vínculo Possível e Desejável. **Revista Alcance**, Itajaí, SC, vol. 14, n.1, p. 7-26, Jan/Abr 2007, 2008.

DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado.** Ed. 30. São Paulo: Editora Saraiva, 2011.

GOVERNMENT ACCOUNTABILITY OFFICE (GAO). **Normas de auditoria governamental.** Salvador: Tribunal de Contas do Estado da Bahia, 2005.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Governance in the Public Sector:** a governing body perspective. New York: IFAC, August 2001. (Study, n. 13)

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). **The Lima declaration of guidelines on auditing precepts.** Viena: INTOSAI, 1998. Disponível em: <http://www.intosai.org/blueline/upload/limadeklaren.pdf>. Acesso em: 14 out. 2019.

INTERNETLAB. **Por que se preocupar com o que o Estado faz com nossos dados pessoais?** 2018. Disponível em: <http://www.internetlab.org.br/pt/privacidade-evigilancia/especial-apps-do-governo/>. Acesso em: 14 out. 2019.

PRZEWORSKI, A. **Reforma do Estado:** responsabilidade política e intervenção econômica. Revista Brasileira de Ciências Sociais, v.11, n. 32, p. 17 - 40, 1996.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Avaliação da voz dos cidadãos e responsabilização:** Moçambique, relatório final. OECD, 2008. Disponível em: <http://www.oecd.org/dataoecd/20/46/41005757.pdf>. Acesso em: 14 out. 2019.

RULE 41. **Search and Seizure.** 2016. Disponível em: <https://www.law.cornell.edu/rules/frcrmp/rule_41>. Acesso em: 16 jun. 2019.

SIU, Marx Chi Kong. Accountability no Setor Público: uma reflexão sobre transparência governamental no combate à corrupção. **Revista do TCU**, Brasília, Set/dez 2011. p. 78-87, 2011.

4.5. A disciplina jurídica do tratamento de dados pelo governo federal do Brasil – *Óthon Castrequini Piccini*[95]

[95] Graduando na Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo (FDRP/USP).

Resumo

Este trabalho, baseado em capítulo de relatório de Iniciação Científica do autor para a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), reunirá os instrumentos normativos (decretos e portarias) do Governo Federal do Brasil responsáveis por disciplinar matérias que guardam relação com o tratamento de dados pessoais, tais como: produção e segurança da informação; compartilhamento de bases de dados, interoperabilidade e comunicação interna; política de dados abertos, cidadania digital e transparência. A descrição destes atos normativos secundários será acompanhada da correlação dos mesmos com a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados. O objetivo da pesquisa é possibilitar um registro completo do estado de coisas vigente do assunto em âmbito federal, oportunizando modelos normativos que sirvam de base para os demais entes federativos. Além disso, poder-se-á avaliar a compatibilidade destes instrumentos com as exigências ocasionadas pelo novo regime jurídico brasileiro de proteção de dados pessoais.

Palavras-chave: Tratamento de dados; Governo Federal do Brasil; cidadania digital.

Abstract

This work will bring together the normative instruments (decrees and ordinances) of the Federal Government of Brazil responsible for disciplining matters related to the processing of personal data, such as: production and security of information; database sharing, interoperability and internal communication; open data policy, digital citizenship and transparency. The description of these secondary normative acts will be accompanied by their correlation with the Access to Information Act and the General Data Protection Act. The objective of the research is to enable a complete record of the current state of affairs of the subject at the federal level, providing opportunities for normative models that serve as a basis for other federative entities. In addition, the compatibility of these instruments with the requirements of the new Brazilian personal data protection legal regime may be assessed.

Keywords: Processing Data. Federal Government of Brazil. Digital citizenship.

Introdução

Considerando as demandas técnicas ocasionadas pelo advento da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), faz-se necessário proceder a um levantamento documental do estado de coisas vigente, no Governo Federal do Brasil, referente aos instrumentos normativos que disciplinam o tratamento de dados em seu âmbito de competência. As fontes normativas reunidas neste trabalho, além de revelarem a atual regulamentação da matéria em âmbito federal, servirão de base para

os demais entes federativos providenciarem suas respectivas normatizações. Além disso, poder-se-á avaliar a compatibilidade destas com as exigências ocasionadas pelo novo regime jurídico brasileiro de proteção de dados pessoais.

Para isso, cabe abordar os seguintes instrumentos: o *Sistema de Administração dos Recursos de Tecnologia da Informação* (Decreto nº 7.579/2011), a *Política de Dados Abertos* (Decreto nº 8.777/2016), a *Política de Governança Digital* (Decreto nº 8.638/2016), a *Estratégia de Governança Digital* (Portaria MP nº 107/2018), a *Plataforma de Cidadania Digital* (Decreto nº 8.936/2016), o *Compartilhamento da Base de Dados* (Decreto nº 10.046/2019), a *Política Nacional de Segurança da Informação* (Decreto nº 9.637/2018).

Desenvolvimento

1. Produção e segurança da informação

No Executivo Federal, esta função fica a cargo do *Sistema de Administração dos Recursos de Tecnologia da Informação* (SISP), regulamentado pelo Decreto nº 7.579, de 11 de outubro de 2011. Dentre suas funções, constam assegurar ao Governo Federal o suporte de informação adequado, dinâmico e eficaz, estimular o uso racional dos recursos de tecnologia da informação (TI), visando à melhoria da qualidade e da produtividade do ciclo da informação, e proporcionar o desenvolvimento, a padronização, a integração, a interoperabilidade, a normalização dos serviços de produção e disseminação de informações, de forma desconcentrada e descentralizada (art. 2º, I, IV e V).

Como órgão central do SISP, o Decreto nº 7.579/2011 aponta a Secretaria de Tecnologia da Informação e Comunicação do antigo Ministério do Planejamento (art. 3º, I), cujas funções são atualmente abarcadas pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia. Dentre suas competências, está promover a disseminação de políticas, diretrizes, normas e informações disponíveis, de interesse comum, entre os órgãos e as entidades abrangidos pelo SISP (art. 4º, V), no qual se incluem, como órgãos setoriais, as unidades de administração dos recursos de TI de cada Ministério (art. 3º, II).

Conforme o art. 2º, §1º, consideram-se *recursos de tecnologia da informação* o conjunto formado pelos bens e serviços de TI que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as *atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação*. Logo, este decreto intenciona balizar, de forma integrada, o *controle dos recursos de TI* para que as diversas unidades do Executivo possam potencializar os respectivos mecanismos de produção e disseminação de informações. Para isso, o órgão central do SISP estabelecerá os limites de valores a partir dos quais os órgãos e as entidades submeterão a contratação de bens ou

serviços de TI à sua aprovação (art. 9º-A), como também realizará a as aquisições e contratações centralizadas de bens e serviços comuns de TI (art. 9º-B).

A Lei de Acesso à Informação (LAI) arrola, em seu art. 23, as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, como aquelas que possam por em risco a defesa e soberania nacionais ou a integridade do território nacional, ameacem as relações internacionais e a estabilidade econômica do país, comprometam a vida, segurança ou saúde da população e prejudiquem planos estratégicos das Forças Armadas, atividades de inteligência e projetos de pesquisa e desenvolvimento científico e tecnológico. A depender do teor ou imprescindibilidade à segurança da sociedade ou do Estado, informações dessa natureza, nos termos do art. 24, poderão ser classificadas como *ultrassecreta* (25 anos de restrição de acesso), *secreta* (15 anos de restrição) ou *reservada* (acesso restrito por cinco anos). Os procedimentos para credenciamento de segurança e tratamento de informação classificada estão previstos no Decreto nº 7.845, de 14 de novembro de 2012, com base nos arts. 25, 27 e 29 da LAI.

Outro importante ato normativo nessa matéria é o recente Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a *Política Nacional de Segurança da Informação* (PNSI). Por este decreto, o Gabinete de Segurança Institucional da Presidência da República estabelecerá norma geral sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal (art. 12, I). Estes últimos, por sua vez, elaborarão política própria com fulcro na norma do GSI, designarão um gestor interno de segurança da informação e instituirão um comitê para deliberar sobre assuntos relativos à PNSI (art. 15, II, III e IV). À CGU, no mais, caberá auditar a execução das ações da PNSI de responsabilidade dos órgãos e entidades (art. 14).

O Decreto nº 9.637 ainda prevê que o Gabinete de Segurança Institucional deverá elaborar e publicar a *Estratégia Nacional de Segurança da Informação* (art. 12, V), a qual será dividida em cinco módulos: (i) segurança cibernética; (ii) defesa cibernética; (iii) segurança das infraestruturas críticas; (iv) segurança da informação sigilosa; (v) proteção contra vazamento de dados. A minuta do primeiro módulo, denominado "*E-Cyber*", encontra-se em debate e foi disponibilizada para consulta pública em setembro de 2019 (BRASIL, 2019).

2. Comunicação interna, interoperabilidade e compartilhamento de dados

Detalhes dessa seara encontram-se, para o Executivo Federal, na *Política de Governança Digital* (Decreto nº 8.638/2016), na *Estratégia de Governança Digital* (Portaria MP nº 107/2018) e no *Compartilhamento de Base de Dados* (Decreto nº 8.789/2016).

O Decreto nº 8.638, de 15 de janeiro de 2016, introduziu o conceito de *governança digital*, definindo-a como a utilização, pelo setor público, de recursos de tecnologia da informação e comunicação (TIC) com o objetivo de melhorar a disponibilização de dados e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo (art. 2º, III). Por sua vez, *tecnologia da informação e comunicação* (TIC) é entendida como um ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações (art. 2º, V).

Como uma das diretrizes do planejamento e execução e programas, projetos e processos relativos à governança digital, o Decreto nº 8.638 prevê, observadas as disposições da Lei de Acesso à Informação, a implementação do compartilhamento de dados entre os órgãos e as entidades da administração federal, sempre que houver necessidade de simplificar a prestação de serviços à sociedade (art. 4º, V). Além disso, para estabelecer os objetivos estratégicos, as metas, os indicadores e as iniciativas da Política de Governança Digital, bem como nortear programas, serviços e atividades a ela relacionados, determina-se que o Ministro do Planejamento, Orçamento e Gestão edite a *Estratégia de Governança Digital* (EGD - art. 5º). Para contribuir com esta, os órgãos e entidades elaborarão planos diretores de TIC (art. 8º).

A versão revisada da EGD foi veiculada pela Portaria MP nº 107, de 02 de maio de 2018. Um dos objetivos estratégicos elencados pelo documento é, justamente, *compartilhar e integrar dados, processos, serviços e infraestrutura* (BRASIL, 2018, p. 45). Como iniciativas a serem promovidas para esse fim, destacam-se as seguintes: (i) simplificar a integração entre serviços digitais por meio da *plataforma de interoperabilidade* de sistemas e dados do Governo Federal; (ii) disponibilizar bases de dados de governo para subsidiar a avaliação de políticas públicas e a melhoria de serviços públicos pelos diferentes órgãos da Administração.

Para a primeira iniciativa, a meta é dobrar o número disponível de *Interfaces de Programação Aplicadas* (APIs – "*application programming interface*"), as quais, de maneira resumida, são mecanismos virtuais de interoperabilidade de dados. Exemplos de serviços simplificados por APIs são a emissão de passaporte, a verificação de quitação eleitoral e do serviço militar obrigatório, dinamizados pelo intercâmbio eletrônico de informações (BRASIL, 2018, p. 40).

A criação de novas APIs atende, inclusive, ao disposto na Lei nº 13.460, de 26 de junho de 2017 (Código de Defesa do Usuário do Serviço Público), que consagra, como *diretriz para os agentes públicos*, a aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao usuário e a propiciar melhores condições para o compartilhamento das informações (art. 5º, XIII). E, como *direitos básicos do usuário*, a atuação integrada e sistêmica na expedição de atestados, certidões e

documentos comprobatórios de regularidade (art. 6º, V) e o acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados (art. 6º, III).

Já a segunda iniciativa supracitada deste objetivo estratégico da EGD relaciona-se com o recentíssimo Decreto nº 10.046, de 09 de outubro de 2019, que complementou a Política Nacional de Governança Digital ao estabelecer as normas e as diretrizes para o *compartilhamento de dados* entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União. Suas finalidades são simplificar a oferta de serviços públicos, otimizar a avaliação de políticas públicas, possibilitar a análise das condições de acesso ou manutenção de benefícios sociais e fiscais, promover a melhoria da fidedignidade dos dados e eficiência das operações internas (art. 1º).

Este novo decreto, inclusive, surge para compatibilizar as disposições infralegais dessa matéria às inovações trazidas pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Nos termos dos art. 25 da LGPD, os dados deverão ser mantidos em formato *interoperável e estruturado para o uso compartilhado*, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Já o art. 26 da mesma lei condiciona o uso compartilhado de dados pessoais somente para fins de execução de políticas públicas e respectivas atribuições legais de órgãos e entidades públicas, respeitados os princípios protetivos elencados no art. 6º da LGPD. Veda-se, ao Poder Público, a transferência a entidades privadas de dados pessoais constantes de bases a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que a exija, quando houver previsão legal ou respaldo em contratos, convênios ou instrumentos congêneres ou na hipótese de prevenção de fraudes ou irregularidades (art. 26, §2º), todas situações nas quais deverá haver consentimento da Autoridade Nacional de Proteção de Dados (art. 27).

Para instrumentalizar estes ditames, o art. 2º do Decreto nº 10.046/2019 define *dados cadastrais* como informações identificadoras perante os cadastros de órgãos públicos, tais como: (i) *atributos biográficos*, a exemplo de nome civil ou social de pessoas naturais, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, endereço, vínculos empregatícios; (ii) os números de inscrição no Cadastro de Pessoas Físicas (CPF), no Cadastro Nacional de Pessoas Jurídicas (CNPJ), no Programa de Integração Social (PIS), no Programa de Formação do Patrimônio do Servidor Público (PASEP); (iii) os números de Identificação Social (NIS) e do Título de Eleitor. Estes, junto a *atributos biométricos* (características biológicas e comportamentais mensuráveis da pessoa natural, como palma da mão, digitais dos dedos, retina ou íris dos olhos, formato da face, voz e maneira de andar), podem compor uma determinada *base integradora* de dados (art. 2º, VI).

Uma *base integradora* instituída pelo Decreto nº 10.046/2019 é o *Cadastro Base do Cidadão* (art. 16), que viabilizará a criação de meio unificado de identificação do cidadão e uma interface comum de atualização

de dados cadastrais, de modo a possibilitar o cruzamento de informações das bases oficiais a partir do número de inscrição do cidadão no CPF. Compete à Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia sua implantação, operação e monitoramento (art. 19) e o SISP emitirá recomendações técnicas para a consolidação da interoperabilidade (art. 17). Foi instituído, também, um *Comitê Central de Governança de Dados* (art. 21), a ser composto por representantes de ministérios e do Instituto Nacional do Seguro Social (INSS), para deliberar sobre orientações e diretrizes para a categorização de compartilhamento, dentre outras questões.

Ainda sob o regime revogado, o Ministério do Planejamento lançou, em 19 de julho de 2017, a "*Plataforma GovData*" ("www.govdata.org.br"), que reúne as vinte bases de dados mais acessadas do Governo Federal, como o CPF, o Sistema Integrado de Administração de Recursos Humanos (Siape), o Sistema Integrado de Administração Financeira do Governo Federal (Siafi) e o Registro Nacional de Veículos Automotores (Renavam). Por meio do SISP, a *GovData* dissemina-se pela Administração. Valendo-se da plataforma, o Ministério do Desenvolvimento Social identificou, em abril de 2018, mais de 151 mil suspeitas de irregularidades no pagamento do Benefício de Prestação Continuada (BPC), apontadas nos registros de pessoas com renda per capita superior a meio salário mínimo e de 17 mil falecidos ainda figurando como beneficiários (BRASIL, 2018).

No mais, o Decreto nº 10.046 também estabeleceu níveis de compartilhamento de dados (art. 4º): (i) *amplo*, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso; (ii) *restrito*, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades para a execução de políticas públicas; (iii) *específico*, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos.

3. Comunicação externa, dados abertos e cidadania digital

Para os fins deste tópico, o Governo Federal conta com a *Política de Dados Abertos* (Decreto nº 8.777, de 11 de maio de 2016) e a *Plataforma de Cidadania Digital* (Decreto nº 8.936, de 19 de dezembro de 2016).

A primeira intenciona promover a publicação das bases de dados de órgãos e entidades da administração pública federal, aprimorar a cultura de transparência pública, franquear aos cidadãos o acesso, de forma aberta (salvo as hipóteses de restrições), os dados produzidos ou acumulados pelo Executivo federal, fomentar o controle social e a pesquisa científica de base empírica sobre a gestão pública e facilitar o intercâmbio de informações entre a Administração Federal e as diferentes esferas da federação (art. 1º do Decreto nº 8.777/2016).

Dado é uma sequência de símbolos ou valores, representados em qualquer meio, produzidos como resultado de um processo natural ou artificial (art. 2º, I). *Dado acessível ao público* é aquele gerado ou acumulado pelo Governo que não esteja sob sigilo ou sob restrição de acesso nos termos da Lei de Acesso à Informação (art. 2º, II). *Dados abertos*, enfim, são *dados acessíveis ao público* representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na Internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte (art. 2º, III). São esses os conceitos jurídicos básicos afixados pelo Decreto nº 8.777.

A gestão da *Política de Dados Abertos*, originalmente atribuída ao extinto Ministério do Planejamento, passou a ser de competência da Controladoria-Geral da União, após as reorganizações administrativas de 2019. A CGU exercerá a sua coordenação por meio da *Infraestrutura Nacional de Dados Abertos* (INDA), esta já existente desde 2012 (Instrução Normativa MP nº 04, de 12 de abril de 2012). A INDA, integrada obrigatoriamente pelos órgãos do SISP e gerida por um comitê composto por representantes indicados por ministérios e pelo IBGE, já permitia a adesão voluntária de outros Poderes e entes federativos para a disponibilização de dados no portal ("*www.dados.gov.br*") criado à época (arts. 3º, 4º e 5º da IN MP nº 04/2012).

O Decreto nº 8.777, assim, aproveitou a estrutura já constante da INDA e instalou-a no bojo de uma política nacional para a área. Para implementá-la, cada órgão e entidade deverá executar um próprio *Plano de Dados Abertos*, a dispor sobre criação e manutenção de catálogos corporativos de dados, cronograma relacionado aos procedimentos de abertura e atualização de suas bases, especificações sobre as responsabilidades de cada uma de suas unidades neste desenvolvimento, e criação de mecanismos de engajamento do cidadão (art. 5º, §2º do Decreto nº 8.777). No mais, a INDA poderá estabelecer normas complementares para a elaboração dos planos, cada órgão e entidade contarão com uma autoridade designada pelo dirigente máximo para supervisionar a execução e compete ao Ministério da Economia definir os padrões e a gestão dos demais aspectos tecnológicos da INDA (art. 5º, §§3º, 4º e 5º).

Já a disponibilização de dados com ênfase na dinamização da prestação de serviços públicos dá-se com a *Plataforma de Cidadania Digital* (Decreto nº 8.936, de 19 de dezembro de 2016), por meio do domínio "*www.servicos.gov.br*" (art. 3º, I do Decreto nº 8.936). O sítio conta com uma ferramenta de solicitação e acompanhamento dos serviços públicos, que contém suas identificações e principais etapas, veículo de solicitação e agendamento eletrônico, acompanhamento das solicitações por etapas e peticionamento eletrônico de qualquer natureza (art. 3º, III). Há, também, uma ferramenta de avaliação da satisfação dos usuários (art. 3º, IV), bem como um painel de monitoramento do desempenho dos serviços públicos prestados, com, no mínimo, as seguintes informações para cada serviço, órgão ou entidade: volume de

solicitações, tempo médio de atendimento, grau de satisfação dos usuários e número de pedidos de simplificação (art. 3º, V).

A partir disso, os órgãos e as entidades da Administração Federal deverão cadastrar e atualizar as informações dos serviços oferecidos no portal, integrar a ele seus sistemas de atendimento e protocolo, implementar ações de melhoria com base nos resultados da avaliação de satisfação dos usuários do serviço (art. 4º do Decreto nº 8.936).

Conclusão

Com as informações reunidas no item "*desenvolvimento*", é possível chegar à constatação do quão recente é a disciplina jurídica do tratamento de dados no Governo Federal, tendo em vista uma ainda incipiente Estratégia de Segurança da Informação e uma nova política de compartilhamento de dados introduzida em meio à elaboração deste estudo.

Além disso, chama a atenção como, em poucos anos, o Poder Executivo Federal do Brasil conseguiu construir uma cadeia normativa capaz de abarcar diversas facetas da proteção de dados, isto é, desde a forma de administração e produção dos recursos de tecnologia da informação, a disseminação e compartilhamento interno, pela interoperabilidade, e a disponibilização aberta de dados, ressalvados os casos de restrição.

Logo, conclui-se que a normatização do tratamento de dados, em âmbito federal, segue, na última década, em uma marcha de expansão e ajustes, que apresenta tendência de intensificação, nos próximos anos, com as demandas técnicas proporcionadas pela Lei Geral de Proteção de Dados Pessoais.

Referências bibliográficas

BRASIL. Câmara dos Deputados. **Lei nº 12.527, de 18 de novembro de 2011.**

_____. Câmara dos Deputados. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm/>. Acesso em: 10 out. 2019.

_____. Câmara dos Deputados. **Lei nº 13.460, de 26 de junho de 2017.**

_____. Governo Federal. **Decreto nº 7.579, de 11 de outubro de 2011.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm/>. Acesso em: 07 out. 2019.

_____. Governo Federal. **Decreto nº 8.777, de 11 de maio de 2016.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8777.htm/>. Acesso em: 08 out. 2019.

_____. Governo Federal. **Decreto nº 8.638, de 15 de janeiro de 2016.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8638.htm/>. Acesso em: 08 out. 2019.

_____. Governo Federal. **Portaria MP nº 107, de 02.05.2018.** Disponível em: <http://www.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MP_n_107_de_02052018.html/>. Acesso em: 12 out. 2019.

_____. Governo Federal. **Decreto nº 8.936, de 19 de dezembro de 2016.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8936.htm/>. Acesso em: 14 out. 2019.

_____. Governo Federal. **Decreto nº 9.637, de 26 de dezembro de 2018.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm/>. Acesso em: 14 out. 2019.

_____. Governo Federal. **Decreto nº 10.046, de 09 de outubro de 2019.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm/>. Acesso em: 14 out. 2019.

_____. Governo Federal. Mais de 151 mil suspeitas de irregularidades são identificadas no pagamento do BPC. *In:* **Secretaria Especial do Desenvolvimento Social.** Disponível em: <http://mds.gov.br/area-de-imprensa/noticias/2018/abril/mais-de-151-mil-suspeitas-deirregularidades-sao-identificadas-no-pagamento-do-bpc/>. Acesso em: 14 out. 2019.

4.6. Segurança pública no Brasil: desafios à luz do tratamento de dados pessoais – *Maria Eduarda Sampaio de Sousa*[96], *Matheus José Chiaramonte de Castro*[97] *& Cíntia Rosa Pereira de Lima*[98]

[96] Graduanda na Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo (FDRP/USP).

[97] Graduado na Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo (FDRP/USP). Advogado.

[98] Professora Associada da Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo (FDRP/USP).

Resumo

Os novos sistemas de tratamento de dados na segurança pública, apesar de aumentarem eficiência, acabam por reproduzir antigos problemas institucionais. O presente trabalho pretende, portanto, analisar a construção da segurança pública brasileira, associada ao estudo do emprego das novas tecnologias da informação na área. A pesquisa realizará a investigação sobre as características e circunstâncias do fenômeno.

Palavras-chave: Segurança pública; Brasil; polícia; tratamento de dados pessoais; tecnologia da informação.

Abstract

The new data processing systems in public safety, while increasing efficiency, end up reproducing old institutional problems. The present work intends, therefore, to analyze the construction of the Brazilian public security, associated to the study of the use of the new information technologies in the area. The research will carry out the investigation into the characteristics and circumstances of the phenomenon.

Keywords: Public safety. Brazil. Police forces. Personal data treatment. Information technology.

Introdução

O crescimento da informação digitalizada está intimamente relacionado à facilidade de geração, manipulação, transmissão e armazenamento de dados (MURRAY, 2016, p. 43). Todos esses fatores contribuem para o aumento do valor intrínseco dos dados digitais, formando um novo mercado explorado por empresas que oferecem serviços de tratamento de dados destinado a finalidades específicas (propaganda direcionada, classificação pessoal etc.).

A digitalização da informação também resulta no aprimoramento de técnicas de exercício do Poder de Polícia do Estado. Aproveitando-se de tal demanda, diversas empresas surgem com o objetivo de explorar o mercado de instrumentos para previsão de atividade criminosa (AGUIRRE, BRADAN e MUGGAH, 2019, p. 04).

Evidente, portanto, a importância da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) e demais legislações específicas como mecanismos de regulação do ambiente informacional. A LGPD apresenta uma série de diretrizes que norteiam o tratamento de dados pessoais, seguindo os fundamentos da autodeterminação informativa, inviolabilidade da intimidade, e outros (art. 2º). Porém, o art. 4º do referido diploma legal isenta o tratamento de dados pessoais realizados para fins exclusivos de segurança pública da aplicação da Lei (art. 4º, III, a).

Apesar da exceção destacada, a LGPD determina que o tratamento de dados para fins de segurança pública seja regido por legislação específica, com previsão de "medidas proporcionais e estritamente necessárias ao atendimento do interesse público" (art. 4º, §1º). Ademais, o parágrafo terceiro também prevê a atuação da autoridade nacional na emissão de opiniões técnicas e recomendações referentes às exceções destacadas na Lei.

Diante de tal cenário, é necessário instituir mecanismos de compatibilização entre o interesse público e a proteção da intimidade dos cidadãos, a fim de conter arbitrariedades estatais. O presente trabalho pretende, desse modo, analisar algumas técnicas de tratamento de dados empregadas no âmbito da segurança pública, especialmente, no que se refere à atuação policial em níveis locais e atividades de vigilância do Estado.

Por fim, empregar-se-á método de pesquisa qualitativa para alcançar o objetivo apresentado, a partir do estudo indutivo da doutrina concernente ao tema, com intuito de construir base teórica hábil a respaldar a análise do fenômeno.

1. Construção da Segurança Pública no Brasil

É notório que o Brasil, nas últimas décadas, tem melhorado seus indicadores econômicos e sociais. Por outro lado, os dados sobre a criminalidade ainda mostram que o país caminha a passos lentos rumo à desejada pacificação social, o que demonstra que os desafios das políticas públicas na área de segurança ainda persistem, sobretudo ao se considerar a taxa de mortes por agressão, que, no ano de 2013, foi de 28,3 por 100 mil habitantes (LIMA, BUENO e MINGARDI, 2016, p. 51). O caminho para a solução desse problema, porém, não passa pelo aumento nos investimentos na área: o Brasil, em 2014, reservou mais de R$ 70 bilhões, cerca de 1,3% do seu PIB, para a segurança pública, mesmo índice observado em países como a Alemanha, que contabiliza taxa de homicídio abaixo de 1 por 100 mil habitantes (LIMA, BUENO e MINGARDI, 2016, p. 53). Tais dados, além de evidenciarem que a solução não passa necessariamente por grandes investimentos, sinalizam que o problema da segurança pública brasileira demandaria reformas decisivas nas próprias instituições responsáveis pela área no país.

As pressões sociais resultantes dos índices alarmantes da violência, contudo, têm contribuído para frear os anseios de reformas estruturais e, assim, têm reforçado as estruturas já existentes, numa tentativa emergencial de solucionar o problema. É por isso que cada vez mais alguns discursos se avolumam no seio popular, como o endurecimento das penas, aumento da repressão policial e até o de armamento da população, respostas penalizantes e diretas, as quais enfraquecem outras técnicas mais eficientes a longo prazo, como o aperfeiçoamento da inteligência, uso intensivo de informações e regras mais claras sobre as funções e relacionamento entre polícias federais e estaduais, civis e militares. Com o discurso repressivo, desconsidera-se que também a investigação, a dissuasão e a prevenção fazem parte da

segurança pública, medidas que, além de custos menores, não apresentam, ao menos a princípio, resultados colaterais danosos, como a perda de vidas e destruição de patrimônio (ZALUAR, 2019, p. 12).

Em outras palavras, as respostas à violência no Brasil passam principalmente pelo chamado combate ao inimigo, artifício que contribui para a consolidação da visão de certos segmentos sociais como naturalmente perigosos e, com isso, tidos como objeto principal de neutralização (LIMA, BUENO e MINGARDI, 2016, p. 57). A paz resultante desse entendimento, entretanto, é apenas imposta, não construída na política, no diálogo e no convencimento, uma vez que os confrontos armados em nada garantem que a paz deles resultantes não será apenas efêmera. Com efeito, conflitos armados deveriam ser a última opção, por se tratar de modelo de segurança pública que atua reativamente e não proativamente (ZALUAR, 2019, p. 12).

Observa-se, assim, que na esteira do combate ao inimigo manipula-se o medo da população, apostando, muitas vezes, nas reações primárias dos cidadãos, que conseguem visualizar o seu "inimigo" abatido (e, muitas vezes, morto), como forma de se legitimar os confrontos armados e garantir popularidade e votos nas eleições ao Executivo (ZALUAR, 2019, p. 13). Desse modo, a violência, seja ela cometida pelos criminosos, sociedade ou pelo próprio Estado, é uma constante no país, onde ela é vista, ainda, como uma resposta legítima para a insegurança e o medo da população (LIMA, 2019, p. 56).

A construção da segurança pública no país é regida pela ideia de que algo precisa ser feito a qualquer custo para o combate ao inimigo, ainda que isso signifique, na prática, medidas de extremo rigor e que apenas reforçam políticas criminais anacrônicas. A partir disso, deixase de considerar que todo o sistema de segurança necessita de reformas mais profundas (LIMA, BUENO e MINGARDI, 2016, p. 65).

Enfim, busca-se, em verdade, a legitimidade para matar. E, nessa guerra contra os inimigos, determinadas mortes serão naturalmente aceitas como resultados intrínsecos a ela, reforçando a fratura social brasileira entre "bandidos" e "cidadãos de bem" (LIMA, 2019, p. 58). Nesse contexto, para além do medo das pessoas envolvidas diretamente em contextos de violência, haveria aquele associado aos cidadãos indiretamente envolvidos nessas situações. Esses, por estarem mais distantes dos centros mais vulneráveis, têm seus medos mais facilmente marcados por ideologias e por discursos transmitidos na mídia tradicional e nos novos meios de comunicação. Como consequência, seus medos e inseguranças são irrefletidamente mais associados a outros sentimentos, como o ódio ao outro, ao ressentimento e à vingança, que auxiliam na perpetuação da violência (ZALUAR, 2019, p. 17).

Nessa manipulação do medo, o "bandido" encarna o mal que deve ser completamente destruído e eliminado da sociedade. Processos de estigmatização, assim, são consolidados, convergindo,

normalmente, para a direção de onde estão homens jovens, pobres, muitos de pele escura e moradores de áreas consideradas mais perigosas (ZALUAR, 2019, p. 18).

A partir dessa perpetuação de círculos viciosos de reprodução da violência no Brasil é que se encontram os dados alarmantes de 60 mil homicídios por ano e os altos índices de mortes envolvendo intervenções policiais, as quais são marcadas pelo padrão de ao menos oito pessoas mortas ao dia nessas intervenções, bem como pelo risco três vezes maior de um policial ser assassinado, em comparação com o restante da população (LIMA, BUENO e MINGARDI, 2016, p. 64-65).

Mais do que a ótica repressiva, que se mostra ineficiente e, em certa medida, discriminatória, é preciso incrementar a lógica da prevenção, a qual passa pela manutenção de equipamentos coletivos de saúde, da educação, da iluminação pública, da eliminação de terrenos baldios e veículos abandonados. De fato, todas essas medidas interferem na sensação de segurança e concretizam direitos sociais, principalmente para as populações mais vulneráveis (ZALUAR, 2019, p. 20). Contudo, a prevenção em termos de segurança pública também perpassa pelo aperfeiçoamento da inteligência e da investigação e pelo uso intensivo de informações (LIMA, BUENO e MINGARDI, 2016, p. 66). Com efeito, o Brasil ainda é carente de uma política de gestão de informações mais consolidada e que sirva ao intento de orientar a formulação, implementação e avaliação dos programas de segurança pública.

Constatou-se, por exemplo, a falta de indicadores plausíveis que atestem a relação entre as percepções sociais (sensação de segurança) e a criminalidade real, o que resulta invariavelmente na manutenção de uma agenda de trabalho por parte dos formuladores de políticas públicas voltada ao que diz a mídia, em contraposição à identificação de padrões e tendências por meio da análise minuciosa de dados (BEATO, 2000, p. 88).

2. Tratamento de dados pessoais no contexto da Segurança Pública

As novas tecnologias da informação e da comunicação (TICs) possibilitam a coleta seletiva, armazenamento, classificação, recombinação e cruzamento massivo de dados, o que permite a construção de perfis dos cidadãos (*profiling*).

Nesse contexto, a proteção da intimidade é fundamental para assegurar tanto o interesse individual quanto a igualdade do tratamento de dados, isto é, a participação democrática na sociedade, aspecto que se sobressai no âmbito da atuação estatal (GEDIEL; CORRÊA, 2008, p. 144). A imprescindibilidade da proteção aos direitos fundamentais acentua-se diante da *sociedade de controle*, caracterizada pelo controle contínuo e comunicação instantânea (DELEUZE, 2000, p. 216), cujas circunstâncias são favorecidas na conjuntura de sociedade informacional e *Big Data*.

Atualmente, contudo, verifica-se a tendência de flexibilização dos direitos fundamentais em favor da segurança pública, utilizando-se da narrativa do medo para justificar o aumento do aparato estatal contra a violência, principalmente, a violência urbana (GEDIEL; CORRÊA, 2008, p. 145).

Enfim, passar-se-á ao exame do emprego de tecnologias digitais nas atividades de vigilância no âmbito da segurança pública.

2.1. Câmeras de vigilância e reconhecimento facial

De maneira geral, as medidas de vigilância desenvolvidas para prevenção de crimes em espaços públicos envolvem tecnologias de câmera e vídeo, conhecidas como circuito fechado de televisão (CFTV) ou, em inglês, *closed circuit television* (CCTV). Na cidade de São Paulo, por exemplo, o governo municipal desenvolveu projeto denominado "City Câmeras", com objetivo de construir rede de videomonitoramento através de câmeras públicas e privadas instaladas na cidade[99].

A difusão dos sistemas de CFTV, como integrantes da política de segurança pública nas cidades, está acompanhada de discussões quanto a sua eficiência no combate à criminalidade. Uma perspectiva clássica defende que a instalação de câmeras de vigilância, especialmente em locais visíveis, pode prevenir a prática do crime ao dissuadir o potencial ofensor à prática do delito, ante maior probabilidade de ser identificado (WELSH; FARRINGTON; TAHERI, 2015, p. 113). Por outro lado, os sistemas de CFTV são acompanhados de sobrecarga de informação, assim, na prática da filtragem dos dados, os controladores tendem a observar certos grupos de indivíduos de maneira mais incisiva, viés que pode ser transferido aos softwares de monitoramento (MURRAY; KLANG, 2005, p. 178).

Ante o excesso de informação e a sobrecarga dos controladores, busca-se a construção de sistemas capazes de analisar os dados coletados automaticamente, por meio de técnicas de identificação dos indivíduos, por exemplo, o reconhecimento facial. Os *softwares* de reconhecimento fácil mapeiam o rosto humano e o reduzem à um código numérico único, que é armazenado. Dessa forma, a partir das tecnologias de reconhecimento fácil é possível identificar o ofensor de determinado crime de forma mais rápida e eficiente. Porém, é necessário estabelecer limites à extensão da vigilância, pois deve-se garantir a proteção da intimidade como fator limitador do interesse público. Nesse sentido, os sistemas de vigilância devem ser utilizados de acordo com os interesses de segurança pública, para identificar indivíduos tão somente quando ocorre a prática de um crime (MURRAY; KLANG, 2005, p. 188).

[99] O Projeto City Câmeras tem como objetivo a instalação de 10 mil câmeras na cidade de São Paulo, com vias à diminuição da criminalidade. A gestão do monitoramento será realizada pela Guarda Civil Metropolitana e as imagens serão compartilhadas aos demais órgãos de segurança (Polícia Militar e Civil). City Câmeras: ação integrada e tecnologia por uma São Paulo mais segura. **Prefeitura de São Paulo**, São Paulo, 2017.

Ademais, é imprescindível a construção de um aparato estatal capaz de garantir segurança aos dados coletados.

2.2. Instrumentos de previsão de crimes

Outra estratégia que compõe as políticas de segurança pública atualmente são os instrumentos de previsão de crimes (*crime forecasting*), que utilizam tratamento de dados e inteligência artificial para determinar padrões em eventos criminosos (HSIEN YU; WARD; MORABITO; DING, 2011, p. 02).

O sistema de previsão de crimes é realizado a partir das seguintes teorias: teoria da atividade de rotina (*routine activity theory*), que defende a dependência da prática do crime à motivação dos ofensores, alvos adequados e ausência de policiamento capacitado; teoria da decisão racional (*rational choice theory*), a qual se baseia na capacidade do ofensor em tomar decisões racionais ao praticar o crime, a partir de estimação de custos e possibilidade de ser condenado; e teoria do padrão criminoso (*crime pattern theory),* que explica o fenômeno criminoso e suas circunstâncias (AGUIRRE; BRADAN; MUGGAH, 2019, p. 03).

A partir da combinação entre as teorias citadas, os novos softwares utilizam base de dados para prever os possíveis locais de ocorrência de crime e potenciais ofensores e vítimas. Os métodos utilizados envolvem o processamento de históricos policiais e dados sobre raça, gênero e idade de indivíduos que são considerados potenciais agentes de crimes (AGUIRRE; BRADAN; MUGGAH, 2019, p. 04). Existem, inclusive, empresas que oferecem tais serviços, por exemplo, a *PredPol*, que vende sistema de informática capaz de apresentar possíveis locais de ocorrência de atividade delitiva, e seus serviços são utilizados por mais de sessenta departamentos de polícia nos Estados Unidos (LYNSKEY, 2019, p. 167).

Evidente que tais instrumentos são controversos, uma vez que os algoritmos podem reproduzir os padrões discriminatórios dos controladores, o que conduz à arbitrariedade da repressão policial e violação aos direitos fundamentais (AGUIRRE; BRADAN; MUGGAH, 2019, p. 08). A técnica da formação de perfis dos cidadãos (*profiling*), realizada por meio das ferramentas de previsão de crimes, pode representar a intensificação de tal viés discriminatório, conduzindo a decisões automatizadas (LYNSKEY, 2019, p. 175).

Insta salientar, ainda, que a LGPD inclui os dados utilizados para formação de perfil comportamental no âmbito de aplicação da lei, pois são considerados dados pessoais, quando permitem a identificação de pessoa natural (art. 12, §2º). Desse modo, aparenta ser imprescindível a consideração do *profiling* em lei especial voltada ao tratamento de dados na segurança pública, a fim de incluir o fenômeno no contexto de proteção dos dados dos cidadãos.

Conclusão

Como observado, a segurança pública no Brasil baseia-se, sobretudo, na manipulação do medo dos cidadãos, a partir da exploração de suas reações primárias. Desse modo, reformas estruturais são renegadas, principalmente em função da opinião pública, que exige respostas imediatas ao problema da violência e da criminalidade. Surgem, como efeito disso, discursos favoráveis ao aumento da repressão policial e do armamento da população, as quais estão fundadas, irrefletidamente, em um discurso de combate ao "inimigo".

Porém, não só de viés repressivo estrutura-se a segurança pública; o problema observado está em que também sob a ótica preventiva a manipulação do medo se faz presente, o que contribui para manter a lógica – muitas vezes discriminatória – de neutralização de supostos inimigos, a partir de técnicas de tratamento de dados e de identificação de potenciais criminosos. Em suma, flexibiliza-se direitos fundamentais em favor do combate à violência e à criminalidade, e o que poderia ser um dos caminhos para solução dos problemas da segurança no Brasil é absorvido pela lógica punitivista e imediatista, própria do viés repressivo.

Desse modo, o desenvolvimento dos processos de digitalização da informação e sua popularização na sociedade atual resultou em consideráveis impactos nas políticas de segurança pública. Porém, o uso de novas tecnologias desacompanhado de alterações nas estruturas anacrônicas da segurança pública brasileira pode acarretar aparente percepção de modernidade e reforço da atividade discriminatória policial.

Diante de tal cenário, é imprescindível, portanto, a elaboração de lei especial para regulamentar o tratamento de dados pessoais no âmbito da segurança pública. Sendo assim, a exceção indicada no art. 4º, III da LGPD não pode converter-se em descaso à regulamentação do tema, pois envolve direitos e garantias individuais que devem ser protegidos. Eventual lei especial, enfim, deve abranger a proteção à intimidade dos cidadãos e assegurar o legítimo interesse público a fim de evitar arbitrariedades da atuação estatal.

Referências bibliográficas

AGUIRRE, Katherine; BADRAN, Emile; MUGGAH, Robert. **Future Crime:** Assessing twenty first century crime prediction. Igarapé Institute Strategic Note 33, Rio de Janeiro, jul. 2019.

BEATO, Cláudio. Fontes de dados policiais em estudos criminológicos: limites e potenciais. *In:* **Encontro do fórum de debates criminalidade, violência e segurança pública no brasil:** uma discussão sobre as bases de dados e questões metodológicas, v. 1, 2000, Brasília. Anais. Brasília: Ipea, 2000.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 08 de out. de 2019.

BRASIL. Prefeitura de São Paulo. City Câmeras: ação integrada e tecnologia por uma São Paulo mais segura. **Prefeitura de São Paulo**, São Paulo, 2017.

DELEUZE, Gilles. **Conversações.** 1ª ed. São Paulo: Editora 34, 2000.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção Jurídica de Dados Pessoais: a Intimidade Sitiada entre o Estado e o Mercado. **Rev. da Faculdade de Direito - UFPR**, Curitiba, v. 47, p. 141-153, 2008.

LIMA, Renato Sérgio de; BUENO, Samira; MINGARDI, Guaracy. Estado, polícias e segurança pública no Brasil. **Rev. Direito GV**, São Paulo, v. 12, n. 1, p. 49-85, Abr. 2016. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S180824322016000100049&lng=en&nrm=iso>. Acesso em: 12 de out. de 2019.

LIMA, Renato Sérgio de. Segurança pública como simulacro de democracia no Brasil. **Estud. Av.**, São Paulo, v. 33, n. 96, p. 53-68, Ago. 2019. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142019000200053&lng=en&nrm=iso>. Acesso em: 12 de out. de 2019.

LYNSKEY, Orla. Criminal justice profiling and EU data protection law: precarious protection from predictive policing. **International Journal of Law in Context**, Cambridge, v. 15, n. 02, pp. 162-176, Jun. 2019. Disponível em: <https://www.cambridge.org/core/journals/international-journal-of-lawincontext/article/criminal-justice-profiling-and-eu-data-protection-law-precariousprotectionfrom-predictive-policing/10FD4B64364191B619FBCB864CD40A7F>. Acesso em: 10 de out. de 2019.

MURRAY, Andrew. **Information Technology Law:** The Law and Society. 3 ed. Oxford: Oxford University Press, 2016.

MURRAY, Andrew; KLANG, Mathias. **Human Rights in the Digital Age.** 1 ed. Londres: Glasshouse Press. Disponível em: <https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-klang-2005.pdf>. Acesso em: 09 de out. de 2019.

ZALUAR, Alba. Os medos na política de segurança pública. **Estud. Av.**, São Paulo, v. 33, n. 96, p. 5-22, Ago. 2019. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142019000200005&lng=en&nrm=iso>. Acesso em: 11 de out. de 2019.

WELSH, Brandon C.; FARRINGTON, David P.; TAHERI, Sema A. Effectiveness and Social Costs of Public Area Surveillance for Crime Prevention. **Anual Review of Law and Social Science**, v.

11, p. 111-130, nov. 2015. Disponível em:<https://www.annualreviews.org/doi/abs/10.1146/annurev-lawsocsci-120814-121649>. Acesso em: 09 de out. de 2019.

YU, Chung-Hsien; WARD, Max W.; MORABITO, Melissa; DING, Wei. Crime Forecasting Using Data Mining Techniques. **IEEE International Conference on Data Mining**, Vancouver, Cadaná, 11 de dez. de 2011. Disponível em: <https://www.researchgate.net/publication/220765686_Crime_Forecasting_Using_Data_Mining_Techniques>. Acesso em: 10 de out. de 2019.

4.7. Meios eletrônicos de comunicação dos atos processuais: uma análise do processo judicial eletrônico no Brasil – *Márcio Martins Marano[100] & Larissa Freitas Okamoto[101]*

Resumo

O presente trabalho enfrenta a evolução tecnológica e sua direta interferência no Direito brasileiro, na medida em que o Processo Judicial Eletrônico se torna a realidade jurídica de praticamente todo sistema judiciário. O trabalho contou com farta pesquisa bibliográfica, tanto de autores de direito processual civil, quanto autores de direito eletrônico e constitucional. Durante o trabalho, fez-se uma análise dos princípios processuais e sua aplicação no Processo Judicial Eletrônico. Ainda, fez-se um estudo do histórico legislativo brasileiro, no seu caminho para a modernização e aplicação de um direito eletrônico. No desenrolar do trabalho foram analisados os diversos meios de comunicação dos atos processuais hoje feitos através de plataformas eletrônicas, bem como, estudou-se o processo judicial eletrônico implementado hoje na maior parte das Comarcas brasileiras.

Palavras-chave: processo judicial eletrônico; tecnologia; modernização.

Abstract

The present coursework faces the technological evolution and its direct interference in the Brazilian Law, as the Electronic Judicial Process becomes the legal reality of practically all judicial system. The coursework counted on abundant bibliographical research, both authors of civil procedural law and authors of electronic and constitutional law. During the coursework, an analysis was made of the procedural principles and their application in the Electronic Judicial Process. Also, a study of the Brazilian legislative historic was made, on its way to the modernization and application of an electronic right. In the developing of the coursework the various means of communication of the procedural acts

[100] Universidade do Estado de Minas Gerais – Campus de Frutal (UEMG).

[101] Universidade do Estado de Minas Gerais – Campus de Frutal (UEMG).

now made through electronic platforms were analyzed, as well as, the electronic judicial process implemented in most of the Brazilian Counties was studied.

Keywords: Electronic Judicial Process. Technology. Modernization.

Introdução

O processo judicial eletrônico implementado hoje na maior parte dos estados brasileiros, abrangendo os tribunais estaduais, bem como nas justiças especiais (militar e do trabalho) veio para ampliar o acesso à justiça, promover um processo mais célere além da economia processual, já que com a informatização, se caminha para a abolição de rotinas manuais, reforça a segurança jurídica com relação à transparência e autenticidade dos atos processuais, além da diminuição dos custos com espaço físico e papel.

A duração do processo é um fator de grande importância, que pode definir a eficácia do sistema judiciário, por isso é necessário que o processo tenha uma duração razoável, até que se chegue à resposta do conflito, pois de nada adianta uma decisão justa, que se tornou ineficaz pelo tempo.

A morosidade do sistema judicial é uma realidade enfrentada hoje pelo judiciário. O volume de demandas processuais cresce mais e mais a cada dia, gerando acumulo de serviços, sobrecarregando servidores e perfazendo um volume de processos físicos que demandam cada vez mais espaço para os suportarem. Essa morosidade compromete além da efetivação do direito buscado, a credibilidade do Poder Judiciário, que vem sendo visto como um depósito de lides que se arrastam ano após ano, sem previsão de final.

Quanto aos trâmites relativos ao andamento processual, há um notório prejuízo em relação ao tempo gasto de um ato para outro, vez que o processo físico depende diretamente de que um ato seja efetuado para que o outro possa ser realizado, ainda que independentes entre si, problema facilmente solucionado na via digital, onde os autos encontram-se disponíveis a qualquer tempo, sem que seja necessário o aguardo de seu retorno para que se tenha vista e possibilidade de efetuar demais atos sem o prejuízo da demora.

Ademais, o uso da via digital para peticionamento ou distribuição de novos feitos prolongou o prazo das partes, já que não é preciso respeitar o horário de funcionamento dos fóruns e tribunais para que seus atos sejam tempestivos.

A lei nº 11.419/2006 dispõe sobre a informatização do processo judicial, além de tornar mais efetivo os dispositivos elencados no Novo Código de Processo Civil assegura a garantia constitucional de uma prestação jurisdicional célere e eficaz, prevista no art. 5º, inciso LXXVIII, necessária, portanto, a análise quanto a sua aplicabilidade e efetividade, sendo contundente para melhor efetividade e ampliação do acesso à justiça.

A criação da lei 11.419/2006 foi um marco na legislação brasileira, pois impulsionou a informatização do poder judiciário. Com a nova redação do Código de Processo Civil, foi criada a possibilidade de atos processuais total ou parcialmente eletrônicos. Vale ressaltar que a lei e o código mencionados não colidem quanto à regulamentação do processo eletrônico, mas caso ocorra, deve-se prevalecer à norma mais recente, conforme disse Luiz Guilherme Marinoni (MARINONI, 2018).

Durante o estudo do presente trabalho, acesso à justiça como direito social básico será tratado levando em conta sua efetividade, destacando além dos benefícios advindos da informatização processual, as dificuldades enfrentadas por operadores internos e externos desta nova roupagem processual, ante a pluralidade de sistemas existentes em território nacional.

1. Meios eletrônicos de comunicação dos atos processuais

Os meios eletrônicos de comunicação dos atos processuais através do processo judicial eletrônico implementado atualmente nos tribunais brasileiros, que hoje abrange a maior parte das comarcas do país.

A lei nº 11.419/2006 dispõe sobre a informatização do processo judicial, além de tornar mais efetivo os dispositivos elencados no Novo Código de Processo Civil assegura a garantia constitucional de uma prestação jurisdicional célere e eficaz, prevista no art. 5º, inciso LXXVIII, necessária, portanto, a análise quanto a sua aplicabilidade e efetividade, sendo contundente para melhor efetividade e ampliação do acesso à justiça.

A tecnologia é uma realidade cada vez mais presente nas rotinas da sociedade como a conhecemos. Essa realidade abrange as mais diversas áreas de atuação, seja na vida pessoal ou profissional.

Na tentativa de se valer deste avanço, o direito busca formas de prover a tecnologia como forma de modificar as relações processuais como a conhecemos, facilitando o desenvolver do processo e chegando a uma solução em tempo hábil, beneficiando operadores do direito e o judiciário.

Neste sentido, explica Sérgio Renato Tejada Garcia (GARCIA, 2018):

> [...] Como efeito do processo eletrônico, cujo maior beneficiado é também o cidadão, consiste o combate à morosidade judicial. Em levantamento realizado, o CNJ concluiu que 70% do tempo gasto com o processo tradicional se referem a atos meramente burocráticos e ordinatórios e que não conduzem ao objeto do processo, que é a prestação jurisdicional. A ministra Ellen Gracie, do STF, costuma chamar esse interstício de tempo neutro, porque nada faz em benefício da causa. O processo eletrônico simplesmente elimina ou automatiza esse tempo neutro para milésimos de segundo, reduzindo o tempo total para 30%, ou seja, só resta a parte nobre do processo. E há ainda outros

> efeitos do processo eletrônico, como redução de custos, não só para o autor de uma ação judicial, mas também para o Erário, e benefícios para o meio ambiente, o que faz com que um cidadão que nunca se utilizou dos serviços da Justiça também seja beneficiado.

Esta constante mutação tecnológica e seus avanços trazem ao judiciário novas questões acerca da validade e dos limites da interferência tecnológica na sua seara. Sobre o tema, recentemente foi aprovado por unanimidade no Conselho Nacional de Justiça a intimação judicial através do aplicativo whats app no sistema dos Juizados Especiais, e vem tomando espaço em algumas varas da família e criminais.

Tal possibilidade é uma forma de desburocratização do sistema judiciário, conferindo mais agilidade e menos custos ao processo, e ainda, estaria de acordo com o princípio da instrumentalidade das formas, previsto no artigo 277 do Novo Código de Processo Civil que traz que "quando a lei prescrever determinada forma, o juiz considerará válido o ato se, realizado de outro modo, lhe alcançar a finalidade".

Por outra ótica, há divergências quanto à validade da intimação feita pelo aplicativo whats app, por representar eventual perigo ao princípio da segurança jurídica. Defende-se nesta vertente que o ato processual realizado desta forma gera uma colisão entre o princípio da celeridade processual e o princípio da segurança jurídica, sendo que para o equilíbrio do ordenamento jurídico se mantenha, um não pode prevalecer sobre o outro, sendo um complemento para o outro.

2. O processo judicial eletrônico

A adoção do processo eletrônico é hoje uma das principais politicas públicas que vem sendo desenvolvida pelo Poder Judiciário. Com destaque, o uso do sistema eletrônico de tramitação processual reduz o tempo da demanda, torna a prestação mais célere e contribui para a garantia da razoável duração do processo. A disponibilidade do processo eletrônico 24horas por dia, todos os dias da semana, o torna mais acessível que o processo físico. Conclui-se que a utilização do processo eletrônico é mais econômica e sustentável.

O questionamento que se faz é se há necessidade de um único sistema para a tramitação do processo judicial eletrônico, adotado por todos os tribunais. Para isso, há necessidade de examinar o problema pelo ponto de vista dos usuários internos (servidores, magistrados, estagiários) e usuários externos (advogados, partes).

No que diz respeito aos usuários internos, a instalação e desenvolvimento do processo eletrônico deve adotar as melhores condições de trabalho, sendo o sistema intuitivo, ergonômico, dotado de funcionalidades que otimizem o tempo de trabalho, de forma mais desburocratizada. Para estes usuários, a utilização de um sistema padrão não é sinônimo de eficiência, já que cada tribunal possui sua

particularidade, sendo na verdade o maior requisito a funcionalidade do sistema para que seja um bom instrumento de trabalho.

Quanto aos usuários externos, estes possuem outro aspecto que deve ser levado em consideração. Existem hoje no Brasil mais de 40 plataformas usadas pelos mais de 90 tribunas brasileiros, entre Tribunais Superiores, Federais, Estaduais, Militares e Trabalhistas.

Dentre os tribunais, há aqueles que possuem mais de um sistema funcionando simultaneamente, a exemplo dos Tribunais de Justiça do Paraná e Roraima que usam o PJE e PROJUDI, e do Tribunal de Justiça do Rio Grande do Norte que usa o PJE e e-SAJ.

Além disso, existem tribunais que não terminaram de implantar a plataforma eletrônica em todas as comarcas. O que se observa neste caso, é que os procuradores sofrem com a pluralidade de sistemas existentes, tendo em vista que cada plataforma possui suas particularidades de acesso. O profissional da advocacia não consegue muitas vezes se capacitar para utilizar essa diversidade de sistemas, o que prejudica sua atuação.

2.1. A criação do PJE

Pensando nisso, o CNJ em parceria com os tribunais e a Ordem dos Advogados do Brasil, desenvolveu o sistema PJE com o principal objetivo de manter um sistema eletrônico capaz de permitir os atos e acompanhamento processual, numa solução única e gratuita, observados os requisitos de segurança e interoperabilidade, independente de o processo tramitar na Justiça Federal, dos Estados, Militar ou do Trabalho. Nas palavras do Magistrado Bráulio Gusmão, gestor executivo do PJE:

> Apesar de termos vários tribunais que fizeram, desde o primeiro momento da lei, uso da tecnologia, nós temos, na verdade, ilhas e isso depõe contra a unidade do Judiciário. Isso não é bom, não é produtivo e implica em duplicidade de gastos públicos. Por isso, o CNJ adotou, há algum tempo, um sistema de processamento judicial eletrônico chamado PJe para nele concentrar seus esforços e levar o Judiciário a um caminho único, de trabalho coletivo. (GUSMÃO, Bráulio. 2015)

O sistema foi lançado oficialmente de 21 de julho de 2011, pelo então presidente do CNJ, Cezar Peluso e desde 03 de fevereiro de 2014 é o sistema oficial do CNJ.

Em 18 de dezembro de 2013, através da Resolução nº 185 do CNJ, o PJE foi reconhecido como o sistema oficial para a tramitação do processo eletrônico, no intuito de torna-lo uniforme em todo território nacional.

O artigo 36 da referida resolução diz:

> Art. 36. A partir da implantação do PJe, o recebimento de petição inicial ou de prosseguimento, relativas aos processos que nele tramitam, somente pode ocorrer no meio eletrônico próprio do sistema, sendo vedada, nesta hipótese, a utilização de qualquer outro sistema de peticionamento eletrônico, exceto nas situações especiais previstas nesta Resolução. (Resolução nº 185 de 18/12/2013)

A resolução em comento ainda prevê estruturas de atendimento e suportes aos usuários, treinamento fornecido ao Ministério Público, OAB, Procuradorias, Defensoria Pública e público externo. Ainda, a resolução veda a criação, desenvolvimento, contratação ou implantação sistema diverso do PJE, em seu artigo 44, nos seguintes termos:

> Art. 44. A partir da vigência desta Resolução é vedada a criação, desenvolvimento, contratação ou implantação de sistema ou módulo de processo judicial eletrônico diverso do PJe, ressalvadas a hipótese do art. 45 e as manutenções corretivas e evolutivas necessárias ao funcionamento dos sistemas já implantados ou ao cumprimento de determinações do CNJ.

Atualmente o PJE funciona em cerca de 75% das unidades judiciárias de 1º e 2º grau. Segundo dados fornecidos no pela revista eletrônica CONJUR, no primeiro semestre de 2017 o número de ações tramitando no PJE chegou a 15,7 milhões, o que representou uma alta de 84% no número de causas incluídas no sistema em relação a julho de 2016.

Como exemplo, o Poder Judiciário do Estado do Maranhão concluiu em agosto de 2019 a instalação do PJE em todas as 107 comarcas instaladas e não agregadas do estado. A implantação do PJE no estado do Maranhão começou em 2013 e hoje, seis anos depois, atende 73.045 usurários internos e externos. Além disso, dados do Comitê Gestor para Implantação do PJE no estado estima que desde o último trimestre de 2017, o número de protocolos de ações, incidentes, cartas precatórias r cartas de ordem em suporte eletrônico superou o número de protocolos em suporte físico.

De acordo com dados do Tribunal Superior do Trabalho – TST, cerca de 75% dos processos que tramitam na via eletrônica pertencem a Justiça do Trabalho, que é a primeira Justiça brasileira que possui 100% de seus processos na via eletrônica. A Justiça do Trabalho adotou a ideia do CNJ de uniformidade de sistema, e instalou o PJE nos 24 Tribunais do Trabalho (TRTs) e nas 1.573 Varas Trabalhistas, sendo atingida a marca de 100% das unidades em 06 de outubro de 2017, quando o sistema foi implantado nas Varas de Abaetetuba, no Pará.

Nas palavras do Ministro Ives Gandra Martins Filho:

> Nós nos engajamos e compramos a ideia vinda do CNJ de que houvesse um único programa para todo o Poder Judiciário [...] Sermos vanguardistas teve um preço caro. Houve resistência, mas, hoje, estamos colhendo os frutos de ser o primeiro ramo da Justiça totalmente eletrônico.

Um dos grandes atrativos da implantação do PJE é a economia que este promoveria ao judiciário. De acordo com uma análise feita pelo CNJ e publicada em 2017 chamada *Políticas Públicas do Poder Judiciário: Uma análise quantitativa e qualitativa do impacto da implantação do processo judicial eletrônico (PJE) na produtividade dos tribunais*, menos de 25% dos processos eletrônicos ultrapassaram a barreira dos 50 meses (cerca de 4 anos) sem a indicação de algum andamento de término processual, enquanto nos processos físicos esse número aumentou para mais de 50%, o que segundo a pesquisa, indicou um ganho de eficiência considerável com a adoção do PJE.

A pesquisa também indicou um ganho substancial em relação ao tempo de cartório do processo, já que grande parte do tempo que um processo leva até o seu termino envolve a movimentação cartorária.

Ademais, segundo a pesquisa, os juízes tendem a decidir mais rápido em processos eletrônicos:

> A análise quantitativa, por sua vez, em seu escopo mais objetivo, foi capaz de demonstrar um efeito positivo do PJe sobre o trâmite processual. Esse efeito se mostrou presente não só no tempo cartorário do processo, conforme esperado pela maioria dos entrevistados, mas também no tempo que leva para que os juízes profiram decisões em processos conclusos. Isso indica um efeito positivo para além dos efeitos óbvios esperados e contrasta com o pessimismo de entrevistados que acreditavam que a resistência natural dos juízes e usuários de gerações mais antigas – tradicionalmente acostumados ao manuseio de processos físicos – iria influir negativamente na comparação entre processos físicos e eletrônicos. A narrativa sustentada pelos dados é justamente a oposta: aparentemente, juízes decidem mais rapidamente os processos judiciais eletrônicos do que os processos físicos.

A pesquisa realizada em 2017 define a implantação do PJE como traumática para alguns entrevistados. Parte da dificuldade é relacionada com a resistência dos servidores e usuários à mudança no processo imposto pelo PJE.

> Essa resistência contribui para dificultar a transição da utilização do processo físico para o processo eletrônico para a tramitação processual, o que é algo comum. Da mesma forma, a instalação e implantação do sistema envolve desafios tecnológicos e logísticos não triviais que, em alguns casos (e.g., TJMG, TRT da 1ª Região), implica um período de transição com

> interrupções do serviço. Essas interrupções (períodos nos quais o sistema está "fora do ar"), por sua vez, reforçam os preconceitos em relação ao PJe por parte dos servidores e já chegaram a motivar protestos de setores da advocacia e jurisdicionados contra a implantação do PJe.

Sobre este tema, a plataforma do PJE apresentou durante seus anos no Justiça uma série de instabilidades, o que acabou gerando certa insatisfação e desconfiança por parte dos usuários, que acabaram optando pela "aposentadoria" do sistema. Neste sentido, a Ministra Carmem Lúcia, à época presidente do Supremo Tribunal Federal parou a implantação do PJE na Corte em 2016, através da resolução nº 594 de 10 de novembro de 2016, quando revogou a resolução 578 de 20 de abril de 2016, que previa a implementação no STF do sistema PJE.

Cita-se também, a troca do sistema PJE pelo e-PROC feita pela Turma Nacional de Uniformização dos Juizados Especiais Federais (TNU), feita em 17 de julho de 2017.

Em notícia mais recente, o CNJ autorizou em setembro deste ano que o TRF da 4ª Região, que compreende os estados do Paraná, Santa Catarina e Rio Grande do Sul, continue usando o sistema e-PROC, afastando então a aplicação da Resolução nº 185 que determinava a implantação do PJE em todos os tribunais.

O sistema e-PROC é usado nos Juizados Especiais da 4ª região desde 2003, sendo o primeiro sistema processual eletrônico da Justiça brasileira. O pedido para seguir com o uso do e-PROC foi feito pelo TRF da 4ª região em 2015, e na ocasião o CNJ aceitou liminarmente o requerimento.

Na decisão favorável, o conselheiro Luciano Frota fundamentou a decisão com base no sistema da 4ª Região já ter implantado o Modelo Nacional de Interoperabilidade (MNI), bem como se integrou ao Escritório Digital, dos quais trataremos em momento oportuno.

Vale destacar que nem só de problemas e instabilidades vive o sistema. No Distrito Federal, desde a implantação do PJE no Tribunais de Justiça do Distrito Federal e Territórios (TJDFT), que ocorreu em 2014, o PJE conta com mais de 790 mil feitos, e possibilitou a economia de mais de R$7.000.000,00 (sete milhões de reais) que antes eram gastos com matérias como capas, papel, plástico, grampos, etiquetas, impressão e Correios.

Em setembro de 2018 o PJE chegou a todos os Juizados de Violência Doméstica e Familiar Contra a Mulher do Distrito Federal, proporcionando para as vítimas deste tipo de violência decisões mais céleres. No Distrito Federal, estima-se que são recebidos cerca de 900 novos processos eletrônicos por dia.

A Portaria TSE nº 344/2019, assinada pela presidente do Tribunal Superior Eleitoral, ministra Rosa Weber, tornou obrigatória a utilização do sistema para proposição e tramitação de todos os processos no âmbito da Justiça Eleitora já a partir da primeira instância. Com isso, até o final de 2019, a Justiça Eleitoral implementará o Processo Judicial Eletrônico em todas as 2.645 zonas eleitorais do país, obedecendo cinco etapas pré-estabelecidas de avanço, que como critério avaliou a capacidade das localidades de conectividade com a internet.

Assim, é importante considerarmos a existência de um ganho de eficiência mensurável a partir da introdução do PJE, para a adoção desse mecanismo pelos tribunais brasileiros. Afinal, parece claro que o PJe ajuda a concretizar um direito fundamental, quanto a razoável duração do processo. Em contrapartida, as falhas apresentadas pelo sistema acabam por afugentar parte do público, sejam usuários internos ou externos, o que acabou por influenciar na uniformização do sistema de processos eletrônicos, e possibilitou que uma diversidade de sistemas continuasse em todo território nacional.

2.2. A pluralidade de sistemas de processo eletrônico no Brasil

Devido a rejeição do PJE por parte dos Tribunais, e a autorização da flexibilização do uso das plataformas eletrônicas pelos Tribunais no país, não há nenhum sistema padrão. Atualmente, os principais sistemas usados no Brasil são o PJE, o Projudi e o e-SAJ. Mas existem outros, como por exemplo, o já mencionado e-PROC, o Tucujuris e o Apolo.

Faz-se necessário analisar que cada tribunal possui suas especificidades, e elas precisam ser contempladas pelo sistema adotado pela instituição. Por isso há quem defenda que cada Tribunal deve operar o sistema que tiver à sua disposição as melhores soluções para sua realidade e especificidade.

Segundo Ilson Stabile, sócio fundador da Softplan, criadora da plataforma eSAJ, usada por diversos tribunais como o Tribunal de Justiça de São Paulo e os Tribunais de Justiça de Santa Catarina e Mato Grosso do Sul, adotar um sistema único de processos eletrônicos resultaria na perda de todo o trabalho feito até agora, o que acarretaria um grande retrocesso tecnológico, que nas palavras do empresário seria "nivelar por baixo", já que a proposta de unificação de sistema desconsidera as peculiaridades de cada Tribunal.

Para os escritórios e advogados, a falta de consistência ou padronização entre sistemas e tribunais é um grande obstáculo. O fato dos tribunais utilizarem sistemas distintos, com diferentes níveis de maturidade tecnológica, importa na necessidade de refazer determinadas funcionalidades já existentes, como atualização de softwares, ou programas específicos de cada plataforma.

A necessidade de diferentes configurações de computador gera a necessidade de aprendizado sobre as particularidades sobre cada programa. Como exemplo, as plataformas não funcionam com qualquer tipo

de navegador (atualmente os mais utilizados são Google Chrome, Mozilla Firefox e Internet Explorer), sendo que algumas plataformas aceitam apenas determinada versão de um navegador específico. Também, podemos citar o tamanho do arquivo suportado por cada navegador, que varia de uma plataforma para outra. Inclusive, sobre o arquivo, há sistemas como o e-SAJ que aceitam apenas o arquivo que for convertido em PDF por aplicativo definido pela plataforma.

2.3. O escritório digital

Há de se destacar que uma das dificuldades em implantar o PJE em todos os tribunais brasileiros é dota-lo com todas as funcionalidades e particularidades existentes nos outros sistemas judiciais. A necessidade de proporcionar aos advogados e usuários externos dos sistemas de processo eletrônico fez com que o CJN desenvolvesse o Escritório Digital.

Trata-se de um *software* desenvolvido pelo CNJ para integrar os sistemas processuais dos tribunais brasileiros, o que permitiria ao usuário acessar todas as plataformas onde tramitam processos de seu interesse em um único endereço.

A principal ideia é que o usuário não precise entrar no PJE ou e-SAJ, ou seja lá qual sistema utilizado para a tramitação do processo e sim um único endereço na internet que reuniria todas as informações dos processos, facilitando as buscas e acompanhamentos por advogados, procuradores, membros do MP e Defensoria Pública, assim como o público em geral.

Para que os Tribunais utilizem o Escritório Digital, é necessário que tenha aderido ao Modelo Nacional de Interoperabilidade (MNI), o qual será tratado no próximo tópico. Não será necessário que o Tribunal adote necessariamente o PJE, mas é indispensável que tenha aderido ao MNI.

Segundo o CNJ, para acompanhar o sistema há três possibilidades:

> 1. Usuário sem cadastro no PJe: para obter acesso ao sistema utilizando usuário e senha, é necessário fazer o cadastro presencial no tribunal. Dirija-se a um posto de atendimento do Processo Judicial Eletrônico (PJe) e leve CPF, RG (Número da Carteira da OAB caso seja advogado) e comprovante de residência. Será necessário informar um e-mail de contato para possibilitar renovações de senha.
>
> 2. Usuário já cadastrado no PJe: clique o botão "Solicitar senha", informe o CPF/CNPJ, o e-mail cadastrado no sistema e clique o botão "Confirma". Você receberá um e-mail com o link para cadastramento de nova senha.
>
> 3. Usuário com certificado digital: clique o botão "Acessar" e efetue o cadastro.

Para os Tribunais que já utilizam o PJE ou já aderiram ao MNI, basta solicitar junto ao CNJ a liberação da logo com a sigla do Tribunal no sistema. Os demais tribunais que utilizam sistemas diferentes ou que não tenham aderido ao MNI precisam desenvolver a interface seguindo o padrão do MNI.

Inicialmente o software foi desenvolvido com foco nos operados do Direito, mas a ideia é que futuramente o Escritório Digital seja disponibilizado para todos os cidadãos que desejem acompanhar a tramitação de processos.

O CNJ informa que o Escritório Digital já funciona na área dos Juizados Especiais do Tribunal de Justiça do Distrito Federal e Territórios, mas há planos de expansão. Além disso, o Tribunal Regional Federal da 1ª Região e o Tribunal de Justiça do Estado do Espírito Santo possuem o modelo MNI 2.2.2 implementado, e estão prontos para que ocorra a integração. Além destes, o sistema Projudi do Tribunal de Justiça do Estado do Paraná e o e-SAJ que roda no Tribunal de Justiça do Estado de São Paulo também já possuem o MNI 2.2.2 e estão prontos para a integração.

O Escritório Digital não chegou a todos os tribunais porque para que isto ocorra dependerá da adesão dos tribunais a um dos sistemas, seja PJE ou MNI. Isto porque sem um destes dois não é possível que ocorra a "conversa" entre os sistemas.

O funcionamento do Escritório Digital funciona através de qualquer navegador de internet e é adaptável a qualquer dispositivo, como computadores, smartphones ou tablets.

Insta salientar que o Escritório Digital não substituirá o PJE, pois é na verdade apenas uma ferramenta que facilita a interação do público externo com os processos que tramitam no PJE.

Sobre a segurança do sistema, o CNJ afirma que a interface é totalmente segura e usa o canal de comunicação confidencial SSL (https), além de trabalhar com certificado de segurança e criptografia de dados, especialmente na autenticação por login e senha e no banco de dados. O CNJ também faz auditoria de dados, com vários níveis de controle sobre a tramitação e o acesso, e usa a versão mais segura de servidores de aplicação. Em termos comparativos, este é o mesmo mecanismo usado pela Receita Federal nas tramitações de restituição do Imposto de Renda.

2.4. O Navegador do Advogado

Seguindo o mesmo princípio do Escritório Digital, a Ordem dos Advogados de Minas Gerais – OAB/MG desenvolveu o Navegador do Advogado. O programa é disponibilizado para *download* no site da OAB de Minas Gerais e já vem pré-configurado com relação a todas as cortes do país.

Segundo a descrição fornecida pela OAB de Minas, "*a função principal do Navegador ADV é centralizar em um único lugar todos os sistemas de peticionamento do Brasil. Você escolhe o estado e o sistema de peticionamento. De forma simples e intuitiva.*" Com o Navegador do Advogado é possível acessar as

plataformas do PJE, Projudi, e-SAJ, e-DOC, SISDOC, entre outros, dos tribunais das Justiças Regionais, Federais, Militares e Trabalhistas. O navegador funciona com os principais certificados digitais disponíveis no Brasil.

O diferencial oferecido pelo Navegador do Advogado é fornecer uma abordagem diferente, voltada para a visão da advocacia, que sofre com o grande número de plataformas diferentes.

2.5. O modelo nacional de interoperabilidade – MNI

A busca do Judiciário brasileiro pela ascensão tecnológica e seu aproveitamento no desenvolvimento no processo eletrônico, fez-se desenvolver diversos tipos de sistemas, uma das grandes dificuldades do judiciário é fazer com que esses sistemas se comuniquem entre si.

Nesta linha de pensamento, o CNJ implementou o Modelo Nacional de Interoperabilidade (MNI), cujo maior desafio é estabelecer padrões para intercâmbio de informações de processos judiciais entre os órgãos da Justiça.

O MNI é fruto do Termo de Cooperação Técnica nº 58/2009, firmado entre o CNJ e as equipes técnicas de órgãos do sistema judiciário como o Supremo Tribunal Federal, Superior Tribunal de Justiça, Conselho de Justiça Federal, Tribunal Superior do Trabalho, Conselho Superior da Justiça do Trabalho, Advocacia Geral da União e Procuradoria Geral da República.

Dentre as metas a serem atingidas, na cláusula segunda do Termo, encontram-se a integridade, a inviolabilidade e a segurança dos dados e informações, o respeito aos princípios constitucionais e garantias processuais, o tratamento adequado às informações sujeitas ao sigilo legal e a possibilidade de implementação em etapas de diversos graus de generalidade, de forma a permitir a evolução modular e abrangente das soluções de integração.

Os partícipes do Termo se comprometeram a detalhas as operações de interação entre sistemas de processos eletrônico, definir as etapas de implementação das operações, identificar o rol de informações a serem tramitadas em casa tipo de operação, publicar nos respectivos portais a documentação relativa a cada operação do respectivo serviço para uso comum dos partícipes, dentre outras.

Neste passo, é necessário definir o conceito de interoperabilidade, que é a troca de dados entre sistemas heterogêneos, na qual o sistema que recebe os dados deve reconhecê-los para identificar e aproveitar o que é útil, desprezando os dados desnecessários. Deve haver a utilização de fato das informações trocadas, ou podem ocorrer problemas como redundância ou inconsistência de dados, falha na qualidade e integralidade de dados, falhas no compartilhamento de informações, de serviços e funcionalidade.

O MNI uma ótima saída para o Judiciário, tendo em vista a pluralidade de sistemas e as diversas realidades de cada órgão. Promover a integração mais efetiva entre os sistemas da Justiça é um desafio. Iniciativas e estruturas são necessárias para que o projeto de interoperabilidade obtenha sucesso.

Atualmente, está em funcionamento a nova versão do MNI, chamada de MNI 3.0., versão atualizada em 15 de fevereiro de 2019. De acordo com o Chefe do Departamento de Tecnologia da Informação do CNJ, Antônio Augusto Silva Martins, entre as principais melhorias do novo sistema estão a autenticação por certificado digital, a remessa de autos digitais e mais informações complementares nas consultas dos processos judiciais

Conclusão

É notório o esforço que o Poder Judiciário tem empenhado para a implantação de uma justiça eletrônica no Brasil. O desenvolvimento de diversas Políticas Públicas para efetivar o funcionamento do Processo Eletrônico é a prova disso.

A possibilidade de uma justiça eletrônica surgiu de forma tímida em alguns dispositivos no começo dos anos 2000, e foi codificada pela Lei 11.419/06, que rege as normas do processo eletrônico no Brasil.

Agora mais que nunca, nos encontramos em um período de avanços tecnológicos. Uma prova disso é que hoje é possível que se procedam atos de comunicação dos atos processuais, como a intimação, através de um aplicativo de celular. Essa possibilidade prova que a interação tecnológica pode ajudar a aumentar a efetividade e celeridade da prestação judicial, tendo em vista que o aplicativo whatsapp é utilizado pela maioria esmagadora da população, que a maior parte do tempo está conectada ao aparelho celular. A visão do Judiciário ao perceber nessa interação constante uma porta para facilitar o trabalho de servidores e otimizar a comunicação com as partes, hoje foi convertida em projeto de lei que tramita para alterar o Código de Processo Civil.

A grande extensão do território nacional, sua diversidade de realidades e as diferenças entre cada estado fez com que a dificuldade de implantar um sistema unificado em todos os tribunais, flexibilizasse as disposições que tornavam a plataforma PJE como exclusiva e obrigatória para a tramitação de processos eletrônicos.

Observa-se que existe hoje no Brasil uma pluralidade de sistemas em diferentes níveis de desenvolvimento, o que acabou por tornar inviável essa padronização, já que alguns destes sistemas se encontram em fase de maior desenvolvimento do que o sistema adotado pelo CNJ. Essa pluralidade é uma consequência da forma como cada organização organiza sua gestão. Há tribunais que investiram em sistemas terceirizados que se adequam às necessidades daquele e não possuem interesse na implantação do PJE. Há também a Justiça do Trabalho, pioneira que possui 100% de seus processos

tramitando hoje através do PJE. Por outro lado, há aqueles Tribunais que adotaram o PJE, mas abandonaram a plataforma por não corresponder às expectativas.

Pela ótica dos usuários internos, sejam magistrados, sejam servidores, a utilização de uma única plataforma parece não ser necessária, mas não se pode deixar de se atentar às necessidades dos demais operadores do Direito, como os advogados e escritórios de advocacia. Estes profissionais na maioria das vezes atual em diferentes tribunais, de diferentes estados e instâncias e têm seu trabalho dificultado pela falta de capacitação e conhecimento para operar um sistema diverso daquele adotado em sua Comarca.

Para o profissional da advocacia, o cenário atual em que o Judiciário se encontra demanda a necessidade de adaptação e estudo, já que a tecnologia agora é predominante no ramo. O investimento para esses profissionais vai além da capacitação técnica, há de se lembrar de que os equipamentos tecnológicos necessitam de constante manutenção e adequação de acordo com as configurações necessárias para o funcionamento de determinado sistema.

Levando em consideração todas as dificuldades enfrentas na unificação das plataformas de processo eletrônico, estão sendo desenvolvidas outras formas de comunicação entre os Tribunais, formas estas que possibilitam o respeito pela plataforma utilizada em cada Tribunal.

O Escritório Digital, o MNI e o Navegador Digital são exemplos de políticas desenvolvidas para facilitar o trabalho tanto do usuário interno, respeitando as necessidades que cada órgão possui, e também facilitando o trabalho do advogado e demais pessoas do público externo, reunindo todas as informações decorrentes de processos em uma plataforma única, sem a necessidade de apenas um sistema operacional de processo eletrônico.

Destaca-se que o MNI tem sua funcionalidade voltada aos usuários internos, para que seus resultados possam refletir para o público externo, que teria acesso a uma interface única, como o proposto no Escritório Digital ou no Navegador do Advogado.

O desenvolvimento dessas políticas e sua efetiva funcionalidade é hoje a melhor solução para acesso ao processo eletrônico. A partir deste cenário onde todos os processos eletrônicos estarão reunidos em um só local, independente do tribunal, com interface única, as reivindicações dos advogados para um sistema único, onde seu trabalho possuirá acesso concentrado se tornará possível, sendo para estes usuários externos irrelevante qual plataforma processual os usuários internos de determinado tribunal utilizam.

Assim, é possível crer que não há a necessidade de um sistema único de processo eletrônico, desde que sejam colocados em funcionamento os ideais de comunicação entre as plataformas.

Não há como negar que a tramitação processual eletrônica ocasiona uma economia muito grande ao Judiciário. Seja em gastos com materiais, seja na sustentabilidade decorrente da não utilização de papel,

ou na economia de tempo, resultando na solução mais célere dos litígios. O tempo gasto com procedimentos cartorários foi otimizado, ademais, menciona-se a disponibilidade dos autos em tempo integral para todas as partes do processo.

O avanço tecnológico é a realidade enfrentada por todos os ramos profissionais, e a efetividade do serviço prestado depende da capacitação tecnológica de quem presta o serviço. Neste interim, é de suma importância que o Poder Judiciário atue em conjunto com os operadores do Direito para traçar um caminho que seja positivo para ambas as partes, mensurando as necessidades e particularidades de cada um, para que o efeito positivo possa ser desfrutado pela parte mais importante do processo, que é o cidadão que move o judiciário em busca de um direito pretendido.

Para este, o Poder Judiciário em conjunto com os profissionais do Direito, independentemente da roupagem processual vigente, deve garantir desde o acesso de forma ampla ao Judiciário, à garantia do devido processo legal, respeitando as prerrogativas processuais, para que ao final haja a efetivação da Justiça.

Referências bibliográficas

ALMEIDA FILHO, José Carlos de Araújo. **Processo eletrônico e teoria geral do processo eletrônico:** a informatização judicial no Brasil. 5 ed. Rio de Janeiro: Forense, 2015.

ALVIM, J.E Carreira; JUNIOR, Silvério Luiz Nery Cabral. **Processo Judicial Eletrônico:** Comentários à Lei 11.419/06. Curitiba: Juruá, 2007.

ANDRADE, Paula. **Nova ferramenta faz integração digital entre tribunais e sistema de justiça.** Disponível em: <http://www.cnj.jus.br/noticias/cnj/87006-nova-ferramenta-fazintegracao-digital-entre-tribunais-e-sistema-de-justica> Acesso em 21 de nov. de 2018.

BATISTELLA, Sérgio Renato. **O princípio da instrumentalidade das formas e a informatização do processo judicial no Brasil.** Disponível em: <http://www.abdpc.org.br/abdpc/artigos/S%C3%A9rgio%20Batistella.pdf.> Acessado em 10.Out.2018.

CLEMENTINO, Edilberto Barbosa. **Processo judicial eletrônico:** O uso da via eletrônica na comunicação de atos e tramitação de documentos processuais sob o enfoque histórico e principiológico, em conformidade com a Lei 11.419, de 19.12.2006. ed. Curitiba: Juruá, 2011.

CONSELHO NACIONAL DE JUSTIÇA. **E-PROC já está integrado com o PJE nos Juizados Especiais Federais.** Disponível em: <http://www.cnj.jus.br/tecnologia-dainformacao?catid=0&id=82318> Acesso em 21 de nov. de 2018.

CONSELHO NACIONAL DE JUSTIÇA. **Escritório digital.** Disponível em: <http://www.cnj.jus.br/sistema-carcerario-e-execucao-penal/334-sobre-o-cnj/quem-equem/quem-e-quem-tecnologia-da-informacao/79534-escritorio-digital> Acesso em 21 de nov. de 2018.

CONSELHO NACIONAL DE JUSTIÇA. Institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. **Resolução nº 185 de 18 de dezembro de 2013.** Disponível em: <http://www.cnj.jus.br/busca-atosadm?documento=2492> Acesso em 22 de nov. de 2018.

CONSELHO NACIONAL DE JUSTIÇA. **PJE:** Justiça do DF poupa R$7 milhões em quatro anos com uso do sistema. Disponível em: <http://www.cnj.jus.br/noticias/judiciario/87723-pje-justica-do-df-poupa-r-7-mi-quatro-anoscom-uso-do-sistema> Acesso em 21 de nov. 2018.

CONSELHO NACIONAL DE JUSTIÇA. **Termo de acordo de cooperação técnica nº 058/2009.** Disponível em: <http://www.cnj.jus.br/transparencia/acordos-termos-econvenios/acordos-de-cooperacao-tecnica/78380-termo-de-acordo-de-cooperacao-tecnica-n0582009> Acesso em 22 de nov. de 2018.

CONSELHO NACIONAL DE JUSTIÇA. **Tribunal compra 150 celulares para intimações por WhatsApp em Minas.** Disponível em: <http://www.cnj.jus.br/noticias/judiciario/85624-tribunal-compra-150-celulares-para-intimacoes-por-whatsapp-em-minas> Acesso em 20 de nov. de 2018.

CONSELHO NACIONAL DE JUSTIÇA. **WhatsApp pode ser usado para intimações judiciais.** Disponível em: <http://www.cnj.jus.br/noticias/cnj/85009-whatsapp-pode-serusado-para-intimacoes-judiciais> Acesso em 20 de nov. de 2018.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira De; MACIEL, Renata Mota. **Direito e Internet IV:** Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

FALCÃO, Joaquim. **Políticas públicas do Poder Judiciário:** uma análise quantitativa e qualitativa do impacto da implantação do processo judicial eletrônico (PJe) na produtividade dos tribunais. Disponível em <http://bibliotecadigital.fgv.br/dspace/handle/10438/22051> .Acessado em 25.Out.2018.

GARCIA, Sérgio Renato Tejada. E-Proc e sustentabilidade. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 71, abr. 2016. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/edicao071/Sergio_Garcia.html> Acessado em: 07. Out. 2018.

GIESEL, Taciana. et al. **Processos recebidos na Justiça do Trabalho já são 100% eletrônicos.** Disponível em: <http://www.tst.jus.br/web/pje/inicio/-/asset_publisher/eHI8/content/processos-recebidos-na-justica-do-trabalho-ja-sao-100-eletronicos?inheritRedirect=false> Acesso em 21 de nov. de 2018.

GONÇALVES, Marcus Vinícius Rios. **Novo curso de direito processual civil**, volume 1: teoria geral e processo de conhecimento (1ª parte). 8ª ed. São Paulo: Saraiva, 2011.

GRECO FILHO, Vicente. **Direito Processual Civil Brasileiro,** v.1: Teoria geral do processo e auxiliares da justiça. 23ª ed. São Paulo: Saraiva, 2013.

GRILLO, Brenno. **Sistema único para processo eletrônico não serve para o Judiciário.** Disponível em: <https://www.conjur.com.br/2016-abr-24/entrevista-ilson-stabile-sociosoftplan-criou-saj> Acesso em 21 de nov. de 2018.

IMHOF, Cristiano. **Novo código de processo civil comentando.** 2. ed. São Paulo: BookLaw, 2016.

JOAQUIM, Falcão. et al. **Políticas públicas do Poder Judiciário:** uma análise quantitativa e qualitativa do impacto da implantação do processo judicial eletrônico (PJe) na produtividade dos tribunais. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/22051> Acesso em 21 de nov. de 2018.

LIMA, Cíntia Rosa Pereira De; PEROLI, Kelvin. **Direito Digital:** *Compliance*, Regulação e Governança. São Paulo: Quartier Latin, 2019.

MACHADO, Magali Cunha; FERNANDO, MIRANDA, Silveira Melo Plentz. Lei nº 11.419/06 – **Processo Eletrônico.** Disponível em <http://docs.uninove.br/arte/fac/publicacoes/pdfs/magali.pdf>. Acesso em 08 de Out. 2018.

MACHADO, Magali Cunha; FERNANDO, MIRANDA, Silveira Melo Plentz. Lei nº 11.419/06 – **Processo Eletrônico.** Disponível em <http://docs.uninove.br/arte/fac/publicacoes/pdfs/magali.pdf>. Acesso em 08 de Out. 2018.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Código de processo civil comentado.** São Paulo: Revista dos Tribunais, 2015.

MORAES, Alexandre de. **Direito Constitucional.** 34 ed. São Paulo: Atlas, 2018.

NERY JUNIOR, Nelson. NERY, Rosa Maria de Andrade. **Código de processo civil comentado.** 16.ed. São Paulo: Revista dos Tribunais, 2016.

PAULA A. Forgioni, Patrícia Aurélia Del Nero, Renata Mota Maciel Dezem, Samantha Ribeiro Meyer-PfLug Marques (Coords.). **Direito Empresarial, Direito do Espaço Virtual e outros desafios do Direito, Homenagem ao Professor Newton De Lucca.** São Paulo: Quartier Latin, 2019.

PORTANOVA, Rui. **Princípios do Processo Civil.** Porto Alegre: Livraria do Advogado, 2003.

PRODANOVE, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do Trabalho científico.** 2ª Ed.Novo Hamburgo: Feevale, 2013.

REVISTA CONSULTOR JURÍDICO. **11 Tribunais já usam o WhatsApp para envio de intimações.** Disponível em: <https://www.conjur.com.br/2018-jan-31/11-tribunais-justicausam-whatsapp-envio-intimacoes> Acesso em 20 de nov. de 2018.

SENADO NOTÍCIAS. **Projeto autoriza intimações judiciais por WhatsApp.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/07/18/projeto-autoriza-intimacoesjudiciais-por-whatsapp> Acesso em 20 de nov. de 2018.

TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO. **CNJ autoriza TRF4 a seguir utilizando e-PROC.** Disponível em: <https://www.trf4.jus.br/trf4/controlador.php?acao=noticia_visualizar&id_noticia=13923> Acesso em 21 de nov. de 2018.

WATANABE, Kazuo. **Da Cognição no Processo Civil.** 2. ed. Campinas/SP: Bookseller, 2000.

4.8. A aplicabilidade da Lei Geral de Proteção de Dados aos condomínios edilícios: Lei n° 13.874/2019 – *Margarida Isabella Malena Macini[102], Natália Matos Santana Lourenço[103] & Tatiana Pereira Chelest Miras Diniz[104]*

Resumo

A informação pessoal está cada vez mais conectada à privacidade, no sentido de associá-la a uma menor disseminação de informações pessoais. Entretanto, tal relação é muito mais complexa do que possa parecer, gerando em nosso ordenamento jurídico a necessidade de proteção das informações pessoais como um desdobramento da tutela do direito à privacidade. Com o crescimento do acesso à informação

[102] Mestranda em Direito pela Universidade Nove de Julho – UNINOVE.

[103] Mestranda em Direito pela Universidade Nove de Julho – UNINOVE.

[104] Mestranda em Direito pela Universidade Nove de Julho – UNINOVE.

e de sua importância, a temática da privacidade emerge no tratamento dos dados pessoais. Neste estudo pretendemos tratar dos aspectos gerais da Lei Geral de Proteção de Dados, também chamada de LGPD e sua aplicabilidade nos condomínios edilícios. Por se tratar de uma lei complexa, abrangente e com previsão de multas altas no caso da inobservância de sua aplicação, há uma série de itens que devem ser levados em conta para que se possa concluir por sua aplicabilidade ou não nos condomínios edilícios, mais especificamente nos condomínios edilícios residenciais, foco desse trabalho.

Palavras-chave: informações pessoais; tratamento de dados pessoais; condomínio edilício.

Abstract

Nowadays the personal information is even more connected to privacy and cannot be disseminated without control. However, such a relationship is much more complex than it may initially appear, generating in our legal system the need to protect personal information as an extension of the protection of the right to privacy. The growth of the access to information implies the discussion about privacy and the processing of personal data. In this study we intend to address the general aspects of the law and its applicability in building condominiums. Because it is a complex, extensive and with high fines for non-compliance law, there are a number of items that must be taken into account in order to conclude whether or not the General Data Protection Law is applicable in the building condominiums, more specifically in residential building, object of this work.

Keywords: Personal Information. Processing of Personal Data. Condominiums.

Introdução

A Lei 13.709/18, denominada Lei Geral de Proteção de Dados ou LGPD, foi sancionada em 14 de agosto de 2018, tendo como justificativa dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, diante do avanço inegável da tecnologia da informação, em especial a internet e suas aplicações nas mais diversas áreas de nossa vida em sociedade.

No texto aprovado, o início da vigência dar-se-ia em 18 meses (fevereiro de 2020), porém, posteriormente, o Presidente Michel Temer, por meio da Medida Provisória 869 postergou sua vigência para agosto de 2020.

Desta forma, faltando alguns meses para o encerramento da *vacatio legis*, faz-se necessário uma reflexão acerca de quais atividades de tratamento de dados deverão ser submetidas à lei, tendo este estudo especificamente, a pretensão de analisar a viabilidade da aplicabilidade da LGPD nos condomínios edilícios.

Analisando o histórico da proposição e da tramitação da Lei aqui estudada, fica claro que seu objetivo é proteger o cidadão dos abusos do uso indevido e inadequado de seus dados pessoais, que passaram a ser usados, constantemente, por empresas para fins abusivos e distintos daquele para o qual foram coletados.

A leitura da lei nos faz perceber que sua concepção (Projeto de Lei 4.060 de 2012) está relacionada ao direito consumerista e ao caráter empresarial das relações, porém ela traz uma série de artigos que, dependendo da interpretação, podem fazer com que a lei aqui estudada passe a ter sua aplicação exigida aos condomínios residenciais já que estes tratam dados pessoais, seja por questões de segurança ou para assegurar seus procedimentos administrativos.

Surge aqui então uma série de indagações, as quais serão foco de algumas considerações e reflexões ao longo deste artigo, entre elas:

a) Uma análise teleológica da Lei Geral de Proteção de Dados permite concluir que ela se aplica aos condomínios edilícios residenciais?
b) O enquadramento da pessoa do condomínio permite que ele seja inserido na competência da LGPD?
c) Os condomínios edilícios residenciais deverão se adequar formalmente à Lei Geral de Proteção de Dados? Em que medida?
d) A coleta de dados realizada pelos condôminos tem potencial de afrontar os princípios da LGPD? Em que medida?

As reflexões acima não serão respondidas de forma sequencial durante o artigo, mas sim, abordadas dentro do raciocínio e das reflexões desenvolvidas.

1. Considerações iniciais

Para analisar a aplicabilidade da Lei Geral de Proteção de dados ao condomínio edilício residencial, cabe fazer uma digressão acerca dos motivos que levaram ao surgimento dos condomínios.

Há notícias de que a propriedade separada por andares já existia nos últimos séculos da Idade Média, havendo regulamentações sobre a propriedade por andares já desde século XIV na cidade de Grenoble e a partir do século XVII na cidade de Bruxelas. O artigo 664 do Código Civil francês de 1804, se ocupou da propriedade por andares nos seguintes termos:

> Art. 664 - Quando os diferentes andares de uma casa pertencerem a distintos proprietários, e os títulos de propriedade não regrarem o modo das reparações e reconstruções, estas deverão realizar-se da seguinte maneira: as paredes mestras e o teto correrão por conta de todos os proprietários, cada um em proporção ao valor do andar que lhe pertencer. O proprietário do segundo andar fará o piso sobre o qual caminha; O proprietário do segundo andar fará, a partir do primeiro, a escada que conduzirá ao seu, e assim sucessivamente.

Após a Revolução Industrial, com a crescente e contínua migração da população ativa da agricultara para as indústrias e comércios, provocou a compressão do espaço servido, assim como o saneamento e outros serviços básicos.

Terminado o período da Revolução Industrial e a sociedade ainda se adaptando com o conjunto de mudanças ocorridas na Europa, iniciou-se um novo grande desafio, vivenciado pela Primeira Guerra Mundial. Surge a necessidade de modificações do modo de vida da população, especialmente quanto à construção de moradia rápida, que ocupasse menos espaço, e fosse barata, garantindo assim o acesso à casa própria. Se estabelece então maior aceitação pela população à divisão condominial:

> O condomínio edilício insere-se em um contexto de crise habitacional, tendo em vista o desorganizado crescimento urbano, principalmente nas grandes cidades[105].

Diante do exposto, conclui-se que a coabitação em condomínios é resultado de uma busca por mais moradia e moradia barata, com custos mínimos a serem divididos entre os condôminos. Apesar de hoje algumas cidades passarem a contar com condomínios de luxo, tem-se que o propósito maior destinado à função social da moradia, está mantido.

A expressão "condomínio edilício" é utilizada no Código Civil Brasileiro, abrangendo tanto condomínios verticais (prédios, os chamados "condomínios de edifícios"), quanto os condomínios horizontais (também conhecidos como "condomínios residenciais").

O condomínio edilício (artigos 1.331 a 1.358 do Código Civil) diferencia-se do condomínio comum (artigos 1.314 a 1.330 do Código Civil), pois, naqueles, há partes comuns e partes exclusivas, ao passo que em um condomínio comum, estão presentes os multiproprietários, visto todos deterem a propriedade comum, sem individualizações.

Voltando agora ao tratamento de dados, percebe-se que ele acontece no condomínio edilício em diversos momentos, sendo de moradores e condôminos (para administração, cobrança e controle de acesso), de visitantes e prestadores de serviços (para controle de acesso e vigilância), de empregados (para registro e pagamento de salários, benefícios e outras questões administrativas e trabalhistas). Os dados coletados, muitas vezes serão, inclusive, exibidos nos rateios condominiais.

[105] LIMA, Cintia Rosa Pereira de. Aspectos Controvertidos da personalidade jurídica do condomínio edilício. *In*: CASSETTARI, Christiano (coord.). **10 anos de vigência do Código Civil Brasileiro de 2002.** Estudos em homenagem ao professor Carlos Alberto Dabus Maluf. São Paulo: Editora Saraiva, 2012.

Os fundamentos previstos no artigo 2º da LGPD legitimam sua aplicação de forma abrangente, culminando no inciso VII, que coloca sua aplicação como protetora dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania pelas pessoas naturais.

Há que se refletir, no entanto, que a referida lei pode vir a colocar em risco um dos direitos fundamentais previstos em nossa carta magna, qual seja, o direito social de moradia. Diante dos altos investimentos que parecem necessários à implementação dos processos e procedimentos da LGPD, bem com, para o pagamento de multas que possam vir a ser aplicadas, os custos condominiais poderão sofrer reajustes significativos, tornando-se inacessíveis aos condomínios ocupados pela população de baixa renda.

Pelos motivos até aqui expostos e pelos demais abordados oportunamente no decorrer deste artigo, não há como negar que haverá dificuldade em atender a diferentes princípios fundamentais previstos em nossa Constituição nos moldes previstos na Lei Geral de Proteção de Dados. Em que se pese a LGPD ter sido promulgada para proteger os dados dos cidadãos, o mote principal é a proteção contra o abuso do uso destes dados por empresas com interesses financeiros. Dessa forma, ter seu entendimento estendido à condomínios residenciais onde a atividade nada tem a ver com interesses comerciais, mas única exclusivamente a habitação, poderá trazer questões administrativas, operacionais e financeiras insuperáveis, ou, se superáveis, não sem sacrifício bastante além daqueles para os quais os condomínios residenciais estão preparados.

2. Interpretação e finalidade da Lei Geral de Proteção de Dados – LGPD

Ao levarmos em conta uma interpretação teleológica da lei, pode-se perceber que a legislação em estudo tem por objetivo proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, fortalecendo a privacidade do titular dos dados, a liberdade de expressão, a informação, a opinião e a comunicação, a inviolabilidade da intimidade da honra e da imagem, e, sobretudo, garantir o desenvolvimento econômico e tecnológico dos negócios. Aliado a isso, depreende-se que a lei está posicionada contra o uso indevido de dados pessoais, levando-se em conta, principalmente, o modelo de negócios da sociedade digital, na qual a informação passou a ser moeda de troca utilizada pelos usuários para ter acesso a determinados bens e serviços.

Com base nestes dados coletados, empresas podem aumentar suas vendas e faturamento.

Hoje, pode-se afirmar que “dados são o novo petróleo” (RIPARI, 2019).

Estaria o condomínio edilício contemplado nesse modelo de negócio da sociedade atual? Naturalmente não, visto que tal ente, por sua própria natureza, não se presta a tal mister.

Verifica-se que a LGPD apresenta dificuldades interpretativas no que tange a sua aplicação aos Condomínios Edilícios, pois a finalidade do condomínio não está vinculada a aspectos econômicos.

Em consulta ao Projeto de Lei 4.020 de 2012, que deu origem à LGPD, pode-se verificar que o objetivo inicial de se tratar a questão dos dados pessoais para garantir a proteção das pessoas de maneira harmônica, está aliado à necessidade de se construir um arcabouço similar entre os países para gerar um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados.

Nesse sentido, fica claro que a finalidade da lei está relacionada também ao aspecto negocial e transfronteiriço.

Aliado a isso, na elaboração do citado PL foram realizadas diversas consultas e seminários com a presença de órgãos e entidades, em sua maioria, relacionados ao direito consumerista, reforçando o caráter das relações de consumo e da atividade empresarial na legislação de proteção de dados.

Um aspecto a ser considerado é que a relação condominial não é uma relação de consumo, visto as taxas condominiais serem destinadas ao pagamento das despesas do condomínio e rateadas pelos condôminos.

Desta forma, pela natureza não econômica do condomínio, bem como por sua destinação e dificuldade em custear a implementação de meios tecnológicos adequados de gestão de dados, deve haver uma análise profunda sobre sua aplicabilidade aos condomínios residenciais.

Além do mais, outros pontos devem ser analisados à frente.

3. Aspectos controversos: condomínios edilícios e a necessidade de adequação à LGPD

3.1. Aplicação da lei às pessoas físicas ou jurídicas, enquanto o condomínio é um ser despersonalizado

A Lei Geral de Proteção de Dados dispõe:

> Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Surge aqui uma primeira questão a ser abordada. De acordo com nossa jurisprudência, o condomínio pode ser considerado um ente despersonalizado, *"o condomínio não possui personalidade jurídica de direito material, pois sua natureza jurídica é tratada como uma massa patrimonial"*[106], não estando, portanto, entre as pessoas abrangidas pela LGPD.

Como cita Cintia Rosa Pereira de Lima, em seu artigo *"Aspectos Controvertidos da personalidade jurídica do condomínio edilício"*, o Código Civil de 2002 perdeu a oportunidade de atribuir personalidade jurídica

[106] Tribunal de Justiça do Rio de Janeiro TJ-RJ - apelação: APL 0036109-77.2011.8.19.0210 RJ 0036109-77.2011.8.19.0210.

ao condomínio edilício, a fim de viabilizar o exercício de alguns direitos que, na prática, têm se mostrado de extrema relevância.

Diante da omissão citada e para compreendermos a extensão do problema, inicialmente faz-se necessário a reflexão sobre o artigo 44 do Código Civil, que nos traz o rol das pessoas jurídicas de direito privado. A primeira questão que necessita ser refletida é o rol do artigo 44 do CC é taxativo ou exemplificativo?

O Enunciado 144 do Conselho da Justiça Federal firmou entendimento de que o rol é meramente exemplificativo. Entretanto, este entendimento vem sendo refutado pelo Tribunal de Justiça do Estado de São Paulo, que em maioria de decisões, entende o rol como taxativo.

Neste sentido, o Desembargador Manoel de Queiroz Pereira Calças, no julgamento da apelação nº 0006384-83.2015.8.26.0153 nega o registro de imóvel em nome de empresário individual por não ser pessoa jurídica, vez que inexistente no rol do artigo 44 do CC.

Desta forma, da mesma maneira que o empresário individual constituído como ME ou EPP não é considerado pessoa física por ausente no rol, nos parece coerente a interpretação de que o rol é taxativo.

Além disso, outra evidência de que o Condomínio Edilício não é pessoa jurídica é o disposto no artigo 167 do Decreto nº 9.580/2018, que dispõe expressamente que os condomínios na propriedade de imóveis não são considerados sociedades em comum.

Não sendo o condomínio abraçado pela LGPD, se considerarmos não ser ele pessoa física ou jurídica, por outro lado, ele também não preenche as características do artigo 4°, que trata expressamente dos excluídos da obrigatoriedade de cumprimento desta lei:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)
>
> III - 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; ou
>
> IV - 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 nesta Lei (...)

Desta forma, vemos que a realidade do condomínio residencial ou passou despercebida pelo legislador, ou, ao contrário senso, já estava implícita a inaplicabilidade da lei a este tipo de ente jurídico.

3.2. Adequação das pessoas do condomínio às pessoas previstas nas nomenclaturas descritas no artigo 5°

O artigo 5° da LGPD dispõe acerca das nomenclaturas utilizadas na lei, no contexto dos dados pessoais, bem como das pessoas responsáveis por sua aplicação e operação.

Nos incisos VI, VII, VIII e IX, estão dispostos os conceitos de controlador, operador e encarregado, respectivamente. Ao analisar as responsabilidades dessas pessoas, podemos visualizar num primeiro momento uma considerável dificuldade em enquadrá-las aos cargos dos administradores dos condomínios residenciais visto que, em sua maioria, são voluntários, que doam seu tempo em prol do bem comum daqueles relacionados ao condomínio em que residem.

Além do mais, mesmo que se defina pela aplicabilidade da lei aos condomínios residenciais, haverá dificuldade em se definir até onde vai a responsabilidade de cada um, quando esta responsabilidade é do condomínio, da empresa administradora ou de empresa terceirizada e se o será de forma exclusiva, solidária ou subsidiária. Há condomínios de pequeno porte, nos quais uma mesma pessoa estaria enquadrada em mais de uma dessas responsabilidades (controlador, operador ou encarregado), ou em outros condomínios mais simples, muitas vezes não haverá alguém que pudesse se enquadrar em uma dessas categorias.

3.3. Necessidade do consentimento para a coleta dos dados

Outra consideração a fazer, versa sobre a necessidade de consentimento inequívoco para tratamento dos dados (art.7º, inciso I, da LGPD).

Em um condomínio residencial, a obtenção de consentimento inequívoco para coleta de dados, como exige a lei, pode trazer consequências à liberdade de ir e vir no condomínio pelo morador e seus visitantes, visto, o não consentimento poder colocar o morador em confronto com as normas do condomínio. Uma das consequências seria, por exemplo, o bloqueio de acesso do morador, por falta de dados para alimentação do sistema, uma vez que não pôde ser feita a coleta. Por outro lado, a liberação do acesso sem a devida coleta de dados pode trazer riscos à segurança ou obstrução à administração.

Cabe, portanto, refletir, se, vindo a lei ser aplicado aos condomínios aqui estudados, poderia este consentimento vir de forma coletiva (em convenção coletiva), diminuindo a problemática do consentimento individual.

Ainda refletindo, o artigo 7º elenca hipóteses taxativas, das quais se destacam além do consentimento para a coleta, o legítimo interesse e o cumprimento de obrigação legal, como forma de legitimar a coleta mesmo sem o consentimento do proprietário do dado. Poderia então, em não havendo o consentimento por parte do morador, os dados serem coletados com supedâneo nos demais incisos do mesmo artigo, como o VII (proteção à vida e à incolumidade física) ou o IX (atender interesses legítimos), por exemplo?

3.4. Tratamento de dados de crianças e adolescentes

A Seção III da Lei trata especificamente do tratamento de dados pessoais de crianças e adolescentes, e aqui nos deparamos com o parágrafo 1º do artigo 14, que nos informa que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico por pelo menos um dos pais ou pelo responsável legal, neste caso não havendo qualquer dispositivo que permita interpretação extensiva dentro da referida lei.

Desta forma, como ficaria o acesso de crianças e adolescentes que, sem a companhia de um responsável, iriam a uma visita à casa de um amigo cujo condomínio, por segurança, coleta os dados de todos os visitantes como única forma de autorização de entrada?

3.5. Sanções

Ao nos depararmos com o campo das penalidades, surgem dificuldades na aplicação de algumas das sanções dispostas na LGPD.

Assim, outro dispositivo que merece atenção, sob a ótica do direito condominial, é o inciso II do artigo 52 da Lei, que dispõe sobre a aplicação de multa de até 2% do faturamento da pessoa jurídica.

Ocorre que o condomínio não possui faturamento, mas sim arrecadação única e exclusiva para a manutenção do edifício. Haveria, tão somente, em uma interpretação extensiva, a possibilidade da utilização de uma base de cálculo alternativa, como por exemplo, o valor venal do imóvel? Tal interpretação, porém, estaria em desacordo com o entendimento que veda a aplicação da analogia in malam partem.

Com este entendimento estariam vedadas sanções pecuniárias ao condomínio.

Conclusão

A Lei Geral de Proteção de Dados traz relevantes avanços ao tema proteção de dados pessoais.

Nos dias atuais, e por questões de segurança, o ingresso de pessoas em condomínios edilícios residenciais está cada vez mais condicionado a sua respectiva identificação e fornecimento de dados pessoais. Câmeras de segurança estão cada vez mais populares e as imagens por elas coletadas podem estar inseridas no termo "dado pessoal" e, mais grave, "dado pessoal sensível", levando em conta, em alguns casos, os dados biométricos.

O estudo e as reflexões sobre a Lei Geral de Proteção de Dados – LGPD indicam a necessidade de haver cautela na análise sobre a aplicabilidade da lei nos condomínios residenciais.

Na prática, pode-se afirmar que os condomínios coletam dados com dois nobres objetivos – manter a segurança dos que a ele se relacionam (moradores) e possibilitar a cobrança da taxa condominial.

Diante da análise do presente trabalho, entendemos que a LGPD, lei destinada àqueles que realizam o tratamento de dados pessoais, encontra diversos fatores que podem obstar sua aplicação nos condomínios edilícios, tais como os relacionados a sua natureza jurídica, à ausência de relação de consumo, à ausência de faturamento, à proibição de coleta de dados de menores sem autorização do responsável, entre outros.

Em tese, os condomínios edilícios ao coletarem dados pessoais deveriam se adequar às exigências da LGPD, no entanto, em termos práticos tal aplicação está longe de acontecer, pelo menos sem trazer consequências onerosas para os condôminos, seja por questões operacionais ou por questões financeiras.

Para uma adequada implementação da lei, seriam necessários programas de gerenciamento de dados, medidas técnicas e administrativas concertadas na proteção dos dados pessoais coletados, ocasionando um alto custo ao condomínio edilício residencial, sobretudo àqueles constituídos por condôminos de baixa renda.

Desta forma, apesar da importância da LGPD, que prima pela tutela dos dados pessoais e pela responsabilidade dos agentes de tratamento, estando relacionada, inclusive, aos princípios que regem os direitos humanos, merece análise cautelosa sobre sua aplicação aos condomínios edilícios residenciais, diante dos apontamentos deste estudo.

Referências bibliográficas

ALMEIDA, Maria Cecília L. de Almeida et al. **Código Civil Interpretado** – Artigo por Artigo, Parágrafo por Parágrafo. 10ª ed. Barueri: Manole, 2017.

ARAÚJO, Nicete Lacerda; GUERRA, Bráulio Madureira; et al. **Marco Legal da Inovação:** breves comentários. Rio de Janeiro: Lumen Juris, 2018.

ASSIS, Olney Queiroz; KUMPEL Vitor Frederico; PERES Iehuda Henrique. **Manual de Direito Condominial:** Uma abordagem interdisciplinar. YK Editora, 2016.

BIONI, Ricardo Bruno. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, regulação dos bancos de dados eletrônicos e arquitetura da internet. 2016. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2016.

_____. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BRASIL. Comissão Especial destinada a proferir Parecer ao Projeto de Lei n° 4060, de 2012. **Tratamento e Proteção de Dados Pessoais.** Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acesso em: 01 nov. 2019.

_____. Comissão de assuntos econômicos do Senado. **Parecer sobre Projetos de Lei n. 53/2018 (Câmara dos Deputados), 330/2013 (Senado), 131/2014 (Senado) e 181/2014 (Senado).** Relator: Senador Ricardo Ferraço. Brasília: Senador Federal, 2018. Disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=7751914&ts=1530801218510 &disposition=inline&ts=1530801218510. Acesso em 21.7.2019.

DE LUCCA, Newton; DEZEM, Renata Mota Maciel Madeira. A proteção de dados pessoais no Brasil a partir da Lei nº 13.709/2018. *In:* JORGE LEMOS, André Guilherme et al. (Coord.) **Direito Empresarial:** estruturas e regulação. Volume 2. São Paulo: UNINOVE. 2018, p 255-276.

LIMA, Cintia Rosa Pereira de. Aspectos Controvertidos da personalidade jurídica do condomínio edilício. *In*: CASSETTARI, Christiano (coord.). **10 anos de vigência do Código Civil Brasileiro de 2002.** Estudos em homenagem ao professor Carlos Alberto Dabus Maluf. São Paulo: Editora Saraiva, 2012.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Vitor Rozatti (Coord.) **Direito Digital:** direito privado e internet. 2 ed. Indaiatuba: Editora Foco Jurídico, 2019.

FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. **Curso de Direito Civil** – 5 – Reais. 11ª edição. São Paulo: Atlas. 2015. FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. Comentários à Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

FIESP. **Cartilha de Proteção de Dados Pessoais.** FIESP, 2019.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** Comentários à lei n. 13.709/2018 (LGPD), 1ª edição de 2018.

RIPARI, César. **Porque os dados são considerados o novo Petróleo?** Disponível em: https://www.itforum365.com.br/por-que-dados-sao-considerados-o-novo-petroleo. Acesso em: 29 dez. 2012.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA Milena; Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro. **Revista dos Tribunais**, 2018.

4.9. Desafios da proteção de dados pessoais: o compartilhamento de dados entre Poder Público e setor privado – *Vitória Mattos Gonçalves*[107] *& Verônica do Nascimento Marques*[108]

Resumo

O presente trabalho tem como referência principal a análise de toda operação que está direta ou indiretamente atrelada ao uso e compartilhamento de dados pessoais entre o Poder Público e o Setor Privado. Nesse passo, serão discutidos todos os principais pontos, desde a inclusão do Setor Público no escopo da Lei Geral de Proteção de Dados (LGPD) e o seu respectivo impacto nas operações da Administração Pública. A inclusão do setor público na LGPD cria a obrigação ao governo de se adequar às novas exigências da lei, como investir em questões de segurança, que são muitas vezes negligenciadas e a atuar de forma a evitar a comercialização de dados pessoais para fins diferentes daqueles aos quais foram coletados. Além disso, o governo tem se tornado cada vez mais digital, com variados aplicativos voltados ao acesso a sistemas gerenciados pelo governo, como DataSUS e E-título, daí a relevância da inclusão do setor na lei. Um pouco mais além, trataremos da influência dos princípios da Administração Pública nos artigos da LGPD, tanto os expressos no artigo 37 da Constituição Federal de 1988, como também os princípios implícitos, como Supremacia do Interesse Público e a crítica a fragilidade desses princípios como fundamento, pois esses possuem enunciados amplos, vagos e abertos, de maneira que, acabam incorporando determinados valores e podem acabar ganhando um caráter arbitrário. Ademais, fazemos uma análise das consequências da edição da Medida Provisória 869, de 27 de dezembro de

[107] Graduanda em Direito pela Faculdade de Direito de Ribeirão Preto – USP e membro do Grupo de Pesquisa "Tutela jurídica dos dados pessoais na internet" da FDRP/USP. E-mail: vitoria.goncalves@usp.br.

[108] Graduanda em Direito pela Faculdade de Direito de Ribeirão Preto – USP e membro do Grupo de Pesquisa "Tutela jurídica dos dados pessoais na internet" da FDRP/USP. E-mail: veronica.nascimento.marques@usp.br.

2018, e, posteriormente, da Lei n. 13.853, de 08 de julho de 2019, que flexibilizaram as exigências para o intercâmbio de dados entre Poder Público e entidades privadas, passando a abarcar de forma desmedida um número maior de hipóteses legais para a transferência de dados pelo Poder Público a entidades privadas. Por fim, abordaremos a importância da comunicação *ex ante* à Autoridade Nacional dos intercâmbios de dados pessoais realizados por entes públicos para maior controle e segurança das operações a fim de evitar casos de compartilhamento indiscriminado e abusivo de dados pessoais sem devida justificativa e autorização.

Palavras-chave: Dados Pessoais; Poder Público; Setor Privado; Compartilhamento de dados.

Abstract

The main reference of this work is the analysis of any operation that is directly or indirectly tied to the use and sharing of personal data between the Public Authority and the Private Sector. In this step, all the main points will be discussed, from the inclusion of the Public Sector within the scope of the General Data Protection Law (LGPD) and its respective impact on Public Administration operations. The inclusion of the public sector in the LGPD creates an obligation on the government to adapt to the new requirements of the law, such as investing in security issues, which are often neglected and to act in a way that prevents the commercialization of personal data for purposes other than those collected. In addition, government has become increasingly digital, with a variety of applications geared toward access to government-managed systems such as DataSUS and E-title, hence the relevance of including the industry in the law. A little further on, we will deal with the influence of the principles of Public Administration in the articles of the LGPD, both those expressed in article 37 of the Federal Constitution of 1988, as well as the implicit principles such as Supremacy of Public Interest and criticism of the fragility of these principles as a foundation, because these have broad, vague and open statements, so that they end up incorporating certain values and may end up gaining an arbitrary character. In addition, we make an analysis of the consequences of the edition of Provisional Measure 869, of December 27, 2018, and, later, of Law nº 13,853, dated July 8, 2019, which made the requirements for the exchange of data between the Public Authorities and private entities more flexible, and now includes a greater number of legal hypotheses for the transfer of data by the Public Authorities to private entities. Finally, we will discuss the importance of ex ante communication to the National Authority of the exchanges of personal data made by public entities for greater control and security of operations in order to avoid cases of indiscriminate and abusive sharing of personal data without proper justification and authorization.

Keywords: Personal Data. Public Authority. Private sector. Data sharing.

Introdução

Baseada no *General Data Protection Regulation* (GDPR) da União Europeia, a Lei Geral de Proteção de Dados brasileira (BRASIL, 2018) cria um microssistema de proteção das informações pessoais dos indivíduos, prevendo que os dados pessoais somente poderão ser utilizados ou compartilhados da forma mínima necessária e para finalidades específicas, devendo serem seus titulares devidamente informados. Quanto à sua abrangência, a LGPD deve ser observado por toda e qualquer pessoa física ou jurídica, não só de direito privado, mas também de direito público, quanto ao tratamento e armazenamento de dados pessoais, seja on-line ou off-line.

Nesse contexto, a necessidade da criação da Lei surgiu diante de escândalos recentes relativos ao vazamento de dados, como por exemplo, o caso envolvendo a rede social Facebook, em que houve o fornecimento de informações de milhões de usuários para empresas, dentre as quais *Cambridge Analytica*, empresa de análise de dados para finalidades políticas. Antes da promulgação da lei, a tutela de dados pessoais no Brasil tinha por fundamento normativo apenas o direito à vida privada e à intimidade, constantes do artigo 5º, inciso X, da Constituição Federal de 1988, e do artigo 21 do Código Civil de 2002.

Em 2014, o Marco Civil da Internet (Lei 12.965/2014), seguindo uma tendência mundial, também trouxe uma gama de princípios, garantias, direitos e deveres para usuários e provedores da internet no Brasil, a fim de oferecer maior proteção e privacidade no meio eletrônico, visto que as novas tecnologias da informação proporcionaram grande alcance e difusão do tratamento de dados pessoais on-line.

Partindo-se destas considerações iniciais, a questão que se coloca em tela no presente trabalho refere-se ao compartilhamento de dados pessoais entre Poder Público e setor privado. Diante do amplo e flexível rol de hipóteses legais de tratamento de dados, bem como da ausência de um efetivo controle prévio, questiona-se se a Lei Geral de Proteção de Dados é suficiente para coibir casos de transferência indiscriminada de dados pessoais, a exemplo do que se verificou em 2013, no Acordo de Cooperação Técnica entre TSE e a empresa privada *Serasa Experian*, que previa, dentre outras condições, o repasse de nome e número eleitoral de eleitores cadastrados para a entidade privada de análise de crédito.

1. Aspectos gerais sobre o tratamento de dados pessoais pelo Poder Público

Hodiernamente, o Poder Público passou a adotar gradativamente o uso de aplicações de internet como estratégia para se aproximar de cidadãos e facilitar o acesso à informação e à prestação de determinados serviços. Novas ferramentas surgiram, como o DataSUS, o E-título, a CNH Digital, o Meu Imposto de Renda e o Documento Nacional de Identidade (documento único criado pela Lei n. 13.444/2017).

Desse modo, vários aplicativos acabam coletando dados desnecessários de seus usuários, ou seja, não adotam a minimização da coleta e ainda, não são verificadas explicações sobre a finalidade específica

para qual o dado é coletado, resultando em uma enorme concentração de dados pessoais, muitos deles dados sensíveis.

Assim, a inclusão do Setor Público na LGPD foi importante na tentativa de adequar a Administração Pública, gerar investimento em questões de segurança que, geralmente, são negligenciadas, vide os casos de ataques *ransomware* (ataques cibernéticos), tais quais os ocorridos recentemente no Hospital de Câncer de Barretos (SP) e no Site da Prefeitura do município de Araçatuba/SP.

Contudo, mesmo com todo o avanço trazido pela LGPD, existem ainda alguns pontos obscuros, principalmente com relação ao inciso III do artigo 7º, em que o diploma normativo acaba criando uma ampla base legal autorizadora ao tratamento de dados pessoais pela Administração Pública. Dessa maneira, permite o uso e compartilhamento à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, fornecendo um escopo muito amplo e aberto que consegue justificar grande parte das operações que envolvem dados pessoais realizadas pelo setor público. Além disso, o artigo 23 segue o mesmo caráter permissivo, com mais definições vagas de "atendimento de sua finalidade pública, na persecução do interesse público" e "com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (BRASIL, 2018).

Diante desse cenário, pode-se identificar de forma cristalina a influência dos princípios da Administração Pública nesses artigos da LGPD, tanto os expressos no artigo 37 da Constituição Federal: legalidade, impessoalidade, moralidade, publicidade e eficiência. Como também os princípios implícitos como supremacia do interesse público, continuidade dos serviços públicos, boa-fé e razoabilidade. Porém, esses princípios possuem enunciados amplos, vagos e abertos de maneira que acabam incorporando determinados valores compreendidos como fundamentais em dado momento histórico da sociedade. A questão é que tal aspecto acaba levando à facilitação e à legitimação de "voluntarismos", tanto da Administração quanto do Judiciário, o que conduz, em último caso, à arbitrariedade. Acerca do tema, Carlos Ari Sundfeld (2014, p. 63-65) leciona que:

> Como achar normas dentro de princípios: (...) chamamos de princípios textos que somos levados a entender como normativos, mas cujo conteúdo, de tão escasso, não nos revela a norma que supostamente contém. (...) [princípios são] normas iniciais, insuficientes, indeterminadas, cujo conteúdo precisa ser especificado por outras (as finais) para poderem funcionar.

Assim, a execução de políticas públicas se torna a principal justificativa para que o setor público realize qualquer tipo de uso e compartilhamento de dados. Desse modo, nesse ambiente amplo, vago e aberto

cria-se a manipulação de dados pessoais pelo setor público e violações a privacidade de cidadãos, uma vez que é inerente à própria existência do Estado a consecução de políticas públicas.

Portanto, é de suma importância a análise e a fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) e pelo Conselho Nacional de Proteção de Dados dos riscos de autoritarismos e violações não apenas de direitos em sua dimensão individual (proteção de dados pessoais e privacidade), mas também de decisões puramente arbitrárias, construídas de modo voluntarista, gerando uma jurisprudência capaz de flutuar ao sabor das instituições e dos azares das garantias inextrincáveis do Estado Democrático de Direito.

2. Condições para o compartilhamento de dados pelo Poder Público

Admitido o tratamento de dados pessoais pelo Poder Público, a Lei Geral prevê que os dados sejam mantidos em formato interoperável e estruturado para o uso compartilhado (BRASIL, 2018a). Assim, o compartilhamento dos dados coletados entre as pessoas jurídicas de direito público é perfeitamente possível quando este tiver por objetivo o atendimento a finalidades específicas de execução de políticas públicas e atribuições legais pelos órgãos e entidades públicas, respeitados, em qualquer situação, os princípios norteadores que constam do artigo 6° do referido diploma normativo.

A questão ganha outros contornos, contudo, no que tange à transferência de dados pessoais pelo Poder Público a entidades privadas. Originalmente, a Lei Geral de Proteção de Dados previa que o compartilhamento nesse caso somente seria possível nas hipóteses de execução descentralizada de atividade administrativa que exigisse a transferência, exclusivamente para esse fim específico e determinado, ou se os dados fossem acessíveis publicamente.

Com a edição da Medida Provisória 869, de 27 de dezembro de 2018, e, posteriormente, da Lei n. 13.853, de 08 de julho de 2019, as exigências para o intercâmbio de dados para entidades privadas foram flexibilizadas, passando a abarcar um número maior de hipóteses. Assim, atualmente, o Poder Público também poderá realizar o compartilhamento quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, e na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (BRASIL, 2019).

Nesse sentido, a crítica que se faz é que tais atos normativos ampliaram de maneira desmedida o espectro de situações em que é legal a transferência de dados pelo Poder Público a entidades privadas. O tópico se torna ainda mais sensível se levarmos em consideração que, nos termos do art. 27 da Lei Geral de Proteção de Dados, as hipóteses anteriormente mencionadas constituem exceção à regra geral segundo a qual deve existir consentimento do titular dos dados pessoais para que estes possam ser compartilhados.

Ainda, deve-se atentar para o fato de que a Medida Provisória dispensou a necessidade, conforme originalmente previsto, de que tal compartilhamento fosse informado à Autoridade Nacional, exigência esta que voltou a vigorar apenas com a edição da Lei n. 13.853/2019.

Dessa forma, o questionamento que se põe é se, diante de um rol amplo e flexível de hipóteses legais, bem como da ausência de um controle *ex ante*, tal norma dará conta de obstar a ocorrência de situações de compartilhamento indiscriminado de dados pessoais, situações essas que já se verificaram inúmeras vezes na prática, tal qual no emblemático acordo entre a Justiça Eleitoral e a empresa de análise de crédito Serasa Experian, ou, mais recentemente, no esquema de venda de dados pessoais pelo Serviço Federal de Processamento de Dados (Serpro).

2.1. Análise do Acordo de Cooperação Técnica TSE n° 7/2013 à luz da LGPD

É inegável que o Poder Público é, não só no Brasil, mas mundialmente, um relevante controlador de dados: centenas de milhares de informações pessoais são coletadas todos os dias por meio do cadastro e navegação em aplicativos governamentais, *e.g.*, a CNH Digital e o Meu Imposto de Renda, ou mesmo mediante o fornecimento direto pelo usuário, como requisito para a obtenção de determinado serviço ou documento perante a Administração Pública.

Com efeito, na lição de Cella e Copetti (2017, p. 41), o exemplo mais marcante da coleta e tratamento de dados pessoais por entes públicos refere-se à recolha de dados biométricos dos cidadãos que solicitam a emissão do título de eleitor perante a Justiça Eleitoral brasileira:

> O indivíduo, além de fornecer informações de caráter pessoal – nome, filiação, data de nascimento, sexo, endereço residencial ou comercial, tempo de vínculo com o município, se possui ou não irmão gêmeo, telefones, escolaridade e profissão – tem sua assinatura coletada digital e fisicamente.

Diante desse cenário, o Tribunal Superior Eleitoral e a empresa privada Serasa Experian S.A. firmaram em julho de 2013 o Acordo de Cooperação Técnica TSE nº 7/2013, por meio do qual o órgão estatal se comprometia a fornecer dados de aproximadamente 142 milhões de eleitores referentes ao nome, número e situação da inscrição eleitoral, além de informações sobre eventuais óbitos e validação do nome da mãe e data de nascimento (TSE apud CELLA; COPETTI, 2017, p. 43).

A Serasa Experian é uma empresa privada que tem por finalidade gerar análises e informações econômico-financeiras e cadastrais para embasar decisões de crédito. Destarte, os dados fornecidos pelo ente estatal poderiam ainda, nos termos do acordo, serem disponibilizados pela empresa a seus clientes quando da consulta a seu banco de dados.

O caso, evidentemente, suscitou enorme repercussão midiática e jurídica, razão pela qual a então presidente do tribunal eleitoral, Ministra Carmen Lúcia, avocou o processo administrativo no qual foi firmado o Acordo e declarou a sua nulidade. Sob o fundamento de ausência de base legal válida para o pacto, a Ministra concluiu que a transferência de dados constantes do cadastro eleitoral haveria de se ater a entidades públicas ou de interesse público direto e vinculadas aos fins da Justiça Eleitoral (TRIBUNAL SUPERIOR ELEITORAL, 2013).

Analisando o Acordo à luz da legislação vigente, o compartilhamento de dados entre Tribunal Superior Eleitoral e Serasa Experian seria possível com supedâneo no inciso IV do artigo 26, § 1º da Lei Geral de Proteção de Dados, que admite o intercâmbio quando for este respaldado em contratos, convênios ou instrumentos congêneres (BRASIL, 2018a), dentre os quais entendemos se inserir os acordos de cooperação. Deve-se atentar também ao fato de que, no caso, o tratamento dos dados eleitorais pela empresa privada se justificaria com base nas concepções de proteção ao crédito e de legítimo interesse do controlador ou de terceiros.

Contudo, o § 2º do mesmo artigo anteriormente mencionado ressalva a necessidade de comunicação à Autoridade Nacional quando da celebração de contratos ou convênios que envolvam a transferência de dados pessoais. No mais, no âmbito da coleta e tratamento de dados pessoais, devem ser respeitados, em qualquer hipótese, os princípios elencados no art. 6° da Lei, dentre os quais destacamos os princípios da finalidade e da adequação.

O princípio da finalidade pressupõe que o tratamento dos dados seja realizado com "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018a). Já o princípio da adequação, o qual constitui uma decorrência lógica do princípio da finalidade, carrega a ideia de compatibilidade do tratamento com as finalidades informadas ao titular dos dados pessoais. Assim, também o poder público deve restringir o uso de informações pessoais do cidadão à finalidade informada quando da coleta dos dados e a outros propósitos compatíveis, nos limites do consentimento do indivíduo.

No caso em análise, temos que quando um indivíduo fornece suas informações pessoais à Justiça Eleitoral, o faz visando tão somente seu alistamento eleitoral. O tratamento de dados pelo Tribunal Superior Eleitoral, *ipso facto*, deveria se ater a sua utilização no processo eleitoral e em outras atividades a este subjacentes.

Ocorre que o dispositivo legal, ao tratar do princípio da finalidade, reproduzindo os mesmos termos do *General Data Protection Regulation* europeu, veda tão somente o tratamento de dados realizado de "forma incompatível" com a finalidade informada previamente ao titular. Nesse sentido:

> According to the purpose or finality principle set out in Article 6 of the data protection Directive, personal data must be collected for specified…purposes and not processed further in a way incompatible with those purposes. **Thus, the Directive does not prohibit the re-use for different, but for incompatible purposes** (RODOTÀ, 2003 – grifo nosso).

Assim sendo, partindo de tal concepção, eventuais contratos ou convênios entre poder público e entidades privadas para a transferência de dados dos primeiros para estas últimas poderiam ser celebrados de maneira indiscriminada sob o fundamento de que não configurariam tratamento incompatível com a finalidade para a qual as informações foram coletadas. Isso, porque o conceito de incompatibilidade é bastante restritivo e pressupõe diferenças essenciais ou a impossibilidade legal para se realizar o tratamento, o que ocorreria apenas nas hipóteses expressamente vedadas por lei.

3. Importância da Autoridade Nacional

O texto original da Lei Geral de Proteção de Dados previa que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado deveriam ser informados à Autoridade Nacional de Proteção de Dados (ANPD). Tal exigência foi suprimida pela Medida Provisória 881/2018, mas voltou a vigorar após as modificações trazidas pela Lei nº 13.853/2019.

Com efeito, a comunicação à Autoridade Nacional dos intercâmbios de dados pessoais realizados por entes públicos é de suma importância para que haja um controle sobre as operações, a fim de se evitar casos de compartilhamento indiscriminado e/ou abusivo tais quais os anteriormente mencionados. Da mesma forma, é premente que tal comunicação seja realizada previamente à celebração de acordos ou de qualquer outra forma de transferência das informações pessoais dos cidadãos.

A disposição contida no *caput* do artigo 27 da Lei Geral, portanto, deve ser vista como uma espécie de controle prévio da atividade administrativo. Ou seja, o dever de informar o uso compartilhado de dados à ANPD representa uma formalidade e um sistema de exame prévio dos atos do poder público indispensável para que estes adquiram eficácia e operatividade (MEIRELLES, 1973, p. 25). Todavia, o desenho institucional de Autoridade Nacional adotado pelo Brasil pode constituir-se como um entrave ao pleno exercício desse controle.

A Autoridade Nacional de Proteção de Dados foi criada pela Lei n. 13.853/2019 como um órgão da administração pública federal, integrante da Presidência da República. Esta vinculação à administração direta, contudo, tem sido vista como um óbice ao reconhecimento da autonomia técnica e política da ANPD, especialmente no que tange à efetividade da proteção de dados em face do próprio Poder Público. Tal cenário, partindo da visão de José dos Santos Carvalho Filho (2012, p. 485), caracteriza a

chamada "teoria da captura política", fenômeno segundo o qual a vinculação promíscua entre órgão fiscalizador, de um lado, e governo instituidor ou entes fiscalizados, de outro, implica em flagrante comprometimento da independência pública.

A partir de tais breves reflexões, questiona-se se a Autoridade Nacional da forma como foi concebida, enquanto órgão integrante da Presidência da República, realizará uma análise vigorosa e imparcial quando da comunicação de um acordo de compartilhamento de dados envolvendo órgãos públicos do governo federal, por exemplo.

Conclusão

Ante o cenário atual de aumento crescente do valor agregado das informações pessoais e de transformação dos dados individuais em mercadoria (RODOTA, 2008, p. 128), o tema da proteção de dados tem ganhado especial relevância. Também as entidades públicas, que têm se tornado cada vez mais digitais, se inserem na seara protetiva consubstanciada pela Lei Geral de Proteção de Dados Pessoais. Valendo-se de inúmeros aplicativos, tais quais o e-título, a CNH Digital, e o Meu Imposto de Renda, e de outras tantas bases de dados, como os cadastros fiscais e eleitorais, pode-se afirmar sem rebuços que o Poder Público está entre os maiores controladores de dados do país.

Por esse ângulo, o tratamento específico dispensado aos órgãos governamentais pela LGPD mostrou-se de extrema importância para a compatibilização da proteção de dados às peculiaridades da Administração Pública e para a garantia de segurança e transparência no tratamento das informações pessoais dos cidadãos, tópico até então negligenciado pelo Poder Público, conforme tem restado evidente pelos vários casos de ataques cibernéticos, acordos de transferência e, até mesmo, venda de dados pessoais envolvendo entidades estatais.

Não obstante os avanços trazido pela LGPD, ainda existem pontos do diploma normativo que necessitarão de um trabalho conjunto da doutrina e, sobretudo, da jurisprudência para sua elucidação e delimitação. Nesse campo inserem-se a ampla base legal autorizadora ao tratamento de dados pessoais pela Administração Pública, bem como as hipóteses bastante flexíveis de compartilhamento de dados entre Poder Público e setor privado trazidas pelas posteriores modificações no texto original da Lei.

Nessa perspectiva, o Acordo de Cooperação Técnica nº 7/2013, envolvendo o Tribunal Superior Eleitoral e a empresa Serasa Experian é paradigmático ao ilustrar a problemática que envolve a transferência indiscriminada de dados cadastrais. Ainda, chama a atenção para o fato de que, ante a amplidão do rol de hipóteses de compartilhamento insculpido pela Lei Geral, poder-se-ia alegar que acordos como este encontram amparo legal, estando, inclusive, de acordo com os princípios norteadores da proteção de dados.

O presente estudo buscou, assim, demostrar a importância da comunicação à Autoridade Nacional de Proteção de Dados para o controle prévio de operações que envolvam o intercâmbio de dados entre pessoa jurídica de direito público e ente privado, exigência que havia sido suprimida do texto original, mas foi restabelecida pela Lei n. 13.853/2019. Contudo, o ponto se mostra sensível no que se refere ao modelo de autoridade adotado pelo Brasil: a vinculação da ANPD como órgão da administração pública direta pode representar um entrave à sua efetiva atuação em relação aos órgãos do governo federal, comprometendo sua autonomia e isenção política enquanto órgão de fiscalização.

Isto posto, destaca-se que uma autoridade independente, a exemplo do direito europeu, é essencial para a efetivação da proteção de dados, especialmente pelo Poder Público. Somente por meio de uma fiscalização vigorosa pela ANPD é que se garantirá a correção e comedimento dos atos praticados pela Administração Pública, evitando que episódios tais quais os tratados, que representam verdadeira afronta à privacidade e aos direitos fundamentais dos cidadãos, voltem a se verificar.

Referências bibliográficas

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018a.** 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: 05 jul. 2019.

BRASIL. **Medida Provisória 869, de 27 de dezembro de 2018b.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 05 jul. 2019.

BRASIL. **Lei n. 13.853, de 08 de julho 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2>. Acesso em: 10 jul. 2019.

BONFIM, Natália Bertolo. **O tratamento de dados pessoais pelo Poder Público**. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI299940,31047-O+tratamento+de+dados+pessoais+pelo+Poder+Publico>. Acesso em: 2 de jul. 2019.

CARVALHO FILHO, José dos Santos. **Manual de direito administrativo**. São Paulo: Atlas, 25. ed., 2012.

CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. **Revista de Direito, Governança e Novas Tecnologias.** Maranhão, v. 3, n. 2, p. 39-58, jul./dez. 2017.

MEIRELLES, Hely Lopes. A administração pública e seus controles. **Revista de Direito Administrativo.** Rio de Janeiro, n. 114, p. 23-33, out./dez. 1973.

RODOTA, Stefano. **Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance.** Brussels: European Union, 2003. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf>. Acesso em: 10 jul. 2019.

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

ROSSO, Angela Maria. **LGPD e setor público: aspectos gerais e desafios.** Disponível em: <https://m.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios>. Acesso em: 2 de jul. 2019.

SUNDFELD, Carlos Ari. **Direito administrativo para céticos.** São Paulo: Malheiros, 2014.

TRIBUNAL SUPERIOR ELEITORAL. **Decisão Procedimento Administrativo n. 29.542/2012-TSE, de 09 de agosto de 2013.** Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-acordo-cooperacao-serasa>. Acesso em: 05 jul. 2019.

4.10. Aspectos controvertidos sobre a edição de leis municipais em face da proteção de dados pessoais – *Richard Bassan*[109], *Cláudio Lázaro Aparecido Junior*[110], *Renato Passos Ornelas*[111] *& Bruno Bastos de Oliveira*[112]

Resumo

Cuida-se o presente estudo da possibilidade de edição de leis municipais sobre proteção de dados pessoais, complementar à LGPD, face aos aspectos controvertidos do tema. Objetiva delinear a constitucionalidade do ato legislativo, assim como a eficácia da lei municipal. Utilizou-se o método dedutivo, pesquisa bibliográfica e legislação nacional.

[109] Universidade de Marília – UNIMAR.

[110] Universidade de Marília – UNIMAR.

[111] Procurador no Município de Amparo, São Paulo, Brasil.

[112] Universidade de Marília – UNIMAR.

Palavras-chave: Leis municipais; proteção de dados pessoais; constitucionalidade.

Abstract

This paper proposes an analysis of the role of prosecutors in the face of data protection challenges within the municipal public administration. It aims to propose mechanisms and legal guidelines in order to comply with the General Data Protection Law. The deductive method, bibliographic research and national legislation were used.

Keywords: Technological advancements. Municipal Attorneys. Protection of personal data.

Introdução

A Constituição Federal delineia as competências legislativas dos entes federados, de modo a reafirmar a constitucionalidade de todas as suas normas. Entretanto, não raro surgem situações no cotidiano que desafiam a autoridade constitucional, ainda que se trate de adequações benéficas ao interesse público. Em geral, as vedações constitucionais são explícitas, mas é claro que existem aquelas que não se mostram gramaticalmente óbvias, e por esta razão dependem do contexto interpretativo para dar razão à sua formalidade.

Acepções acerca da matéria têm sido ventiladas nas discussões pautadas na edição de leis municipais sobre a proteção de dados pessoais, cuja derivação decorreria do regramento geral esposado na LGPD. Ao ensejo de adequar-se à matéria colocada, os municípios, de posse de situações específicas de âmbito local, questionam a possibilidade de legislar acerca da matéria de forma adjacente, sem que isso represente uma incursão legislativa afora da seara constitucional.

É dizer que o ordenamento jurídico não está preparado para deslindar todas as novéis matérias que surgem na práxis jurídica, mormente aquelas que têm conteúdo legislativo constitucional. Claramente, os questionamentos surgem ainda quanto à amplitude desses regramentos, pois poderiam ensejar a edição de normas semelhantes e com isso surgiriam riscos de haverem conflitos entre elas.

Não se pode negar a transversalidade dos temas aqui perseguidos, e por esta razão, a pesquisa objetiva analisar as questões que envolvem a edição de normas de caráter municipal e de conteúdo complementar, como forma de auxiliar na adequação dos diversos setores aos ditames legais da LGPD, assim como assegurar o exercício do direito fundamental à proteção de dados pessoais, tão essencial para toda sociedade.

1. Proteção de dados como direitos fundamentais e a competência da União

Das mais delicadas às mais controversas e aguerridas discussões acerca da matéria, a maioria tem em consenso o fato de que a proteção de dados pessoais permeia diversos direitos fundamentais e é de

extrema importância na sociedade. Seu uso indevido e indiscriminado evidencia a violação desses direitos, relativos essencialmente à intimidade e à privacidade. Ao abrigo dos ditames constitucionais, o art. 5º, X da CF, ao lado de outros direitos, tornou a vida privada um bem jurídico tutelado, inserida no recorte aportado neste.

A convencionalidade de que os dados pessoais fossem garantidos constitucionalmente levou o legislador infraconstitucional a editar projetos de lei que movimentaram o mundo jurídico. O aporte legislativo da Lei Geral de Proteção de Dados (Lei 13.709/18) foi um deles, cujo objetivo, além de promover a guarida dos direitos de personalidade a exemplo dos dados pessoais sensíveis, foi a de adequar-se juridicamente no âmbito internacional, tendo em vista a vanguarda do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia.

A partir daí, se percebe que a proteção dos dados pessoais se tornou uma interface para o albergue dos direitos de personalidade, que compreendem as informações pessoais e dados sensíveis dos indivíduos e também da coletividade. No escorreito entendimento de Matos et al (2017, p. 277):

> O conjunto das informações as quais compõe o corpo eletrônico são igualmente merecedoras de tutela, todavia, deve-se conferir a categoria dos dados sensíveis uma proteção reforçada, ao passo que a coleta e divulgação destes é suscetível de causar práticas discriminatórias e, portanto, violar, de modo mais intenso, o corolário do princípio jurídico da dignidade da pessoa humana.

A seara das tutelas, portanto, se deu a partir dos contornos jurídicos-constitucionais dos direitos de privacidade, alocados principalmente na CF, mas pulverizados por todo o ordenamento jurídico. Logo vieram as indagações acerca da constitucionalidade legislativa acerca da matéria, que apontava fortes indícios de vícios formais. Deve-se levar em conta que a previsão constitucional da proteção da vida privada do art. 5º, X da CF também se encontra previsto no art. 21 do Código Civil, que prevê que "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" (BRASIL, 2012).

Estando pois, alocada no art. 22, I do texto constitucional, que trata da competência privativa da União, a competência para legislar sobre matéria de direito civil só poderá ser feita no âmbito federal, o que leva ao entendimento de que os estados e os municípios não poderiam legislar sobre a matéria. A autorização para tanto poderia vir por meio de delegação expressa da União, feita por meio de Lei Complementar. Entende-se, na esteira das alusões a competência de Estados e Municípios, que é possível que ambos legislem a respeito, mas apenas para disciplinar determinadas atividades afetas

especificamente aos referidos entes, sem que essas venham a criar normas gerais a respeito, nem tampouco definir conceitos acerca de seus elementos.

Existem diversas incursões legislativas estaduais e municipais que visam disciplinar a proteção de dados pessoais. Sob a análise da constitucionalidade, comunga-se o entendimento de Cunha (2019, p. 125):

> [...] mesmo considerando louváveis as iniciativas estaduais e municipais supracitadas, devemos observar a competência legislativa privativa da União, prevista na Constituição da República. Nestes termos, o inciso I do art. 22 da Carta Magna dispõe que questões de direito civil (dentre as quais, no nosso entendimento, incluem-se a proteção de dados pessoais e a privacidade), são de competência privativa da União. Frente a isto, defendemos não ser cabível que os estados e os municípios legislem sobre o tema em estudo.

Na esteira das discussões, tramita no Congresso Nacional a o Projeto de Emenda Constitucional n. 17/2019, que trata da inserção da proteção de dados pessoais como direito fundamental, assim como a fixação da competência bem como fixar a competência privativa expressa da União para legislar sobre a matéria. Haveria, portanto, a inserção de um inciso ao art. 22 da CF, cessando qualquer questionamento a respeito. Referido projeto, cuja última movimentação legislativa foi a aprovação no plenário da Câmara de Deputados, traz as seguintes informações:

> **Ementa:** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. **Explicação da Ementa:** Assegura o direito à proteção de dados pessoais, inclusive nos meios digitais. Inclui entre as competências de a União legislar sobre proteção e tratamento de dados pessoais (BRASIL, 2019).

A positivação da proteção de dados na seara jurídica constitucional aponta diversas implicações, dentre elas a de que os próprios órgãos que compõe a administração pública sejam compelidos a cumpri-las, malgrado esse regramento já esteja em vigor com o advento da LGPD. Imersa no teor normativo constitucional, a proteção de dados, em especial dos dados sensíveis, reclama uma atuação mais acintosa por parte do Estado.

Nos dias atuais a informação pessoal, "desponta como uma verdadeira *commodity* em torno da qual surgem novos modelos de negócio que, [...] procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias da informação." (DONEDA, 2011, p. 15). Essa é uma das razões pelas quais a informação contrai a condição de bem jurídico e/ou econômico.

Pode-se entender, portanto, que o tratamento de dados sensíveis está mergulhado em dois universos que necessitam dialogar para garantir que todos os envolvidos no processo estejam seguros ao manipulá-los.

2. Controvérsias acerca da edição de Leis municipais de proteção de dados: interesse local ou multiplicidade de normas semelhantes e riscos de normas conflitantes?

É assente na doutrina que a proteção dos dados pessoais por aqueles que têm a sua guarda é um direito fundamental, escorado no direito à intimidade e à vida privada. Sabendo dessas premissas, a discussão se expande para o campo da constitucionalidade da edição de leis municipais em matéria de proteção de dados pessoais, de forma complementar às regras esculpidas na Lei Geral de Proteção de Dados.

De início, é importante estabelecer parâmetro abrangente acerca da competência legislativa da União, vertida no art. 21 da CF, que dispõe sobre sua competência geral. Considerada ampla, abrange "[...] temas que envolvem o exercício de poderes de soberano, ou que, por motivo de segurança ou de eficiência, devem ser objeto de atenção do governo central" (MENDES; BRANCO, 2018, p. 746).

Minudando as competências da União, Tavares (2017, p. 909) acentua que "a Constituição Federal procedeu a uma partilha bastante minuciosa e complexa dos poderes legislativos de cada ente federativo, e, ademais, entre os "poderes" existentes no âmbito da União [...]", além do que, "[...] especificou a competência exclusiva do Congresso Nacional (art. 49) e a competência privativa do Presidente da República (art. 84)" (TAVARES, 2017, p. 909).

Entretanto, é interessante o apontamento feito por Mendes e Branco (2017, p. 746), ao dizerem que "é copioso o acervo de precedentes do STF julgando inconstitucionais diplomas normativos de Estados-membros, por invadirem competência legislativa da União.", dando ênfase à obediência que deve ser dada à matéria de competência privativa da União. Adiante, conservam os autores o entendimento que mitiga a afirmação anterior, quando asseveram que "o parágrafo único do art. 22 prevê a possibilidade de lei complementar federal vir a autorizar que os Estados-membros legislem sobre questões específicas de matérias relacionadas no artigo" (MENDES; BRANCO, 2017, p. 746).

Nesta senda, a União possui competências legislativas privativas e exclusivas, com as quais convive e eventualmente divide com os outros entes federativos. Tavares (2017, p. 911) comenta:

> A Constituição brasileira optou por estabelecer matérias privativas da União e outras que são compartilhadas com outras entidades federativas, a chamada competência concorrente [...] Contudo, ao elencar e repartir esses temas, parece que o constituinte não percebeu a dificuldade que há em classificar certas questões como exclusivamente pertencentes a um ou a outro assunto.

A discussão, portanto, não é fruto de mero capricho por parte dos operadores do direito, o fundamento da celeuma é de ordem constitucional. Tavares (2017, p. 911) explica ainda que "o problema é extremamente relevante para bem compreender a extensão das competências privativas, para as quais parece haver uma predileção em situações que rendam dúvidas de enquadramento.".

Dentre as competências privativas da União está alocada aquela que define normas de Direito Civil, cuja cautela é pronunciada pelo art. 22 da Constituição brasileira, e apresenta um rol extenso de matérias. Na seara do conhecimento jurídico interpretativo das normas constitucionais, Sarlet et al (2018, p. 971) sustenta:

> Como não existe hierarquia entre leis federais e as leis editadas pelos outros entes federativos, eventual conflito, representado pela invasão da esfera de competência legislativa privativa da União, resolve-se pela inconstitucionalidade da legislação que usurpa a competência, a ser declarada pelo STF.

Nesse sentido, eventual conflito cumpriria a denominação de norma inconstitucional, e seria rechaçada do mundo jurídico. Entretanto, o art. 30, II da CF delineia a previsão de que os municípios poderão exercer competência legislativa suplementar de forma vertical, à legislação federal e estadual no que couber.

Trata-se, de acordo com Sarlet et al (2018, p. 974) "[...] de uma modalidade de competência concorrente, embora não expressamente inserida no art. 24 da CF], sendo frequentemente (majoritariamente, poder-se-á afirmar) analisada a tal título pelos cursos e manuais e mesmo outras obras de direito constitucional."

No seio dessa competência concorrente, não há empecilhos que removam a iniciativa legislativa do município para edição de normas de caráter suplementar à LGPD. O entendimento, portanto, é que eventuais antinomias não seriam aceitas em projetos de leis municipais em seu nascedouro, sendo afastadas por ocasião ainda do processo legislativo. O conflito de normas, portanto, não seria possível, já que ao município não cabe legislar sobre matéria em âmbito civil. Aponta-se aqui, de acordo com as lições de Tavares (2017, p. 920) a seguinte premissa:

> Vale retomar, aqui, o vetusto postulado de que as leis são gerais e abstratas, conquista devida em especial às revoluções burguesas, particularmente à Revolução Francesa. Geral, aqui, é sinônimo de não particular; contrapõe-se às leis e normas com endereço certo, que estabeleciam privilégios de toda sorte.

Estaria a lei municipal acoimada de inconstitucionalidade caso invadisse a esfera de competência privativa da União e legislasse sobre matéria de ordem geral, consoante o entendimento majoritário da doutrina (Sarlet; Marinoni; Mitidiero; Tavares; Mendes; Branco). Entretanto, o art. 24 da Constituição brasileira indica o estabelecimento de um "condomínio legislativo" entre entidades federativas. (TAVARES, 2017, p. 919). Segundo o autor, trata-se daquilo que a Constituição denominou "[...] como competência concorrente entre União, Estados-membros e DF. Compete a esses entes legislar, em caráter concorrente, ou seja, concomitantemente, sobre os temas ali elencados."

É certo que o rol ali expressado não contempla matéria de Direito Civil, conquanto se apontem algumas especificidades naquela enumeração taxativa. Apesar disso, consoante ensina Tavares (2017, p. 918-919):

> Ocorre, aqui, uma técnica de repartição vertical das competências. Não se confunde com a competência comum (ou cumulativa), do art. 23, que é administrativa e paralela (horizontalmente distribuída). Na competência legislativa concorrente as normas gerais cabem à União, e aos Estados membros cabem as normas particulares. Por isso a competência dos Estados membros é denominada complementar, por adicionar-se à legislação nacional no que for necessário. Também à União cabe legislar sobre normas particulares para seu âmbito.

Haveria, no entanto, uma dificuldade de subcategorizar os assuntos a serem tratados pelo município, o que poderia ensejar a sua declaração de inconstitucionalidade face ao conflito de competência. Nessa senda a expressão "limitar-se-á" constante do art. 24 é elucidativa "[...] a respeito da "limitação" da União na elaboração da norma geral, com o propósito de reservar aos demais entes federativos espaço legislativo para suplementar a legislação editada no plano federal."(SARLET et al, 2018, p. 976).

Voltando à análise da competência dos municípios, a discussão agora se mostra na dúvida em saber quando cabe a suplementação legislativa por parte do Município, o que não constitui algo imune a controvérsias. De acordo com Sarlet et al (2018, p. 980):

> Uma primeira delimitação, que já foi objeto de referência e encontra suporte (para além do texto constitucional) na doutrina, é a que diz respeito ao interesse local, pois em todo caso este deverá se fazer (ainda que não em caráter exclusivo, como já visto) presente. Tal limitação, portanto, se aplica genericamente a toda e qualquer hipótese de exercício da competência legislativa suplementar dos Municípios.

Entende-se, em face dessas premissas, que o município possui duas possibilidades de exercer a competência suplementar, que se configure o interesse local e que haja compatibilidade com a legislação

federal e estadual. Tavares (2017) concorda que compete aos Municípios legislar sobre assuntos de predominante 'interesse local. O autor aponta que "uma correta interpretação constitucional dessa norma há de concluir ser prescindível a exclusividade do interesse local. Basta que predomine o aspecto local do assunto."

A depender do texto da lei municipal, ainda que verse sobre interesse loca, pode ser que extrapole a sua competência suplementar, ainda que se diga que pode ser considerada como de competência exclusiva do município. Por esta razão, à luz dos preceitos doutrinários apontados, é prudente que, caso haja edição de lei municipal relacionada à proteção de dados pessoais sejam observados os gatilhos permissivos (interesse local e compatibilidade com legislação estadual e federal), bem como que sejam suplementares, de modo a não imiscuir-se na esfera de competência privativa e exclusiva da União.

Conclusão

A pesquisa demonstrou que normas constitucionais referentes a competências legislativas possuem natureza cogente e ensejam a declaração implacável de inconstitucionalidade, caso venham desrespeitar os preceitos ali encartados. Com acentuada razão, quis o legislador constituinte originário delimitar a independência legislativa dos entes federados, com o objetivo de manter a hegemonia constitucional à luz da norma hipotética fundamental.

A concepção de que o direito à proteção dos dados pessoais decorre da proteção estatal à intimidade e à vida privada do cidadão se confirma pela edição da LGPD, cuja natureza *erga omnis* atua para todos e contra todos. Na seara dos entendimentos, é possível compreender a preocupação dos municípios em editar normas capazes de facilitar a transição e adequação de sua estrutura para cumprir os ditames legais, à luz do exercício do princípio da legalidade. Ainda que não se tenha observado uma vedação expressa acerca da edição de normas suplementares acerca da possibilidade dos municípios legislarem sobre matéria afeta à proteção de direitos fundamentais, colimando o entendimento doutrinário, a reserva constitucional dada à União para legislar sobre matéria de Direito Civil alimenta as discussões.

Entretanto, o próprio texto constitucional não afere o engessamento das competências legislativas, dando azo à concepção da possibilidade de que os municípios legislem sobre a proteção de dados pessoais, desde que configurados o interesse local e que não causem conflitos mútuos com as legislações estaduais e federais.

Referências bibliográficas

BRASIL. **Código Civil Brasileiro.** Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 10 out. 2019.

BRASIL. **Proposta de Emenda à Constituição n. 17, de 2019.** Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 10 out. 2019.

CUNHA, Juliana Falci Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual – Direito Contemporâneo e Constituição.** Aracaju, ano VIII, v. 13, n. 02, p.115-145, jul/2019. Disponível em: <http://pidcc.com.br/08072019.pdf>. Acesso em: 10 out. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico Journal of Law.** Joaçaba/SC, vol. 1, n. 2, p. 91-108, jul/dez. 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658>. Acesso em: 23 jul. 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** São Paulo: Saraiva, 2017.

MATOS, Liliane Gonçalves et al. Limites à implantação de chips subcutâneos: a tutela da privacidade como instrumento de proteção da pessoa na sociedade da informação. **Revista de Direitos e Garantias Fundamentais.** Vitória, v. 18, n. 3, p. 267-300, set./dez. 2017. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Dir-GarantiasFundamentais_v.18_n.3.11.pdf.>. Acesso em: 10 out. 2019.

SARLET, Ingo Wolfgang; MARINONI, Luis Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** São Paulo: Saraiva Jur, 2018.

TAVARES, André Ramos. **Curso de Direito Constitucional.** 15. ed. rev. e atual. São Paulo: Saraiva, 2017.

4.11. Análise da proteção de dados na América Latina e a possibilidade de aplicação do sistema multinível como

garantidor dos direitos fundamentais digitais – *Leonardo de Andrade Alberto*[113] *& Moacir Henrique Júnior*[114]

Resumo

O trabalho é parte da iniciação científica PAPq/UEMG "Análise das fontes de Direito Constitucional num sistema constitucional multinível" e tem por escopo o estudo da aplicação do constitucionalismo multinível na América Latina com o fim de trazer maior proteção aos direitos digitais dos usuários, partindo da análise de legislações de vários países.

Palavras-chave: Proteção de dados; Constitucionalismo multinível; América Latina.

Abstract

This paper is part of undergraduate research PAPq/UEMG "An analysis of the sources of Constitutional Law in a constitutional system multi-level", and the purpose is study the implementation of multi-level constitutionalism in Latin America, with the aim of bringing a better protection to the digital rights of the user based on an analysis of the legislation of the countries.

Keywords: Data protection. Multi-level constitutionalism. Latin America.

Análise da proteção de dados na América Latina e a possibilidade de aplicação do sistema multinível como garantidor dos direitos fundamentais digitais

Na União Europeia (EU), a proteção entorno dos dados surge pela primeira vez no artigo 8º da Convenção Europeia dos Direitos do Homem de 1950 garantindo o direito ao respeito a vida privada, familiar, domicílio e correspondência. Entretanto, com o advento da tecnologia nos anos sessenta, é criada a Convenção 108, a qual conta com 45 países europeus e 1 latino-americano, sendo o Uruguai, como signatários e "[...] visa proteger os cidadãos contra os abusos que possam surgir com a recolha e tratamento de dados pessoais, tendo também como objetivo regular o fluxo transfronteiriço de dados pessoais" (SALDANHA, 2018, p. 04).

[113] Graduação em Direito em andamento pela Universidade do Estado de Minas Gerais, Unidade Frutal, Bolsista de iniciação científica Edital 01/2019 PAPq/UEMG, pesquisador do Laboratório Americano de Estudos Constitucionais Comparados (LAECC). E-mail: leonardoaalberto@hotmail.com

[114] Doutor em Direito e Ciência Política e Mestre em Criminologia e Sociologia Jurídico Penal, ambos pela Universitat de Barcelona, pesquisador do Laboratório Americano de Estudos Constitucionais Comparados (LAECC). Professor do Curso de Direito da Universidade do Estado de Minas Gerais, Unidade Frutal. E-mail: moacir.henrique@uemg.br

Já a Diretiva n°95/46/CE de 1995 foi o primeiro meio jurídico pelo qual a proteção de dados esteve atrelada com o fim de "[...] tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais" (SALDANHA, 2018, p. 04).

Evoluindo, chegamos a Carta dos Direitos Fundamentais da União Europeia de 2000, consagrando o direito à proteção de dados. Neste ínterim, em 2018 foi criado um manifesto político em forma de lei que visa proteger direitos no âmbito digital, chamado de *Charter of Digital Fundamental Rights of the European Union* ou, em tradução livre, Carta de Direitos Fundamentais Digitais da União Europeia.

Segundo José Joaquim Gomes Canotilho, a Carta "[...] não pretende substituir a valiosa elaboração jurídico-dogmática já efectuada em torno de alguns direitos fundamentais digitais", mas sim "[...] reforçar e constituir os direitos fundamentais já existentes partindo do desafio colocado pela regulação de sistemas inteligentes" (CANOTILHO, 2019, p. 70).

A Carta reconhece em seu preâmbulo os dispositivos de documentos internacionais como a Declaração Universal dos Direitos Humanos, Convenção Europeia de Direitos Humanos, Carta de Direitos Humanos da União Europeia, os Padrões de Proteção aos Direitos Fundamentais e os Dados da União Europeia e de seus Estados Membros.

O documento protege direitos como a dignidade, liberdades de informação e comunicação e de opinião e publicidade, igualdade de participação no mundo digital, eleições não atadas ao uso de mídias digitais, dentre tantos. Assim, o manifesto visa:

> proteger os direitos fundamentais e princípios democráticos também na era digital por meio da primazia do Direito, a comprometer atores estatais e não estatais para a validação dos direitos fundamentais na era digital, a criar, dessa forma, o fundamento para um Estado de direito na era digital, a compreender o meio digital não como fonte de medo, mas sim como oportunidade para uma vida boa em um futuro global (CARTA DE DIREITOS FUNDAMENTAIS DIGITAIS DA UNIÃO EUROPEIA, 2018).

No artigo 6° da referida Carta de Direitos, é garantido que "(1) Todo ser humano tem direito ao acesso a informações de órgãos estatais. Deve-se garantir a proteção principalmente de dados pessoais" e "(2) Deve-se proteger apropriadamente denunciantes que divulguem informações sobre o comportamento incorreto de uma organização".

Já o artigo 7º trata sobre a esfera privada, confiança e proteção de dados e dispõe, dentre outros, que "(2) Dados pessoais só podem ser coletados e processados de boa-fé para fins determinados à pessoa afetada, e se existir base legal para tal." E continua dispondo que "o processamento dos dados deve ser concebido de forma segura, justa, transparente e segundo o estado da arte".

No mesmo ano, entrou em vigor, na União Europeia (UE), o *General Data Protection Regulation* – GDPR, ou em português, Regulamento Geral de Proteção de Dados – RGPD, o qual dispõe sobre as regras de tratamento por qualquer pessoa física ou jurídica de dados pessoais relativos às pessoas que estejam na UE. Todavia, a Comissão Europeia destaca em quais situações será necessária a aplicação do Regulamento, conforme informativo *in verbis:*

> As regras não se aplicam ao tratamento de dados por motivos exclusivamente pessoais ou no exercício de atividades domésticas, desde que não haja qualquer ligação com uma atividade profissional ou comercial. Quando uma pessoa utiliza os dados pessoais fora da sua "esfera pessoal", por exemplo para o exercício de atividades socioculturais ou financeiras, a legislação relativa à proteção de dados tem de ser respeitada (COMISSÃO EUROPEIA, 2018).

O Regulamento de n° 2016/679 advindo do Parlamento Europeu e Conselho, é uma norma geral que visa a harmonização de leis sobre o tema nos diversos países da UE. O documento é dotado de vários princípios, tais como a informação aos titulares dos dados sobre o tratamento dos dados coletados; o consentimento dos titulares dos dados que, segundo o texto legal, "[...] deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito [...]" Tal consentimento pode ser, por exemplo, a positivação de uma opção ao visitar um sítio eletrônico.

Também no RGPD há a garantia do exercício dos direitos dos titulares dos dados que "[...] passam a ser monitorizados e documentados com prazos máximos de resposta" para direitos relativos "[...] à portabilidade dos dados, à eliminação dos dados e à notificação de terceiros sobre a retificação, o apagamento ou a limitação de tratamento solicitados pelos titulares dos mesmos" (SIMÕES, 2018).

Um estudo do *Institute for Business Value* (IBM) intitulado *The end of the beginning - Unleashing the transformational power of GDPR*, que tem o objetivo de mostrar como líderes de empresas estão abordando questões relativas à segurança, privacidade, dados e envolvimento do cliente, obteve os seguintes resultados:

> […] realizado com 1,5 mil líderes de negócios em 34 países, 60% das organizações está adotando o GDPR como uma oportunidade para melhorar a privacidade, a segurança e o gerenciamento de dados ou como um catalisador de novos modelos de negócios, em vez de simplesmente um problema ou impedimento de conformidade. 96% acreditam que a prova de conformidade com o GDPR será vista como um diferenciador positivo para o público. 76% disseram que o GDPR permitirá relacionamentos mais confiáveis com os titulares de dados, que criarão novas oportunidades de negócios. Mas apenas 36% acreditam que estariam totalmente em

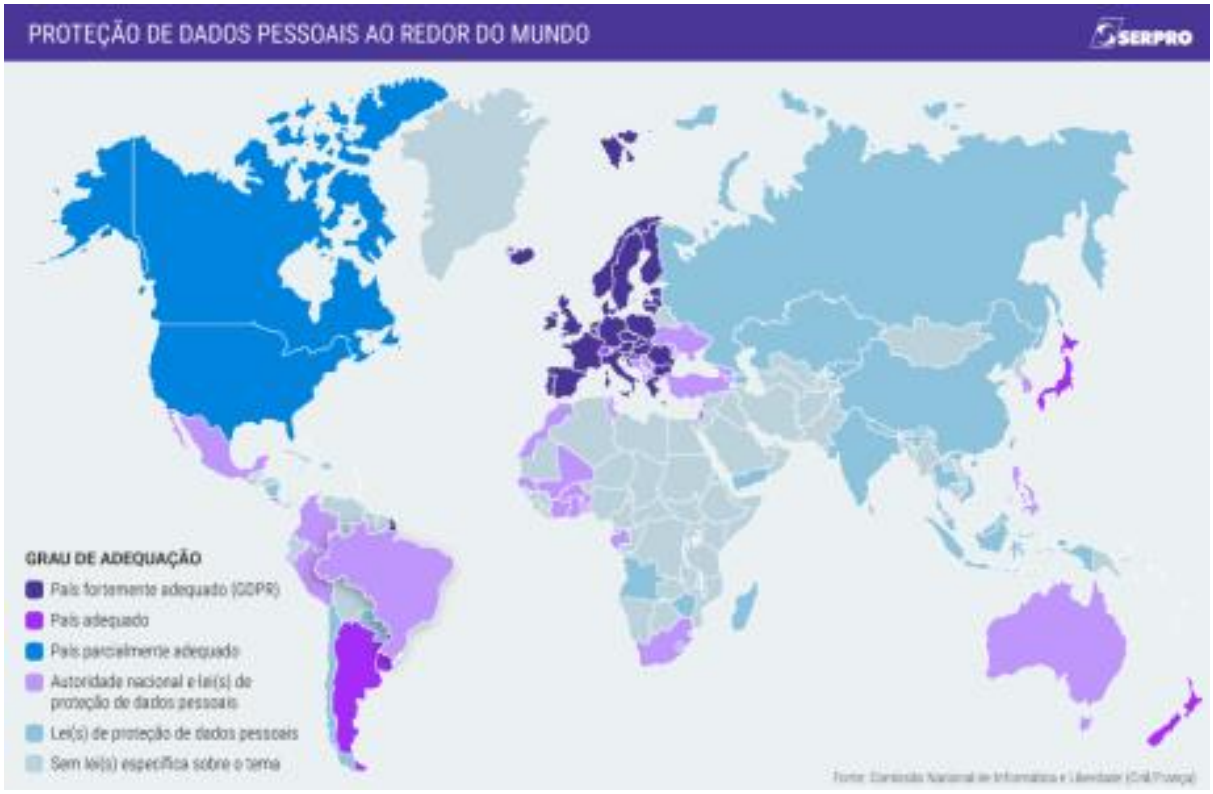
> conformidade com o GDPR até o prazo final de 25 de maio (IBM *apud* FEREEIRA; BRANCHER; TALIBERTI; CUNHA, 2018).

Assim, tamanha é a importância do RGPD que a legislação impacta não apenas empresas europeias, mas também de outras nacionalidades, conforme dispositivo 23 do referido diploma, *in verbis:*

> A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento. A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio web do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.

A importância de legislações sobre a proteção de dados pessoais é de extrema relevância para que a sociedade saiba como instituições públicas e privadas tratam e usam os dados de seus usuários, além de garantir a postulação de direitos na esfera digital, como direito de portabilidade ou exclusão de dados.

Entretanto, apesar da importância, poucos países possuem legislações adequadas sobre o tema. Segundo o "Mapa da Proteção de Dados", elaborado pela Comissão Nacional de Informática e Liberdade-CNIL/França e divulgado pela estatal brasileira SERPRO (Serviço Federal de Processamento de Dados), os países da União Europeia apresentam proteção "fortemente adequada" no que tange a dados pessoais graças ao RGPD.



Proteção de Dados Pessoais ao redor do mundo. Fonte: SERPRO. *Mapa da proteção de dados.* Disponível em: http://www.serpro.gov.br/lgpd/menu/algpd/mapa-da-protecao-de-dados-pessoais. Acesso em 04 out. 2019.

Em contrapartida, quando voltamos olhares para a América do Sul, observamos que apenas a Argentina e Uruguai atingem o nível de "países adequados" à proteção de dados e a Guiana Francesa o nível de "fortemente adequada", tendo em vista ser um território ultramarino da França e, assim, regido por normas da União Europeia. Neste sentido, façamos uma breve análise das principais legislações de proteção de dados dos países sul-americanos que são destacados no "Mapa da Proteção de Dados" acima.

O Chile, em 1999, foi o primeiro país da região a legislar sobre uma lei de proteção de dados pessoais. A lei n° 19.628/1999, ainda em vigor, dispõe que "Qualquer pessoa pode realizar o processamento de dados pessoais [...]" devendo "[...] respeitar o pleno exercício dos direitos fundamentais dos proprietários dos dados [...]", tradução livre do texto original, *in verbis:*

> [...] tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre [...]

No Uruguai, a Lei n° 18.331/2008 dispõe sobre a proteção de dados pessoais inerentes à pessoa humana e aplica-se, também, às pessoas jurídicas.

A Colômbia possui a "Autoridade Colombiana de Proteção de Dados" e a lei "[...] inclui a proteção dos direitos dos usuários, a criação de obrigações para quem coleta e gerencia dados, a regulamentação da proteção de dados pessoais financeiros e de crédito e o controle do Registro Nacional de Bancos de Dados". Com relação a este Registro, a legislação colombiana prevê o registro dos bancos de dados.

A Lei n° 29.733/2001 garante a proteção de dados pessoais como direito fundamental, no Peru.

A respeito do tema em estudos, a legislação sul-americana mais recente é a Lei brasileira n°13.709, de 14 de agosto de 2018, que dispõe sobre a Lei Geral de Proteção de Dados – LGPD, cuja vigência dar-se-á em agosto de 2020.

Neste sentido, tendo em vista a existência de diversas legislações sobre o mesmo tema nos países do MERCOSUL, o presente estudo que encontra-se em andamento – proveniente de desmembramento do Projeto de Iniciação Científica do Edital 01/2019 – PAPq/UEMG intitulado "Análise das fontes de Direito Constitucional num sistema constitucional multinível" – visa estudar as legislações sul-americanas de proteção de dados pessoais e o constitucionalismo multinível como forma de trazer maior proteção aos direitos digitais.

A expressão constitucionalismo multinível pode designar a necessidade/possibilidade de construção de ordem normativa mundial/regional, com vários níveis de autoridades estatais ou supraestatais/internacionais, e com várias estruturas radicais de fontes normativas, mas com um sistema unitário e coerente de vinculação jurídica e normativa.

Esta unidade e coerência de sistema constitucional multinível opera com a manutenção de algumas estruturas nucleares do constitucionalismo nacional-estatal, mas com uma "perpetuação transformada" deste modelo, e a ascensão de um novo conceito formal e material da constituição em direção à constitucionalização multinivelada (NEVES, 2009) (NEVES, 2014) (GRIMM, 2016) (ISIKSEL, 2016) (NEIL WALKER, 2011) (MATEJ AVBELJ, 2012) (BORGES, A. W.; COELHO, S. O. P.; HENRIQUE JÚNIOR, M, 2019).

O constitucionalismo multinível está ligado ao direito comunitário visando integrar várias nações com objetivos comuns, como por exemplo, o bloco econômico MERCOSUL, além de buscar interesses comuns entre os países.

Com relação ao constitucionalismo multinível no âmbito digital, Nuno Saldanha doutrina que "a história do direito comunitário abre agora uma nova etapa, como o RGPD, [...] ao entrar diretamente na jurisdição de todos os Estados-Membros, cria um espaço legislativo uniforme e harmonizado" (SALDANHA, 2018, p. 05).

Assim, com um ordenamento supraestatal de aplicabilidade comum entre os Estados, é possível que os indivíduos tenham maior proteção e rigor no tratamento dos seus dados pessoais por pessoas físicas e/ou jurídicas, tendo em vista vigorar uma legislação com caráter *jus cogens*.

Destarte, a presente pesquisa de natureza qualitativa é realizada com consulta às fontes bibliográficas, periódicos, documentos legislados, documentos políticos de órgãos estatais e de órgãos multinacionais/organismos internacionais e utiliza-se o método dedutivo partindo do pressuposto de que a aplicação do sistema multinível no MERCOSUL poderá trazer maior proteção aos dados pessoais de usuários.

Referências bibliográficas

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE/BCN. **Ley 19628/1999.** Sobre Proteccion de la Vida Privada. Santiago, Chile: Ministerio Secretaría General de la Presidencia, 1999. Disponível em: https://www.leychile.cl/Navegar?idNorma=141599. Acesso em 04 out. 2019.

BORGES, A. W.; COELHO, S. O. P.; HENRIQUE JÚNIOR, M. **Interculturalidade, Interconstitucionalidade e Interdisciplinaridade: desafios e níveis de inter-relação em um mundo global.** Uberlândia: LAECC, 2019.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018.** Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 04 out. 2019.

CANOTILHO, José Joaquim Gomes. Sobre a indispensabilidade de uma Carta de Direitos Fundamentais Digitais da União Europeia. **Revista do Tribunal Regional Federal da 1ª Região,** v. 31, n.1, p. 69-75, 27 mar 2019. Disponível em: http://revista.trf1.jus.br/trf1/article/view/17. Acesso em 04 out. 2019.

COMISSÃO EUROPEIA. **Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-doesgeneral-data-protection-regulation-gdpr-govern_pt. Acesso em 04 de out. 2019.

CONGRESO DE LA REPÚBLICA DEL PERÚ. **Ley n° 29733/2011.** Ley de protección de datos personales. Lima, PE: Congreso de la Republica, 2011. Disponível em: http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf. Acesso em 04 out. 2019.

FERREIRA, Ricardo Barretto; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA,Vitor Koketu da. **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia,** 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao. Acesso em 04 out. 2019.

FUNDAÇÃO HEINRICH BÖLL STIFTUNG. **Carta de Direitos Fundamentais Digitais da União Europeia,** 2018. Disponível em: https://br.boell.org/pt-br/2018/07/25/carta-dos-direitos-fundamentaisdigitais-da-uniao-europeia. Acesso em 04 out. 2019.

GRIMM, D. **Constitutionalism.** Past, Present, and Future. Oxford: Oxford. u. p., 2016.

ISIKSEL, T. **Europe's Functional Constitution.** A Theory of Constitutionalism Beyond the State. Oxford: Oxford u. p., 2016.

MATEJ AVBELJ, J. K. **Constitutional Pluralism in the European Union and Beyond.** Oxford; Portland: Hart publishing, 2012.

NEIL WALKER, J. S. S. T. **Europe's Constitutional Mosaic.** Londres: Bloomsbury. Publishing, 2011.

NEVES, M. Do diálogo entre as cortes supremas e a corte internacional de direitos humanos ao transconstitucionalismo na AL. **Revista de informação legislativa,** Brasília, jan./mar. 2014, pp. 193-214.

NEVES, M. **Transconstitucionalismo**. São Paulo: Saraiva, 2009.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. **Ley 25.326/2000.** Proteccion de los Datos Personales. Argentina: Congreso, 2000. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em: 04 out. 2019.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. **Ley n° 18.331/2008.** Protección de datos personales y acción de "Habeas Data". Uruguai: Senado y Cámara, 2008. Disponível em: http://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20y%20Acci%C3%B3n%20de%20Habeas%20Data.pdf. Acesso em 04 out. 2019.

PAIXÃO, Pedro. **Proteção de dados na América Latina.** CIO from IDG. 2018. Disponível em: https://cio.com.br/protecao-de-dados-na-america-latina. Acesso em 04 out. 2019.

SALDANHA, Nuno. **Novo regulamento geral de proteção de dados.** Lisboa: FCA, 2018.

SERPRO. **Mapa da proteção de dados.** Disponível em: http://www.serpro.gov.br/lgpd/menu/algpd/mapa-da -protecao-de-dados-pessoais. Acesso em 04 out. 2019.

SERVIÇO DAS PUBLICAÇÕES DA UNIÃO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Jornal Oficial da União Europeia.** Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=DA. Acesso em 04 out. 2019.

SIMÕES, José Augusto. Proteção de dados e o novo regulamento geral da União Europeia. **Revista Portuguesa de Medicina Geral e Familiar,** vol.34, n.5, Lisboa out. 2018. Disponível em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2182-51732018000500001. Acesso em 04 out. 2019.

Capítulo 5

5. Perspectivas multissetoriais da regulação em proteção de dados pessoais e privacidade

5.1. Os desafios da ANPD diante das bases de dados pessoais legadas – *Lucas Del Vecchio Soares*[115]

Resumo

O futuro regulatório da ANPD é insipiente: não há, até o momento, elementos mínimos que possam nos permitir arriscar os primeiros standards regulatórios da autoridade. O presente artigo busca analisar os principais desafios e perspectivas quanto a informação acumulada e legada pelas empresas a partir da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – a "LGPD"). A questão central sobre o destino da base legada se inicia em razão do paradigma de big data superado pelos princípios da LGPD, tais como, essencialidade e finalidade para a coleta e tratamento da informação pessoal. Assim a cultura do acúmulo de informações e estoque descomedido dos bancos de dados que formavam *data likes* profundos e repletos de dados está superada pelo novo paradigma de *data minimization*. Dessa forma,

[115] Advogado. Pós-graduando em LLM em Direito Civil, na Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo – FDRP/USP.

o artigo propõem algumas alternativas de tratamento as bases legadas, no entanto, e independentemente da alternativa de tratamento destinado as bases legadas, o que deve ser realizado como essencial e primordial é o inventário desse ativo, mediante a criação de mapeamento personalizado as necessidades do negócio para posterior reflexão de estratégia a ser tomada.

Palavras-chave: Lei n. 13.709/2018; Lei Geral de Proteção de Dados – LGPD; proteção de dados pessoais; privacidade; *marketing*.

Abstract

The regulatory future of the ANPD is insipient: there are, to date, no minimum elements that could allow us to risk the first regulatory standards of the authority. This article seeks to analyze the main challenges and perspectives regarding the information accumulated and bequeathed by companies as of Law 13.709 / 2018 (General Law for the Protection of Personal Data - the "LGPD"). The central question about the fate of the legacy base begins because of the big data paradigm overcome by the LGPD principles, such as, essentiality and purpose for the collection and treatment of personal information. Thus, the culture of accumulation of information and excessive stock of databases that formed data likes deep and full of data is overcome by the new paradigm of data minimization. Thus, the article proposes some treatment alternatives to the legacy bases, however, and regardless of the treatment alternative intended for the legacy bases, what should be performed as essential and paramount is the inventory of this asset, by creating a personalized mapping of the assets. business needs for further reflection on the strategy to be taken.

Keywords: Law 13.709/2018. General Data Protection Law. Personal Data Protection. Privacy. Marketing.

Introdução

A Lei nº 13.853/2019 foi publicada em julho de 2019 para findar, ao menos por ora, as discussões sobre a criação de uma Autoridade Nacional de Proteção de Dados Pessoais independente ou passível de captura pelos principais agentes de mercado.

Independentemente dos desafios inaugurados pela sua estrutura institucional, a recém-criada ANPD já pode ser considerada sobrecarregada face às inúmeras matérias eleitas para regulação.

O futuro regulatório da ANPD é insipiente, não há, até o momento, elementos mínimos que possam nos permitir arriscar os primeiros standards regulatórios da autoridade.

Todavia, dentre as mais urgentes necessidades de regulação, residem as bases de dados pessoais compostas por informações legadas e conquistadas ao longo de toda a operação dos agentes de tratamento.

Este espeque de dados acumulados pelas empresas antes da vigência da LGPD, ou até mesmo antes do início dos processos de implementação *in house* pelos agentes de tratamento de dados pessoais que já se adequaram para novas coletas, resulta em principal alerta operacional. Isso pois, independentemente do segmento comercial ou industrial analisado sob a LGPD, ocorrerão impactos globais no dia-a-dia de qualquer operação, consequentemente sobre as bases de dados pessoas já coletadas, tratadas e armazenadas antes de agosto de 2020.

A base legada é composta por todas as informações que permitem identificar um indivíduo, tais como, e-mails, endereço de IP, perfil comportamental, cadastros, currículos, fichas, ou seja, informações pessoais armazenadas, tratadas ou não, antes da vigência da norma de proteção de dados pessoais.

Esse ecossistema de informações compõe o ativo das operações e tornam-se indispensáveis para algumas atividades, a título de exemplo, *e-commerce, marketing* digital, operadoras de planos de saúde, instituições de ensino e uma infinidade de outras atividades não poderiam atuar um dia sequer sem sua base de dados pessoais.

A questão central sobre o destino da base legada se inicia em razão do paradigma de big data superado pelos princípios da LGPD, tais como, essencialidade e finalidade para a coleta e tratamento da informação pessoal. Assim a cultura do acúmulo de informações e estoque descomedido dos bancos de dados que formavam *data lakes* profundos e repletos de dados pessoais sem finalidade específica, apenas pela cultura do acúmulo de informações, está superada pelo novo paradigma de *data minimization.*

Entretanto, adequar bases de informações pessoais conjecturadas sobre outro paradigma (*big data*) e torná-las conformes é tarefa que depende do auxílio tecnológico e estrutural da ANPD, sob pena dos riscos decorrentes da ausência de regulação inviabilizarem o desenvolvimento de tecnologias disruptivas e sufocar a competitividade daquelas operações intimamente dependentes do tratamento de dados pessoais.

Desenvolvimento

Conforme introito, a principal chamada de demandas para implementação da LGPD por agentes de tratamento atuantes no mercado é a destinação de suas bases de dados ativas e o pool de informações em seus sistemas e registros[116].

Muitos desses agentes, embora aparelhados com tecnologia de ponta, pouco sabem sobre a totalidade de sua base de dados pessoais. Assim, há uma surpreendente lacuna tecnológica e operacional quanto ao mapeamento dessas bases.

Tal realidade, a de desconhecimento de si mesmo, necessita de rompimento imediato. Independentemente de regulamentação progressiva pela ANPD, desenvolvimento de *softwares* para gestão e *tracking* de dados pessoais pelos agentes de tratamentos e empresas de soluções tecnológicas, o inventário dos dados pessoais, presentes nas bases operacionais dos agentes de tratamento, é mandatório e o método adequado para que o agente de tratamento possa conhecer a própria base de dados pessoais e os riscos decorrentes desse ativo.

Em primeiro lugar, o adequado mapeamento da informação legada é mandatório, em razão de ser o método mais adequado para que se possa conhecer a própria base, sua origem, suas finalidades e a necessidade de sua manutenção. O inventário e o conhecimento prévio dos dados pessoais de toda a operação é a mínima medida a se tomar, independentemente da regulação posterior com relação às bases legadas, ou seja, independente.

A principal celeuma sobre a informação legada advém da própria LGPD, que prescreve em seu artigo 63 que a Autoridade Nacional de Proteção de Dados Pessoais estabelecerá parâmetros de adequação progressiva para bancos de dados pessoais fomentados antes da vigência da Lei.

A norma possui sua *ratio* em virtude da complexidade operacional e tecnológica decorrente da adequação de dados pessoais coletados, tratados e armazenados antes da regulamentação brasileira, ao se vislumbrar uma operação, como a de *e-commerce*, por exemplo, verificar-se-á que a informação é coletada por diversos pontos, ativa ou passivamente e tratada por inúmeros operadores que se utilizam de diversas ferramentas e soluções de software para outros tantos quantos fins, tais como marketing, setor fiscal, logística, gerenciamento, e que por fim, armazenam dados e os espelham ao redor de todo o globo.

Ou seja, a própria natureza de adequação de informações coletadas antes da LGPD pressupõe um nível de complexidade extremo e sem solução que adviria de mera norma de comando, razão pela qual a LGPD reservou esse assunto para sua Autoridade, a fim de que a ANPD dialogue com diversos dos setores afetados, além da sociedade civil, para que de alguma forma, coletivamente, possam compor a

[116] Informação decorrente de consultas práticas e implementação de projetos de conformidade com a LGPD do qual o Autor se envolveu profissionalmente. A opinião é limitada a sua prática profissional.

mais adequada solução de implementação progressiva das informações de dados pessoais coletados antes da vigência da LGPD.

Até o momento, a adequação ainda não foi esboçada pela recém Autoridade criada, a projeção do tratamento legado deve ser realizada por setor (Publicidade, E-commerce, Saúde, Educação, Aviação etc.), por meio de suas diversas associações existentes, a fim de trazer as necessidades especificas de cada seguimento e tentar conciliar as obrigações legais da LGPD com as demandas técnicas e individuais de cada setor, a fim de viabilizar o cumprimento legal da norma de proteção de dados e jamais interromper o processo de desenvolvimento de tecnologias disruptivas, ambos preceitos devem ocorrer harmonicamente.

Em relação ao *e-commerce*, a principal entidade representativa brasileira (ABCOMM) até o momento do fechamento desse Resumo em nada se posicionou em relação as bases legadas e sua progressiva adequação, nem mesmo ocorreram manifestações das principais agências independentes e reguladoras do Brasil. O BACEN – Banco Central e a ANS – Agência Nacional de Saúde, à título de exemplo, também não editaram qualquer normativa sobre informações de dados pessoais tratados ou coletados pelos seus tutelados.

A ausência de regulamentação, no entanto, não pode ser tomada como justificativa legal para a inércia da adequação das bases legadas pelos agentes de tratamento, isso pois, independentemente de regulamentação superveniente, o mapeamento da informação deve ser mandatório, em razão de ser o método adequado para que os agentes de tratamento preservem a sua memória e consequentemente resguardem um dos maiores ativos da operação, seu banco de dados e suas informações.

O que se pretende esclarecer é que não há necessidade de aguardar o movimento da ANPD, ou até mesmo a vigência da LGPD para se inicie o processo de adequação dos dados pessoais coletados antes da vigência da Lei, tal processo é complexo e independentemente de qualquer diretriz a ser editada, o inventário dos dados pessoais que são tratados pelos agentes de tratamento é a medida mais óbvia para se iniciar qualquer processo de adequação.

Ao se verificar o tratamento dado às bases legadas por agentes de tratamento europeus, quando do início da vigência do Regulamento Europeu, observaram-se soluções de toda as ordens, das mais drásticas como a exclusão de todas as bases de dados, até a mais inerte, como espera de regulação própria pelas autoridades de cada país.

A alternativa de exclusão da informação pôde ser vista em diversos setores europeus, inclusive com alguns provedores de aplicação que reiniciaram completamente suas operações, e trataram o início da vigência do regulamento europeu como dia 0 da operação.

O que se conclui é a existência da possibilidade de exclusão da informação em homenagem aos princípios da necessidade e finalidade, no entanto, tal ação deve pressupor um fluxograma claro do *tracking* da informação e um mapeamento prévio e adequado dos dados pessoais existentes em todas as operações, para que se exclua apenas aquilo que for desnecessário ou inadequado, sob pena de inviabilizar comercialmente e operacionalmente a atividade empresarial.

Sobre o ponto da exclusão, necessário consignar que a integridade dos dados é necessária para se confiar em uma verdadeira eliminação da informação, tratando-se de sistemas operacionais, é sabido que a exclusão de dados em determinado local não significa sua real e definitiva eliminação, por essa razão, sempre é necessário ter o *tracking* da informação, a fim de conferir integridade ao dado deletado, para que não restem cópias ou possibilidades de restauração, caindo por terra a solução de exclusão de bases de dados pessoais.

Obviamente, a possibilidade de se adotar a medida mais drástica de destinação das bases legadas é alternativa totalmente inviável para diversos setores, também não é viável a inércia em razão de se aguardar regulamentação ulterior da ANPD, haja vista estarmos a menos de um ano da vigência da LGPD sem qualquer sinalização de produção regulatória por sua Autoridade.

Dessa forma, este Resumo propõe a criação de um modelo individualizado ao negócio, com a ressalva de inexistência de prescrição padrão sem imersão detalhada na operação de cada agente de tratamento, para que seja viabilizada a adequação da informação legada e permitir seu armazenamento e tratamento por uma das possíveis bases legais aplicáveis ao caso concreto(Art. 7º da LGPD), pois cada agente de tratamento possui características específicas que permitem diversos enquadramentos (bases legais) no tratamento de dados pessoais.

Para tanto, a primeira diretriz a ser tomada é a criação de um projeto de trabalho claro para o mapeamento da informação, tendo como norte os princípios e fundamentos da legislação. O projeto de adequação deve buscar extrair o necessário para adequação de uma base legada, dessa forma, sugere-se a aplicação de alguns filtros na informação inventariada, sendo o primeiro filtro aplicado aquele que identifica se a informação pode ser convalidada ou considerada adequada em detrimento da informação manifestamente em desconformidade.

Por exemplo: bases compradas e informações discriminatórias devem ser consideradas manifestamente inadequadas por incompatibilidade legal, e devem ser excluídas de toda as operações, arquivos, nuvens, registros e servidores, sem qualquer possibilidade de restaurações, ao passo, que outras bases de dados podem ser mantidas, mediante a aplicação de novos filtros.

Após a aplicação do filtro e exclusão da informação manifestamente ilegal, teremos uma base residual, excluído em definitivo os dados acima mencionados, deve sofrer nova filtragem. A depender da natureza

da operação, uma das principais bases e *inputs* de dados coletados pode vir por intermédio da base legal do consentimento art. 7º, I (em harmonia com os princípios e fundamentos da LGPD), assim a base residual deve ser classificada como base não consentida.

Necessário asseverar que o consentimento deve ser o consentimento proposto pela LGPD, sendo importante principalmente a gestão desse consentimento, a transparência a finalidade, podendo ser dissociado o tratamento da informação em ERPs das demais operações (consentimento granulado), qual informação que não seja possível tal enquadramento, deve ser considerada como base não consentida.

O último filtro será segmentado entre as demais bases legais existentes nos 11 (onze) incisos do artigo 7 da LGPD. Os dados pessoais que compõem a classificação "sem consentimento LGPD" devem receber tratamento individualizado para nova classificação.

Nesse ponto, o trabalho de conformidade será desenhado conforme o fluxograma remanescente, implicando em diversas hipóteses, como por exemplo, dados tratados no CRM (marketing) que não receberam consentimento LGPD, podem ser classificados em legitimo interesse mediante exercício de balanceamento de interesses (campanha publicitária adequada a expectativa do usuário), ou deverão ser excluídos do tratamento no CRM, mas mantidos para exercício regular de direito (registro de emissões de notas fiscais, envio de dados para transportadoras, à título de exemplo).

Também, como exemplo, aquelas informações armazenadas no ERP de uma operação dentro do período prescricional, podem ser armazenadas e mantidas sob à proteção do cumprimento de obrigação legal, em decorrência de obrigações fiscais, ou ainda, tornar os dados anonimizados por tecnologias específicas a fim de tratar a informação, o que encontraria guarida tanto na possibilidade de anonimização quanto na manutenção da informação por segredo comercial.

Ou seja, o tratamento de informações legadas a vigência da LGPD é casuístico e depende sobretudo da realização das duas primeiras filtragens propostas, a fim de se encontrar a base legal (art. 7º) adequada a cada momento da operação e do ciclo de vida dos dados pessoais dentro da operação de cada agente de tratamento.

O resultado das três camadas (Inadequados – aqueles manifestamente indevidos, com descriminações de indivíduos ou sem origem lícita, como bases compradas; Consentidos – em plena conformidade com os critérios de consentimento da LGPD; Outras Bases Legais – outras hipóteses de adequação, como cumprimento de obrigação legal, legitimo interesse, saúde e etc.) será um dado pessoal precário que poderá ter três destinações, sua exclusão permanente, sem qualquer hipótese de restauração, seu reengajamento por meio de *aproaching* comercial, com medidas a fim de se obter consentimento, e ainda a anonimização da informação, com todos os requisitos técnicos necessários para essa forma de tratamento.

Essa alternativa (mapeamento e aplicação dos filtros propostos) visa não apenas à adequação dos agentes de tratamentos de dados pessoais, mas também evitar o trabalho com o reengajamento descomedido de toda a base de dados. Isso, pois, o reengajamento ocorrerá de forma mais precisa e adequada, podendo gerar maiores proveitos comerciais do que um simples disparo de *SMS* ou *e-mails marketing* sem qualquer critério.

Conclusão

A convalidação da base legada não deve limitar o tratamento dos dados existentes e a capacidade operacional de prestação dos serviços prestados pelos agentes de tratamento, isso, pois, mediante cada tratamento é possível empregar base legal distinta e prevista no artigo 7º da Lei.

Para aplicação das bases legais do artigo 7º da LGPD é mandatório o mapeamento de dados pessoais e seu *tracking*, além de recomendável política de níveis de acesso da informação, medidas que permitem compatibilizar a informação coletada e seu tratamento em relação a operação da empresa.

Dessa forma, independentemente da alternativa de tratamento das bases legadas (exclusão ou adequação), o que deve ser realizado como essencial e primordial é o inventário desse ativo, mediante a criação de mapeamento personalizado as necessidades do negócio.

Ressalta-se que a regulamentação da ANPD pode não vir a ocorrer a tempo da vigência da LGPD, o que tornará a base legada a mercê da interpretação judicial e dos órgãos de regulamentação e de proteção ao consumidor, que apenas terão como base os princípios, fundamentos e prescrições normativas da própria LGPD, sem qualquer análise crítica das necessidades de cada negócio.

A proposta de trabalho desse Resumo objetiva resolver problema natimorto, pois o destino da informação legada será ao longo da vigência da norma amplamente absorvido pelas novas ferramentas e adequações aplicadas pelos agentes de mercado, como softwares e programas de implementação.

A proposta do *privacy by design* e *privacy by default*, visam, sobretudo, eliminar intercorrências do novo sistema protetivo da informação pessoal. Essa realidade inaugura um novo *mind set* operacional, sendo certo, que, independentemente de regulamentação, a informação legada merece um destino apropriado, tanto pela memória que representa, como a efetivação do primeiro grande passo de rompimento de um mundo analógico que nossa realidade disruptiva já não permite mais.

Referências bibliográficas

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 out. 2019.

CHRISTENSEN, Clayton M. **O dilema da inovação:** quando as novas tecnologias levam empresas ao fracasso. São Paulo: M.Books do Brasil, 2012

MALDONADO. Viviane Nóbrega; BLUM, Renato Ópice. **LGPD – Lei Geral de Proteção de Dados Comentada.** São Paulo: Revista dos Tribunais, 2019.

MALDONADO. Viviane Nóbrega. **Advocacia 4.0.** São Paulo: Revista dos Tribunais, 2019.

<https://econsultancy.com/why-did-jd-wetherspoon-delete-its-social-media-accounts-andwas-it-the-right-marketing-decision/>

5.2. Autoridade Nacional e sua efetividade na preservação da privacidade – *Bárbara de Sordi Faria*[117] *& Iara Pereira Ribeiro*[118]

Resumo

Pretende-se apresentar aspectos da Autoridade Nacional de Proteção de Dados Pessoais, bem como sua importância na preservação do direito fundamental da privacidade diante a sociedade da informação, além da sua potencial efetividade a partir da vigência da Lei Geral de Proteção de Dados Pessoais.

Palavras-chave: Autoridade Nacional; proteção de dados pessoais; privacidade.

Abstract

It's intended to present aspects of the National Authority of Personal Data Protection, as well as its importance in the preservation of the fundamental right of privacy before the information society and its potential effectiveness from the validity of the General Law of Personal Data Protection.

Keywords: National Authority. Protection of personal data. Privacy.

Introdução

No Brasil a Autoridade Nacional de Proteção de dados pessoais (ANPD) foi criada e instituída pela Lei n° 13.853 de 8 de julho de 2019, que alterou a Lei Geral de Proteção de Dados Pessoais (LGPD- Lei nº 13.709 de 14 de agosto de 2018), esta Autoridade surge para suprir a lacuna deixada pela LGPD, que apesar de fazer regulações a respeito da proteção de dados pessoais não criou uma Autoridade

[117] Especialista em Direito Civil pela Faculdade de Direito de Ribeirão Preto Universidade de São Paulo. E-mail: barbarasordi@adv.oabsp.org.

[118] Doutora em Direito Civil pela Pontifícia Universidade Católica de São Paulo. E-mail: iararibeiro@usp.br.

fiscalizadora naquela oportunidade, fato que gerou insegurança a respeito de sua efetividade, não obstante sua vigência ser a partir de agosto de 2020.

Assim, com a criação da ANPD cultiva-se perspectivas positivas em relação a efetiva proteção de dados em um momento importante, tendo em vista que o constante avanço tecnológico que alicerça a sociedade da informação traz inseguranças e coloca em evidência a possibilidade de exposição excessiva da privacidade.

Neste contexto o questionamento que impulsiona o presente artigo é: a ANPD será capaz de preservar a privacidade plenamente? O objetivo é apontar como poderá ser possível a concretização dessa potencialidade.

O assunto será abordado em três eixos interligados, inicialmente serão analisados alguns aspectos da ANPD, após haverá uma inserção no direito fundamental da privacidade e seus reflexos na sociedade da informação; e, por fim analise de alguns desafios a serem enfrentados pela ANPD para efetiva proteção de dados pessoais face amplitude da tecnologia.

1. Autoridade Nacional de Proteção de Dados Pessoais

A ANPD é órgão da administração pública federal integrante da Presidência da República, sendo responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, sendo, portanto, o órgão que terá importante participação na proteção de dados pessoais e preservação da privacidade.

Entre as competências da ANPD está a de receber reclamação, que não for previamente resolvida pelo controlador no prazo legal, bem como providenciar meios para registro da mesma de forma simplificada inclusive por meio eletrônico, fato que demonstra que a população poderá auxiliar a Autoridade na realização de seus trabalhos.

Ocorre que também há autorização na legislação para que a análise da reclamação ocorra de forma agregada e que as providências sejam tomadas de forma padronizada, situação que tem grande potencial para afetar a privacidade dos indivíduos.

Além das competências acima citadas a ANPD terá importante participação no auxílio à interpretação à nova legislação de proteção de dados pessoais, devendo atuar de forma transparente para que os indivíduos possam confiar em seus trabalhos.

Portanto, as expectativas a respeito da atuação da ANPD são grandes, ocorre que a ANPD estará vinculada ao Poder Executivo, o que a deixa distante do ideal fiscalizatório, conforme demonstra a experiência internacional (América Latina em países com legislações mais próximas da brasileira) ser importante à desvinculação de Autoridades do Poder Executivo, tendo em vista o conflito evidente de

interesses, vez que o Poder Executivo será fiscalizado por seu próprio órgão podendo haver influência até mesmo política (SIMÃO; OMS; TORRES, 2019, p. 36).

Ademais, a LGPD adota a interação internacional de dados pessoais, o que permite a transferência de dados para países estrangeiros ou organismo internacional ao qual o Brasil seja membro, respeitados alguns requisitos, de modo que a recente criação da ANPD demonstra que o país está se adequando à nova ordem mundial, sem que ocorra violação ou relativização de direitos ou garantias fundamentais (PINHEIRO, 2018, p. 92).

No entanto, apesar do ambiente digital ser internacional, a soberania de cada nação deve ser respeitada, e não obstante a criação da ANPD é importante para que o Brasil seja qualificado pelo Comitê Europeu para a Proteção de Dados (CEPD), como um país apto a realizar e receber transferências de dados com segurança.

2. Privacidade na sociedade da informação

A sociedade da informatização estruturada pela tecnologia, e impulsionada pela internet, proporciona novos meios de tratar dados e obter dados desejados, o que tem potencial para afetar diretamente à privacidade.

A internet sendo uma rede mundial de indivíduos que interliga diferentes culturas (PINHEIRO, 2016, p. 47), possui importante impacto na sociedade. No Brasil, a internet já atingia em 2018 70% da população, ou seja, 126,9 milhões de pessoas, conforme pesquisa TIC Domicílios 2018, divulgada pelo Comitê Gestor da Internet no Brasil (CGI.br).

Aliás, a internet associada a outras tecnologias pode levar a discriminação e lesar a privacidade, a exemplo da utilização de inteligência artificial que tem como "[...] objetivo principal o estudo e a construção de sistemas capazes de exibir comportamentos normalmente associados às pessoas, como aprendizado e resolução de problemas" (BIGONHA, 2019), para tratamento de dados em *big data* (grande volume de dados não estruturados). “Essa tecnologia permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades” (BIONI, 2019, p. 37).

Não obstante aos benefícios que inegavelmente a tecnologia traz a população, a mesma encontra um entrave na privacidade, caracterizando um trade-off (expressão utilizada por Laura Schertel Mendes), consistente na necessidade de uma escolha em detrimento a outra (MENDES, 2014, p. 34).

A privacidade (advindo do termo americano *right to privacy*), prevista expressamente na LGPD, tendo sua proteção entre seus objetivos, e sendo ainda um de seus fundamentos, juntamente com o livre desenvolvimento da personalidade dentre outros, é uma novidade, tendo em vista que até então o termo

não era utilizado, vez que apenas o termo vida privada está previsto na Constituição Federal de 1988, em seu artigo 5º, inciso X.

Neste contexto e compreendendo a privacidade como um dos desdobramentos da personalidade esta acompanhará o indivíduo durante toda a sua existência, apenas cessando com a morte (PEREIRA, 2018, p. 178), e por ser definidora da essência do indivíduo é intransmissível e irrenunciável, conforme estabelecido no artigo 11, do Código Civil de 2002.

Pelo exposto, evidencia-se que a privacidade contém reflexos da personalidade, portanto os dados pessoais que revelam comportamentos, preferências, hábitos de consumo, devem ser protegidos mesmo diante da sociedade da informação.

Aliás, a privacidade, no que tange aos dados pessoais, está ligada a autodeterminação do indivíduo, sendo que apenas será protegida se o indivíduo puder determinar a maneira da coleta e da utilização de seus próprios dados, lhe pertencendo à faculdade de restringir o acesso a suas informações, decidindo quem terá ou não acesso a determinadas informações; estabelecendo limites entre o interesse público e o interesse privado, aqui evidenciando a importância da ANPD em assegurar estes direitos.

A proteção e preservação da privacidade também é uma preocupação que afeta a União Europeia, tanto que foi criada a Agência dos Direitos Fundamentais (FRA), organismo independente que presta assistência no que tange direitos fundamentais às instituições e aos Estados Membros, tendo atualmente entre seus temas a sociedade da informação e, em especial, o respeito pela vida privada (privacidade) e a proteção dos dados pessoais (UNIÃO EUROPEIA, 2019a).

Portanto, a Autoridade Nacional terá a difícil tarefa de preservar a privacidade, a fim de evitar a violação dos direitos fundamentais, mantendo o equilíbrio entre o digital/tecnológico, privacidade e interesse público e social.

3. Proteção de dados pessoais

A União Europeia, ao estabelecer o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR) nº 679, aprovado em 27 de abril de 2016, cuja aplicação de penalidade se iniciou em 25 de maio de 2018, incentivou os outros países a adequarem suas legislações, a fim de evitarem entraves comerciais e negociais, criando um movimento mundial de adequação da legislação em relação à proteção de dados pessoais.

A GDPR surge com o objetivo de proteger os dados pessoais dos indivíduos nos seus respectivos tratamentos e sua livre circulação, conhecido pela expressão free data flow (PINHEIRO, 2018, p.18), definido os dados pessoais como sendo a "informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar

à identificação de uma determinada pessoa". (UNIÃO EUROPEIA, 2019b), no mesmo sentido é a definição apresentada pela legislação brasileira, no seu artigo 5º, inciso I.

Tendo em vista a amplitude que os dados podem atingir mundialmente, e a consequente necessidade de adequação às peculiaridades da sociedade da informação, o direito a proteção de dados pessoais está sendo abordado na legislação de diversos países, conforme levantamento realizado "*National Comprehensive Data Protection/Privacy Laws and Bills 2019*" já há mais de 120 países espalhados por todo o mundo que adotam leis abrangentes de proteção à privacidade de dados pessoais mantidos por órgãos públicos e privados, além de outros quase 40 países que têm projetos ou iniciativas pendentes (BANISAR, 2019).

Portanto é de suma importância à proteção de dados pessoais, para evitar a exposição da privacidade, sendo certo que a proteção não é exclusiva do Brasil, pois é garantido em diversos países (PINHEIRO, 2018, p. 19).

No Brasil, apesar da Lei 13.709/2018 regular a proteção de dados pessoais, ainda faltava a criação da Autoridade fiscalizadora, que ocorreu apenas com a Lei 13.853/2019.

Assim, os dados pessoais identificam e representam o indivíduo na sociedade, quando este não pode estar presente, neste sentido: "Os dados pessoais acabam por identificar ou mesmo representar a pessoa em uma série de circunstâncias nas quais a sua presença física não é possível ou conveniente." (DONEDA, 2014, p. 61).

Desse modo, tudo que identifica um indivíduo em sua essencialidade é considerado dado pessoal, mesmo que de forma remota, devendo ser protegido, a fim de que sua exposição não cause prejuízos irreversíveis ao titular.

A possibilidade de utilização de dados pessoais de forma indevida, por meio de tratamentos inadequados e evasivos a privacidade gera a necessidade de proteção, sendo que ANPD terá um importante papel na efetivação desta mas para chegar ao resultado de proteção satisfatório terá que cultivar uma cultura da privacidade, juntamente com a população, setor público e setor privado, principalmente por meio de *compliance*.

Conclusão

Ressalta-se que a criação da ANPD é um importante passo na concretização da proteção de dados pessoais e consequentemente da privacidade e gera expectativas neste sentido, proporcionando inclusive a possibilidade de qualificação no CEPD.

No entanto, a ANPD terá grandes desafios para fiscalizar de forma satisfatória, as relações digitais que envolvem o tratamento de dados pessoais e suas implicações no direito fundamental da privacidade, tendo em vista o constante avanço da tecnologia.

Deduz-se que a denúncia de utilização indevida de dados através de reclamação pelo próprio titular dos dados será de suma importância para que a ANPD possa realizar seus trabalhos, demonstrado a importância do indivíduo na efetiva proteção de seus dados, sem excluir a necessidade de um trabalho integrado entre população, setor público e setor privado para o estabelecimento de uma cultura da privacidade.

A ANPD tem potencial para proteger e preservar o direito fundamental da privacidade, mesmo diante da sociedade da informação, mas para tanto deverá agir de forma transparente para que os indivíduos possam confiar em seu trabalho e auxiliá-la em sua efetivação, criando expectativa neste sentido.

Referências bibliográficas

BANISAR, David. National Comprehensive Data Protection/Privacy Laws and Bills 2019. **Article 19**: Global Campaign for Free Expression, 01 ago. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416. Acesso em: 05 out. 2019.

BIGONHA, Carolina. Inteligência Artificial em perspectiva. **Panorama setorial da Internet.** Out. 2018. Disponível em: https://nic.br/media/docs/publicacoes/1/Panorama_outubro_2018_online.pdf. Acesso em: 05 out. 2019.

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

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. **Diário Oficial da União**, Brasília, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 05 out. 2019.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 05 out. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 05 out. 2019.

DONEDA, Danilo. O Direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães (Coord.). **Direito privado e internet.** 1ª. ed. São Paulo: Atlas, 2014.

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

PEREIRA, Caio Mário da Silva. **Instituições de direito civil:** Introdução ao Direito Civil, Teoria Geral de Direito Civil. 31ª. ed. rev. e atual. por Maria Celina Bodin de Moraes. Rio de Janeiro: Forense, 2018, v.1.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

PINHEIRO, Patricia Peck. **#Direito Digital.** 6ª. ed. rev. ampl. e atual. São Paulo: Saraiva, 2016.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. Autoridades de Proteção de dados na América Latina: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. **Instituto Brasileiro de Defesa do Consumidor.** 03 mai. 2019. Disponível em: https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina. Acesso em: 05 out. 2019.

UNIÃO EUROPEIA. Agência dos Direitos Fundamentais da União Europeia. **Apresentação da FRA.** Disponível em: https://fra.europa.eu/pt. Acesso em: 05 out. 2019a.

UNIÃO EUROPEIA. Comissão Europeia. **O que são dados pessoais?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 05 out. 2019b.

UNIÃO 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia.** Disponível em: https://eur-lex.europa.eu/legal content/PT/TXT/?uri=celex:32016R0679. Acesso em: 05 out. 2019c.

Capítulo 6

6. Utilização econômica dos dados pessoais: os limites e as tendências face a monetização dos dados pessoais

6.1. Fluxo informacional e autodeterminação informativa: o dilema do consentimento informado – *Afonso Fratti Penna Rispoli*[119] & *Hebert Fabrício Tortorelli Quadrado*[120]

Resumo

O presente artigo objetiva analisar a autodeterminação informativa – e o consequente dilema do consentimento informado - no âmbito da arquitetura da rede (mercado informacional), caracterizada pela relação assimétrica entre os atores envolvidos, pautada na hipervulnerabilidade do titular dos dados

[119] Graduado em Direito pela FDRP/USP. Graduando em Ciências Contábeis pela FIPECAFI. Membro do Grupo de Pesquisa "Observatório do Marco Civil da Internet no Brasil" na FDRP/USP, sob coordenação da Profa. Dra. Cíntia Rosa Pereira de Lima. Advogado. E-mail: rispoli.adv@gmail.com

[120] Aluno especial do Programa de Mestrado em Direito pela FDRP/USP. Pós-graduado em "Direito Civil - Novos Paradigmas Hermenêuticos nas Relações Privadas" pela FDRP/USP. Pós-graduado em Processo Civil pela PUC/SP. Membro do Grupo de Pesquisa "Observatório do Marco Civil da Internet no Brasil" na FDRP/USP, sob coordenação da Profa. Dra. Cíntia Rosa Pereira de Lima. Advogado. E- mail: hebertquadrado@hotmail.com

pessoais e nas falhas da contratualização dos mecanismos de segurança (políticas de privacidade). Nesse contexto, o estudo tem como base uma comparação entre a Diretiva de Proteção de Dados Pessoais (95/46/CE), o Regulamento Geral de Proteção de Dados da União Europeia (2016/679), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Nesse contexto, a autodeterminação informativa será estudada considerando seu conceito, natureza jurídica e os princípios da teoria geral de proteção de dados que a norteiam.

Palavras-chave: autodeterminação informativa; consentimento informado; proteção de dados pessoais.

Abstract

This article aims to analyze informative self-determination - and the consequent dilemma of informed consent - within the network architecture (informational market), characterized by the asymmetrical relationship between the actors involved, based on the hypervulnerability of the personal data holder and the failures of the contractualisation security mechanisms (privacy policies). In this context, informative self-determination will be studied considering its concept, legal nature and its principles of the general theory of data protection that guide it.

Keywords: Information self-determination. Informed consent. Personal Data Protection.

Introdução

Não é incomum receber propostas de ofertas em formato publicitário de um supermercado enquanto se percorre as suas fileiras de produtos, estrategicamente dispostas conforme ensina o marketing de varejo. Talvez seja desejável, oportuno até, pois facilita ou torna mais confortável e à mão estabelecer comparativos de preços entre as empresas concorrentes. Mas, como o aplicativo instalado no dispositivo *Android* ou *IOS* sabe que o usuário (do aparelho) está no interior do supermercado?

Ofertas em formato de "notificações", "seleções de hoje", "sugerido para você", ou espaços reservados para outras plataformas digitais de venda na modalidade *e-commerce* surgem aos borbotões. É ou não curioso que tais propostas coincidam exatamente com a cesta de bens de consumo e/ou prestações de serviço pesquisada recentemente pelo mesmo usuário?

Sucumbir às ofertas vinculadas aparentemente de forma aleatória e inofensiva entre as publicações de determinadas redes sociais tem se tornado regra, olvidando-se o consumidor de analisar de forma atenta - para indagar-se logo em seguida - acerca do propósito negocial de tais preferências induzidas, e, daí, da real finalidade dos forjados mecanismos facilitadores de busca.

Exsurgem tais questionamentos em momento oportuno, no qual despontam escoteiros diversos estudos acerca do paradigma normativo. Contudo, aqui será apresentada análise limitada à relação assimétrica

no mercado informacional de dados, caracterizada, por um lado, pela hipervulnerabilidade do titular dos dados pessoais – sendo estes considerados verdadeiras projeções de personalidade individual - e, por outro, pela arquitetura de rede dependente do livre trânsito de informações. A análise revela diversas falhas de contratualização (políticas de privacidade), ensejando situações que deverão ser objeto de normatização específica.

O objeto de estudo será decotado no uso secundário dos dados pessoais na era do Big Data, e na autodeterminação informativa dos cidadãos sobre seus próprios dados pessoais. Nesse sentido, analisa-se a viabilidade da privacidade contextual, proposta por Helen Nissenbaum[121] , consistente no dirigismo informacional pautado pelo sintagma *usable-friendly* (contexto + integridade = normas informacionais), distanciada portanto do dirigismo contratual, uma vez que a proteção contratual tem efeito *ex post* mediante a invalidação de cláusulas contratuais abusivas (BIONI, 2019, p. 210).

Constatada, portanto, a relevante valoração do fator consentimento perante a assimétrica relação entre o titular dos dados e os *players* presentes na estrutura da rede, bem como evidenciada a necessidade de um ambiente regulatório condizente com os oito princípios[122] insculpidos pela estruturas normativas vigentes, no qual (ambiente) se prime pela adoção e cotejamento de uma linguagem informacional (mediante intelecção do que é apropriado ou não, de acordo com o valor social e o contexto em que estão inseridas as informações pessoais - *usable-friendly*), o presente artigo tem por escopo a análise da problemática do paradigma da autodeterminação informativa enquanto inserida no contexto atual do desenvolvimento do mercado informacional.

1. Contextualização

Verifica-se que as tecnologias criadas ao longo dos últimos anos, notadamente a internet, provocaram intensa revolução social, repercutindo, inclusive, na esfera privada das pessoas[123]. Toda essa conectividade e tecnologia têm, contudo, um preço. Isso porque demanda para o seu funcionamento um ininterrupto fluxo informacional, isto é, quantidades cada vez maiores de dados pessoais que deverão ser

[121] Professora lotada na Universidade de Nova Iorque, diretora do *Law Information Institute*. Para maiores informações: http://www.nyu.edu/projects/nissenbaum/main_bio.html.

[122] Limitação da coleta (*collection limitation principle*); qualidade dos dados (*data quality principle*); especificação dos propósitos (*purpose specification principle*); limitação do uso (*use limitation principle*); padrões mecanismos de segurança (*security safeguards principle)*; abertura (*openness principle*); participação individual (*Individual participation principle*); responsabilidade (*accountability principle*).

[123] "Cabe ao direito a tarefa de zelar pelo melhor interesse da sociedade de forma global, à mercê, muitas vezes de vontades individuais que não consideram a generalidade das circunstâncias envolvidas" (PICCELLI, 2018, p. 114).

coletados, tratados, transferidos e compartilhados, supostamente para única e imediata satisfação dos interesses do usuário.

Tal prática se perfaz sem que os titulares dos dados pessoais ao menos percebam o valor monetário agregado ou potencialmente agregável às informações coletadas, muito menos tenham consciência dos perigos decorrentes de potenciais vazamentos ou, ainda, de seu uso/aplicação indevidos.

Indo além, e só à título exemplificativo, a ânsia consumerista que incita as ilimitadas e desenfreadas tentativas de obtenção de crédito esbarra, necessariamente, na análise prévia pelas instituições financeiras. Estas, por seu turno, a condicionam ao amplo, irrestrito e inadvertido fornecimento de dados pessoais, que serão tratados e transferidos para instituições que gerenciam bancos de dados com escopo único de qualificar os usuários ("bons pagadores" ou, por outro giro, como inadimplentes).

Esse risco, concretizado na possibilidade de exposição e utilização indevida dos dados (DONEDA, 2019, p. 35), especialmente durante a vigência dos novos negócios jurídicos celebrados sob a égide da Sociedade da Informação, ensejou a criação de complexas estruturas normativas voltadas exclusivamente à proteção do titular dos dados, de forma a possibilitar o efetivo exercício de preservação de sua intimidade[124] e da própria privacidade[125] , bem como o direito de não ser lembrado por determinados fatos ocorridos em sua vida (autodeterminação informacional).

Os dados pessoais[126], considerados como o mais novo e precioso ativo econômico, com vasto mercado negocial e de ampla gama de aplicações, foi erigido à categoria de direito da personalidade. Inclusive, se aprovada a proposta de emenda à Constituição nº 17, de 2019, passará a ser direito fundamental[127], o que torna indispensável a análise aprofundada acerca de sua amplitude e dos impactos sociais e jurídicos decorrentes de seu uso, ainda que consentido.

[124] Artigo 7, Lei nº. 12.965/2014. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação.

[125] "Estudos demonstram que nem sempre as pessoas são capazes de administrar adequadamente a sua própria privacidade. Em amostra colhida por Acquisti e Grosslags, nada menos que 89,2% das pessoas inquiridas afirmaram preocupação moderada ou alta com a privacidade e 73,1% responderam faltar privacidade na sociedade contemporânea (PICELLI, 2018, p. 115).

[126] "A primeira diferenciação que deve ser estabelecida é exatamente a entre dado e informação. Embora sejam ocasionalmente tratados como equivalentes, os 'dados' constituem matéria-prima e 'informação', os dados processados, ou seja, o conjunto de dados relevantes a que se atribui um significado determinado" (SANTOS, 2008, p. 357).

[127] A proposta de emenda à Constituição, se aprovada da forma como proposta, acrescenta o inciso XII-A ao artigo 5º, e o inciso XXX, ao artigo 22, ambos da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixa a competência privativa da União para legislar sobre a matéria.

Nesse âmbito, o paradigma normativo da autodeterminação informacional faz surgir a discussão acadêmica a respeito do efetivo dilema do consentimento informado nas relações de contratualização em rede, até porque os dados podem vir a possuir expressivo vínculo objetivo com o usuário a ponto de revelar algo a seu respeito (DONEDA, 2019, p. 36), sobretudo se o dado for objeto de anonimização imperfeita ou insuficiente.

Desponta relevante compreender que a proteção dos dados pessoais é, na verdade, o direito de um indivíduo autodeterminar as próprias informações pessoais, coletáveis, processáveis e transmissíveis mediante consentimento destacado, específico e informado. Exatamente por conta disto, o consentimento do titular dos dados pessoais foi erigido, observando-se a técnica legislativa, como um pilar normativo (BIONI, 2016, p. 19).

Outro conceito importante é o da autodeterminação informacional, considerada como a "faculdade de o particular determinar e controlar a utilização de seus dados pessoais" (CANOTILHO, 2000, p. 507). O consentimento, por seu giro, pode ser definido como uma "condição para o acesso aos dados" (PICELLI, 2018, p. 120).

Feitos tais esclarecimentos, a normativa europeia a respeito da proteção de dados, vista como norte referencial, pressupõe que a privacidade e, portanto, os dados pessoais, se revelam sob a forma de direito fundamental, impedindo que sejam objeto de regulação única e exclusivamente pela dinâmica do mercado informacional - ou setorial, no modelo norte americano (CHAVES, 2011, p. 104/105).

O regramento europeu, notavelmente mais protecionista, estabeleceu um padrão de segurança que impele a sua adoção por todos os países que tenham a pretensão de acessar, coletar ou, ainda, transmitir os dados pessoais de cidadãos europeus. Trata-se do Regulamento Geral de Proteção de Dados na União Europeia (GDPR)[128], que acabou por codificar a jurisprudência do Tribunal de Justiça da União Europeia (TJUE) em relação à interpretação da Diretiva 95/46.

Merecem, nesse ponto, breve destaque as quatro gerações de leis voltadas à proteção dos dados pessoais. Verifica-se nos idos da formação do Estado Moderno um interesse governamental peculiar, consistente na percepção de que havia nas informações pessoais extraídas de seus cidadãos uma potencialidade não

[128] 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 e que revogou a Diretiva 95/46/CE. Em termos práticos, representa um avanço na proteção de dados, em especial: regula a forma e as condições do consentimento dos titulares dos dados, quando é condição de licitude do tratamento; estabelece novas exigências quanto aos dados sensíveis, que passam a abranger os dados biométricos, em especial a exigência de designação de um encarregado de proteção de dados; impõe obrigações de documentação e registro de atividades de tratamento, incluindo quanto efetuadas por subcontratantes, etc.

explorada, sobretudo no que tange ao planejamento e à coordenação das ações sociais (BIONI, 2019, p. 113).

Evidenciado o processamento massivo dos dados pessoais pelas entidades estatais, e apurada a necessidade de uma estrutura regulatória, visto pairar por sobre a liberdade do cidadão a temível sombra do "Grande Irmão", foram criados mecanismos de controle, consistentes em concessões de autorização para o funcionamento dos bancos de dados estatais.

Contudo, a primeira geração normativa de proteção de dados, voltada tão-somente à regulação dos bancos de dados estatais, sucumbiu ao processamento de dados também por atores da esfera privada ("Pequenos Irmãos"). Inviabilizada a regulação pelo Estado de todos os bancos de dados (públicos e privados), foi adotada nova estratégia normativa (segunda geração), consistente na transferência, para o titular dos dados, da responsabilidade de protege-los (BIONI, 2019, p. 115).

Em outras palavras, o fluxo informacional de dados, antes autorizado pelo Estado, agora estava sob a ingerência do seu próprio titular, à mercê de seu consentimento, limitada entretanto à decisão de autorizar - ou não - o processamento. É, portanto, na segunda geração que se encontra o embrião que vincula os dados pessoais ao direito à autonomia da própria privacidade.

O protagonismo do titular dos dados ganha real amplitude apenas na terceira geração normativa, quando aquele (titular) se depara envolvido com todo o processo de processamento de dados (coleta, armazenamento e transmissão), desenhando diretrizes mais marcantes para o sintagma "autodeterminação informacional", além de inovar na criação de deveres específicos para quem coleta e processa os dados pessoais.

Caso emblemático e inaugural da autodeterminação informacional, a lei do censo populacional alemão de 1982 (*Volkszählungsurteil*) consistia na coleta dos dados pessoais no censo e ulterior utilização na formação de perfis, de modo a permitir a identificação de cidadãos e emprego de tais dados para finalidades secundárias, *v.g.*, as autoridades locais poderiam efetuar correções nos cadastros de moradores dos municípios (CHAVES, 2011, p. 104).

Instaurado um sentimento de insegurança generalizado, muito por conta do método de coleta das informações e da sua destinação, sobreveio a decisão do Tribunal Constitucional Federal, de 25 de dezembro de 1983, que julgou parcialmente inconstitucional a referida lei, ao manter sua finalidade estatística, mas extirpando a transferência de dados obtidos no recenseamento do governo federal para autoridades locais, visto que evidenciada a inconstitucionalidade. A referida sentença, pela primeira vez, fez menção ao termo autodeterminação informativa (CHAVES, 2011, p. 104).

Esse deslocamento de poder decisório (Estado para titular dos dados) se revelou, todavia, contrário ao próprio desenvolvimento das relações sociais. Isto porque a autonomia do consentimento suprimiu o fluxo informacional que servia de instrumento para o pleno exercício da cidadania ou, como bem colocado por Doneda (DONEDA, 2019, p. 35), para caminhar com autonomia nos corredores da Sociedade da Informação. A plena autonomia, destarte, carecia de cirúrgico ajuste para o sadio fomento das políticas sociais.

Sobreveio, para tanto, a quarta geração, estruturada por autoridades independentes para adequada aplicação das disposições normativas voltadas à proteção dos dados pessoais. Note-se que ainda se mantém o protagonismo do titular dos dados pessoais. Nessa fase, o consentimento passou a ser adjetivado (devendo ser livre, informado, inequívoco, explícito e/ou específico), seguindo os passos do direito comunitário europeu e se confirmando até os dias atuais, como norte para novas legislações sobre o assunto (BIONI, 2019, p. 116/117).

2. O dilema do consentimento

O consentimento do usuário para o tratamento de seus dados pessoais constitui o cerne da discussão da disciplina da proteção de dados pessoais, pois pondera o consentimento, estrutura e delimita a autonomia da vontade e os direito fundamentais, o que acaba por ajustar os efeitos deste consentimento à natureza dos interesses em questão (DONEDA, 2006, p. 371), visto que expressão direta de sua própria personalidade (DONEDA, 2019, p. 35).

Dessa forma, considerando a evolução tecnológica, o consentimento há de ser interpretado como um instrumento de manifestação da escolha individual, fazendo referência direta a valores fundamentais. Assim, permite a reflexão sobre questões como privacidade e imagem, identidade pessoal, disposições sobre o próprio corpo, etc (DONEDA, 2006, p. 371).

A natureza jurídica do consentimento na autodeterminação informacional flerta mais com a área de direito da personalidade do que efetivamente com a estrutura contratual, em que pese ter indireta vinculação com esta última. Na verdade, o consentimento pode ser analisado sob duas dimensões ou óticas, quais sejam, a) o consentimento como instrumento por excelência para a autodeterminação informacional e, portanto um aspecto relacionado a tutela pessoal; e, b) o consentimento como instrumento de legitimação para que os dados pessoais sejam parcialmente tratados por terceiros (DONEDA, 2006, p. 378).

Diante desse panorama, encontra-se justificado que o consentimento não possui natureza de negócio jurídico, porquanto não pode ser dito que há uma vantagem para aquele que permite o tratamento de seus dados pessoais e o tratamento dos dados propriamente dito (DONEDA, 2006, p. 379).

Em tempo, também não pode deixar de ser observado que o consentimento para tratamento de dados pessoais é norteado por dois princípios: princípio da finalidade e da informação. O princípio da finalidade[129], que completa a disciplina do consentimento restringindo a generalidade (o consentimento para o tratamento de dados deve ser interpretado restritivamente em relação a sua finalidade), em apertada síntese permite, em última análise, que o titular mantenha o controle de suas próprias informações[130] (DONEDA, 2006, p. 383).

Decorrente do acima mencionado, o princípio da informação permite ao usuário que este tenha consciência tanto da coleta e do armazenamento de seus dados pessoais, bem como que seja informado detalhadamente acerca da destinação dos mesmos dados. Mais: deverá ser informado acerca da finalidade e da duração do tratamento, assim como da pretendida transmissão dos referidos dados para terceiros. Isto sem descurar do direito de franco acesso a toda e qualquer informação que seja útil no caso concreto, permitindo que o titular (ora interessado) possa formar sua convicção (DONEDA, 2006, p. 383).

Outrossim, destaca-se que o consentimento do titular dos dados pessoais no sentido de permitir o seu tratamento, por si só, não extirpa, *ad eternum*, o poder de controle sobre eles [dados]. De fato, a relação jurídica existente entre o responsável pela coleta e tratamento dos dados pessoais e o usuário titular deles perdura enquanto os dados estiverem sob a guarda e/ou sob tratamento daquele (LIMA, 2015, p. 250).

Em tempo, não se pode deixar de examinar, ainda que superficialmente, o conceito de base de dados ou banco de dados[131], devido a íntima conexão com o tema tratado. É possível inferir que as bases de dados são uma compilação de dados, de obras ou, ainda, de outros materiais, organizados e ordenados sistematicamente sob critérios com finalidade específica, que permitam o acesso individual a esses dados, por meio eletrônico ou não (SANTOS, 2005, p. 321/322).

3. O consentimento nos modelos legislativos

[129] "Os dados não podem ser utilizados de forma incompatível com a finalidade para que foram obtidos. Essa regra também é denominada de 'princípio da limitação do uso'. (SANTOS, 2008, p. 363).

[130] "Nessa perspectiva, não seria possível o consentimento genérico para tratamento de dados pessoais, porém somente quando é especificada sua finalidade, bem como não seria cabível sua interpretação extensiva para hipóteses fora das expressamente previstas" (DONEDA, 2006, p. 383).

[131] "Em geral, os termos bases de dados e banco de dados são usados como sinônimos, ainda que inicialmente se pretendesse estabelecer uma distinção entre ambos, reservando o termo base de dados para aquelas que são acessadas por computador. No uso corrente, bases de dados eletrônicas são justamente aquelas disponibilizadas através dos meios eletrônicos (SANTOS, 2005, p. 322).

A Organização para a Cooperação e Desenvolvimento Econômico - OCDE[132] foi responsável pela elaboração de dois documentos, denominados de *privacy guidelines* (1980) e de *declaration on transborder data flows* (1985)[133]. Tais documentos podem ser tratados como legítimos princípios-motores normativos da proteção de dados, pois visavam justamente a transferência de dados entre os países signatários do acordo internacional multilateral.

Antes de tratar definitivamente do RGPD, pondera-se sobre o consentimento no âmbito da Diretiva 95/46/CE; previsto no artigo 2º, alínea "h", é entendido como qualquer manifestação de vontade livre, específica e informada, pela qual a pessoa aceita que seus dados pessoais sejam tratados. À época, resumiam-se a apenas três adjetivações ao consentimento, isto é, três requisitos determinantes para a sua validade, quais sejam, que este fosse livre, específico e informado.

Com o advento do RGPD, o consentimento passou a ser definido no artigo 4º, "11", exigindo-se que o consentimento fosse uma manifestação igualmente explícita, externável mediante declaração ou ato positivo inequívoco.

No artigo 7º foram impostas diversas condições como forma de tangibilizar a adjetivação do consentimento, despontando como princípio cardeal o da especificação dos propósitos (BIONI, 2019, p.238), conforme já visto. Com efeito, quando o usuário consentir com o tratamento de seus dados pessoais, deve fazê-lo assentindo de forma expressa, determinada e específica, carreando o ônus da demonstração da necessidade do tratamento ao player que se dispôs a processar os específicos dados para realização ou execução de determinado contrato. Nos casos em que a permissão se aperfeiçoe na modalidade escrita, exige-se ainda que o consentimento figure em cláusula ou condição destacada das demais, ficando garantida ainda a revogação da autorização a qualquer tempo.

Em relação a crianças, o artigo 8º. determina que os dados só poderão ser tratados mediante autorização dos pais ou dos responsáveis legais; quando maior de 16 anos, a autorização será expressa por seu respectivo titular, ressalvando-se que esta idade pode ser reduzida para 13 anos no direito interno dos países que compõem a União Europeia.

[132] "A OCDE é um organismo internacional multilateral criado após a Segunda Guerra Mundial, em 1948, cuja missão é promover o bem-estar econômico e social global. [...] Tem como objetivo estabelecer uma relação de cooperação entre seus países-membros para a solução de problemas comuns que os afligem" (BIONE, 2019, p. 118).

[133] Os documentos estabeleciam padrões normativos para a proteção de dados pessoais, permitindo o livre fluxo informacional entre seus países-membros. Dessas normas, decorreram direitos que complementariam a ideia de autodeterminação informacional, como o poder do usuário de retificar, emendar, apagar e/ou completar seus dados. (BIONI, 2019, p. 118/119).

Ainda, o RGPD apresenta hipóteses em que não poderá ocorrer o tratamento de dados pessoais, elencando-os no artigo 9º, "1". Tais casos estão relacionados aos dados pessoais sensíveis, pois podem revelar a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, ou, ainda, a filiação sindical. O mesmo tratamento proibitivo foi estendido aos dados genéticos e biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa.

Os casos acima mencionados admitem exceção; com efeito, os dados poderão ser tratados se o titular tiver manifestado seu consentimento para determinada finalidade específica; se estiver física ou legalmente incapacitado de dar o seu consentimento; por fim, por uma fundação, associação ou qualquer outro organismo sem finalidade lucrativa, com fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros ou a pessoas que com ele tenham mantido contatos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros, sempre no âmbito das suas atividades legítimas e mediante garantias adequadas.

No Brasil, a disciplina normativa teve início com o Marco Civil da Internet (MCI - Lei nº 12.965, de 23 de abril de 2014), o qual visou assegurar os direitos e garantias do cidadão no ambiente eletrônico, fundando-se, para tanto, sobre três pilares: a proteção à privacidade e dos dados pessoais, a neutralidade da rede e a liberdade de expressão (BIONI, 2019, p. 130).

O consentimento, previsto no artigo 7º, será livre, expresso e informado; o titular dos dados pessoais será obrigatoriamente informado sobre a coleta (justificada), uso, armazenamento, tratamento e proteção de seus dados pessoais. Se por escrito, o consentimento estará em cláusula destacada das demais e justificada sua necessidade, limitando-se a coleta à finalidade do uso da aplicação ou serviço.

Na sequência normativa, é promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709, de 14 de agosto de 2018[134]). Ainda em *vacatio legis*, o diploma apresenta um panorama geral, não apenas sobre o consentimento e autodeterminação informacional de forma expressa, mas sobre toda a matéria afeta à proteção dos dados pessoais.

Esse novo regramento normativo reflete, na verdade, alguns valores do regulamento europeu, exigindo-se que o consentimento seja uma manifestação livre, informada e inequívoca da vontade, pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, devendo ser feita por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Se por

[134] Com as alterações trazidas pela Lei nº 13.853, de 2019.

escrito, deverá constar de cláusula separada das demais e toda autorização genérica para tratamento de dados será considerada nula.

Anota-se que para que o consentimento seja tido como livre (adjetivo relacionado à ideia de livre-arbítrio), o titular deve avaliar o tratamento dos próprios dados inclusive sob o aspecto de sua potencial utilização (BIONI, 2019, p. 197).

Quando se fala em consentimento informado, o usuário deve dispor de informações no mínimo suficientes acerca da proposta de tratamento de seus dados, inclusive por quem será feito, a fim de que possa entender os liames obrigacionais presentes no contrato a ser celebrado para uma tomada consciente de decisão (BIONI, 2019, p. 191). Desta forma, as informações devem ser analisadas tanto sob o aspecto qualitativo, ou seja, mediante forma adequada e clara, bem como sob o aspecto quantitativo, isto é, se suficientes e, às derradeiras, sob o aspecto formal, devendo ser ostensiva (BIONI, 2019, p. 204).

Vale destacar que o consentimento inequívoco depende de manifestação por meio de uma ação afirmativa do titular dos dados pessoais, indicando sua aceitação com o tratamento e que não deixe dúvida sobre a intenção do usuário (BIONI, 2019, p. 199). Dessa forma, a interação do usuário, considerando grau e qualidade, serão determinantes para qualificar o consentimento como inequívoco (BIONI, 2019, p. 200).

Assim como no RGPD, o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, através de procedimento gratuito e facilitado. Assim sendo, todos os tratamentos de dados pessoais realizados no período de vigência do consentimento estarão ratificados.

Como pode ser demonstrado, todas as legislações nos levam a figura de um "cidadão-usuário" consciente do fluxo de seus dados pessoais e com o poder de controlá-lo por meio do consentimento. Tal perspectiva surge na coleta dos dados pessoais, no compartilhamento com terceiros, ou até deletando-os se assim o quiser (BIONI, 2019, p. 132).

Portanto, um dos maiores desafios suscitados pelo dilema do consentimento consiste, na verdade, na superação das limitações cognitivas dos cidadãos-usuários. Com efeito, reconhecida a condição de (hiper) vulnerabilidade dos titulares de dados pessoais, vez que inseridos em uma relação assimétrica no mercado informacional, ainda que existente proteção normativa neste sentido (*v.g.*, Código de Defesa do Consumidor), as pessoas naturais devem se adaptar à nova faceta no mercado dos negócios: a de seus próprios dados pessoais (BIONI, 2019, p. 166).

4. Da exteriorização do consentimento nos contratos de adesão eletrônico

O acesso a algumas páginas e aplicativos na internet está condicionado, de alguma forma, à aceitação dos termos e condições de uso, compartilhamento de informações do usuário e armazenamento e tratamento do seu histórico de navegação. Assim, se o usuário ou titular de dados expressa seu acordo acerca de tais mecanismos ou procedimentos de captura de dados (*cookies, beacons e pixels*), acaba por legitimar essa conduta (PICCELLI, 2018, p. 113). Desta forma, além das formas tradicionais de expressão da vontade, as declarações volitivas passam a também ser produzidas e/ou transmitidas eletronicamente (LIMA, 2009, p. 455).

Impende destacar que a manifestação do consentimento feita mediante adesão a contratos eletrônicos é evento extremamente comum. Em brevíssimas considerações, quando falamos em contratos de adesão eletrônicos, temos três figuras recorrentes: *shrink-wrap, clickwrap,* e *browse-wrap* (LIMA, 2009, p. 455/456).

a) Nos casos de *shrink-wrap*, o consentimento é manifestado por uma conduta - ação positiva (abrir o CD, instalar o programa de computador) e pelo silêncio (não devolução do produto pela discordância com as cláusulas contratuais);

b) Nos casos de *click-wrap*, o consentimento é manifestado através de expressões típicas como "eu concordo", "aceito", "sim" ou expressões correlatas. O importante é que o usuário tenha conhecimento prévio das cláusulas contratuais para poder decidir, conscientemente, evitando a racionalidade limitada[135];

c) Em relação ao *browse-wrap*, os termos e condições de uso são impostos por uma das partes e outra parte, condicionando a navegação pelo site à anuência irrestrita. Constata-se, contudo, verdadeira ausência de consentimento, o que importa em nulidade contratual.

Ainda e por fim, deve ser consignado que há outras formas eletrônicas de expressão do consentimento, como *e-mail* ou conversas em tempo real através de aplicativos (LIMA, 2009, p. 455).

Conclusão

[135] A teoria da racionalidade limitada, traduzida do termo inglês *bounded rationality*, apresentada por Maria da Conceição Pfeiffer, em singelas palavras, por fugir do escopo do presente trabalho, provém da teoria de economia comportamental, que visa entender e projetar os futuros comportamentos de todos os agentes de mercado, incluindo-se aqui os consumidores. Assim, racionalidade limitada do consumidor pode ocorrer quando este for efetivamente impossibilitado de fazer escolhas de modo racional, pelos seguintes motivos: a) falta de todas as informações úteis; b) dificuldade de reconhecer e selecionar o que é útil, como no caso de excesso de informação; c) no caso de veiculação parcial de informações (PFEIFFER, 2011, p. 23).

Após a promulgação do Marco Regulatório Civil da Internet Brasileira (Lei nº. 12.964/14), o legislador brasileiro se viu desamparado ante a complexificação, a dinamicidade e a sofisticação crescentes da estrutura da rede. Para não tatear às cegas, e após certa resistência, foi promulgada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais ou LGPD, com clara inspiração no Regulamento Geral de Proteção de Dados da União Europeia 2016/679 (RGPD). A nova disposição normativa estabelece uma série de regras às organizações (públicas ou privadas) atuantes no Brasil que deverão ser seguidas em relação à coleta, armazenamento e tratamento de dados pessoais. Em outras palavras, um verdadeiro manual de boas práticas deve ser redigido e adotado pelas sociedades inseridas no mercado informacional.

A despeito das gerações normativas em matéria de proteção de dados, o consentimento foi erigido a valor fundamental e central desse "sistema", pois, confere ao titular dos dados pessoais o direito e os instrumentos necessários para limitar e/ou impedir o tratamento de suas informações, ressalvadas, naturalmente, as hipóteses legais de dispensa.

Como visto, o consentimento do titular passou a ser adjetivado, em princípio espelhando a lídima manifestação livre, informada e inequívoca da vontade do usuário, direcionada a uma finalidade específica por escrito (desde que separada dos demais) ou por outro meio que demonstre a manifestação de vontade do titular, o que extirpa a possibilidade de usos secundários dos dados coletados. Quando envolver menores de idade, os dados somente poderão ser tratados com o consentimento dos pais ou responsáveis legais.

Se houver mudança de finalidade ou repasse de dados a terceiros, um novo consentimento deverá ser solicitado. Em caso de vazamento de dados, esse fato deverá ser comunicado às autoridades competentes, para que sejam tomadas as medidas civis e criminais necessárias, destacando nesse ponto a atuação da Autoridade Nacional de Proteção de Dados (ANPD), criada e disciplinada pela Medida Provisória MP nº 869/18.

Ainda, o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, através de procedimento gratuito e facilitado. Assim, como observado, as legislações convergem no sentido de existir o "cidadão-usuário" consciente do fluxo de seus dados pessoais e com o poder de controlá-lo por meio do consentimento.

Infere-se, do exposto, que as disposições normativas estabelecidas até o momento, notadamente com o advento da Lei Geral de Proteção de Dados e a criação da Autoridade Nacional de Proteção de Dados, já espelham diversos avanços relevantes: a um, no tocante ao desenvolvimento da consciência do cidadão-usuário, titular dos dados pessoais, no sentido de entender e, em seguida, exercer seu legítimo direito; a dois, no que se refere à necessária atualização e preparo da própria estrutura em rede que deverá

se adaptar a esta nova realidade de equilíbrio informacional; a três, a iminente necessidade dos *players* em se adaptar, conferir celeridade e transparência em todo o processo de gestão dos dados pessoais dos respectivos titulares, imprimindo em suas cláusulas boa-fé e transparência em seus atos e decisões; a quatro, a criação do binômio "finalidade *versus* utilidade social", consistente na importância de analisar a finalidade do dado pessoal coletado e o ambiente no qual está ou será inserido, exatamente para se perquirir a utilidade social decorrente da coleta, de forma a entender e aplicar o sintagma *usable-friendly* proposto por Helen Nissenbaum quanto ao dirigismo informacional.

Referências bibliográficas

BIONI, Bruno Ricardo. **Autodeterminação informacional:** Paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. 309f. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de São Paulo. São Paulo. 2016.

_____. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Seção 1, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 abr. 2019.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Seção 1, p. 59. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 abr. 2019.

_____. **Proposta de Emenda à Constituição nº 17, de 2019.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1773684&filenam e=PEC+17/2019. Acesso em: 01 abr. 2019.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição.** 5ª ed. Coimbra: Almedina, 2000.

CHAVES, Christian Frau Oliveira Obrador. A luta contra o terrorismo e a proteção de dados pessoais: análise crítica de um precedente constitucional alemão (Bundesverfassungsgericht). **Revista da AGU.** Brasil, ano 10, nº 28, p. 99 - 11, abr/jun. 2011.Trimestral. Disponível em: https://doi.org/10.25109/2525-328X.v.10.n.28.2011.163. Acesso em: 01 abr. 2019.

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

_____. O direito fundamental à proteção dos dados pessoais. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). **Direito Digital:** direito privado e internet. 2ª ed. São Paulo: Editora Foco, 2019, p. 35-53.

LIMA, Cíntia Rosa Pereira de. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap):** um estudo comparado entre Brasil e Canadá. 2009. 701f. Tese (Doutoramento em Direito) - Faculdade de Direito, Universidade de São Paulo. São Paulo. 2009.

_____. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.** 2015. 487f. Tese (Livre docência em Direito) - Faculdade de Direito, Universidade de São Paulo. São Paulo. 2015.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. *In:* AGRE, Phillip E.; ROTEMBERG, Marc. (org.). Technology and Privacy: The New Landscape. Cambrigde: The MIT Press, 1997, p. 219-242 *apud* BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 116-117.

PFEIFFER, Maria da Conceição Maranhão. **Direito à informação e ao consumo sustentável.** 2011. 166 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo. São Paulo, 2011.

PICCELLI, Roberto Ricomini. **A dimensão política da privacidade no direito brasileiro.** Rio de Janeiro: Lumen Juris, 2018.

SANTOS, Manoel J. Pereira dos. Considerações iniciais sobre a proteção jurídica das bases de dados. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.) **Direito & Internet** vol. I - Aspectos Jurídicos Relevantes. 2 ed. São Paulo: Quartier Latin, 2005, p. 321 - 335.

_____. Princípios para formação de um regime de dados pessoais. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.) **Direito & Internet** vol. II - Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2008, p. 355 - 375.

UNIÃO 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 01 abr. 2019.

_____. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à**

livre circulação desses dados. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 01 abr. 2019.

6.2. Valor patrimonial dos dados pessoais em mercados de preço zero – *Pietra Daneluzzi Quinelato*[136]

Resumo

O cenário tecnológico atual traz consigo a facilidade na transmissão de informações e a liquidez do conceito da privacidade. Diante disso e com base na decisão da Autoridade da Concorrência Alemã de fevereiro de 2019 em face do Grupo Facebook, o presente trabalho pretende apontar o funcionamento de mercados de preço zero e condutas anticompetitivas que podem ocorrer a partir do processamento do Big Data. Isso porque os dados pessoais passaram a representar ativos econômicos para as empresas, sendo processados de forma indiscriminada e não transparente, o que coloca em xeque a proteção de direitos fundamentais de seus titulares, como a privacidade e a intimidade. Discorre-se sobre a possibilidade de atuação das Autoridades de Proteção de Dados e os limites de Autoridades da Concorrência em casos como o mencionado.

Palavras-chaves: Dados Pessoais; Mercados de preço zero; Concorrência.

Abstract

The current technologic scenario brings the ease of information transmission and the liquidity of the concept of privacy. Therefore, and according to the decision of the German Antitrust Authority of February 2019 in the face of Facebook Group, the present paper aims to point out the operation of zero-price markets and the anticompetitive behaviors that may occur on Big Data processing. This is because of personal data which now amounted economic assets for companies, being processed indiscriminately and lacking in transparency, which challenges fundamental rights, such as privacy and intimacy. It also points the possibility of action of Data Protection Authorities and the limits of Antitrust Authorities in cases, as shown before.

Keywords: Personal data, Zero-price markets, Competition law.

[136] Graduada e Mestranda na Faculdade de Direito de Ribeirão Preto (USP). Advoga em propriedade intelectual e proteção de dados.

Introdução

Em poucas décadas, vivenciamos uma transformação exponencial nas formas de comunicação e consumo, que, sob um de seus aspectos, pode ser representada pela instantaneidade na transmissão de informação e na ausência de fronteiras territoriais propiciadas com a internet, culminando em novos modelos de mercado. DONEDA dispõe sobre a informação pessoal como elemento fundamental em inúmeros negócios na chamada Sociedade da Informação:

> As tecnologias da informação contribuíram para que a informação pessoal se tornasse capaz de extrapolar a própria pessoa. A facilidade da sua coleta, armazenamento e a sua utilidade para diversos fins tornou-a um bem em si, ligado à pessoa, mas capaz de ser objetivado e tratado longe e mesmo a despeito dela – não é por outro motivo que a informação pessoal é o elemento fundamental em uma série de novos negócios típicos da Sociedade da Informação. (DONEDA, p. 35)

A informação, atualmente, pode ser direcionada a milhares de destinatários em um mesmo instante, com um simples clique no ambiente virtual de computadores. As compras realizadas *online* são preferência da maioria dos indivíduos[137] e, geralmente, concluídas pelo aparelho celular. Tais exemplos demonstram a transformação vivenciada no mundo globalizado, conforme PECK elucida:

> Há pouco mais de trinta anos, a Internet não passava de um projeto, o termo "globalização" não havia sido cunhado e a transmissão de dados por fibra óptica não existia. Informação era um item caro, pouco acessível e centralizado. (...) Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigma. Essa nova era traz transformações em vários segmentos da sociedade – não apenas transformações tecnológicas, mas mudanças de conceitos, métodos de trabalho e estruturas. (PECK, p. 1)

A distribuição da informação e o novo modelo de mercado – virtual – não são apenas simultâneos, como interagem para criar uma publicidade direcionada ao comportamento do indivíduo. Em 1973, Stéfano Rodotà já demonstrava que as mudanças realizadas pelas novas tecnologias refletiriam, principalmente, na transformação da informação dispersa em informação organizada. (RODOTÁ, p. 14)

1. Dados como ativos econômicos nas plataformas digitais

[137]Disponível em: https://www.ecommercebrasil.com.br/noticias/compra-online-preferencia-de-consumidores-brasileiros/. Acesso em: 30.11.19.

Nessa Era Digital, a informação coletada dos indivíduos é tratada e, posteriormente, utilizada pelos anunciantes de produtos e serviços, retornando sob forma de uma propaganda personalizada. Essa dinâmica acentua o poder do comércio eletrônico e a quantidade de consumidores no cenário digital, conforme BIONI (p. 18): *"Cada vez mais os usuários da Internet subvertem-se em consumidores, sendo uma clara amostra de tal afirmação o crescimento exponencial do comércio eletrônico".*

Os consumidores, ao navegarem em websites e redes sociais, buscando suas preferências, deixam pegadas digitais que, se tratadas, serão convertidas em um desenho de suas predileções, o qual retorna sob a forma de produto ou serviço. Assim, as informações instantâneas e sem fronteiras não são apenas destinadas aos indivíduos, mas deles provenientes, representando um instrumento de poder econômico. Portanto, a informação não é só recebida, mas refletida (PECK, p. 28). BIONI reitera o retorno das publicidades de forma direcionada no cenário digital:

> Quando o usuário navega na internet, há uma série de cliques que revela uma infinidade de informações sobre as suas predileções, possibilitando que a abordagem publicitária as utilize para estar preciosamente harmonizada com elas. (BIONI, p. 19)

Os bancos de dados, apesar de existirem há muito, se aperfeiçoam tecnologicamente a ponto de reunir informações que, de forma organizada, podem representar de maneira variada preferências e características de milhares de indivíduos. Nesse sentido, BAPTISTA esclarece:

> Com a evolução da linguagem e expansão da capacidade de armazenamento, se potencializou o uso de uma variedade maior de informações e a retenção de dados de uma quantidade muito maior de usuários. (BAPTISTA, p. 20)

Conforme DONEDA, a administração de tais bancos de dados se torna cada vez mais fácil com advento de tecnologias, possibilitando a extração de informações pessoais em um conjunto que representará valor àquele que as trata.

> A sistematização da informação pessoal em grandes volumes teve seu potencial exponencialmente incrementado com o advento da informática, que tornou possível a administração de banco de dados gigantesco contendo informações pessoais. (DONEDA, p. 39)

Com isso, os bancos de dados representam ativos valiosos às empresas, sendo a principal fonte de estudo de mercado e informação dos destinatários de seus produtos e serviços ofertados.

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica. Essa lógica

> procura refletir um caráter utilitarista, procurando proporcionar a extração do máximo proveito possível a partir de um conjunto de informações. (DONEDA, p. 39).

Diante desse cenário, foi possível não apenas sistematizar informações pessoais em um único banco de dados, mas mesclá-las de forma sistematizada produzindo conteúdo personalizado sobre os indivíduos titulares das informações coletadas. Em um ato corriqueiro na rede social Facebook, pesquisas demonstraram que com 150 "curtidas", determinados algoritmos podem saber mais de uma pessoa do que o seu companheiro e com 250, mais do que ela própria (FRAZÃO, p. 27).

Portanto, a evolução da tecnologia permite que empresas tratem as informações e seus bancos de dados classificando os consumidores de acordo com suas preferências, extraídas de seus rastros digitais. Tal fato permite que aqueles que tratam dados pessoais tenham um certo poder sobre a própria pessoa titular dessas informações, conforme DONEDA menciona:

> Os bancos de dados que contém dados pessoais (...) proporcionam uma nova definição dos poderes e direitos sobre as informações pessoais e, consequentemente, sobre a própria pessoa. (DONEDA, p. 39).

Surge o conceito de *Big Data*, correlacionando diversos bancos de dados e extraindo informações de forma organizada, transformando-as em ativos para as empresas. Com esse novo paradigma de tratamento dos dados, volumes consideráveis de informações podem ser organizados de diversas maneiras, em velocidades antes inexistente e com a veracidade dos dados obtidos garantida.

> O acentuado aumento no volume de informações pessoais colhidas e passiveis de serem submetidas a tratamento introduziu, nos últimos anos, um novo paradigma no tratamento da informação. A disponibilidade de diversos bancos de dados e de informações pessoais em volumes bastante consideráveis fez com que fossem desenvolvidos mecanismos capazes de prospectar informações não propriamente em um único banco de dados, porém em diversas fontes de informações disponíveis e, através de uma determinada sistemática que envolve o estabelecimento de correlações em blocos de informações a princípio dispersos, gerar uma nova informação (Big Data). (DONEDÁ, p. 39-40).

BAGNOLI, de forma didática, caracteriza o Big Data sob uma perspectiva não apenas econômica, mas jurídica, com a identificação dos 6V's, isto é, a partir de (i) volume, (ii) velocidade, (iii) variedade, (iv) valor, (v) veracidade e da possibilidade de (vi) validação (p. 47). PFEIFFER (pp. 55-56), de forma cristalina, define:

> A característica mais conhecida é volume, devido à alta quantidade de dados que podem ser coletados e processados. Como enfatizado anteriormente, a tecnologia facilitou não apenas o armazenamento de dados, mas a sua transmissão. A variedade dos dados é muito importante porque permite que empresas explorem publicidades e desenvolvam novos produtos e serviços. Outro aspecto importante é a verificabilidade: a capacidade de verificar a veracidade e precisão dos dados coletados. Isso é de grande importância para evitar desenhar conclusões erradas dos dados coletados. A rapidez da coleta, armazenamento, análise e transmissão dos dados é também de vital importância. Consequentemente, a velocidade é outra característica que melhora a função dos dados na economia digital. Finalmente, a característica que efetivamente melhora a função dos dados na economia digital é o enorme e crescente valor. (tradução nossa)

Dessa perspectiva, o valor que o Big Data representa é um dos ativos mais valiosos das empresas nesse novo modelo de mercado, conforme MASSENO (p. 376) esclarece: *"O Big Data constitui a nova fronteira para a criação de valor, com um aumento radical da eficiência nos processos e na alocação de recursos"*.

> Com a possibilidade de organizar tais dados de maneira mais escalável (e.g. big data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. (BIONI, p. 13)

No modelo de mercado atual, os dados pessoais se mostram *commodities* às empresas que os tratam, cabendo unicamente a estas a sua transformação em vantagem competitiva, isto é, em valor econômico. Portanto, os dados pessoais, sistematizados em bancos de dados, tornam-se imprescindíveis para o sucesso das empresas que atuam, principalmente, no meio digital. As análises e informações extraídas do conjunto de dados permitem que o oferecimento de produtos e serviços seja feito de maneira personalizada e direcionada, aumentando as chances de compra dos consumidores.

Contudo, para que tais dados sejam coletados e, posteriormente analisados, é necessário que os indivíduos os disponibilizem de alguma maneira. O presente trabalho trata, principalmente, do funcionamento dos mercados de preço zero, como a plataforma Facebook, que oferece o acesso a um serviço "gratuito" em troca da coleta de informações pessoais.

> Os dados privados são, muitas vezes o ativo mais valioso de uma empresa e são capturados por meio de diversos serviços digitais, como e-mail, redes sociais e aplicativos de geolocalização, obtidos supostamente por serviços oferecidos "gratuitamente" aos consumidores. (BAGNOLI, p. 48)

Algumas empresas se tornaram "indústrias de banco de dados" (SOLOVE, p. 19), proprietárias de um capital bilionário apesar da prestação gratuita de seus serviços, como os mercados de preço zero. A dinâmica de tais empresas é sustentável economicamente pois o preço dos serviços não é verdadeiramente zero: os dados pessoais dos usuários são usados como "moeda" em troca do uso do serviço gratuito (TAUFICK, p. 6).

Em tais mercados, apesar de o oferecimento da navegação (e.g. Google *Search*) ou na interação de redes sociais (*e.g.* Facebook e Instagram) não cobrar do usuário, outros lados da plataforma pagam para ter acesso às informações lá tratadas, visando ao oferecimento de seus serviços e produtos de forma direcionada, conforme esclarece BIONI.

> Sob um novo modelo de negócio, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. São os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico. Dessa forma, tal relação torna-se plurilateral, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário, para haver retorno financeiro nesse modelo de negócio. (BIONI, p. 25)

De forma resumida, o modelo das superplataformas é centralizado na coleta de dados, que serão tratados e possibilitarão a agregação de valor econômico à empresa por inúmeras maneiras, como o desenvolvimento de inteligência artificial, aprimoramento de buscas, o oferecimento de serviços e produtos personalizados, definições de perfis a serem vendidas às empresas interessadas, etc.

Essas plataformas econômicas são, portanto, intermediárias entre dois ou mais grupos distintos, fornecendo uns aos outros os benefícios da conexão em rede. O alto valor obtido em tal modelo de negócio é extraído das interações diretas entre os distintos tipos de clientes afiliados, como os usuários de redes sociais de um lado e os anunciantes de outro (PFEIFFER).

> O modelo de negócios realizado pelo Google e pelo Facebook e outras empresas do ramo, consiste na reunião e organização de uma grande quantidade de informação de forma agregada. (BAPTISTA, p. 23)

Nota-se um efeito de rede no funcionamento das plataformas, pois o valor do negócio depende do número de usuários a ele associado. Em paralelo, o aumento dos usuários de um dos lados da plataforma, pode diminuir o custo dos produtos oferecidos de outro lado, caracterizando uma economia em escala.

> Nas operações com consumo, além de facilitar um muito melhor apoio à decisão nas empresas com um enorme aumento na eficiência organizacional,

> a Big Data releva essencialmente na estruturação da oferta. (MASSENO, p. 377)

Em um simples exemplo, tem-se que usuários querem acesso a uma rede de contatos maior, aumentando a utilização da plataforma que é meio para atingir tal objetivo. Esta, por outro lado, aumenta suas margens e capacidade de análises em proporção direta ao aumento da sua base de usuários.

Não é incomum que, visando à atração de um grupo de usuários, o patrocinador da rede subsidie o outro. Segundo KHAN, plataformas digitais parecem envolver estratégias representadas por períodos longos de baixos lucros e perdas para atingir uma massa crítica de dados e depois receberem os desejados lucros do monopólio, por meio de acumulação de dados pessoais. Como exemplo, o Facebook lucra no oferecimento de publicidades aos anunciantes. Para isso, oferece o acesso "gratuito" aos usuários da rede social. BIONI explica o funcionamento de tais plataformas:

> Em um primeiro momento, atrai-se o usuário para que ele usufrua do produto ou serviço para, em um segundo momento, coletar seus dados pessoais e, então, viabilizar o direcionamento da mensagem publicitária, que a fonte da rentabilização. (BIONI, p. 26)

E conclui, como é a nossa opinião, que os serviços oferecidos apesar de gratuitos, são, em verdade, pagos com informações pessoais.

> Nessa perspectiva, afirma-se de forma contundente que o pagamento seja ele integral ou parcial de muitos produtos e serviços é realizado com os dados pessoais do próprio consumidor. (BIONI, p. 27)

Diante disso, um novo modelo de negócio se consolida.

2. Condutas anticompetitivas – o caso Facebook na Alemanha

Ocorre que o tratamento de informações pelas plataformas digitais, muitas vezes, não é feito de forma transparente ou sequer informada ao titular. O Ministro Ruy Rosado de Aguiar, há mais de vinte anos, demonstrou a preocupação crescente com o tema:

> A inserção de dados pessoais dos cidadãos em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado de diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita a sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita

> de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. STJ. REsp 22.337/RS, rel. Min. Ruy Rosado de Aguiar, dj. 20.03.1995, p. 6119.

Apesar de não ser uma preocupação recente[138], há alguns anos o tema da proteção aos dados pessoais se tornou mais latente na sociedade, com a promulgação do Regulamento Europeu de Proteção aos Dados Pessoais na Europa em 2016 (GDPR) e, no Brasil, a Lei Geral de Proteção de Dados em 2018 (LGPD).

Tais regulações, por meio de diretrizes, princípios, direitos dos titulares e sanções em caso de descumprimento, impõem uma mudança de *"mindset"* como resultado de um processo de adequação das empresas às exigências legais, visando à autodeterminação informacional do titular do dado pessoal a partir de um tratamento transparente.

Caso contrário, a utilização de bases de dados estruturadas com dados pessoais pode conduzir a práticas indesejadas entre empresas. DOMINGUES, GABAN e SILVA (p. 173-176) elencam condutas anticompetitivas que são prováveis de ocorrer em mercados digitais, como exemplo a predação, a recusa de contratar, a venda casada de produtos e serviços, o estrangulamento de margem, o oportunismo compulsório, a alavancagem discriminatória e a discriminação de concorrentes. No mesmo sentido, BAGNOLI esclarece:

> Existem vários tipos de condutas relacionadas com os dados que possui uma empresa que podem suscitar preocupações concorrenciais, tais como fusões e aquisições, condutas excludentes como recusa de acesso, acesso discriminatório a dados, contratos exclusivos, vendas e uso cruzado de conjuntos de dados, dados como veículo para discriminação de preços e dados, poder de mercado e preocupações com privacidade. (BAGNOLI, p. 53)

Portanto, o Big Data pode ser tanto vantajoso, usado como vantagem competitiva da empresa que sabe processar os dados ali contidos e transformá-los em um ativo econômico, quanto prejudicial às demais empresas se utilizado de forma que as impeça de competir de maneira sadia e leal no mercado.

> Se por um lado o Big Data pode ser extremamente poderoso como uma vantagem competitiva, que fornece respostas mais rápidas e resultados mais eficientes para as empresa, por outro lado, pode ser usado como um

[138] Em 1980, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) expôs Diretrizes sobre Proteção de Privacidade e Circulação Transfronteiriça de Dados Pessoais. Em 1981, houve a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento de Automatizado de Dados Pessoais. Diretiva 95/46/CE da Comissão Europeia foi substituída pelo GDPR.

> mecanismo astuto para restringir a concorrência, por meio de condutas competitivas, incluindo o aumento de barreiras à entrada e a exclusão do acesso a insumos essenciais, consolidando o domínio de mercado. (BAGNOLI, p. 46)

No cenário nacional, o artigo 36, parágrafo 1º da Lei 12.529/11 abaixo reproduzido reforça que, em termos concorrenciais, a posição dominante da empresa não constitui ilícito em si. O problema se configura quando ocorre um abuso de tal posição.

> Art. 36. Constituem infração da ordem econômica, independentemente de culpa, os atos sob qualquer forma manifestados, que tenham por objeto ou possam produzir os seguintes efeitos, ainda que não sejam alcançados:
>
> I - limitar, falsear ou de qualquer forma prejudicar a livre concorrência ou a livre iniciativa; II - dominar mercado relevante de bens ou serviços; III - aumentar arbitrariamente os lucros; e IV - exercer de forma abusiva posição dominante.
>
> § 1º A conquista de mercado resultante de processo natural fundado na maior eficiência de agente econômico em relação a seus competidores não caracteriza o ilícito previsto no inciso II do caput deste artigo.
>
> § 2º Presume-se posição dominante sempre que uma empresa ou grupo de empresas for capaz de alterar unilateral ou coordenadamente as condições de mercado ou quando controlar 20% (vinte por cento) ou mais do mercado relevante, podendo este percentual ser alterado pelo Cade para setores específicos da economia. (...)

Diante disso, como reconhecer o abuso de posição dominante em plataformas digitais? A legislação nacional da concorrência baseia-se, principalmente, em valores econômicos para a apuração de ilícitos e condutas anticompetitivas, o que dificulta a análise de tais condutas nesse cenário de mercados digitais.

Diferentemente do panorama nacional, a Alemanha, em junho de 2017, por meio de sua 9ª Emenda na Lei da Concorrência (*Act against Restraints of Competition* - GWB), estabeleceu que dados seriam considerados como fonte de poder de mercado, deixando clara a necessidade de observância dos impactos que podem ser causados por tais informações em ambos os lados de uma plataforma digital, por exemplo.

Foi nesse cenário que em fevereiro de 2019 a Autoridade da Concorrência Alemã – Bundeskarllamamt (BKT), após alguns anos de estudo, condenou o Grupo Facebook, composto pelas empresas Facebook Inc. Facebook Ireland Ltda. e Facebook Germany GmbH, pela prática de condutas anticompetitivas, abusando do poder econômico que possuía. Em sua opinião, o grupo estaria violando dados pessoais de usuários e terceiros (Case B2-22/16). Como consequência, os usuários perderiam o controle de seus dados pessoais e as empresas concorrentes sofreriam consequências negativas de tal abuso.

Com fundamento nas Seções 19 (1) e 32 do GWB e pela violação dos artigos 6 (1) e 9 (2) do GDPR, a BKT decidiu que a empresa estava proibida de combinar dados provenientes dos produtos do grupo Facebook (*e.g.* Whatsapp, Instagram) e daqueles coletados pela ferramenta Facebook Business Tools. O grupo deveria realizar alterações nas formas de processamento de dados e em seus termos de uso, sem condicionar o acesso dos usuários à aceitação irrestrita das condições. Isso porque o grupo Facebook, sob alegação de "legítimo interesse", teria coletado dados sem o consentimento dos usuários e extrapolado a finalidade do tratamento para exibição de publicidade dirigida. Para a BKT, os termos de uso seriam genéricos e amplos.

Demonstrou-se que o processamento de dados pelo grupo era realizado sem o consentimento do usuário e a coleta era feita de forma injustificada para o titular, extrapolando a finalidade de *profiling* do usuário e o consequente direcionamento de campanhas publicitárias. De forma geral, a autoridade concluiu que o princípio da transparência contido no GDPR estava sendo frontalmente desrespeitado pelo grupo empresarial.

Contudo, a decisão da BKT foi suspensa[139] em agosto de 2019 pela Corte de Dusseldorf, sob suspeita de ilegalidade da decisão, que, entre os fundamentos, estava a possível extrapolação dos limites de sua atuação, invadindo a seara da proteção aos dados pessoais, que seria de competência da Autoridade Nacional de Proteção de Dados Alemã.

Contrariamente à opinião da BKT, a Corte alega que o processamento de dados pelo Facebook não geraria nenhum dano competitivo relevante ou qualquer desenvolvimento indesejável da concorrência. Isso se aplicaria tanto a um abuso exploratório em detrimento dos consumidores que participam da rede social do Facebook quanto a um abuso excludente em detrimento de um concorrente real ou potencial do Facebook.

Do ponto de vista da concorrência, o único fator decisivo para a configuração do abuso de posição dominante do grupo seria se o consentimento exigido dos consumidores ao se registrar na rede social para processar e vincular os dados adicionais fosse determinado por terceiros. Ou seja, devido à posição dominante do Facebook, a declaração de consentimento dos usuários não poderia ser considerada

[139] O caso encontra-se aguardando o julgamento da apelação da BKT.

autônoma. Na opinião da Corte de Dusseldorf, a BKT carregaria o ônus da avaliação a esse respeito e não provou que fosse o caso.

Diante disso, entre tantas, reacendeu-se uma indagação no cenário nacional: caberá à Autoridade Nacional de Proteção de Dados (ANPD) a análise de condutas anticompetitivas realizadas a partir da violação da proteção dos dados pessoais ou será matéria sob a égide das entidades de defesa da concorrência?

3. Ponderações da atuação da ANPD no caso Facebook

A ANPD foi criada pela Medida Provisória 869/2018, convertida na Lei 13.835/2019, possuindo autonomia técnica e decisória para as atribuições elencadas no artigo 55-J da LGPD, resumidas em funções preventivas, regulatórias, fiscalizatórias, sancionatórias e reparatórias. Nasce, contudo, com vários desafios, entre eles, o conflito tratado no presente trabalho.

Nesse contexto, a LGPD dispõe, em seus artigos 55-J e 55-K, uma possível solução para a questão suscitada de conflito de competência entre demais órgãos da esfera pública e a Autoridade Nacional de Proteção de Dados (ANPD):

Art. 55-J. Compete à ANPD:

> (…) XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
>
> (...) § 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

Portanto, nos termos incluídos pela Lei 13.853 de 2019, caberá à ANPD a articulação com demais órgãos da esfera pública em atividades reguladas. Não obstante a abrangência e indefinição trazida pela referida disposição, o parágrafo 3º do artigo 55-J aborda a possiblidade de órgãos e entidades públicos, de setores específicos, coordenarem entre si de quem será a competência para analisar o adequado tratamento de dados pessoais.

Já o artigo 55-K, que dispõe sobre as sanções previstas na LGPD, mostra-se mais específico quanto à prevalência da competência da ANPD em face de competências de outras entidades e órgãos da administração pública. No parágrafo único do dispositivo, deixa-se claro que a ANPD será o órgão

central de interpretação da legislação, também no que tange ao estabelecimento de normas para que seja aplicada.

> Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.
>
> Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

Diante disso, a resposta para tais questionamentos nos faz acreditar que caberá à ANPD a análise e averiguação de violações às disposições sobre a proteção aos dados pessoais definida na LGPD. Esclarecem, LIMA e PEROLI (p. 428):

> (...) Ao se abordar a autorregulação, não se pretende a substituição da regulação estatal, mas que esta seja complementada por normas que levem em conta a realidade dos setores envolvidos, conexos à privacidade e as suas intersecções com a tecnologia, o que faz da autorregulação um modelo conveniente ao auxílio da efetividade das leis de proteção de dados pessoais.

PFEIFFER (p. 462) reforça que será de extrema importância o estabelecimento de convênios entre a ANPD, agências reguladoras e órgãos de proteção de defesa do consumidor, prevendo mecanismos de atuação conjunta. Complementa reiterando que as agências reguladoras não poderão editar normas que desrespeitem a LGPD ou normas expedidas pela ANPD, salvo legislação especial expressa.

Transpondo de forma simplificada o caso narrado para o cenário nacional, em que se suscitou a ilegitimidade da decisão da BKT em face do grupo Facebook, presume-se que o órgão de defesa da concorrência - CADE, regulado pela Lei 12.529/2011, não estaria apto para a tomada de decisão nos mesmos termos que a BKT, seja pela (i) ausência de critérios específicos para a apuração de ilícitos em mercados digitais na legislação brasileira ou pelo (ii) respeito aos dispositivos supramencionados, em que a competência para assuntos envolvendo violação à proteção de dados é desviada para a ANPD.

PFEIFFER (p. 81) aponta a decisão da BKT é muito controversa, estando sujeita a críticas porque seria uma aplicação incorreta do direito da concorrência para proteger dados pessoais. E continua demonstrando que, por outro lado, uma abordagem abrangente para preocupações com Big Data é apoiada pela Autoridade Europeia de Proteção de Dados, que sugere uma cooperação mais estreita entre

as autoridades de proteção de dados, proteção ao consumidor e antitruste na investigação e aplicação das regras de proteção de dados pessoais.

De forma sábia, PFEIFFER (p. 82) reproduz argumento da BKT de que as questões de privacidade não poderiam ser excluídas da análise sob o aspecto concorrencial pela mera natureza, isso porque *"a falta de transparência na coleta e processamento de dados pessoais pode ter, paralelamente, implicações na dimensão da concorrência*".

A responsabilidade e a lista de afazeres da ANPD são extensas e ainda sem a sua criação, os elementos que podem responder o questionamento suscitado se mostram vagos. Resta-nos a espera por uma breve criação da ANPD e a posterior emissão de resoluções que respondam inúmeras dúvidas já debatidas no cenário nacional por pesquisadores e profissionais da área. Nesse sentido, dispõe LIMA e PEROLI (p. 427):

> A Lei 13709/2018 se utiliza de dispositivos de eficácia limitada, que dependem de regulação, cuja conexão com a tecnologia propicia a atribuição às autoridades de proteção de dados pessoais a tecnorregulação.

Evidencia-se, pois, mais uma questão em aberto, na ânsia da futura criação da ANPD. Algo é certo: uma atuação solitária será praticamente impossível em face de tantos desafios a serem enfrentados e, inclusive, regulados.

Conclusão

Na dinâmica empresarial tecnológica atual, bases de dados pessoais são ativos concorrencialmente relevantes para empresas, que podem impactar tanto no controle de estruturas (haja vista que as bases de dados pessoais podem ser consideradas um ativo intangível com valor econômico de difícil avaliação, sendo difícil a sua precificação), como em controle de condutas, causando efeitos negativos à defesa da concorrência.

O presente artigo trata do Big Data como uma ferramenta muito importante para a economia digital, possibilitando que empresas processem dados de diversas formas, em grandes volumes e velocidade antes não conhecidos, culminando na posterior monetização de tais informações. Ocorre que tal tratamento, muitas vezes, não é feito de forma clara ou sequer é informado ao titular do dado, suscitando problemas de proteção aos dados pessoais, principalmente com o GDPR e a LGPD.

Como exemplo, no caso do Grupo Facebook, a Autoridade da Concorrência Alemã concluiu que haveria um excesso no tratamento de dados dos usuários, desiquilibrando interesses individuais e comerciais, culminando em uma assimetria informacional do titular da informação. Tal decisão, no

entanto, ainda não é definitiva pela possibilidade de ilegalidade. Teria, a BKT, extrapolado os limites da sua atuação e adentrado na seara da Autoridade Nacional de Proteção de Dados?

No Brasil, ainda não se sabe qual será o desfecho de conflitos de competência entre entidades da administração pública e a ANPD. Presume-se que, com a existência dos artigos 55-J e 55-K, a competência para a averiguação de assuntos atinentes à proteção de dados será da ANPD. Contudo, trata-se de legislação ordinária, que pode colidir frontalmente com as disposições de outras, como a própria Lei 12.529/11. Diante disso, o cenário para a averiguação de condutas anticompetitivas causadas pela violação de dados pessoais se mostra incerto até que a ANPD seja criada e emita resoluções, sejam individuais ou em parceria com outras entidades.

A responsabilidade e a lista de afazeres da ANPD são extensas e ainda sem a sua criação, os elementos que podem responder o questionamento suscitado se mostram vagos. Resta-nos a espera por uma breve criação da autoridade e a posterior emissão de resoluções que respondam inúmeras dúvidas já debatidas no cenário nacional por pesquisadores e profissionais da área. Evidencia-se, pois, mais uma questão em aberto, na ânsia da futura criação da ANPD. Algo é certo: uma atuação solitária será praticamente impossível em face de tantos desafios a serem enfrentados e, inclusive, regulados.

Em paralelo, ao direito da concorrência caberá a atualização e evolução de conceitos tradicionais que realizam a análise de condutas possivelmente anticompetitivas (PFEIFFER, p. 84), como o exemplo do presente trabalho.

Referências bibliográficas

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

BUNDESKARTELLAMT. **Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing: B6-22/16, case summary**. Disponível em: <https://bit.ly/2KMHHxY>. Acesso em: 29.06.2019.

BUNDESKARTELLAMT. **The Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V).** Disponível em: <http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf>. Acesso em: 01.12.2019.

DE LUCCA, Newton; SIMAO FILHO, Adalberto; LIMA, Cintia Rosa (coor.). **Direito e Internet III - Tomo I**. São Paulo: Ed. Quartier Latin. 2015.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P.; MACIEL, Renata M. (coord.) **Direito e Internet IV: Sistema de Proteção de dados Pessoais.** São Paulo: Ed. Quartier Latin, 2019.

DOMINGUES, Juliana O.; GABAN, Eduardo; MIELE, Aluísio; SILVA, Breno F. M. (Orgs.). **Direito Antitruste 4.0: fronteiras entre concorrência e inovação**. 1ª Ed. São Paulo: Ed. Singular, 2019, pp. 185-196.

DOMINGUES, Juliana O.; GABAN, Eduardo; SILVA, Breno F. M. **Direito Antitruste 4.0 e o abuso de posição dominante nos mercados digitais: um desafio atual para o CADE.** In:

FORGIONI, Paula. **Os fundamentos do antitruste**. 4. ed. rev. atual. e ampl. São Paulo: RT, 2010.

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais – noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Coord. FRAZÃO, Ana; OLIVA, Milena D.; TEPENTINO, Gustavo.1 Ed. São Paulo: Thomson Reuters Brasil, 2019.

GABAN, Eduardo M.; DOMINGUES, Juliana Oliveira. **Direito Antitruste**. 4. ed. São Paulo: Ed. Saraiva, 2016.

KHAN, Lina M. Amazon's Antitrust Paradox. **The Yale Law Journal.**, Vol. 126, no. 3, 2017. pp. 564-907. Disponível em: < https://bit.ly/2JeXa6S >. Acesso em 26.06.2019.

KREIN, Julia. Novos Truster na Era Digital: efeitos anticompetitivos do uso de dados pessoais pelo facebook. **Revista de Defesa da Concorrência,** Vol. 6, n° 1, maio 2018, pp. 198-231.

LIMA, Cintia R. P.; PEROLI, Kelvin. **Desafios para a atuação independente da Autoridade Nacional de Proteção de Dados.** In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P.; MACIEL, Renata M. (coord.) **Direito e Internet IV: Sistema de Proteção de dados Pessoais.** São Paulo: Ed. Quartier Latin, 2019.

PFEIFFER, Roberto A. C. **A saga da Autoridade Nacional de Proteção de Dados – do veto à Lei 13.853/2019.** *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P.; MACIEL, Renata M. (coord.) **Direito e Internet IV: Sistema de Proteção de dados Pessoais.** São Paulo: Ed. Quartier Latin, 2019.

PFEIFFER, Roberto A. C. Digital Economy, Big Data and Competition Law. **Market and Competition Law Review.** Volume III. N. 1. Abril 2019, pp. 53-89.

PECK, Patricia. **Direito Digital**. 3 Ed. Ver., atual., ampl. São Paulo: Saraiva, 2009.

RODOTÀ, Stéfano. **Elaboratori elettronici e controlo sociale.** Bologna: Il Mulino, 1973.

RODRIGUES, Eduardo Henrique Kruel. **O Direito Antitruste na Economia Digital: implicações concorrenciais de acesso a dados.** Dissertação para obtenção do título de mestre em Direito, Estado e Constituição na Universidade de Brasília. Brasília, 2016.

SOLOVE, Daniel. **The digital person: technology and privacy in the information age.** New York: New York University, 2004.

TAUFICK, Roberto D. **Over-The-Top Content and Content Regulation.** Disponível em: <http://ssrn.com/abstract=2708278>. Acesso em: 20.06.2019.

6.3. Propaganda comportamental, consentimento para coleta de dados e a proteção consumerista – *Victor Sader Oliveira, Bruno Otávio Simozako Sadano & Caio César Domingues de Almeida*

Resumo

Este trabalho, sob a perspectiva protecionista do Código de Defesa do Consumidor em conjunto a novel LGPD, aborda os riscos na obtenção, industrialização e análise de dados. Aborda, ainda, a questão dos danos daí decorrentes e informações pessoalmente identificáveis.

Palavras-chave: Direito do Consumidor; direito à privacidade; Responsabilidade Civil; monetização de dados; *Online Profiling*; *Marketing* preditivo.

Abstract

This paper, through the purviews of consumer protection law and the new LGPD, takes on the risks in obtaining, whole-selling and analyzing data. It also touches on the damages due to misuse or mismanagement of consumer data and the risk of personally identifiable information.

Keywords: Consumer Law. Right to Privacy. Civil Liability. Data Monetization. Online Profiling. Predictive Marketing.

Introdução

Popularizada por Thomas Hobbes, a noção de que conhecimento é poder se prova cada vez mais verdadeira. Em tempos vigentes, ante o fácil acesso de informações, o cidadão médio detém nas pontas dos dedos mais conhecimento que qualquer um de seus antepassados. Entretanto, até em proporções oceânicas, as informações ali disponíveis empalidecem contrastadas ao poder extraído da análise e manipulação de grandes bancos de dados (*big data sets*).

Os recentes anos representaram um avanço colossal nas relações consumeristas. Esta marcha adiante, impulsionada pela disseminação das redes sociais e a facilitação de acesso à internet e serviços atrelados, serviu para diminuir a distância entre os fornecedores e seu público-alvo. O que outrora era objeto de estudo por meio de pesquisas de mercado, agora pode ser apurado mediante análise de dados diretos e indiretos.

A criação de serviços especializados na análise, manipulação e extrapolação de tais bancos de dados deu origem à indústria da *Big Data*. Em termos sumários, traduz-se em três pilares: a) a maximização de poder computacional e otimização de algoritmos utilizados na análise de quantias vultosas de dados; b) a utilização de ferramentas para segregar, agregar ou de diversos modo catalogar *big data sets* e; c) a crença que, quanto maior a base de dados disponível, mais fiéis os resultados atingidos. A noção de que seria possível extrapolar, a partir de um ou mais conjuntos de dados, verdades objetivas e subjetivas ensejou o investimento maciço por parte de colossos da indústria de telecomunicação e serviços atrelados.

Nasce, desta imensa fonte de dados, uma indústria especializada em angariar, segregar e analisar bases de dados de proporções colossais, a fim de melhor direcionar não apenas a publicidade, como também a atuação dos fornecedores. Contudo, o agrupamento indiscriminado de tais dados, bem como o seu fornecimento por parte daqueles que controlam a maior extensão das redes, como os gigantes da informática e as empresas de telecomunicação, coloca em xeque a privacidade dos consumidores e a transforma em moeda de câmbio.

Embora hoje regularizado pela Lei 13.709/2018, o acesso, extração e comercialização de dados mediante o uso de serviços por anos foi limitado apenas pelos mandamentos constitucionais, no que concerne a privacidade, e o regime protecionista do Código de Defesa do Consumidor. A conjugação de tais normas, aplicada às práticas de coleta, uso e vendas de dados particulares, deveria ser o suficiente para coibir e impedir a má utilização. Entretanto, faz-se necessário que avance a doutrina o estudo das normas e as aproxime do cotidiano.

O presente trabalho visa conjugar as diretrizes protecionistas da Lei 8.078/1990 com a Lei 13.709/2018, confrontando-as com a prática da publicidade comportamental (*behavioral marketing*) e a elaboração de perfis individualizados do consumidor (*online profiling*). Também será abordada a questão dos riscos

relacionados à publicidade embasada em reconhecimento de padrões futuros ou consectários da base de dados (*predictive marketing*).

1. Do consentimento para coleta, agrupamento e análise de dados

Uma pequena alteração com proporções hercúleas é a exigência do consentimento informado para a utilização, ou tratamento, de dados inserida no art. 7º da Lei 13.709/2018, com definição pelo art. 5º, XII do mesmo diploma. A exigência de que a parte alvo da coleta, e posterior tratamento, de dados deve expor o seu consentimento informado é marco histórico para a regularização da *Big Data.* Em específico, ao que concerne o uso de algoritmos preditivos voltados ao marketing e à possibilidade de tais análises ensejarem a obtenção de *Personally Identifiable Information* (PII) dentro de um *data set.* Isto é, a possibilidade de, além de redigir ou direcionar publicidade voltada ao perfil do público-alvo, ter à disposição, dentro daquele grupo de dados, informações o suficientes para oferecer publicidade específica ao ponto de serem rompidas as proteções à privacidade do indivíduo.

Estabelecida a relação de consumo, porém, temos que o consumidor se vê em desvantagem técnica quanto ao fornecedor. Ao concordar com os chamados "termos de uso", muitas vezes uma contratação necessária para permitir o acesso a determinado site, acaba por contratar sem possuir informações precisas acerca das consequências inevitavelmente atreladas à manipulação e uso de seus dados pessoais.

Diante de tais fatos, é possível constatar uma afronta aos direitos sociais do consumidor, em específico aqueles elencados no art. 6º, III da Lei 8.078/1990, ante o vácuo informacional específico concernente ao serviço contratado e a utilização do consumidor como produto secundário de dados.

Distantes dos princípios basilares da lei consumeristas, estes contratos de adesão são muitas vezes densos e de difícil leitura. Não obstante, constam, ainda, com a mera informação de que dados pessoais poderão ser coletados, não desincumbindo através de tal passagem a empresa do seu ônus de informar ao consumidor o propósito e a metodologia de monetização dos seus dados. Neste sentido, as ferramentas do Facebook Ads, programa de impulsão de publicações da mídia social Facebook (cujo conglomerado também é dono do Instagram e WhatsApp), utilizam-se do *data set* coletado dos usuários em tais redes sociais para, mediante pagamento, alcançar clientes com determinado grupo de características escolhidas pelo publicista.

Inexiste, portanto, consentimento informado. O consumidor não está ciente, no momento de criação de sua conta vinculada às redes sociais ou outros sites, que seu cadastro, informações pessoais e rotina de uso serão transformadas em mercadoria. Os contratos de adesão intitulados "termos de uso" são insuficientes para afastar a responsabilidade civil pelos danos decorrentes da ingerência de dados ou, ainda, da sua venda indiscriminada.

Recentemente, o Google foi multado em R$213 milhões por violação das regras de privacidade da União Europeia. Em 2012, nos Estados Unidos, já havia a mesma empresa sofrido sanção similar, à monta de US$22,5 milhões por invadir a privacidade de seus usuários. Há apenas onze meses, o gigante das mídias sociais Facebook foi multado em míseras 500 mil libras pelo Reino Unido por não proteger de maneira suficiente as informações de seus usuários.

Inegável que a comercialização dos dados pessoais e o seu uso desenfreado, transfigurando os consumidores em produto secundário de informações, está distante das proteções estabelecidas no Códice Consumerista e na Lei Geral de Proteção de Dados. Em desrespeito à legislação, sem o consentimento informado do consumidor ante a ausência de informações claras e precisas, são tais condutas ilegais e afrontam a boa-fé objetiva

2. *Online Profiling:* quando a análise de dados objetivos enseja reconhecimento subjetivo

O marketing online se tornou prática disseminada no cotidiano. Raras as vezes em que não visualizamos algum anúncio, seja antes de um vídeo ou durante o uso de alguma mídia social. Contudo, apenas com os avanços na análise de dados coletados dos usuários é que estes anúncios passaram a ser cada vez mais específicos e direcionados, aperfeiçoados ao ponto de se inserirem no âmbito dos interesses de seu alvo.

O marketing comportamental, cujo desdobramento intitulado *online profiling* nos interessa, é o aplicar do resultado da análise de vastos conjuntos de dados para determinado fim. Ou seja, mediante averiguação de um *data set*, aplicando-se algoritmos para seleção de determinadas características de interesse, é possível traçar um perfil de atuação dos usuários de determinado local, grupo ou raça.

Por métodos de captação de dados, como rastreamento de cookies, informações de GPS atreladas à aplicativos de mídia social ou mapeamento, as empresas inseridas na comercialização e análise de *data sets* são capazes de oferecer um perfil fidedigno do público-alvo a quem almeja a sua utilização. Ao acompanhar as atividades online de seus usuários, as redes sociais e serviços atrelados são capazes de alcançar a sua esfera mais íntima, extrapolando o seu interesse confesso e adentrando a sua real motivação.

Não tratamos, ademais, de alarmismos infundados. Pelo contrário, são diversos os casos em que a capacidade de traçar um perfil a partir dos dados coletados de um determinado grupo ensejou na obtenção, ainda que de maneira indireta, de informações pessoalmente identificáveis. É dizer, através de uma análise objetiva de um *data set*, visando conhecer o público-alvo, extrapolou-se informações *subjetivas* quanto aos integrantes daquele público-alvo.

O caso mais conhecido envolve um dos gigantes do comércio estadunidense, a empresa Target, e o seu uso indiscriminado de dados adquiridos e comprados para antecipar quando suas compradoras poderiam

estar grávidas, a fim de alterar os seus rituais de consumo em um momento de fluxo na rotina. Contudo, o alcance das informações obtidas mediante análise e *cross referecing* de dados é muito mais amplo que apenas um palpite acerca das gestações de clientes.

É possível, mediante a aplicação do algoritmo correto, perquirir acerca dos reais e íntimos interesses dos clientes. Por exemplo, se um usuário da rede social Instagram segue diversas personalidades do mundo fitness, perfis de receitas saudáveis e motivacionais, mas por ter aceito os termos de uso permitem que o aplicativo saiba a sua localização, é plenamente possível verificar que os seus interesses superficiais podem ser distantes daqueles em seu âmago. Neste exemplo, através das informações de sua localização seria possível discernir não apenas os locais que visita, mas a frequência, sendo plausível inferir os seus hábitos alimentícios. Se, por diversas vezes e em frequência regular o consumidor se dirige à um restaurante de fast food, infere-se que os seus interesses superficiais (comida saudável, perfis fitness) são antitéticos àquilo que realmente o interessa em seu âmago. Sabe-se, neste sentido, que publicidade voltada aos seus interesses superficiais surtirá menos efeito que aquela voltada para os seus interesses íntimos, ao mesmo tempo em que se constrói uma rede de informações pessoalmente identificáveis.

Em suma, prediz-se informações, a partir da análise do conjunto de dados, tão específicas, que a sua aplicabilidade acaba por alcançar o íntimo e o privado do consumidor.

Conclusão

Conquanto o suficiente tenha sido dito pela doutrina e pelas Cortes Superiores acerca da validade dos contratos de adesão, é certo que a evolução das relações de consumo, em específico aquelas em que há uma mescla entre o serviço ou produto prestado e a monetização do consumidor em si, devem ser analisadas sob nova ótica. Consoante o acima afirmado, mostra-se evidente que os termos enclausurados dos contratos de adesão em massa, como atualmente utilizados por gigantes das áreas de telecomunicação e mídias sociais, deixam de atender às estipulações da Lei 13.709/2018 e o dever de informação constante no bojo do Código de Defesa do Consumidor.

O necessário consentimento informado se traduz, em conjugação com as diretrizes de proteção da Lei 8.078/90, em barreira essencial à angariação e utilização dos dados pessoais do consumidor. Barreira, esta, que não está servindo a sua função no momento atual de desenvolvimento da doutrina e da atuação judiciária. Conquanto se respeite a inércia do Poder Judiciário, temos que a inércia dos doutrinadores acerca deste tema é inescusável.

De um lado, possuímos contratos adesivos cuja densidade, por si, atua como impedimento ao dever de informação, e, de outro, possuímos consumidores hipossuficientes quanto ao conhecimento técnico acerca da utilização de seus dados. Um aviso breve, como o utilizado pela empresa Facebook (cujo

conglomerado também é dono das plataformas Instagram e WhatsApp) de que os seus dados estão sendo coletados é insuficiente para atender ao estipulado na legislação.

Ao revés, temos que a simples menção à coleta de dados e sua utilização, sem a informação correta dos seus riscos vinculados e extrapolação monetária daí decorrente, é insuficiente para satisfação do consentimento informado. Em extremos, a ausência de consentimento informado pode nos remeter à casos como ao de Lisa Magrin, professora estadunidense cujos dados coletados foram vendidos como parte de um *data set*, mas que eram tão específicos a ponto de traduzirem-se em PII.

A possibilidade de ser pessoalmente identificado, como uma gota resgatada de um oceano, assim como os vícios no consentimento presentes no modelo atual de contratação para captação de dados, enseja em violações inequívocas ao direito constitucionalmente garantido à privacidade e aos direitos sociais. Isto é, não apenas na ocorrência de um vazamento de informações seriam as empresas responsáveis pelos danos emergentes ou decorrentes, mas também pela má análise e pela leviandade com a qual são monetizados estes dados.

Havendo vício no consentimento e má utilização dos dados coletados, independente de se por terceiro comprador, em razão da relação consumerista estabelecida, é possível rastrear a responsabilidade pelos danos diretamente ao fornecedor. A partir desta noção, pode-se, ainda, alegar a ocorrência de danos morais pelo uso indevido – seja na análise ou na comercialização – dos dados coletados, ainda que não aparente a individualização do consumidor.

Referências bibliográficas

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17/10/2019.

_____. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17/10/2019.

BROTHERTHON, A. Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine, **61 EMORY Law Journal** 555, 558 (2012). Disponível em: http://law.emory.edu/elj/content/volume-61/issue-3/comments/big-brother-gets-amakeover.html. Acesso em: 17/10/2019.

FRANÇA, R. Limongi. **Hermenêutica Jurídica**; atualização: Antônio de S. Limongi França; prefácio à 8ª edição: Giselda M.F. Novaes Hironaka. São Paulo. Revista dos Tribunais, 2015.

HOBBES, Thomas. Leviatã. **Matéria, forma e poder de um Estado eclesiástico e civil.** (Tradução de João Paulo Monteiro e Maria Beatriz Nizza da Silva). 3. ed. São Paulo: Abril Cultural, 1983. Col. Os Pensadores.

MADDEN, Mary; GILMAN Michele; LEVY Karen, e MARWICK Alice. Privacy Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 **Wash. U.L. Rev.** 053 (2017). Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6. Acesso em: 17/10/2019.

TENE Omer & POLONETSKY Jules, Privacy in the Age of Big Data: A Time for Big Decisions, 64 **STAN. L. REV. ONLINE** 63, 65–66 (2012). Disponível em: http://www.stanfordlawreview.org/online/privacyparadox/big-data. Acesso em: 17/10/2019.

6.4. A LGPD aplicada ao *marketing*: desafios e perspectivas – *Mariana Martins Ferreira*[140]

Resumo

Numa época em que não se pode mais imaginar viver sem comércio eletrônico, e-mail, ferramentas de mensagens instantâneas e redes sociais, o marketing digital baseado em perfis comportamentais e em alta segmentação de públicos-alvo torna-se ferramenta absolutamente vital a empresas dos mais diversos segmentos da economia. O presente artigo busca analisar os principais desafios e perspectivas para as atividades de marketing (especialmente o digital) a partir da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – a "LGPD"), considerando especialmente a aplicação de seus princípios e a aplicabilidade de suas bases legais sobre tais atividades. Com o novo regramento, os profissionais do marketing precisarão exercitar sua criatividade de modo a adaptar ferramentas já consagradas, como o e-mail marketing, às exigências legais, sem desmotivar o engajamento de seu público-alvo. Ao contrário do que se possa pensar, essa mudança de paradigma poderá efetivamente melhorar a qualidade das bases de dados e trazer ganhos de competitividade aos agentes da comunicação, ao mesmo tempo em que a oferta de marketing aos consumidores se tornará mais precisa e, certamente, menos incômoda.

Palavras-chave: Lei 13.709/2018; Lei Geral de Proteção de Dados Pessoais; proteção de dados pessoais; privacidade; marketing.

Abstract

In a time in which we could no longer imagine living without e-commerce, e-mail, instant messaging tools and social networks, digital marketing based on behavioral profiling and high segmentation of

[140] Mestre em Direito Civil pela Universidade de São Paulo e Advogada.

target audiences becomes a vital tool to companies in various sectors of economy. This article proposes to analyze some of the challenges and perspectives for marketing activities concerning law 13.709/2018 (the Brazilian General Data Protection Law – "LGPD"), taking in consideration especially the application of its principles and legal basis regarding such activities. With the new rule, marketing professionals are going to have to exercise their creativity in such a way as to adapt established tools such as e-mail marketing to the legal demands, but without demotivating the engagement of their target audience. Contrary to what one might think, this shift in paradigm could effectively improve database quality and bring competitiveness gain to communication agents, at the same time as it can make marketing offer more accurate and, certainly, less bothering to consumers.

Keywords: Law 13.709/2018. General Data Protection Law. Personal data protection. Privacy. Marketing.

Introdução

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – a "LGPD") definitivamente revolucionou o modo como será encarado o tratamento de dados pessoais no Brasil.

Seguindo a tendência internacional e fortemente inspirada no *Regulation (EU) 2016/679 - General Data Protection Regulation* (o "GDPR"), a LGPD implementará uma mudança de paradigma verdadeiramente cultural, a começar pela alteração na própria perspectiva da titularidade sobre os dados pessoais, que "voltam" a pertencer à pessoa natural a que se referem, e não mais às bases de dados e às empresas e agentes que os tratam.

Com a garantia de diversos direitos e prerrogativas aos titulares dos dados pessoais e o estabelecimento de regras (especialmente as hipóteses expressas e restritas de bases legais para tratamento de dados) e (o mais importante) a imposição de severas sanções aos agentes que tratam esses dados, a LGPD tutela, em última medida, os direitos fundamentais de liberdade e de privacidade e do livre desenvolvimento da personalidade da pessoa natural, objetivos previstos em seu artigo 1º.

A despeito das perspectivas extremamente positivas que desde logo podem ser vislumbradas com a regulamentação do uso de dados pessoais trazida pela LGPD, é certo, por outro lado, que, em razão de seu caráter altamente principiológico e dos diversos preceitos abertos que contempla, a LGPD traz consigo um grande desafio de implementação prática, cujo enfrentamento não poderá se dar isoladamente pelos operadores do direito, mas sim pela união destes com os profissionais de tecnologia, com os próprios agentes que passarão a ser regulados e, especialmente, com o amparo da Autoridade Nacional de Proteção de Dados (ANPD).

Numa época em que não se pode mais imaginar viver sem comércio eletrônico, e-mail, ferramentas de mensagens instantâneas e redes sociais, o marketing digital baseado em perfis comportamentais e em alta segmentação de públicos-alvo torna-se ferramenta absolutamente vital a empresas dos mais diversos segmentos da economia.

Com a entrada em vigor da LGPD, tal setor certamente será afetado e deverá ter respostas e ações para diversas questões envolvendo a aplicabilidade prática da LGPD, desde o enquadramento nos princípios e bases legais para o tratamento de dados pessoais para fins de marketing (sobre os quais comentaremos a seguir), até o uso de bases de dados pessoais legadas anteriores à LGPD (aspecto que comportaria reflexão e debate à parte[141]) e a própria caracterização de agentes de marketing como controladores ou operadores de dados pessoais (tema que, por si só, também demandaria outro debate[142]).

A partir do novo *mindset* de *privacy by design* (desde a concepção do projeto ou atividade) e *privacy by default* (privacidade por padrão), os profissionais do marketing precisarão exercitar, agora mais do que nunca, sua criatividade, de modo a adaptar ferramentas já consagradas, como o e-mail marketing, às exigências legais, sem desmotivar o engajamento de seu público-alvo.

Ao contrário do que se possa pensar, essa mudança de paradigma poderá efetivamente melhorar a qualidade das bases de dados e trazer ganhos de competitividade aos agentes da comunicação, ao mesmo tempo em que a oferta de marketing aos consumidores se tornará mais precisa e, certamente, menos incômoda.

1. Os princípios sob a ótica do marketing

Como já salientado acima, dados pessoais são um ativo valioso na sociedade atual e as atividades de marketing, mais do que quaisquer outras, dependem intimamente do tratamento de dados pessoais e das suas bases de dados, que abarcam os seus vários clientes, leads[143] e contatos obtidos das mais diversas formas, além de bases de perfis comportamentais, que permitem a segmentação de campanhas e o melhor direcionamento de produtos e serviços de forma personalizada. Essa realidade não será (e nem precisa ser) extinta pela LGPD.

[141] Vide aliás, disposição da própria LGPD que determina que caberá à ANPD estabelecer normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados (artigo 63).

[142] E de tão amplo já foi inclusive objeto de parecer do Article 29 Working Party. **Opinion 1/2010 on the concepts of "controller" and "processor".** Disponível em: Acesso em: 8 dez 2019.

[143] "*Lead* – uma informação ou contato que pode derradeiramente se transformar numa transação de venda" (SILVA, 1976, p. 123)

O que ocorre é que partir da LGPD, as ações de marketing precisarão ser repensadas e reestruturadas de maneira a se garantir a sua conformidade legal, o que já começa com a incidência dos princípios legais elencados em seu artigo 6º.

Segundo o princípio da finalidade (LGPD, art. 6º, I), o tratamento dos dados pessoais deve se dar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Sendo assim, a captação de bases de dados para posterior uso para finalidades diferentes daquelas que motivaram a coleta e até mesmo a compra de bases de dados de terceiros (prática outrora comum no segmento da comunicação e do marketing) passarão a ser práticas irregulares perante a LGPD.

Pelo princípio da necessidade, o tratamento de dados pessoais deve se restringir ao mínimo necessário para a realização das finalidades do agente, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III). Por conseguinte, não se poderá mais adotar como prática a coleta de inúmeros dados para simples guarda e futura definição de propósitos para seu uso. Todo dado coletado terá uma finalidade previamente determinada. Para a realização de um cadastro em uma plataforma de e-commerce, por exemplo, enquanto dados como nome, CPF e endereço serão considerados necessários, a profissão e o grau de escolaridade do usuário podem não o ser. Cada agente deverá analisar, casuisticamente, a pertinência dos dados que coleta.

Em observância ao princípio da transparência (LGPD, art. 6º, VI), a finalidade deverá ser informada ao titular dos dados previamente à coleta do dado, já que o titular tem direito à prestação de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Dessa forma, muitas políticas de privacidade e avisos de *cookies* de websites comportarão revisão jurídica, especialmente no que concerne ao uso de dados no âmbito do marketing, mas desafiadora mesmo será a prestação de informações aos titulares nos casos de coleta de dados em meios físicos, assim como eventos e feiras que recolham fichas de interesse em produtos, ou ainda em pontos físicos de vendas, lojas físicas, dentre outros.

Ainda, por conta do princípio do livre acesso (LGPD, art. 6º, IV), os titulares poderão ter acesso aos dados pessoais coletados e tratados pelas agências de marketing, as quais, por sua vez, deverão estar tecnicamente preparadas e amparadas para oferecer tais informações de modo célere aos titulares. Daí a importância da adequação das bases de dados pessoais por meio de tecnologias e softwares que permitam catalogar os dados de maneira ordenada, assim permitindo a sua categorização e utilização em observância à base legal de tratamento, ao período de guarda específico para a situação, às finalidades específicas de cada dado e ao exercício de direitos pelos usuários (solicitações de exclusão, pedidos de informação, portabilidade, dentre outros). Os agentes de marketing, em seu atual *modus operandi* de

fácil circulação e obtenção de dados, muito provavelmente não dispõem desse nível preparo, e precisarão se adequar.

Por fim, a forma de coleta de dados também precisará ser refletida. Isso porque é irrelevante se o dado pessoal é coletado pelo agente de tratamento de forma ativa (isto é, o dado foi fornecido expressamente pelo titular) ou passiva (o dado foi coletado pelo agente sem ação direta do titular ou foi até mesmo criado por meio de cruzamentos e análises feitas pelo próprio agente de tratamento).

São igualmente objeto de proteção pela LGPD tanto as informações que um titular de dados preenche em um formulário de cadastro, como aquelas coletadas indiretamente por tecnologias de rastreamento como *cookies*[144] e até mesmo um perfil de consumo traçado por empresas pelo cruzamento de outros dados anteriormente obtidos. Dada a importância dos perfis comportamentais para os agentes de marketing, será necessária atenção redobrada no adequado esclarecimento aos titulares acerca das formas de coleta utilizadas e especialmente sobre elaboração e utilização de perfis comportamentais.

Por conseguinte, também deverão ser revistas as tecnologias de rastreamento empregadas online, bem como criadas políticas de informação claras sobre o seu uso aos titulares dos dados. Tais tecnologias e as ferramentas que elas viabilizam são cruciais para as ações de marketing (a exemplo de ferramentas como anúncios patrocinados em sites e redes sociais), mas não precisam ser descontinuadas, desde que a coleta originária dos dados tenha obedecido aos ditames da LGPD para tais finalidades.

2. Bases legais de tratamento de dados pessoais aplicáveis à atividade de marketing

2.1. Consentimento

Para além da aplicação dos princípios da LGPD, outro ponto crucial para o tratamento de dados pessoais no âmbito das atividades de marketing será a base legal que legitimará esse tratamento sob a vigência da LGPD.

A primeira e mais evidente base legal aplicável no caso do marketing seria o consentimento, que vem sendo na maioria das vezes apontada em primeiro lugar (apesar de ser apenas uma das bases legais previstas pela LGPD) especialmente por apresentar alto grau de transparência perante o titular e, por consequência, acabar trazendo maior segurança jurídica aos agentes de tratamento, segundo pontuam Maldonado e Blum (2019, p. 117).

[144] *Cookies* são pequenos arquivos catalogados que são arquivados nos diretórios dos navegadores de internet ou pastas de dados de programas, pelos quais se pode rastrear os movimentos do usuário dentro de um website, permitindo, por exemplo, customização de preferências, memorização de buscas, manutenção de produtos em carrinho de compras, dentre outras finalidades. Disponível em: <https://www.allaboutcookies/>. Acesso em: 08 dez 2019.

O fato é que a maneira como o consentimento é colhido no caso do marketing certamente comportará revisão, afinal quão comum tem sido a prática de envio de e-mail marketing a bases de dados de parceiros comerciais com os quais o titular jamais teve relacionamento algum?

A simples menção à possibilidade de *opt-out* passará a ser insuficiente para atender aos ditames da LGPD. Sob a vigência da lei, o "li e concordo" não será mais mero formalismo vazio. A LGPD impõe diversos requisitos para que o consentimento seja considerado válido, especialmente que tenha sido fornecido de forma livre, informada e inequívoca (LGPD, art. 5º, XII).

Assim, para garantir a liberdade de consentir, tem-se sugerido a aplicação da chamada "granularização" do consentimento (MALDONADO; BLUM, 2019), que significa a possibilidade de consentir separadamente para algumas finalidades e operações, mas para outras não. A recomendação vem do Considerando de nº 43 do GDPR (2016, p. 8):

> (43) [...] Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Um exemplo de consentimento granulado no âmbito do marketing seria a realização de um cadastro em website (portal de notícias, por exemplo), com as opções separadas de *checkboxes* para aceite quanto ao recebimento de newsletter periódica e ao recebimento de ofertas de produtos e serviços do provedor e/ou de seus parceiros.

Já para garantir que o consentimento seja informado, uma política de privacidade clara e completa deve ser disponibilizada de forma prévia à aposição dos dados pessoais pelo titular e antes de qualquer prosseguimento do cadastro. Muito tem-se visto (especialmente em websites europeus, após a entrada em vigor do GDPR) a prática do impedimento de prosseguimento no cadastro e navegação em websites antes que seja feita a rolagem da política de privacidade até o seu final pelo usuário e o clique no *checkbox*, ou mesmo a aceitação/alteração da política de cookies, sem a qual o site é impedido de funcionar.

Finalmente, para garantir que o consentimento seja inequívoco, já se tem visto a prática em websites de se evitar os *checkboxes* "li e concordo" pré-marcados com o aceite, de modo que o titular seja obrigado a adotar uma conduta ativa de clicar e só assim manifestar consentimento positivo e inequívoco.

Outro desafio (técnico, sobretudo) de utilização da base legal do consentimento é a gestão e guarda das manifestações de consentimento dos titulares, sobretudo porque o ônus da prova da obtenção de

consentimento válido é do controlador (LGPD, art. 8º, §2º). Assim, não basta mais a coleta do aceite, é necessário que o controlador tenha condições de demonstrar sua ocasião temporal e material (data e informações de identificação de usuário), as informações prestadas quando fornecido, bem como a conduta positiva e inequívoca do titular. Os agentes de marketing precisarão, portanto, investir em ferramentas de tecnologia que permitam operacionalizar a gestão e guarda do consentimento dos titulares atingidos por suas campanhas.

2.2. Legítimo interesse

Além da base legal do consentimento, também seria possível o enquadramento do tratamento de dados pessoais realizado pelo marketing sob a base legal do legítimo interesse (LGPD, art. 7º, IX, e art. 10), como sendo uma hipótese de "apoio e promoção de atividades do controlador".

Lembre-se, todavia, que o legítimo interesse é uma base legal subsidiária e não deve ser a primeira opção em atividade alguma. Por se tratar de uma hipótese de conceito aberto (e, portanto, muito mais propensa a abusos), a própria LGPD já lhe estabeleceu restrições, impondo que esse interesse seja sempre considerado em situações concretas, devendo ser tratados apenas os dados estritamente necessários à finalidade pretendida, ser garantida a transparência do tratamento perante o titular e ser mantido registro das operações de tratamento (LGPD, art. 10 e 37).

De qualquer forma, a necessidade de adoção dessa base legal para as atividades de marketing estaria fundada na tentativa de não se inviabilizar a o marketing por completo ou mesmo criar-lhe uma dificuldade excessiva – o que poderia ocorrer caso a única base legal passível de aplicação ao tratamento de dados pessoais realizado pelo marketing fosse o consentimento, hipótese em que os agentes de tratamento ficariam sujeitos exclusivamente ao arbítrio dos titulares dos dados e não poderiam mais contatá-los sem o seu consentimento expresso e específico.

Por isso, verifica-se o surgimento de uma tendência para a adoção da base legal do legítimo interesse para as atividades de marketing, tanto no direito brasileiro (MALDONADO; BLUM, 2019) como sob o GDPR.

Contudo, uma das principais preocupações do tratamento de dados pessoais sob a base legal do legítimo interesse é o caráter extremamente vago e amplo do conceito. Autoridades de proteção de dados estrangeiras têm buscado trazer maior concretude interpretativa, a exemplo da ICO (UK)[145], que propõe um teste de três partes a ser realizado no caso concreto, sempre que se pretender aplicar a base do legítimo interesse a alguma operação de tratamento de dados pessoais: identificar um interesse legítimo,

[145] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/>. Acesso em: 10 out. 2019.

demonstrar que o tratamento de dados pessoais é necessário para atingi-lo e fazer o balanceamento desse tratamento em face dos direitos, liberdades e interesses do titular dos dados.

Da mesma maneira, em opinião exarada pelo *Article 29 Working Party*[146], ainda com relação à aplicação do conceito de legítimo interesse sob a Diretiva 95/46/EC da UE, já se mencionava como um dos principais contextos nos quais a questão do legítimo interesse poderia ser levantada como sendo as atividades de marketing e propaganda. Entretanto, ainda assim se deveria ponderar se, no caso concreto, o interesse do controlador deveria prevalecer sobre o interesse do titular dos dados.

Conclusão

Como se pôde perceber ao longo desta brevíssima exposição, são diversos os desafios de aplicabilidade da LGPD ao marketing. Buscou-se, não obstante, colocar em perspectiva o que se pode esperar a partir da entrada em vigor da lei no setor de marketing, um dos mais diretamente afetados pela regulamentação, dada a sua dependência intrínseca do tratamento de dados pessoais.

Buscou-se, dessa forma, analisar a incidência dos princípios da LGPD à atividade de marketing, demonstrando alguns (dentre os diversos) impactos na própria forma de se fazer marketing, tendo sempre em mente os conceitos de *privacy by design* e *privacy by default*.

Verificou-se, ainda, que o enquadramento das atividades de marketing nas bases legais da LGPD também será desafiador e demandará um esforço conjunto, não somente da ANPD, dos estudiosos do tema e operadores do direito e de tecnologia, mas também dos próprios empresários e titulares dos dados. A experiência europeia certamente será um parâmetro, mas deve ser sopesada com a realidade local e a *mens legis* própria e peculiar da legislação pátria.

O campo interpretativo deixado pela lei é vasto e, ao mesmo tempo em que se devem evitar abusos, é necessário propiciar segurança jurídica aos agentes de tratamento (especialmente do setor de marketing para os quais o tratamento (legal) de dados pessoais é vital).

Por outro lado, a partir do momento em que a LGPD comece a se solidificar no âmbito prático, também é certo que a conformidade legal propiciará bases de dados muito mais qualificadas e *leads* muito mais engajados e interessados com os produtos e serviços oferecidos. Muito mais que simplesmente cumprir

[146] Grupo de trabalho composto por representantes das autoridades de proteção de dados dos países-membro da União Europeia, da Comissão Europeia e da *European Data Protection Supervisor*, com atuação consultiva. A partir do GDPR, foi substituído pela *European Data Protection Board*. Disponível em: <https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents/>. Acesso em: 08 dez 2019.

uma obrigação legal, os agentes de marketing em conformidade com a LGPD certamente agregarão valor ao seu serviço e terão diferencial competitivo no mercado.

Referências bibliográficas

All About Computer Cookies. What are cookies in computers? Disponível em: <https://www.allaboutcookies.org/cookies/>. Acesso em: 08 dez 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 out. 2019.

EUROPEAN UNION (EU). **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).** Disponível em: <https://eurlex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 08 dez 2019.

EUROPEAN UNION (EU). **ARTICLE 29 DATA PROTECTION WORKING PARTY.** Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em: <https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> Acesso em: 08 dez 2019.

INFORMATION COMISSIONER'S OFFICE (ICO). **When can we rely on legitimate interests?** Disponível em: <https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/whencan-we-rely-on-legitimate-interests/> Acesso em: 10 out. 2019.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP). **All of the Article 29 Working Party guidelines, opinions, and documents.** Disponível em: <https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinionsand-documents/>. Acesso em: 08 dez 2019.

MALDONADO. Viviane Nóbrega; BLUM, Renato Ópice. **LGPD – Lei Geral de Proteção de Dados Comentada.** São Paulo: Revista dos Tribunais, 2019.

SILVA, Zander Campos da. **Dicionário de Marketing e Propaganda.** Rio de Janeiro: Pallas, 1976.

6.5. Internet das Coisas e privacidade: o tratamento e a comercialização de dados pessoais no ciberespaço – *Bruna Bastos*[147], *Eduardo Missau Ruviaro*[148] *& Rafael Santos de Oliveira*[149]

Resumo

O desenvolvimento da internet enquanto ferramenta capaz de conectar o mundo dentro do ciberespaço revolucionou o modo como a sociedade visualiza a própria privacidade, especialmente ao se pensar em todos os dados fornecidos diariamente pelos usuários em tempos de *web 3.0*. A Internet das Coisas é exemplo dessa nova realidade constituída no mundo virtual, onde objetos antes desconectados aparecem *online* para facilitar a vida dos consumidores. Contudo, alguns perigos podem surgir no estudo de como esses dados são tratados e comercializados pelas empresas desenvolvedoras desses objetos conectados à internet. Assim, cumpre indagar: quais os limites e as possibilidades de se buscar uma regulamentação ao tratamento e à comercialização de dados pessoais em tempos de Internet das Coisas? Para responder ao problema de pesquisa, utiliza-se o método dedutivo para a abordagem, e a pesquisa bibliográfica e documental para o procedimento, tendo em vista o objetivo geral deste trabalho, que é analisar o fenômeno da Internet das Coisas sob a ótica do tratamento e da comercialização dos dados pessoais que são disponibilizados *online* pelos usuários e os impactos negativos que essa estrutura pode causar. Dessa forma, é possível concluir que é necessária uma nova regulamentação que garanta transparência e segurança aos dados pessoais e à privacidade dos usuários, além de um posicionamento positivo das empresas desenvolvedoras no sentido de garantir a segurança dos seus usuários diante das possíveis ameaças que uma quebra desses padrões pode gerar aos dados pessoais.

Palavras-chave: *Big Data*; dados pessoais; Internet das Coisas; privacidade; *software*.

Abstract

The development of internet as a tool capable of connecting the world within the cyberspace revolutionized the way society sees its own privacy, specially when it comes to all the data available

[147] Mestranda do Programa de Pós-graduação em Direito da Universidade Federal de Santa Maria, em Santa Maria, no Rio Grande do Sul, com bolsa CAPES, e pesquisadora do Centro de Estudos e Pesquisa em Direito e Internet.

[148] Mestrando do Programa de Pós-graduação em Direito da Universidade Federal de Santa Maria, em Santa Maria, no Rio Grande do Sul, e pesquisador do Centro de Estudos e Pesquisa em Direito e Internet.

[149] Doutor em Direito pela Universidade Federal de Santa Catarina. Professor do Programa de Pós-graduação em Direito da Universidade Federal de Santa Maria. Coordenador do Centro de Estudos e Pesquisa em Direito e Internet.

everyday by users in times of web 3.0. The Internet of Things is an example of this new reality constituted inside the virtual world, where objects not connected show up online to make life easier. However, some dangers may appear when studying how the data is treated and commercialized by developer companies of these objects connected online. So, it's possible to ask: what are the limits and possibilities of searching for a regulation to treat and commercialize personal data in times of Internet of Things? To answer the research problem, it's used the deductive method to the approach, and the bibliographical and documental research for the procedure, considering that the main objective is to analyze the Internet of Things as a phenomenon from the treatment and the commercialization of personal data available *online* by users and the negative impacts that this structure may cause. It's possible to conclude that a new regulation is needed to ensure transparency and safety to personal data and users' privacy, as well as a positive position of developer companies in a way to make sure their consumers have security in front of the threats that a breach can cause to personal data.
Keywords: Big data. Personal data. Internet of Things. Privacy. Software.

Introdução

Com o surgimento da rede mundial de computadores, notam-se inúmeros benefícios à vida daqueles que a utilizam. Desde a democratização da comunicação até o fortalecimento de movimentos sociais, a Internet conectou pessoas e, consequentemente, aparelhos, tornando um mundo desconectado em uma tríade de atores virtuais. Os telefones, portanto, passaram a ser conectados à *web*, assim como os veículos, as cafeteiras e outros objetivos que, antes, estavam desconectados. Esse fenômeno da conexão de tudo é denominado Internet das Coisas (*IoT*), e pode garantir grandes inovações tecnológicas aos habitantes do ciberespaço.

Por outro lado, aquelas relações humanas *off-line*, que outrora desconectadas não possuíam o âmago de produzir dados, ao passar a ser parte do mundo digital, tornaram-se objeto de cobiça das aplicações que fazem parte da Internet das Coisas. Por essa razão, no Brasil, fora editada a Lei n. 13.709, visando regulamentar o ciberespaço no que toca à proteção de dados pessoais daqueles que navegam no mundo *on-line*. Dessa forma, a proteção de dados pessoais é premissa emergente dos direitos da sociedade em rede, razão pela qual é importante que se discuta o tratamento conferido aos dados e informações pessoais que são disponibilizados todos os dias pelos usuários desses objetos conectados à internet.

Assim, cumpre indagar: quais os limites e as possibilidades de se buscar uma regulamentação ao tratamento e à comercialização de dados pessoais em tempos de Internet das Coisas? Como objetivo geral, portanto, almejou-se revisar o fenômeno da Internet das Coisas e a proteção de dados pessoais que a circunda. Por sua vez, como objetivos específicos buscou-se descrever o fenômeno da Internet das Coisas, revisar eventuais violações à proteção de dados pessoais através de aplicações de Internet das Coisas e, por último, quis-se responder especificamente ao problema de pesquisa para entender os aspectos referentes ao tratamento e à comercialização de dados pessoais diante dessa realidade virtual.

Essa pesquisa, a partir da obra Internet das Coisas, de Eduardo Magrani, orientou-se pelo método de abordagem dedutivo, uma vez que se buscou revisitar a Internet das Coisas e a proteção de dados pessoais no ciberespaço, a fim de demonstrar como, por um lado, o que se chama de IoT representa uma avanço tecnológico e de inovação para a sociedade, ao passo em que, por outro lado, a proteção de dados pessoais pode ser violada pelos institutos que se valem da Internet das Coisas, tanto através do tratamento desses dados quanto pela comercialização indevida.

Como método de procedimento, valeu-se do bibliográfico, a fim de consultar a doutrina escrita sobre Internet das Coisas e proteção de dados pessoais, e documental, para que se analisasse efetivamente a cessão de dados pessoais através das aplicações de IoT, bem como a legislação brasileira que regulamenta a matéria. Para tanto, utiliza-se das técnicas de pesquisa de confecção de fichamentos e resumos de livros e produção de tabelas dos documentos estudados.

Desenvolvimento

A Internet é instrumento que se modifica diariamente na medida em que, a cada dia que passa, novas aplicações conectadas à rede mundial de computadores surgem para suprir inovadoras demandas da sociedade do ciberespaço. Contudo, mesmo que hoje seja utilizada para as mais variadas tarefas da sociedade civil, nem sempre a Internet fora acessível à população de modo geral – o que remonta especialmente ao seu surgimento. Conforme refere Manuel Castells, "a história da criação e do desenvolvimento da Internet é a história de uma aventura humana extraordinária" (2003, p. 13).

E é nessa teia de aventura que a *web*, já membro da sociedade civil organizada, passou por diversas eras, desde o que se concebeu por *web 1.0* até a *web 3.0*, o atual estado da arte da sociedade em rede. A primeira era da Internet, conhecida como *web 1.0*, dava conta de que a rede mundial de computadores servia como uma "ferramenta exclusiva para leitura e formação de cognição", segundo tradução livre de Fuchs, Hofkirchner, Schafranekm Rafflm Sandoval e Bichler (2010, s/p), ou seja, um instrumento de busca, sem a participação da sociedade. A segunda era da Internet, por sua vez, foi definida, pelos autores anteriormente mencionados, como uma *web* de leitura e escrita (2010, s/p), na qual os atores do ciberespaço poderiam, além de colher informações e formar sua convicção, estruturar a arquitetura da Internet. A *web 3.0*, terceira era da Internet, é chamada de *web* semântica porque possui como característica "a inserção e consolidação da tecnologia da inteligência artificial, *machine learning* e algoritmos de personalização baseados na coleta de dados pessoais do usuário na experiência de navegação" (SANGOI, 2019, p. 29). E é aqui, na *web 3.0*, que se insere o fenômeno da Internet das Coisas (*Internet of Things* – IoT).

Em que pese não haver um conceito único para IoT, Eduardo Magrani (2018) qualifica o termo como sendo

> um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de imputação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade. (MAGRANI, 2018, p. 20).

A Internet das Coisas, portanto, nada mais é do que a hiperconectividade de dispositivos entrelaçados com o fito de que, ligados à Internet, executem tarefas de forma automatizada para criar facilidades no cotidiano das pessoas. Eduardo Magrani (2018, p. 21) ainda afirma que hiperconectividade significa o "estado de disponibilidade dos indivíduos para se comunicar a qualquer momento". Ocorre que não são apenas os indivíduos que estão conectados, mas também as máquinas, uma vez que, para que a IoT opere, necessariamente deve haver a comunicação entre indivíduos e máquinas (*human-to-machine*, H2M, ao se ordenar um comando ao computador para que este se programe a executar uma tarefa) e entre máquinas com máquinas (*machine-to-machine*, M2M, ao entrelaçar dados e executar tarefas de forma automatizada e inteligente).

Nesse sentido, André Lemos e Elias Bitencourt (2018, s/p) chamam de sensibilidade performativa o que entendem ser "uma das características essenciais dos sistemas de IoT" (LEMOS; JESUS, 2017, p. 68). Parafraseando os autores, Lemos e Jesus (2017, p. 68) dizem que

> os novos objetos dotados de qualidade infocomunicacioais são sencientes e produzem, a partir de uma sensibilidade eletrônica, agências algorítmicas complexas em uma rede ampla. Assim, por exemplo, as lixeiras inteligentes de Dublin [...] podem saber quando estão cheias, avisar os poderes públicos, montar a rota de coleta e servir como instrumento de discursos sobre eficiência, melhoria da limpeza urbana e da qualidade de vida.

Dessa forma, a expressão IoT "é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à internet" (MAGRANI, 2019, p. 44). Daí o termo *Internet* associado ao termo *das coisas*, porque as coisas (objetos, itens, instrumentos), que anteriormente eram analógicas, *off-lines*, passaram a compor o ciberespaço conectados à rede mundial de computadores. A sigla IoT refere-se a um mundo onde coisas e seres humanos interagem uns com os outros durante todo o tempo e em

qualquer espaço (NASCIMENTO, 2015, s/p), e fora alcunhada por Kevin Ashton, do *Massachusetts Institute of Technology*, em 1999. De acordo com Ashton (2009), em publicação ao RFID Journal, as pessoas necessitam estar conectadas à Internet das mais variadas formas, devido à falta de tempo para realizarem tarefas mais simples do cotidiano, o que é delegado aos aplicativos que se utilizam da Internet das Coisas. A IoT, quando criada, portanto, veio a ser um instrumento facilitador do cotidiano de seus usuários. (ASHTON, 2009, s/p)

Dessa forma, vários são os exemplos de aplicações conectadas à Internet das Coisas. Desde *smart cities* até cafeteiras que programam o café sozinhas, passando por casas inteligentes auxiliadas por dispositivos como Alexa e Google Home, a Internet das Coisas é um grande emaranhado de encantadores apoiadores da vida humana. Esses exemplos demonstram como a Internet das Coisas pode ser enfrentada como um fenômeno hábil a trazer maior conforto a seus usuários. Fato é que se trata de inegável avanço tecnológico, inovação que fora criada para auxiliar aqueles que a utilizam. Através da IoT, como demonstrado, a administração pública pode tornar mais eficiente a prestação de seu serviço, através da implementação de cidades inteligentes, retificando eventuais problemas de trânsito e evitando catástrofes ambientais. Na iniciativa privada, por sua vez, a conexão de dispositivos à rede é capaz de destacar quais são as reais necessidades dos consumidores, a fim de que se otimize a prestação de serviço e a criação de produtos pelas empresas. Já no âmbito individual, os carros inteligentes, a exemplo da Tesla Motors, podem garantir maior segurança e conforto aos seus motoristas e passageiros, na medida em que automatiza a tomada de algumas decisões, como o acondicionamento da temperatura interna do veículo, evitando que conforto excessivo gere ligeira desatenção ao motorista.

Entretanto, como bem refere Eduardo Magrani ao parafrasear Jeff Jarmoc[150], "a Internet foi projetada para resistir a uma explosão nuclear. Mas não a um ataque de torradeiras" (2018, p. 31). Por essa razão, em que pese garantir inúmeras utilidades, a IoT possui seu lado sombrio: a violação à proteção de dados pessoais. Nesse sentido, atento à preocupação com os dados pessoais depositados e tratados na Internet, Magrani aponta para um estudo realizado pela Universidade de Harvard, no ano de 2015, sobre o desafio central do Brasil envolvendo o desenvolvimento de IoT (2018, p. 77).

Nessa investigação, publicada na *Harvard Business Review*, os investigadores concluíram que o mais importante entrave ao Brasil frente à Internet das Coisas permeia o que eles nomearam de capacidade nacional de absorção (PURDY, DAVARZARI, OVANESSOF, 2015, s/p). Dentre os índices utilizados para medir a capacidade nacional de absorção de cada país, há também a ética na utilização

[150] A frase originalmente fora editada por Jeff Jarmoc, em sua conta na rede social Twitter. No original, disse Jarmoc que "in a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters". Disponível em: https://twitter.com/jjarmoc/status/789637654711267328?lang=pt. Acesso em: 15 jun. 2019.

de dados pessoais dos usuários. E, conforme diz Magrani, "a CNA do Brasil é bastante insatisfatória" (2018, p. 78). Isso ocorre porque "as empresas não conseguiram garantir suficientemente a segurança e a privacidade dos dados com a mesma velocidade e empenho com que vêm desenvolvendo os dispositivos de IoT" (MAGRANI, 2018, p. 92).

A conta é fácil: ao navegar na rede mundial de computadores, obrigatoriamente o internauta produz rastros. Tudo o que se faz na rede deixa vestígios, que também são conhecidos como dados e que englobam o que se chama de *big data*. Magrani diz que "todos os dias, as coisas se conectam à internet com capacidade para compartilhar, processar, armazenar e analisar um volume enorme de dados entre si" (MAGRANI, 2018, p. 22) e que essa prática é o que "une o conceito de IoT ao de big data (MAGRANI, 2018, p. 22). Mas o que se faz com o tratamento de dados pessoais capturados através da Internet das Coisas?

Um dos grandes perigos de se utilizar indiscriminadamente a Internet das Coisas, e o que fez o Brasil editar e aprovar a Lei Geral de Proteção de Dados no ano de 2018, é o tratamento e a comercialização de dados pessoais pelas empresas que detêm sítios eletrônicos. Danilo Doneda (*apud* FACHIN, 2018, p. 3), pesquisador brasileiro sobre a temática da privacidade na internet, referiu em entrevista recente que "o tratamento de dados é algo que acontece fora da vista das pessoas, ou seja, os dados são coletados, tratados e utilizados por alguém de forma que não é possível fiscalizar diretamente". Dessa forma, a comercialização desses dados se constitui como conduta capaz de ferir a privacidade, tendo em vista que importa "a revelação de informações que a pessoa não queria divulgar". (FACHIN, 2018)

Em tempos de redes sociais, muitas plataformas utilizam-se dos termos de uso e das políticas de privacidade para receber autorização para tratar os dados fornecidos, voluntária ou inconscientemente, pelos usuários, de modo que tudo o que é feito *online* pode ser utilizado pelas empresas que compram esses dados para fornecer serviços e anúncios direcionados aos gostos e opiniões de quem está acessando aquele conteúdo. (DONEDA, 2006) Contudo, quando esse panorama é transferido para a realidade da Internet das Coisas, "essa interconectividade pode acarretar uma vasta gama de problemas e questões discutíveis, entre as quais as fragilidades em relação à privacidade e à segurança dos usuários". (MAGRANI, 2018, p. 91)

O que se percebe ao analisar os dispositivos de IoT e as empresas que desenvolvem essa tecnologia é que os próprios desenvolvedores não têm muita certeza do que fazer em termos de segurança para o usuário dos produtos – tanto em relação aos dados gerados por eles quanto no tocante a possíveis violações dos

dispositivos de segurança naturalmente instalados (diante da notória vulnerabilidade de *softwares* a *hackers*[151], por exemplo). (MAGRANI, 2018)

> O desafio da segurança de dados no cenário de IoT também envolve dar enfoque a questões como gestão de armazenamento, servidores e redes de *data center*, bem como à responsabilidade de cada empresa que opere nessa cadeia de produtos e serviços. Isso decorre do crescimento da quantidade dos dispositivos conectados, o que aumenta o volume de dados capturados e de operadores que atuam nessa cadeia econômica. Tendo em vista que a IoT abrange diversos setores, alguns delicados, como saúde e meio ambiente, isso nos faz crer que deverão surgir novos desafios de segurança envolvendo o grande fluxo de dados, sendo necessário acompanhar a complexidade da segurança no tratamento de *big data.* (MAGRANI, 2018, p. 92)

O tratamento e comercialização de dados pessoais disponibilizados pelos usuários através da internet foi o que possibilitou o crescimento da Google no ambiente virtual, tendo em vista que seu negócio é essencialmente publicitário. Isso porque o Google capta e armazena informações pessoais e conteúdo criativo dos seus milhões de usuários todos os dias, e vende essa informação a empresas que desejam anunciar na sua página, adequando o conteúdo que aparece para cada usuário de acordo com o perfil e os gostos que a pessoa explicita *online* e fornecendo as informações que são requisitadas no buscador. Isso significa dizer que o Google lucra com a venda de dados dos seus usuários (VAIDHYANATHAN, 2011).

Nesse sentido, tendo em vista que os dados pessoais são algo bastante importante para o funcionamento da internet das coisas, que depende muito de inteligência artificial e alimentação dos dados, a rentabilidade da grande produção de dados é imperativa. Os dados, nesse diapasão, comportam-se como verdadeiras *commodities*, ou seja, bem comercializável no ambiente digital. E esse comércio é desempenhado sobretudo pelas grandes aplicações da rede. E, diante desse cenário de rentabilidade na comercialização de dados, a relação entre privacidade e IoT pode ficar um pouco mais complexa. (DONEDA, 2006)

É possível visualizar o perigo dessas incertezas a partir de um exemplo de IoT dado anteriormente nesse trabalho: o Google Home, que permite pensar em uma residência assessorada por esse aplicativo, onde

[151] "Pesquisas recentes sobre o tema demonstram graves falhas de segurança em aparelhos ligados a IoT. A HP Security Research detectou que 70% dos dispositivos têm falhas de segurança, estando propensos a ataque de *hackers*". (MAGRANI, 2018, p. 93)

todos os dispositivos (como geladeira, televisão, computador, ar condicionado) estão conectados à internet e ao automóvel da família, de modo que tudo começa a funcionar de forma sincronizada quando todos se dirigem para casa depois do trabalho. A quantidade de dados produzidos por esses aparelhos é infinita, desde questões mais simples relacionadas à temperatura ambiente até aspectos complexos, como o horário em que a residência fica vazia.

> As possibilidades de hackeamento de veículos são múltiplas. Pode ocorrer de forma geral ou direcionada (com acesso interno ou remoto), em milhares de automóveis ou apenas em um determinado, podendo também ser direcionado a sistema específicos destes. [...] Alguns casos podem ser citados, como [...] a descoberta de que as *smart TVs* da Samsung capturavam as conversas pessoais dos usuários utilizando sua funcionalidade de ativação por voz e coletavam o histórico de programas assistidos, tudo isso sem a permissão do consumidor. (MAGRANI, 2018, p. 94)

E não é necessário pensar em eventuais quebras dos padrões de segurança desses equipamentos, ou invasões da rede de internet do local para extrair informações dos dispositivos, ou ainda de como diversas empresas conseguem ativar as câmeras e os microfones dos aparelhos celulares remotamente (VAIDHYANATHAN, 2011). Pensando no exemplo da área da saúde trazida por Eduardo Magrani (2018, p. 92), o perigo na comercialização desses dados reside na possibilidade de eles serem adquiridos por empresas que irão mapear a qualidade de vida do consumidor para aumentar ou reduzir o preço dos planos de saúde. Ainda, é possível visualizar a comercialização de dados de automóveis, como velocidade média, para deliberar o preço do seguro do veículo.

A verdade é que a Internet das Coisas, por abarcar muitos dispositivos e conectá-los à internet, gera muito mais dados pessoais do que as atuais redes sociais e aplicativos de celular. Magrani (2018) identifica diversos riscos para o usuário desses produtos, como identificação, rastreamento, dossiês de informações e, por último, mudanças no controle da própria tecnologia, e tudo isso ocorre mediante a coleta, o armazenamento e a venda desses dados a empresas interessadas tanto na venda de produtos e oferecimento de serviços através da publicidade quanto no uso dessas informações para formar o perfil dos consumidores.

É nesse ponto que surge a possibilidade de resposta ao problema de pesquisa proposto no presente trabalho, de modo que a regulamentação do tratamento e comercialização desses dados é uma necessidade diante dos perigos que a Internet das Coisas (e os dados coletados) pode causar para os consumidores. Mas, também, é imperioso ressaltar a importância do papel das empresas desenvolvedoras desses produtos em garantirem a segurança e a privacidade dos usuários, especialmente em tempos de uma nova estrutura social baseada na virtualidade.

Conclusão

Diante dos argumentos expostos nesse trabalho, percebeu-se que, desde seu surgimento, a *internet* teve como um de seus principais predicados auxiliar afazeres que outrora eram desconectados. Assim foi, em um primeiro momento, com os telefones e com os computadores, realidade hoje que se estende desde carros até torradeiras. Essa nova gama de produtos conectados à rede é o que se chamou Internet das Coisas, isto é, a comunicação máquina com máquina, independentemente de controle humano, que criou facilidades aos seus usuários com a contrapartida da produção e captura de seus dados pessoais.

Desta forma, com o objetivo de discutir quais são os limites e as possibilidades da regulamentação ao tratamento e à comercialização de dados pessoais em tempos de Internet das Coisas, concluiu-se que é uma necessidade diante dos perigos que a Internet das Coisas (e os dados coletados) pode causar para os consumidores, tanto em relação ao tratamento dos dados veiculados no mundo virtual quanto no que tange à comercialização desses dados para empresas de todos os ramos, além das possíveis falhas que esses dispositivos podem gerar. De igual forma, ressaltou-se a importância do papel das empresas desenvolvedoras desses produtos em garantirem a segurança e a privacidade dos usuários, especialmente em tempos de sociedade rede, onde inúmeras informações são passadas para o mundo virtual.

O presente artigo, por não possuir como propósito o exaurimento da matéria, buscou realizar uma reflexão crítica acerca da proteção de dados pessoais em tempos de Internet das Coisas, momento no qual foi possível demonstrar as facilidades e os perigos dessa nova realidade, e como o tratamento e a comercialização de dados, quando feitos de forma indiscriminada, podem acarretar prejuízos para consumidores e usuários dos objetos inseridos no contexto da Internet das Coisas. Muitas outras faces dessa relação ainda podem ser apontadas, e este trabalho foi apenas o começo de uma longa pesquisa sobre direitos emergentes do mundo virtual, contribuindo, socialmente e academicamente, para o aprofundamento da temática.

Referências bibliográficas

ASHTON, Kevin. **That 'Internet of Things' Thing**. 2009. Disponível em: https://www.rfidjournal.com/articles/view?4986. Acesso em: 08 out. 2019.

CASTELLS, Manuel. **A Galáxia da Internet:** reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

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

FACHIN, Patrícia. **A regulação de dados pessoais e a perda de controle sobre alguns aspectos da vida.** Entrevista especial com Danilo Doneda. 2018. Disponível em: http://www.ihu.unisinos.br/159-

noticias/entrevistas/578297-a-regulacao-de-dados-pessoais-e-a-perda-de-controle-sobre-alguns-aspectos-da-vida-entrevista-especial-com-danilo-doneda. Acesso em: 13 out 2019.

FUCHS, Christian et al. Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. **Future Internet**, [S.l.], v. 1, n. 2, p.41-59, fev. 2010. Disponível em: https://www.researchgate.net/publication/41667703_Theoretical_Foundations_of_the_Web_Cognition_Communication_and_Co-Operation_Towards_an_Understanding_of_Web_10_20_30. Acesso em: 07 out. 2019.

LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. http://dx.doi.org/10.29146/eco-pos.v20i3.14474.

MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018.

NASCIMENTO, Rodrigo. **O que, de fato, é internet das coisas e que revolução ela pode trazer?:** a resposta saberemos nos próximos anos, mas uma coisa é certa, uma nova revolução digital está prestes a acontecer. 2015. Disponível em: https://computerworld.com.br/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/. Acesso em: 07 out. 2019.

PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. **Como a Internet das Coisas Pode Levar à Próxima Onda de Crescimento no Brasil**. 2015. Disponível em: https://hbrbr.uol.com.br/como-a-internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/. Acesso em: 08 out. 2019.

SANGOI, Rafael Martins. **A Necessidade de Adaptação do Direito ao Tempo da Internet:** desafios e perspectivas para a cidadania digital contemporânea. 2019. 120 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação Stricto Sensu em Direito, Departamento de Ciências Sociais Aplicadas, Universidade Regional Integrada do Alto Uruguai e das Missões, Santo Ângelo, 2019.

VAIDHYANATHAN, Siva. **A Googlelização de tudo** (e por que devemos nos preocupar): a ameaça do controle total da informação por meio da maior e mais bem-sucedida empresa do mundo virtual; tradução Jeferson Luiz Camargo. São Paulo: Cultrix, 2011.

6.6. Violação da privacidade de dados pessoais para fins econômicos, de acordo com a Lei 13.709/2018 – *Guilherme Lourenço da Silva Menezes Cunha*[152] *& Joseane Isabel Becker*[153]

Resumo

O presente artigo analisa a violação dos dados pessoais, sua utilização para fins econômicos e como a Lei Geral de Proteção de Dados Pessoais tratará do assunto. Abordará também a compreensão da privacidade na era digital e os princípios que norteiam o novo texto legal.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; dados pessoais; privacidade; violação; fins econômicos.

Abstract

This article examines the violation of personal data, its use for economic purposes and how the General Data Protection Law will deal with the matter. It will also address the understanding of privacy in the digital age and the principles that guide the new legal text.

Keywords: General Data Protection Law. Personal data. Privacy. Rape. Economic purposes.

Introdução

Vivemos em uma era tecnológica em que nossos dados pessoais são coletados diariamente por diversas empresas e de várias formas, seja em um contrato assinado em qualquer esfera econômica, como, por exemplo, uma compra de um medicamento em um estabelecimento farmacêutico e, principalmente, em cadastros digitais de empresas pela internet. Nesta seara, a privacidade destes dados passou a ser violada e utilizada para fins comerciais e econômicos, tornando-se um ativo muito valioso e se transformando, nos últimos tempos, em um dos negócios mais lucrativos do planeta.

Por outro lado, estes dados são coletados, até então, sem nenhum regramento ou fiscalização que possam minimizar sua violação. Após o advento da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), que entrará em vigência no próximo ano, aumentaram as responsabilidades das empresas que coletam, armazenam, tratam e processam estes dados.

[152] Mestrando do Programa de Mestrado em Direito da Universidade Nove de Julho – UNINOVE.

[153] Mestranda do Programa de Mestrado em Direito da Universidade Nove de Julho – UNINOVE.

Desta forma, através de um estudo dedutivo e bibliográfico, serão abordados no presente artigo, os aspectos inseridos na nova legislação que tratam da proteção e não violação dos dados pessoais.

Inicialmente serão abordadas algumas noções a respeito do que são dados pessoais e como vem explicitado na Lei Geral de Proteção de Dados Pessoais. Após, será demonstrada a vulnerabilidade da privacidade na era da comunicação, onde ataques cibernéticos, mau uso dos dados coletados e até a má fé de grandes empresas, violam cada vez mais a privacidade e intimidade dos dados pessoais, causando, por diversas vezes, situações constrangedoras e até ações criminosas contra os cidadãos, que estão vulneráveis a estas práticas.

Em um segundo momento, será exposta uma breve explanação sobre como os dados pessoais se tornaram uma fonte de riqueza e um importante ativo para as grandes empresas.

E, por fim, será tratado dos princípios fundamentais que norteiam o novo texto legal.

Assim, o presente artigo tentará elucidar se a nova legislação terá eficácia no combate ao mau uso dos dados pessoais para fins econômicos.

1. Dados pessoais

Quando abordamos a questão referente a dados pessoais, importante descrever o que é considerado para fins da Lei nº 13.709/2018. Conforme seu artigo 5º, inciso I, o legislador considera dados pessoais como: toda a informação que está relacionada à pessoa natural identificada ou identificável.

Igualmente, o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, já prevê em seu artigo 4º idêntica conceituação e, vai além, complementando e explicando também o que se deveria entender por pessoa identificável, conforme segue:

> É considerada pessoa identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos de identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

Segundo o Professor Doutor Danilo Doneda: "a informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por revelar aspectos que lhe dizem respeito." (DONEDA, 2006, p. 157) O mesmo autor assevera:

> Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser

> gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. (DONEDA, 2006, p. 27)

Importante ressaltar que nossa Lei Geral de Proteção de Dados Pessoais, em seu artigo 5º, inciso II, também trata da questão dos dados pessoais sensíveis, conforme segue:

> 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.

Segundo Marcio Cots e Ricardo Oliveira, especialistas em Direito Digital:

> Os dados sensíveis merecem proteção extraordinária da LGPD por dois aspectos principais: mergulham ainda mais na privacidade do ser humano, alcançando sua intimidade, como é o caso dos dados relativos à vida sexual ou saúde, bem como são passíveis de trazer ao titular discriminação ou preterimento, como os dados concernentes à posição política ou filiação sindical. (COTS; OLIVEIRA, 2019, p. 104)

Desta forma, resta claro afirmar que toda informação pessoal merece uma tutela jurídica do Estado, seja ela uma informação pessoal simples ou dados considerados sensíveis, por se tratarem de elementos que podem colocar em risco a integridade, privacidade e dignidade da pessoa envolvida.

2. Privacidade na era digital

Quando tratamos de dados pessoais, inerente se faz dialogar com a privacidade. Pois, como já mencionado anteriormente, os dados pessoais tratam de aspectos muito particulares de cada indivíduo, capaz de causar danos irreparáveis e até irreversíveis quando utilizados de maneira irresponsável.

A quebra de privacidade que, no início do século passado era tratada como "o direito de estar só", nos dias atuais, em que a tecnologia alcança patamares inimagináveis, a capacidade de transmissão, armazenamento, controle e processamento de dados vem crescendo numa velocidade, onde não conseguimos vislumbrar até onde chegará.

Neste sentido, Patricia Peck Pinheiro comenta:

> A espionagem internacional digital e a violação da privacidade dos usuários da Internet são alguns dos problemas conhecidos da rede no mundo inteiro, mas por enquanto não existe uma instituição que determine até onde

> governos, serviços de segurança ou empresas podem ir. (PINHEIRO, 2016, p. 482)

Em uma abordagem muito interessante, a Professora Doutora Laura Schertel Mendes, explica a relação da personalidade da pessoa com o tratamento de dados, conforme segue:

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade da informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados. (MENDES, 2014, p. 32)

Partindo desta análise, podemos compreender que a grande preocupação atual se dá no aspecto do controle, tratamento e processamento destes dados a fim de proteger o indivíduo quando da manipulação de seus dados pessoais. O jurista italiano Stefano Rodotà esclarece:

> O processo evolutivo experimentado pelo conceito de privacidade fez com que seu conteúdo fosse preenchido não apenas pela garantia de isolamento e reserva do indivíduo, mas também pela possibilidade de ele manter controle sobre a circulação de suas informações pessoais e de determinar como sua esfera privada deve ser constituída. (RODOTÀ, 2008, p. 17)

Podemos observar que a grande preocupação nos dias atuais é no sentido de como estes dados são manipulados. Em um mundo ocidental cada vez mais capitalista, onde os dados pessoais ganham valor econômico, a grande preocupação gira em torno da captação desses dados sem o consentimento ou ciência de seus titulares.

3. Exploração econômica dos dados pessoais

Todos sabemos que a manipulação, ou seja, a captação, o armazenamento, o tratamento e o processamento dos dados pessoais pelos grandes conglomerados empresarias vem se tornando um negócio rentável. A grande preocupação nos dias atuais é que esses dados, por muitas vezes, são coletados sem o consentimento ou autorização das pessoas. Indo um pouco mais além, sem o conhecimento que seus dados estão sendo coletados.

Conforme menciona a Professora e Advogada Ana Frazão:

> Do ponto de vista econômico, dados importam na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Consequentemente, os dados precisam ser processados para que possam gerar valor. (FRAZÃO, 2019, p.26)

Em relação a como os dados são coletados a Professora Doutora Laura Schertel Mendes, traça alguns exemplos:

> Os dados de transações comerciais podem ser obtidos pela empresa por meio da realização de cadastros dos consumidores no momento da compra do produto ou da realização do serviço. Geralmente, na primeira transação comercial, a empresa solicita a realização do cadastro do consumidor, para maior segurança, em caso de pagamento com cartão de crédito ou cheque, ou simplesmente para o registro dos dados do cliente. (MENDES, 2014, p. 96)

Nesta mesma linha, a ilustre professora continua:

> Nesses registros, é comum constar não apenas os dados do consumidor, mas também os seus hábitos de consumo, possibilitando que posteriormente a empresa possa ofertar-lhe produtos específicos. Grandes lojas de departamentos possuem enormes cadastros com dados de milhares de consumidores. (MENDES, 2014, p. 96-97)

Como já mencionado anteriormente, o grande receio é a ausência de informações na coleta dos dados no que concerne no consentimento do indivíduo.

A Professora Ana Frazão comenta a respeito:

> Entretanto, o ponto de partida de toda essa engrenagem é a coleta de dados, cada vez mais maciça e muitas vezes realizada sem o consentimento e até sem a ciência dos titulares desses dados. Se os cidadãos não conseguem saber nem mesmo os dados que são coletados, têm dificuldades ainda maiores para compreender as inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas. (FRAZÃO, 2019, p.26)

Com a facilidade da coleta de dados por diversos segmentos empresariais, vem emergindo cada vez mais a atividade dos *data brokers*, que vislumbram nos dados pessoais coletados uma grande possibilidade de negócio, por sinal muito rentável, seja na venda de pacotes de dados de consumidores de maneira segmentada para campanhas publicitárias ou simplesmente um banco de dados de e-mails.

Estes dados que são coletados possuem inúmeras destinações, como, por exemplo, ditar o comportamento do consumidor e extrair inferências sensíveis a eles.

Diante de tantos abusos e violações da privacidade dos dados pessoais, que são utilizados para fins econômicos, o Brasil, através da Lei nº 13.709/2018, tenta disciplinar a matéria, já muito discutida na

União Europeia e alguns países latino-americanos, aplicando alguns princípios constitucionais que tutelam a privacidade dos cidadãos.

4. Princípios da Lei Geral de Proteção de Dados Pessoais

Em se tratando de dados pessoais na era digital, importante salientar que os princípios norteadores da Lei nº 13.709/2018 buscam, além das garantias tuteladas pela Constituição Federal, garantir a privacidade, finalidade e destinação dos dados. Laura Schertel Mendes posiciona-se claramente a esse respeito: "*Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que possa controlar o fluxo dos seus dados.*" (MENDES, 2014, p. 68).

Em seu artigo publicado no compêndio coordenado por Gustavo Tepedino, Ana Frazão e Milena Donato Oliva, intitulado *Lei Geral de Proteção de Dados e suas repercussões no direito Brasileiro*, os autores Marco Aurélio Bellizze Oliveira e Isabela Maria Pereira Lopes discorrem:

> Com efeito, o Brasil foi desenvolvendo um sistema de proteção de dados, que também se refletiu na atuação de tribunais superiores e órgãos da administração pública. Os princípios indicados na LGPD refletem a formação desse sistema, pois nenhum deles representa uma novidade em si, mas a cristalização de avanços que foram alcançados pelas leis anteriores, muitas vezes com viés mais pragmático do que principiológico. (OLIVEIRA; LOPES, 2019, p. 82)

Entre os diversos princípios elencados ao longo do texto legal, notadamente em seu artigo 6º, podemos destacar três: o princípio da finalidade, da transparência e do consentimento. A Professora Doutora Laura Schertel Mendes, a respeito do princípio da finalidade assevera:

> Um princípio fundamental que todas as atividades de processamento de dados devem seguir é o princípio da finalidade, que indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta de dados. (MENDES, 2014, p. 70).

Em relação ao princípio da transparência, a mesma autora sustenta:

> O princípio da transparência, também chamado de princípio da publicidade, exige que a existência de um banco de dados pessoais seja de conhecimento público. [...] Com base nesse princípio, surge para o banco de dados de publicar seu nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia desse direito. (MENDES, 2014, p. 71).

E, por último, a professora discorre sobre o princípio do consentimento:

> Para possibilitar o controle do titular acerca dos seus dados, outro princípio relevante é o princípio do consentimento. Afinal, o exercício da liberdade de controle de dados pessoais baseia-se no consentimento do titular, que pode determinar um maior nível de proteção ou um maior fluxo dos seus dados. Segundo esse princípio, o consentimento deve ser livre, específico e informado, e apenas situações excepcionais (previstas legalmente) justificam o processamento de dados sem o prévio consentimento do titular. (MENDES, 2014, p. 71).

Podemos perceber que, os princípios apresentados na nova legislação se preocupam com a proteção dos dados pessoais em uma era da comunicação onde não há limites para sua violação e comercialização econômica. Quando a autora destaca estes três princípios deixa muito claro esta preocupação e aponta uma importante direção a ser seguida por todos os entes envolvidos na questão do direito digital.

Conclusão

O presente artigo procurou demonstrar a importância de uma nova legislação para tratar da proteção e garantia dos cidadãos, em uma era digital onde não há limites para a violação da privacidade, principalmente para fins econômicos.

Em um mundo ocidental cada vez mais capitalista, onde o tratamento de dados pessoais por grandes conglomerados empresariais tornou-se um ativo financeiro de grande valor, necessário se faz um regramento com a finalidade de proteger os direitos individuais do cidadão.

Nesta seara, a Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), muito se aproximou do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, no qual apresentou princípios norteadores, definiu alguns conceitos, como, por exemplo, dados pessoais, tratamento de dados, entre outros, e também disciplinou a sua utilização, sempre com o respeito a privacidade, transparência e boa-fé.

Um regramento que trate da manipulação de dados pessoais torna-se de suma importância em um mundo empresarial onde grandes corporações faturam milhões com bancos de dados, muitas vezes captando informações sem o consentimento do indivíduo, ou, até mesmo, compartilhando ilegalmente informações sigilosas.

Ainda temos muito a caminhar com a nova legislação que entrará em vigor no próximo ano, como, por exemplo, a criação da autoridade nacional que fiscalizará e punirá os infratores. Porém, seguindo os padrões internacionais, o Brasil se mostrou atento aos problemas ocasionados pelo grande

desenvolvimento tecnológico sem precedentes e que vem ocasionando, por muitas vezes, a violação irreparável da intimidade e personalidade de pessoas, que nem se quer sabem que seus dados estão sendo comercializados, a fim de enriquecer um grupo seleto de empresários que detém grande parte da renda mundial.

Referências bibliográficas

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 12/10/2019.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados comentada.** 2ª ed. São Paulo: Thomson Reuters, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em 11/10/2019.

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

FRAZÃO; Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.** 1ª ed. São Paulo: Thomson Reuters, 2019.

MARINELI, Marcelo Romão. **Privacidade e redes sociais:** sob a égide da Lei 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. 2ª e.d. São Paulo: Thomson Reuters, 2019.

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

PINHEIRO, Patricia Peck. **Direito Digital.** 6ª ed. São Paulo: Saraiva, 2016.

_____. **Proteção de Dados Pessoais:** comentários à Lei n.13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância.** Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

6.7. A economia de dados pessoais no contexto da LGPD: há necessidade de regulação dos modelos de negócios pela

Autoridade Nacional de Proteção de Dados? – *Renato Barros Cabral*[154] *& Alexandre Multini Mihich*[155]

Resumo

A partir da edição do Marco Civil da Internet, do Decreto nº 8.771/16 e da Lei Geral de Proteção de Dados (LGPD) os modelos de negócios pautados nos dados pessoais começaram a ser discutidos. A ideia que precede a denominada "economia de dados pessoais" é simples: os indivíduos deveriam ter a possibilidade de assumir o controle sobre seus dados pessoais, compartilhá-los como bem entenderem e lucrarem com seu compartilhamento. É fato que os usuários da internet, por meio de uma simples navegação, fornecem mais e mais os seus dados pessoais, anuindo à utilização de *cookies*, ao baixar um aplicativo, ao fazer o *login* do Facebook, do Instagram.... isso sem contar que a localização geográfica de cada passo do usuário é monitorada pelo *wi-fi* e pelo GPS ativado nos celulares e smartphones das pessoas. A forma como esses dados estão sendo usados e monetizados, a partir da criação de modelos de negócios, é a grande questão da economia digital e, a partir da premissa de que os dados são de propriedade do usuário, as empresas só poderiam armazenar e compartilhar esses dados com o consentimento de quem os concede. Nesse cenário é que surge o conceito de "economia de dados pessoais" e a ideia – ainda remota – de que cada um de nós poderia ganhar dinheiro com seu próprio dado. A realidade, entretanto, a partir do poder econômico das empresas de tecnologia pressupõe, de um lado, o usuário que "cede" os seus dados pessoais (o seu ativo imaterial), na maior parte das vezes de forma não onerosa e, de outro lado, diversas empresas, com os mais variados e impensados modelos de negócios que conseguem, quase como mágica, monetizar o dado pessoal. Nesse contexto, a partir da LGPD deveria existir algum tipo de regulação da proteção de dados, em detrimento do interesse econômico dos agentes do mercado de tecnologia e, mais do que isso, a ausência de controle destes modelos de negócio seria suficiente para neutralizar a atividade da ANPD a ponto de torná-la inócua e apenas formal? A investigação está em curso e pretende-se apresentar as suas conclusões no Congresso Internacional "Desafios e perspectivas das Autoridades de Proteção de Dados Pessoais e Privacidade".

Palavras-chave: dados pessoais têm valor econômico? Modelo de negócios monetizados; regulação da atividade empresarial; poder econômico; proteção de dados pessoais; Autoridade Nacional de Proteção de Dados; tecnologia.

Abstract

[154] Mestrando em Direito pela Universidade Nove de Julho – UNINOVE.

[155] Mestrando em Direito pela Universidade Nove de Julho – UNINOVE.

From the edition of the Marco Civil of Internet, Decree n. 8.771/16 and the General Data Protection Act (LGPD), business models based on personal data began to be discussed. The idea preceding the so-called "personal data saving" is simple: individuals should be able to take control of their personal data, share it as they see fit, and profit from sharing it. It is a fact that internet users, by simply browsing, provide more and more your personal data, by consenting to the use of cookies, downloading an app, logging in from Facebook, Instagram .... not to mention that the geographical location of each user's step is monitored by wi-fi and GPS enabled on people's mobile phones and Smartphone. How this data is being used and monetized from the creation of business models is the big question of the digital economy, and from the premise that the data is owned by the user, companies could only store and share such data with the explicit consent of the grantor. In this scenario comes the concept of "personal data saving" and the still remote idea that each of us could make money from our own data. Reality, however, based on the economic power of technology companies, presupposes, on the one hand, the user who "gives in" his personal data (his immaterial asset), most of the times in a non-costly way and, on the other hand, several companies, with the most varied and thoughtless business models that can almost monetize the personal data. In this context, from the LGPD, there should be some kind of data protection regulation, to the detriment of the economic interest of technology market players and, moreover, the lack of control of these business models would be sufficient to neutralize the activity of the National Data Protection Authority (ANPD) to the point of making it innocuous and only formal? The research is ongoing and it is intended to present its findings to the International Congress "Challenges and Prospects of Personal Data Protection and Privacy Authorities"

Keywords: Personal data have economic value? Monetized business model. Business regulation. Economic power. Personal data protection. National Data Protection Authority. Technology.

Introdução

O problema formulado neste estudo é o de que em função da dificuldade de identificar o estabelecimento (virtual) e o ativo (bem imaterial) no modelo de negócio originado na chamada 'economia de dados pessoais' teria a Autoridade Nacional de Proteção de Dados – ANPD, prevista na Lei Geral de Proteção de Dados – LGPD (Lei n. 13.709/18) legitimidade e *enforcement* para regular esses modelos de negócios que monetizam os dados pessoais.

A partir dele, foram formuladas as seguintes hipóteses:

a) haveria conflito evidente entre o "interesse geral de agentes econômicos" e o "interesse geral de usuários dos serviços prestados", especificamente em matéria de proteção de dados;

b) a conformação da estrutura da ANPD deverá levar em conta as particularidades dos modelos de negócio que (i) são realizados a partir de estabelecimentos virtuais, (ii) contemplam bens imateriais (dados pessoais) e (iii) que são, na imensa maioria dos casos, formalizados e concretizados virtualmente;

c) a análise da regulação da proteção de dados deve levar em conta vetores abrangentes e não apenas o interesse econômico dos agentes do mercado de tecnologia, sob pena de neutralizar a atividade da ANPD a ponto de torná-la inócua e apenas formal, com consequências graves para o desenvolvimento nacional.

O método utilizado será o hipotético-dedutivo indutivo; a partir das normas que regulam o Marco Civil da Internet e a Lei Geral de Proteção de Dados, mediante hipóteses, busca-se investigar as consequências para a regulação da atividade empresarial voltada à coleta, uso e tratamento de dados, advindas da aplicação desse novo marco legal em cotejo com a LGPD.

A propósito, tem-se que a LGPD não proíbe o desenvolvimento comercial de modelo de negócios que utilizem dados pessoais, desde que os tais dados sejam utilizados (tratados) de maneira criteriosa, observando-se os princípios estabelecidos no artigo 6º.

A proteção de dados pessoais é, sem nenhuma dúvida, um dos pilares mais importantes do Estado Democrático de Direito, cujo principal fundamento é a dignidade da pessoa humana.

Por outro lado, em um ambiente de globalização é certo que a economia baseada na internet cada vez mais depende de dados para se sustentar (*data driven economy*) e, por isso, o ambiente de negócios no espaço virtual mitiga o conceito de estabelecimento comercial tradicional e o conceito de bem corpóreo, produzindo, entretanto, vantagens para a comunicação e escalando os lucros auferidos no comércio eletrônico.

A LGPD contém bases legais para que os dados pessoais possam ser tratados, quais sejam: *i)* manifestação livre, informada, inequívoca através da qual o titular concorde com o tratamento dos seus dados pessoais para uma finalidade determinada; *ii)* cumprimento de obrigação legal ou regulatória pelo controlador; *iii)* pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; *iv)* para a realização de estudos por órgão de pesquisa; *v)* para a execução de contrato ou de procedimentos preliminares, relacionados a contrato do qual seja parte o titular; *vi)* para o exercício regular de direitos em processo judicial, administrativo ou arbitral; *vii)* para a proteção da vida ou da incolumidade física do titular ou de terceiros; *viii)* para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; *ix)* quando necessário para atender aos interesses legítimos do controlador ou de terceiro, consideradas a partir de situações concretas, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais; *x)* para proteção do crédito.

A LGPD estabelece que são direitos dos titulares dos dados pessoais: a) confirmação da prática de tratamento de dados; b) acesso aos dados; c) correção de dados incompletos, inexatos ou desatualizados; d) anonimização, bloqueio ou eliminação de dados desnecessários; e) portabilidade mediante requisição;

f) eliminação a qualquer momento de dados pessoais com cujo tratamento o titular tenha consentido; g) aplicação de normas de defesa do consumidor.

Nessa toada, o artigo 7º da Lei nº 12.965/14 (Lei do Marco Civil da Internet) prevê que o titular dos dados tem o direito de remoção dos mesmos, após o término da relação obrigacional que ensejou o tratamento, atribuindo à pessoa natural o "poder" de autogerir (autotutelar) os seus dados pessoais.

Para prestigiar Bruno Ricardo Bioni é certo que a LGPD tem como escopo garantir a *"autodeterminação informativa"* e, ao mesmo, tempo escalar o desenvolvimento da atividade econômica e da tecnologia em um ambiente de regulação, assegurando os interesses de todas as pessoas envolvidas na chamada *"data driven economy"* (economia baseada em dados/informações)[156].

A partir dos conceitos expostos, indaga-se até mesmo se teria a LGPD apresentado um novo paradigma regulatório para o Brasil, dado que eventual flexibilização da ordenação em matéria de regulação, para além de aspectos políticos e de direcionamento econômico, com vistas a formular indicadores para o mercado interno e externo, têm potencial para a geração de consequências ainda mais complexas, como em matéria de proteção de dados, recorte proposto no presente estudo.

Nesse contexto é que se apresentará o papel da Autoridade Nacional de Proteção de Dados – ANPD e se analisarão a necessidade e a legitimidade para a ANPD regular os modelos de negócios monetizados e gerados a partir da nova economia baseada nos dados pessoais.

Embora a pesquisa esteja em curso, a revisão de bibliografia inicial, a partir do problema e das hipóteses formuladas permitiu, como primeira conclusão, afirmar que os modelos de negócios não podem retirar do usuário o seu poder de decidir sobre os "seus dados pessoais" e não devem sobrepujar o interesse das empresas em detrimento dos direitos do usuários sendo certo que a ANPD, se necessário for, deverá garantir a regulação da atividade econômica, nos moldes constitucionais e, nos moldes da própria regulamentação prevista na LGPD, sem, entretanto, causar óbices ao incremento da atividade empresarial.

1. A LGPD e os novos modelos de negócios que monetizam dados e que implicam em mitigar os conceitos tradicionais de estabelecimento comercial e de bens materiais

Retomando a expressão anteriormente utilizada na *data driven economy*, tem-se uma infinidade de dados, produzidos tão rapidamente, de tipos e origens diferentes, que se convencionou chamar esse

[156] BIONI, Ricardo Bruno. Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, regulação dos bancos de dados eletrônicos e arquitetura da internet. 2016. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo. 2016

cenário (e as soluções para sua lide, como os algoritmos, *machine learning* e *business inteligence*) de *big data*.

Neste ambiente virtual de dados produzidos e armazenados diariamente na internet, encontram-se os dados pessoais, que podem ser, em poucas palavras, definidos como os dados relacionados à pessoa natural identificada ou identificável.

Nesse contexto econômico, os dados se tornaram tão valorizados que receberam a alcunha de "novo petróleo". Sobre os dados pessoais, especificamente, está baseado um dos modelos de negócio, dos mais rentáveis, denominado "publicidade dirigida".

Nesse contexto, tem-se que os negócios baseados em dados surgem como uma atraente alternativa. Em outras palavras, trata-se de um ativo que se produz em escalas imensas diariamente, e cujo acesso, coleta e armazenamento tornam-se mais barato quanto mais evoluem as tecnologias para tanto.

É bem por isso que determinados serviços aparentemente gratuitos, como por exemplo, *Facebook, WhatsApp, Twitter, Instagram* e *YouTube*, monetizam os dados pessoais, ou seja, os tais serviços somente admitem o acesso 'gratuito' desde que o usuário ceda seus dados pessoais.

E é exatamente neste particular que a monetização dos dados pessoais ganha relevância já que cria uma preocupação quanto à violação da privacidade dos dados pessoais dos titulares.

É neste cenário de coleta e uso dos dados pessoais com fins de monetização que se desenvolvem modelos de negócio que apresentam potencialidade de conformação e violação da privacidade dos titulares dos dados. Em outras palavras, é neste cenário sem território físico, sem fronteiras geográficas, sem limites nacionais explicitamente definidos que estão os fluxos e intercâmbios de dados e informações.

Por meio da atividade de tratamento de dados é possível aprimorar, por exemplo, a publicidade dirigida, parametrizando os padrões de acesso e consumo, e até mesmo influir no hábito do usuário da internet, escolhendo o que mostrar e o que não mostrar e, até mesmo, influenciando o resultado de processos políticos, como sugere Alec Ross na obra "*The industries of the future*" (2016).

Os dados, entretanto, são colhidos, não raro, sem o devido consentimento dos usuários, que também ignoram o destino de tais dados e o que deles será feito ficando os titulares alijados da necessária autodeterminação informacional.

É certo que a exploração dos dados pessoais de uma maneira desmedida, sem limites e regulações, pondo a necessidade por lucro acima dos interesses da coletividade e de direitos fundamentais certamente produzirá consequências nefastas no tocante à privacidade dos usuários da internet.

Este direito fundamental – privacidade – pode ser violado diretamente, através, por exemplo, do acesso não autorizado aos dados pessoais, conforme ocorreu nos idos de 2017 quando do vazamento da base de dados da Equifax, *case* que foi denominado "***Equifax Data Breach***", analisado por Lee Mathews na Revista Forbes[157].

Para concluir é inegável que existem benefícios decorrentes do uso e do tratamento de dados pessoais, tendo em vista a existência de inúmeros serviços que facilitam a vida cotidiana e que fazem uso de nossos dados, como os aplicativos de mapas e trânsito.

É possível imaginar, igualmente, que o uso de dados relativos à saúde dos titulares – dados considerados sensíveis – em estudos e pesquisas científicas, podem permitir *insights* e novas descobertas em termos de tratamento médico.

É igualmente prático e agradável poder encontrar produtos especialmente direcionados aos interesses de cada consumidor, aproveitando descontos e promoções em itens que muitas vezes precisam.

Novos modelos de negócios surgem diariamente, fundamentados nas inúmeras oportunidades que decorrem do tratamento de dados e, nesse particular, a livre iniciativa, a liberdade de modelos de negócio e a livre concorrência, são fundamentos e princípios protegidos e promovidos pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados e, exatamente por isso, a atividade empresarial deve ser encorajada e não tolhida.

2. A atuação regulatória da Autoridade Nacional de Proteção de Dados – ANPD neste novo ambiente negocial

Neste item será analisada a necessidade (ou não) de regulação das atividades de monetização dos dados pessoais ante a precisão de se proteger a privacidade e as liberdades nela inclusas.

Não se trata, obviamente, de tarefa simples, especialmente a partir do que se expôs acerca da sociedade em rede e da realização de negócios por meio de uma rede de fluxos supranacionais. Nessa toada, a Autoridade Nacional de Proteção de Dados, criada a partir da Lei Geral de Proteção de Dados deverá aplicar, fiscalizar e realizar o *enforcement* da referida lei e das normativas nacionais para garantir um ambiente de negócios saudável.

No contexto da regulação, tem-se que a presença do Estado é essencial neste cenário, devendo atuar na regulação da monetização de dados pessoais por meio de um ente regulador próprio, neste caso, a

[157] Disponível em: https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143millionamericans/#248efd3f356f. Acesso em: 15 set. 2017.

Autoridade Nacional de Proteção de Dados, que se prestará a desenvolver e criar todos os meios possíveis para a proteção da privacidade e dos valores conexos dos titulares dos dados pessoais.

Conclusão

O objetivo da LGPD é permitir maior transparência e controle no uso de dados pessoais, para que a autorregulação individual possa facilitar as novas formas de atividade econômica, ou, dito de outra forma, para que possa escalar os novos modelos de negócios pautados em dados pessoais e realizados em ambiente virtual.

Os dados, entretanto, são uma mercadoria heterogênea, isso porque, os dados de uma pessoa não são iguais aos de outra. Além disso, quem entende melhor o valor comercial dos dados não são os indivíduos que os geram, mas as empresas que já possuem muitos deles e dedicam recursos extensos para analisá-los.

Nesse contexto, tem-se que os dados pessoais de um indivíduo, isoladamente, fornecem informações sobre o que ele fez anteriormente, mas não são necessariamente tão informativos sobre coisas novas que ele pode gostar ou que podem acontecer com ele (dados de outras pessoas ajudam a resolver isso).

Como consequência lógica, os dados pessoais agregam maior valor quando combinados com dados de muitas outras pessoas, sendo certo que o processamento analítico de grandes quantidades de dados será responsável por gerar valor agregado àquele conjunto de dados tratados e analisados para determinada finalidade.

Os dados individuais, ao contrário (e no contexto dos modelos de negócios atualmente vigentes), provavelmente têm valor limitado. A título meramente exemplificativo, no contexto da publicidade, normalmente o valor dos dados de consumo de determinado grupo de usuários vem da capacidade de exibir anúncios para um grande número de pessoas, e há algumas evidências empíricas que sugerem que o valor de poder segmentar anúncios é comparativamente baixo.

Nesse contexto, tem-se que os gigantes da Internet capturam a maior parte do valor da economia digital enquanto escapa aos "criadores" do conteúdo (obras, informações, arquivos) o recebimento da devida contrapartida pecuniária pela obra e/ou pela informação produzida.

Há que garantir – e obrigar - que os *players* da economia digital observam os limites de propriedade para garantir a proteção dos usuários quanto ao "*seu*" conteúdo, mediante o devido compartilhamento de receita, tendo em vista que vários dos modelos de negócios pressupõe o *revenue share* (compartilhamento de receita).

A LGPD e a própria ANPD devem garantir ao titular dos dados caminhos mais equitativos, que envolvem mais transparência no comércio, o retorno do controle sobre a propagação dos dados compartilhados, os meios técnicos e legais aos indivíduos proprietários de dados, bem como o fortalecimento do poder de autorregulação e de negociação em detrimento do poder político e econômico dos empreendedores digitais.

Na mesma esteira, e tomando em consideração este cenário protetivo, a ANPD deverá atuar como ente central regulador de forma a garantir a proteção dos dados pessoais, capaz de conjugar o *expertise* técnico necessário às prerrogativas próprias de um agente regulatório: editando atos, fiscalizando sua aplicação e sancionando as possíveis violações, tudo em adequação e consonância às complexidades que a monetização de dados enseja e sem limitar as liberdades que a sociedade em rede proporciona.

Nesse contexto, a Autoridade Nacional de Proteção de Dados é esperança de otimismo para o cenário de monetização de dados pessoais, conferindo maior segurança jurídica aos modelos de negócio e imprimindo maior força à proteção dos direitos dos usuários de serviços na internet.

Por isso, superado o discurso inicial, mostra-se premente a necessidade de análise cuidadosa dos reflexos da LGPD e da ANPD no plano regulatório da atividade econômica e, para o enfoque desta pesquisa, na atividade empresarial relacionada à coleta, ao uso e ao tratamento de dados pessoais e, principalmente, aos modelos de negócios originados a partir destes "dados pessoais", monetizados e concretizados em ambiente virtual.

Referências bibliográficas

ARAÚJO, Nicete Lacerda; GUERRA, Bráulio Madureira; *et al.* **Marco Legal da Inovação:** breves comentários. Rio de Janeiro: Lumen Juris, 2018.

BENABOU, Valérie-Laure; ROCHFELD, Judith. **À qui profite le clic ?** Le partage de la valeur à l'ère du numérique. Collection Corpus dirigée par Thomas Clay et Sophie Robin-Olivier. Paris: Odile Jacob, 2015.

BIONI, Ricardo Bruno. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, regulação dos bancos de dados eletrônicos e arquitetura da internet. 2016. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo. São Paulo, 2016.

_____. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

CARVALHO, Vinícius Marques de; MATTIUZZO, Marcela. Confiança, reputação e redes: uma nova lógica econômica? In: ZANATTA, Rafael A. F.; PAULA, Pedro C. B.; KIRA, Beatriz (Org.). **Economias do compartilhamento e o Direito.** Curitiba: Juruá, 2017, p. 41-57.

COMPARATO, Fabio Konder. A reforma da empresa. *In:* **Direito empresarial:** estudos e pareceres. São Paulo: Saraiva, 1995, p. 3-26.

DE LUCCA, Newton; DEZEM, Renata Mota Maciel Madeira. A proteção de dados pessoais no Brasil a partir da Lei nº 13.709/2018. In: JORGE LEMOS, André Guilherme et al. (Coord.). **Direito Empresarial:** estruturas e regulação. Volume 2. São Paulo: UNINOVE. 2018, p 255-276.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Vitor Rozatti (Coord.). **Direito Digital:** direito privado e internet. 2 ed. Indaiatuba: Editora Foco Jurídico, 2019.

LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção de dados pessoais no cenário futuro do Brasil.** Tese de Livre-Docência apresentada à Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. Ribeirão Preto: Universidade de São Paulo, 2015.

PINTO, Renata Ávila. Digital Sovereignty Or Digital Colonialism. **Sur – International Journal on Human Rights,** v. 15, n.27, 2018, p. 15-27. Disponível em HeinOnline. Acesso em 10.7.2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Editora Renovar, 2008.

ROSS, Alec. **The industries of the future.** New York. Simon & Schuster. 2016.

SALOMÃO FILHO, Calixto. **Teoria crítico-estruturalista do Direito Comercial.** São Paulo: Marcial Pons, 2015.

SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016.

VANIAN, Jonathan. Why Data Is The New Oil. **Fortune,** July 11, 2016. Disponível em https://fortune.com/2016/07/11/data-oil-brainstorm-tech/. Acesso em 17.7.2019.

VOSS, W. Gregory. Internet, New Technologies, and Value: Taking Share of Economic Surveillance. **Journal of Law, Technology & Policy,** University of Illinois, vol. 2017, no. 2, Fall 2017, p. 469-485. Disponível em HeinOnline. Acesso em 14.7.2019.

6.8. Violação do livre consentimento: um estudo de caso da Ação Civil Pública movida pelo IDEC – em face da VIAQUATRO –

Rafaela Rabelo Daun[158], *André Lucas Fontana*[159], *Jaqueline Yurie Miura*[160] *& Vinicíus Silva Luiz*[161]

Resumo

O presente artigo pretende analisar a ação civil pública movida pelo Instituto Brasileiro de Defesa do Consumidor em face da empresa Via Quatro, avaliando a fundamentação legal da ação sob a ótica do consentimento e da Lei Geral de Proteção de Dados.

Palavras-chave: Lei Geral de Proteção de Dados; Consentimento; Ação Civil Pública; Direito Digital.

Abstract

This article intends to analyze the Public Civil Action lawsuit filed by the Brazilian Institute of Consumer Protection against the company Via Quatro, evaluating the legal basis of the action from the perspective of consent and the General Data Protection Law.

Keywords: General Data Protection Law. Consent. Public Civil Action. Digital Law.

Introdução

O presente artigo pretende analisar o caso da Ação Civil Pública movida pelo IDEC (Instituto Brasileiro de Defesa do Consumidor) em face da Concessionária da linha 4 do metrô de São Paulo S.A, conhecida pelo nome fantasia VIAQUATRO.

A referida ação foi movida devido a uma suposta coleta de dados de forma compulsória, visto que a empresa havia instalado câmeras próximas a grandes telões de propaganda fixados nas entradas dos trens, as câmeras em questão supostamente gravavam todas as reações do público que observava as propagandas. O IDEC alega que as gravações coletavam dados sensíveis e que tais dados foram

[158] Advogada. Mestranda em Teoria do Direito e do Estado - Programa de Mestrado do UNIVEM/Marília-SP, bolsista na modalidade Bolsa de Estudos CAPES/PROSUP, Bacharel em Direito pelo Centro Universitário Eurípides de Marília – UNIVEM. Integrante do NEPI (Núcleo de Estudos e Pesquisas em Direito e Internet) do UNIVEM. E-mail: rafaela.daun@hotmail.com.

[159] Advogado. Pós-graduando em Direito do Trabalho e Processo do Trabalho pelo Instituto Damásio de Direito. Bacharel em Direito pelo UNIVEM – Centro Universitário Eurípedes de Marília. E-mail: andrelfontana@outlook.com.

[160] Graduanda em direito pelo UNIVEM – Centro Universitário Eurípedes de Marília. E-mail: jaquelinemiura@hotmail.com.

[161] Graduando em direito pelo UNIVEM – Centro Universitário Eurípedes de Marília. E-mail: viniciusluiz01@hotmail.com.

utilizados para fins econômicos, mesmo que nenhum dos passageiros ao menos soubesse o que estava acontecendo.

Importa ressaltar, que a ação também teve como fundamentos a proteção as informações pessoais dos usuários de serviços públicos, nos termos da Lei 12.527 de 18 de novembro de 2011 (BRASIL), a proteção contra prática abusiva presente no artigo 6º, IV do Código de Defesa do Consumidor (BRASIL, 1990), a necessidade de informar aos consumidores os preços de produtos e serviços ofertados, presente no art. 6º e 31º, do CDC, bem como o direito constitucional a proteção de imagem, presente no artigo 5º da Constituição Federal (BRASIL, 1988), dentre outros fundamentos.

Em tese de contestação, alegou a VIAQUATRO que não houve violação da privacidade ou de dados pessoais dos usuários da linha quatro amarela, uma vez que o sistema de funcionamento dessas "Portas Interativas Digitais", somente detecta possíveis rostos, e não é capaz de reconhecer pessoas. Portanto, não envolve qualquer uso de imagem de pessoas ou dados pessoais, pois os dados coletados são anonimizados, o que inviabiliza a identificação dos indivíduos que utilizam a linha.

Alegou também ter expressa aprovação por parte do Poder Concedente em relação à aferição de receitas complementares à prestação de serviço público por meio de publicidade, inclusive quanto ao projeto em comento, por essa razão não haveria ilicitude na tecnologia contratada.

Nesse sentido o presente artigo realizar uma interpretação analógica, visando não reconstruir os argumentos utilizados na ação, mas adequá-los a Lei Geral de Proteção de Dados caso aplicável fosse, lembrando que a referida lei ainda não é vigente.

Portanto, o artigo irá os elementos fáticos do caso, bem como o direito sob a ótica do consentimento e da Lei Geral de Proteção de Dados, visando debater se realmente houve aproveitamento econômico da situação, ou ilicitude por parte da empresa com a suposta coleta de dados. Destaca-se no presente caso, que o consentimento não é a única base legal, porém em razão do grande destaque trazido pela nova lei sobre este conceito, o artigo terá seu foco nesta questão.

Por fim cabe ressaltar que a ação supracitada ainda se encontra em andamento, portanto mesmo na esfera judiciária a discussão não teve fim. Insta salientar que levou em conta fundamentos jurídicos diversos, incluindo dispositivos constitucionais e do Código de Defesa do Consumidor, porém neste caso a análise será limitada aos dispositivos que versam sobre a proteção de dados, como a LGPD. A análise é bibliográfica e documental, com uso da legislação e do conteúdo doutrinário acerca do tema, e o método adotado é o dedutivo, uma vez que deduz como seria analisada a referida ação sob a vigência da Lei Geral de Proteção de Dados.

1. O consentimento de acordo com a Lei 13.709/2018

Ao buscar o conceito de consentimento, tem-se o estabelecido na lei que regulou a proteção de dados no ordenamento jurídico brasileiro, qual seja a Lei 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de dados (LGPD), que atualmente se encontra em período de vacância. Neste cenário, o artigo 5º XII da referida lei expõe que o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Ademais, seu artigo 2º acrescenta expressamente a questão do consentimento de forma implícita, como pode ser observado no texto legal a seguir:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: 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. (BRASIL, 2018)

Isto porque, é possível extrair o consentimento dentro dos incisos I, IV e VII, visto que o respeito à privacidade, à inviolabilidade da intimidade e à garantia dos direitos da personalidade são inerentes ao homem. Ainda, nesse mesmo sentido, a legislação traz expressamente em seu artigo 5º o conceito como "Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018).

Desse modo, a ação movida pelo IDEC foi fundamentada com a alegação de vício em razão do não consentimento, vez que a VIAQUATRO não demonstrou nenhum meio de manifestação de vontade dos titulares dos dados. Porém a empresa ré de modo totalmente diverso se defendeu alegando a falta de necessidade de consentimento, com embasamento na diferença entre detecção e reconhecimento facial a qual será analisada em tópico específico.

Nesta toada, o consentimento de acordo com o artigo 7º inciso I da mencionada lei, é requisito para o tratamento de dados pessoais, e quando este não for fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, é considerado viciado, ou seja não é válido, como dispõe o artigo 8º §3º da LGPD.

Complementa ainda, o artigo 9º § 1º desta mesma lei que o consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Assim, o IDEC muito bem argumenta em petição inicial que os passageiros da VIAQUTRO não tiveram o conhecimento de que estavam participando da pesquisa e muito menos sabiam a finalidade específica da coleta de seus dados.

Contudo, e se houvesse um consentimento nesta situação, faria alguma diferença na prevenção dos riscos? Qual seria a liberdade deste consentimento? Diante das reflexões postas, tem-se que a LGPD nos coloca, em linhas gerais que o consentimento como o cerne da lei, por meio do qual o direito a proteção de dados é exercido. Mas, na prática, como por exemplo, no caso em comento, leva-se a crer que o consentimento não passa de uma mera ficção ou burocracia da lei, pois este não tem força sozinho, vez que não basta apenas definir se os determinados dados dos titulares podem ou não serem coletados, quando não deixa translúcido em que contexto os dados serão usados e para qual finalidade foram coletados.

Pelo exposto, temos que o consentimento é sem dúvida, muito importante, mas não é possível somente por meio dele, sanar os riscos ou garantir que determinada informação não seja interpretada em determinado contexto.

2. O "profiling" no caso concreto

Ademais, após elencado o conceito de consentimento, importa trazer a tona o conceito de "*profiling*", técnica empregada por diversas empresas que utilizam dados sem o consentimento dos consumidores com vias a potencializar o lucro. Um dos principais pontos no caso analisado é a acusação da possibilidade da empresa ré utilizar para fins econômicos os dados dos usuários.

Nesse sentido, o fato se enquadra perfeitamente no que se conhece como "*profiling*", segundo Bruno Ricardo Bioni, o "*profiling*" é a pratica "em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet." (p. 122, 2019).

Ao instalar as câmeras próximas aos telões de propaganda havia a possibilidade de captação das reações dos consumidores, desse modo, ao captar um grande número de reações a empresa poderia formar um perfil dos principais usuários do metrô, bem como quais grupos tiveram as reações mais positivas a determinada propaganda.

Ocorre que embora a acusação seja que a empresa estaria realizando essa prática sua defesa foi que as câmeras não guardariam dados do consumidor, portanto seria impossível montar um perfil de consumidores de modo que o "*profiling*" não existiria no caso. Após essa defesa, a ré trouxe à tona alegações importantes como a diferença de detecção e reconhecimento, as quais impactam amplamente

nas formas em que as empresas que trabalham com dados operam, desse modo o tópico a seguir dissertará sobre o assunto.

2.1. Detecção *versus* Reconhecimento facial

Segundo a Viaquatro, apenas estaria sendo utilizado o sistema de detecção, ou seja, as câmeras apenas detectariam que havia um rosto ali, porém sem guardar dados das pessoas.

Nesse sentido, Antônio Henrique Dianin, 2019, defende que a detecção de faces é o processo que o *software* de computador precisa percorrer para determinar se existe realmente uma ou mais faces na imagem de uma foto ou vídeo. Ele não alude a identidade dos rostos que estão na foto, apenas detecta se existem rostos na mesma. Portanto detecção facial por si só não se lembra ou armazena detalhes de rostos. Se o *software* identifica um rosto de uma pessoa em particular em uma imagem, e depois detecta o mesmo rosto em outra imagem, ele não reconhece que eles são a mesma pessoa, somente reconhece que há um rosto de alguém em cada imagem. A detecção de rostos pode ser capaz de pegar algumas informações demográficas, por exemplo, a idade ou o sexo da pessoa em cada imagem, mas não muito mais do que isso. O *software* de detecção facial por si só não é capaz de reconhecer indivíduos.

Todavia, o IDEC corrobora que não houve detecção e sim reconhecimento facial. Sendo assim, Karina Menezes, 2019, entende que diferente da detecção há o sistema de reconhecimento facial, que funciona com a probabilidade de um rosto ser o mesmo de um documento ou de algum rosto armazenado em base de dados. E esse processo é realizado a partir dos seguintes passos: inicialmente, a ferramenta realiza uma captura do rosto do ser humano por meio de uma foto ou de um vídeo; após é feita uma análise da imagem, e é neste momento que as características únicas da pessoa são analisadas, por meio do que se conhece como pontos nodais, que são a medida entre os olhos, o tamanho da mandíbula ou as maçãs do rosto; a partir dessa análise, é extraída uma espécie de "assinatura" única do indivíduo, que é comparada a outras assinaturas capturadas por meio de documentos e imagens, armazenadas em um banco de dados; por fim, a ferramenta estabelece o grau de compatibilidade entre as imagens analisadas. A partir dessa aproximação, determina-se o quanto a pessoa é ou não a mesma das demais imagens analisadas.

Portanto, o reconhecimento facial vislumbra um dado sensível, ou seja, uma nova categoria criada pela Lei 13.709/2018, que o dado capaz de revelar a origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa, essa definição ressalta a gravidade do caso se configurado o *profilling*, ou mesmo a mera captura de dados. É possível perceber que nesse ponto a LGPD, trouxe conceitos importantes aptos a coibir práticas como estas.

De acordo com os conceitos acima, a estratégia de defesa da VIAQUATRO toma por base que a descaracterização do reconhecimento também tornaria a ação ineficaz, uma vez que a mera detecção não guardaria dados, apenas detectaria que havia um rosto em determinado local, desse modo toda a discussão no tocante ao reconhecimento seria ineficaz.

Ocorre que embora a empresa ré tenha alegado essa questão, não houve comprovação de que utilizava as câmeras apenas para a detecção. Tem-se um caso em que embora acertadamente tenha prescrito sobre a questão dos dados sensíveis a legislação não foi abrangente o suficiente, embora exista uma abordagem quanto ao consentimento, as técnicas de "*profiling*" são ainda mais complexas, exigindo detalhamento por parte do legislador.

Conclusão

Por fim, ao analisar o caso, pode-se observar que a técnica de "*profiling*", mesmo com a legislação vigente pode persistir, de forma que as empresas de modo ardiloso podem tentar se desvencilhar da acusação por meio da alegação de mera detecção.

Nesse sentido, o Judiciário tem atuado de forma ativa a impedir essa situação, com a determinação de retirada das câmeras e cessação das filmagens. Tem-se que uma mera perícia que possa indicar se houve uso para fins econômicos pode trazer uma resposta, porém não garante a prevenção dos riscos da utilização para fins desconhecidos dos dados já coletados. Assim, somente em ponto mais avançado do litígio haverá o esclarecimento, visto que não há até o momento a diferenciação expressa entre reconhecimento e detecção na legislação.

Portanto, mesmo sem uma resolução do caso concreto, pode-se observar que a legislação avançou muito no tocante a proteção de dados, embora ainda existam lacunas, estas podem ser preenchidas pelo Judiciário, ou mesmo pela Agência Nacional de Proteção de Dados, a qual dispõe do poder de interpretar a lei, ainda que o ideal seja uma legislação especificando os abusos a serem coibidos.

Referências bibliográficas

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

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 de outubro de 2019.

_____. **Lei nº. 8.078, de 11 de setembro de 1990.** Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 07 de outubro de 2019.

_____. **Lei nº. 12.527, de 18 de novembro de 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 05 de outubro de 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 de outubro de 2019.

BRASIL. Tribunal de Justiça de São Paulo. **Ação Civil Pública n. 1090663-42.2018.8.26.0100,** 30/08/2018. Proposta pelo Idec – Instituto Brasileiro de Defesa do Consumidor contra Concessionaria da Linha 4 do Metro de São Paulo S.A. (Via Quatro).

COSTA, Mariana Monteiro. **A Era da Vigilância no Ciberespaço e os Impactos da nova Lei Geral de Proteção de Dados Pessoais no Brasil:** Reflexos no direito à privacidade, 2018. Trabalho de conclusão de curso – Universidade Federal do Rio de Janeiro, Rio de Janeiro 2018.

DE SOUZA MACHADO, Fernando Inglez; RUARO, Regina Linden. Publicidade comportamental, proteção de dados pessoais e o direito do consumidor. **Compedi Law Review**, v.3, n.2, p.421-440,2017.

DIANIN, Antonio Henrique. **As diferenças entre detecção de rosto e reconhecimento de rosto.** Disponível em: https://www.portaleducacao.com.br/conteudo/artigos/informatica/asdiferencas-entre-deteccao-de-rosto-e-reconhecimento-de-rosto/67656. Acesso em: 10 de setembro de 2019.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 1ª ed. Goiânia: RM, Digial Education, 2019.

MENEZES, Karina. **Você sabe a diferença entre autenticação, detecção e reconhecimento facial?**

PECK, Patricia. **Direito Digital,** 5ª Ed. São Paulo: Saraiva, 2013.

6.9. Da livre publicidade ao dever de respeito pelos dados pessoais – *Gabriel Oliveira de Aguiar Borges*[162], *Luciano Nunes Marques*[163] *& Arthur Pinheiro Basan*[164]

Resumo

[162] Centro Universitário do Triângulo (Unitri/MG).

[163] Centro Universitário do Triângulo (Unitri/MG).

[164] Universidade de Rio Verde (Unirv/GO).

A sociedade atual se mostra vulnerável a abusos do mercado. Assim, é comum que a publicidade utilize técnicas de cruzamento de dados pessoais, moldando a mente do consumidor. Este trabalho almeja a analisar as abusividades das publicidades virtuais, frente ao direito à proteção de dados.

Palavras-chave: Privacidade; publicidade; proteção de dados.

Abstract

Nowadays society is vulnerable to marketing abuses. Therefore, it is common to publicity to use personal data crossing techniques, sculpting the consumers' minds. This work aims to analyses the abuses of virtual publicities, from the point of view of the right to data protection.

Keywords: Privacy. Publicity. Data Protection.

Introdução

A sociedade contemporânea, em constante transformação, é marcada pela fluidez das relações sociais, em um contexto em que o consumo ganha destaque na formação da identidade. Essa sociedade de consumo se vê inserida em um ambiente de intensa produção e disseminação de informação e a sociedade da informação possui riscos altíssimos, frente à imediatidade, instantaneidade e liquidez da informação (PINHEIRO, 2018, p. 218).

Nesse contexto, deve-se adotar instrumentos que garantam que essa dimensão de convivência global seja um *locus* de promoção da pessoa humana, nunca de aviltamento ou rebaixamento da qualidade de vida (MARTINS, 2018, p. 401).

Assim, há que se balancear a tecnologia e a privacidade, como direito fundamental essencial ao livre desenvolvimento da personalidade, frente à perspectiva que os dados, especialmente os dados pessoais, não possuem apenas valor econômico e social, mas, também, valor jurídico, sendo, pois, exigentes de ampla tutela (MARTINS, 2018, p. 405).

Nesse diapasão, é possível constatar ampla evolução do conceito de privacidade, vez que, hoje, existe o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada. É dizer, o direito à privacidade é verdadeiro instrumento fundamental contra a discriminação e a favor da igualdade e da liberdade (RODOTÀ, 2008, p. 7).

O tratamento de dados pessoais, especialmente por processos automatizados, é atividade de risco, que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais. Assim, há que se instituir mecanismos que possibilitem à pessoa conhecer e controlar seus próprios dados, que são expressão direta de sua própria personalidade. Por isso, a proteção de dados pessoais é considerada direito fundamental em diversos ordenamentos jurídicos (DONEDA, 2011, p. 91-108).

A Lei Geral de Proteção de Dados cria regulamentação para o uso, proteção e transferência de dados pessoais, tanto no âmbito privado quanto no âmbito público. Tal norma se encontra fundada sobre os direitos fundamentais de liberdade e privacidade, sem falar na livre iniciativa e desenvolvimento econômico e tecnológico do país, dispondo de diversos fundamentos, dentre os quais se destaca o da transparência para o uso de dados pessoais e a respectiva responsabilização, bem como o da finalidade, mediante o qual os dados só poderão ser utilizados para as finalidades para as quais foram coletados e previamente informados aos seus titulares.

Sendo assim, pergunta-se: como equalizar a livre publicidade e o dever de respeito pelos dados pessoais em um contexto em que estes são constantemente utilizados com vistas à realização de publicidade dirigida?

1. Da relevância da atividade publicitária e da proteção de dados

É relevante o papel da publicidade na sociedade, vez que é por meio dela que se oferece acesso rápido e fácil a bens e serviços, ajudando a satisfazer as mais diversas necessidades humanas e ainda possibilitar a inovação em práticas de empreendedorismo, gerando novas fontes de riqueza. Há quem defenda, inclusive, que a publicidade encontra supedâneo no direito fundamental à liberdade de expressão (BARROSO, 2001, p. 263).

De qualquer maneira, enquanto atividade mercadológica, há que se entender que a publicidade se liga à livre iniciativa da atividade econômica, de forma que não se pode olvidar que a atividade econômica se vê limitada por vários princípios, como é o caso da defesa do consumidor, presente no art. 170, V, da Constituição da República.

Assim, em que pese a era da informação seja excelente espaço para a promoção da pessoa e da democracia, ela também se constitui como terra fértil para abusos por parte do mercado, em seu desejo exacerbado pelo lucro (SANDEL, 2012, p. 11), o que impulsiona a efetivação de uma sociedade cada vez mais consumista (BAUMAN, 2008). Assim, demonstra-se a necessidade de cada vez mais atenção e cuidado por parte do Direito, especialmente com vistas à concretização dos direitos fundamentais, fragilizados pela exposição à sociedade informatizada (MARQUES, 2004, p. 94).

Portanto, há que se questionar se as normas vigentes são adequadas e suficientes para a finalidade de promoção da integral tutela das pessoas expostas às práticas publicitárias do mercado virtual, cumprindo o *mandamus* constitucional de promoção da dignidade humana.

Neste diapasão, interessante ressaltar que todas as maneiras de publicidade praticadas no mundo virtual, mesmo as que se alimentam de dados pessoais e sensíveis das pessoas, são detectáveis e tratáveis pelo direito pátrio, com destaque para a proteção garantida pelo Código de Defesa do Consumidor, que

garante aplicabilidade plena e imediata sobre as novas modalidades de publicidade oriundas das práticas virtuais.

Outrossim, menciona-se a Lei 12.965/14 (Marco Civil da Internet), que consolida a proteção de dados pessoais como um princípio para o uso da *internet* no Brasil (art. 3º, III), o que garante o direito da pessoa de só fornecer seus dados pessoais mediante consentimento livre, expresso e informado (art. 7º, VII).

Neste ponto, destaca-se que o Brasil não foi pioneiro nas tratativas a respeito da privacidade e do uso da dados pessoais, como se observa, por exemplo, pela promulgação, na Europa, da Regulamentação Geral de Proteção aos Dados (GDPR), que garantiu aos consumidores maior proteção sobre seus próprios dados. Segundo tal regulamento, antes de armazenar qualquer tipo de dado do consumidor, a empresa deve especificar de forma clara e compreensível as finalidades do tratamento dos dados e, mesmo assim, o usuário, a qualquer momento, poderá pedir acesso a todo o banco de informações que a empresa detém sobre si, bem como solicitar alterações ou até a exclusão do cadastro.

No Brasil, foi promulgada a Lei 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), com vistas à normatização do tratamento de dados, que até então era uma "terra sem lei" no país (COTS; OLIVEIRA, 2018, p. 22).

Insta salientar que não só o Estado possui o dever de proteção dos direitos fundamentais (CANARIS, 2003), em especial os dados pessoais, mas também os particulares o têm, demonstrando a eficácia horizontal das normas fundamentais (DUQUE, 2013).

Despiciendo lembrar que, na sociedade contemporânea, marcada pela cada vez maior globalização econômica, a informação é elemento substancial e vital para as relações sociais e se tornou, em especial os dados pessoais, o principal insumo da atividade econômica (MAGRANI, 2018, p. 90), em todos os setores possíveis. Assim, quem tem acesso a dados tem poder na sociedade, tanto no setor público como no setor privado (PINHEIRO, 2018, p. 13).

Por isso é que uma das características mais importantes da LGPD é a expressa disposição de que a norma é aplicada contra o tratamento ilegal de dados pessoais praticado tanto por pessoa natural quanto por pessoa jurídica, independentemente se de direito público ou de direito privado.

É dizer, da mesma forma que o Código de Defesa do Consumidor decorre do dever fundamental de proteção do consumidor como agente constitucionalmente designado, a LGPD trata de legislação que tutela direitos fundamentais de modo transversal, ou seja, independentemente se em relação de direito público ou privado.

Entretanto, ao se considerar que a grande maioria das relações jurídicas envolvendo dados pessoais no âmbito privado são consumeristas, é notória a vulnerabilidade de uma das partes, o que demanda maior atenção e, portanto, uma tutela mais ampla (BIONI, 2019, p. 274).

2. Liberdade publicitária *versus* proteção de dados pessoais no contexto da "virada kantiana"

No âmbito do *Common Law*, o direito à Privacidade decorre da Liberdade, ao passo que, no *Civil Law*, ele é corolário da Dignidade Humana (WHITMAN, 2004).

A liberdade é um direito de característica normogenética, com a capacidade de criar muitos outros direitos, *e.g.*, direito de locomoção.

Kant traz uma noção de dignidade contraposta à de "preço": o que tem preço pode ser trocado por algo equivalente. Quando algo não pode ser trocado, nem substituído, diz-se que não tem preço, mas dignidade (2000, p. 134). Na lição de Nelson Rosenvald, enquanto imperativo categórico, "a dignidade é um valor moral intrínseco ao homem que jamais poderá ser relativizado pelo Estado ou pela sociedade" (2005, p. 3).

Assim, Kant aproxima dignidade humana e liberdade, uma vez que o ser humano age conforme a sua vontade no uso da razão, tornando a liberdade um princípio fundamental, sem o qual o homem não passa de um instrumento.

No final do século XX, alguns filósofos, denominados *neokantianos*, começaram a descrever uma evidente relação entre ética e direito e a busca por valores. Segundo Torres (2009, p. 503-525), em meados da década de 1970, O. Höffe cunha a expressão "virada kantiana" para designar o movimento, o que marca uma reaproximação entre direito e moral.

Interessante mencionar que, nesse contexto de aproximação entre Direito e moral é que se destaca a objetividade dos valores, em especial nos princípios de justiça, revelando, conforme exposição de Robert Nozick, a importância da argumentação jurídica (*apud* TORRES, 2009, p. 511).

Nesse diapasão, consideramos que a "virada kantiana" é expressão do que se encontra acima de qualquer preço, a exemplo da pessoa humana, e, portanto, compreende uma dignidade, de forma que a própria finalidade do Direito justifica esse ideal (MEIRELES, 2009, P. 301).

Em uma primeira análise, deve-se considerar que essa "virada kantiana" no Direito nada mais é do que o redirecionamento da pessoa humana para o epicentro do sistema jurídico.

Com efeito, neste momento da pesquisa, será feita uma abordagem pelo modo com que esse fenômeno se deu no ordenamento brasileiro, inicialmente, de uma maneira geral por toda a jurisdição pátria, para,

em seguida, descrever a transformação no direito privado e, assim, compreender a especial proteção dada à pessoa humana no nosso direito privado.

De uma maneira geral, Barroso afirma que um dos marcos filosóficos de transformação jurídica brasileira ocorreu a partir da aproximação entre Filosofia e Direito, causada pelo desenvolvimento da teoria dos direitos fundamentais e edificada sob a égide da dignidade humana. O autor defende, assim, que o marco teórico e histórico que justifica essa "virada kantiana" no ordenamento pátrio é a promulgação da CF/88 (BARROSO, 2010, p. 214).

Importante destacar que a CF/88 fez um giro epistemológico ao eleger a dignidade humana como fundamento da República Federativa do Brasil, o que se depreende de seu art. 1º, III, que institui a cláusula geral de tutela e promoção da pessoa humana, posicionando a pessoa no centro do nosso Direito (TEPEDINO, 2008, P. 54). Sobre isso, Piero Perlingieri afirma que "o princípio da tutela da pessoa, como supremo princípio constitucional, funda a legitimidade do ordenamento e a soberania do Estado" (1999, P. 460-461).

Assim, frente ao contexto de uma ordem constitucional que foi tão protetiva aos direitos fundamentais, como é a nossa, o Direito Privado passa a sofrer fortes influências não só da Lei Maior, como, também, das próprias mutações da sociedade, que passa a exigir leis privadas mais condizentes com os anseios democráticos, sociais e humanistas que o constituinte originário instituiu.

É dizer, das mudanças sociais que culminaram com a nova CRFB, em um contexto de "virada kantiana", também saiu a influência para mutações no direito privado enquanto "direito dos particulares como portadores de sua própria singularidade" (MARTINS-COSTA, 2002, p. 131).

Sobre isso, vale colacionar a lição de Gustavo Tepedino, no sentido de que

> A pessoa humana, portanto – e não mais o sujeito de direito neutro, anônimo e titular de patrimônio -, qualificada na concreta relação jurídica em que se insere, de acordo com o valor social de sua atividade, e protegida pelo ordenamento segundo o grau de vulnerabilidade que apresenta, torna-se a categoria central do direito privado (2006, p. 342).

Frente a esse contexto, o Direito privado também enquadra a pessoa humana como fonte primária de todo o seu ordenamento, praticando, pois, uma verdadeira "virada kantiana".

Com relação a essa importância da pessoa humana para o Direito Privado, Perlingieri afirma que

> o primado dos valores da pessoa humana e dos seus direitos fundamentais exclui que a área do direito privado possa ser exaurida em uma concepção patrimonialista, fundada ora sobre a centralidade da propriedade, ora sobre a

> noção de empresa. O direito civil constitucional – segundo a tendência do constitucionalismo contemporâneo – reconhece que a forte ideia do sistema é não somente o mercado, mas também a dignidade da pessoa, de uma perspectiva que tende a despatrimonializar o direito (2008, p. 5).

Note-se que nem todas as pessoas possuem situações patrimoniais a serem protegidas (crédito, propriedade, posse, dentre outras), mas há situações existenciais comuns a qualquer pessoa humana que vão exigir tutela: vida, saúde, honra, nome, etc (MEIRELES, 2009, p. XVIII). Tal fato dá indícios de que, sob essa ótica, o vértice do direito privado só pode estar contido no *ser* em supremacia ao *ter,* isto é, na realização dos legítimos interesses existenciais das pessoas (FACHIN, 2015, p. 75).

Nesse contexto, sob a égide da "virada kantiana" no direito privado, para além do fundamento humanista, destaca-se a função social de seus institutos, de modo que, nas situações existenciais, fica evidente que não há linha divisória entre interesse individual e interesse coletivo ou social, vez que afeitas à tutela da pessoa humana, não havendo, no nosso Direito, maior fim social que este. Em outras palavras, pelas lentes da solidariedade, a tutela da pessoa humana sempre terá análise prioritária, com vistas, no caso do presente trabalho, a reparar o dano sofrido pelos pais e pelo filho que nasce com a deficiência congênita.

Nesse sentido é que, tratando da primazia da pessoa humana no Direito privado, Tepedino defende que "a pessoa humana é o centro do ordenamento, impondo-se assim tratamento diferenciado entre os interesses patrimoniais e os existenciais. Em outras palavras, as situações patrimoniais devem ser funcionalizadas às existenciais" (2008, p. 365).

Na mesma linha, dessa primazia da dignidade humana, situando a pessoa nas peculiaridades de sua subjetividade, afirma Martins-Costa que

> se em primeiro plano está a pessoa humana valorada por si só, pelo exclusivo fato de ser pessoa – isto é, a pessoa em sua irredutível subjetividade e dignidade, dotada de personalidade singular e por isso mesmo titular de atributos e de interesses não mensuráveis economicamente -, passa o Direito a construir princípios e regras que visam a tutelar essa dimensão existencial, na qual, mais do que tudo, ressalta a dimensão ética das normas jurídicas. Então o direito civil reassume a sua direção etimológica e do direito dos indivíduos passa a ser considerado o direito dos civis, dos que portam em si os valores da civilidade (MARTINS-COSTA, 2002, p. 132).

Pelo exposto, a partir dos aspectos supramencionados, de tutela da pessoa dentro do ordenamento, em nível constitucional ou infraconstitucional, por leis gerais ou especiais, é notável a existência dessa

"virada kantiana" no direito brasileiro, dando ainda maior relevância, no que diz respeito ao direito privado, à promoção das situações existenciais das pessoas humanas.

Agora, pergunta-se como conceituar a privacidade. Em princípio, um significado básico poderia ser a capacidade que o indivíduo tem de controlar o fluxo de informações disponíveis sobre si mesmo (LEONARDI, 2012, p. 67).

Por sua vez, Túlio Lima Vianna assevera que é direito a partir do qual advém a tutela de três interesses: não ser monitorado, não ser registrado e não ser reconhecido, o que implica na não publicação de registros pessoais (2014, p. 73).

Muitas companhias têm realizado a coleta e o uso de informações armazenadas em bancos de dados para estimular o consumo, por intermédio do que ficou conhecido como "publicidade dirigida".

Nestes casos, o provedor faz uso do chamado *cross marketing*, que consiste em ações promocionais de determinados produtos e serviços, que, embora não gerem renda por si próprios, podem levar a lucros exorbitantes por meio da venda de outro produto.

Exemplo disso seria uma rede social que, não obstante seja de uso gratuito, faz a exigência de que o usuário seja submetido a um cadastro e concorde com condições de prestação de serviço que geram um banco de dados que pode ser usado para uma infinidade de fins comerciais.

Acerca do tema, Jonathan Zittrain indaga se é justo, por exemplo, um *website* de vendas gravar o tempo que cada usuário gasta olhando um item antes de efetivamente adquiri-lo (2008, p. 204).

Entendemos que não, pois esse tipo de conduta viola a privacidade do consumidor, oferecendo-lhe produtos conforme o que ele anda pesquisando, tornando mais alta a probabilidade de o consumidor clicar num anúncio e adquirir um produto por impulso, sem maiores reflexões, o que acaba tolhendo a liberdade do consumidor de refletir sobre uma conduta de consumo antes de praticá-la.

Conclusão

A partir da linha de raciocínio exposta alhures, evidencia-se que a utilização de dados, outrora sem limitação aparente, fora a desvairada ampliação do uso de publicidades de consumo, sob a lente do Estado Democrático de Direito, deverá ceder espaço às garantias de privacidade, intimidade e autodeterminação das pessoas.

Na realidade, a concepção de que a publicidade virtual, dentro da lógica do livre mercado, pode subsistir sob o amparo da liberdade absoluta, deve ceder ao sistema jurídico que deve combater condutas abusivas e, assim, proteger a pessoa humana em sua integridade, física ou psíquica, atenta à nova dimensão do ser humano, inserido na sociedade da informação.

Referências bibliográficas

BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição**: fundamentos de uma dogmática constitucional transformadora. 7ª ed. São Paulo: Saraiva, 2010.

_____. **Liberdade de expressão, direito à informação e banimento da publicidade de cigarro.** Temas de direito constitucional. Rio de Janeiro: Renovar, 2001.

BAUMAN, Zygmunt. **Vida para o consumo: a transformação das pessoas em mercadorias.** Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2008.

BIONI, Bruno Ricardo. **Proteção de dados pessoais** – A função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019.

CANARIS, Claus-Wilhelm. **Direitos fundamentais e direito privado**. Trad. de Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra, Almedina, 2003.

COTS, Márcio e OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada.** Thomsons Reuteres Brasil: São Paulo, 2018.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico.** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez/ 2011.

DUQUE, Marcelo Schenk. **Direito privado e constituição**: *drittwirkung* dos direitos fundamentais, construção de um modelo de convergência à luz dos contratos de consumo. São Paulo: Editora Revista dos Tribunais, 2013.

FACHIN, Luiz Edson. **Direito Civil:** sentidos, transformações e fins. Rio de Janeiro: Renovar, 2015.

KANT, Emmanuel. **Fundamentos da metafísica dos costumes.** São Paulo: Nova Cultural, 2000 (Col. Os pensadores).

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

MAGRANI, Eduardo. **A internet das coisas.** FGV Editora: Rio de Janeiro, 2018.

MARQUES, Cláudia Lima. **Confiança no Comércio Eletrônico e a Proteção do Consumidor**. São Paulo: Editora Revista dos Tribunais, 2004.

MARTINS, Fernando Rodrigues. Sociedade da informação e promoção à pessoa: empoderamento humano na concretude de novos direitos fundamentais. In: **Direito privado e**

policontexturalidade: fontes, fundamentos e emancipação. Rio de Janeiro: Lumen Juris, 2018.

MARTINS-COSTA, Judith. O novo Código Civil brasileiro: em busca da "ética da situação". In: MARTINS-COSTA, Judith e BRANCO, Gerson Luiz Carlos. **Diretrizes Teóricas do Novo Código Civil Brasileiro.** São Paulo: Saraiva, 2002.

MEIRELES, Rose Melo Vencelau. **Autonomia privada e dignidade humana.** Rio de janeiro: Renovar, 2009.

PERLINGIERI, Pietro. A doutrina do direito civil na legalidade constitucional. *In*: TEPEDINO, Gustavo (Org.) **Direito civil contemporâneo: novos problemas à luz da legalidade constitucional:** anais do congresso nacional de Direito Civil. Constitucional da Cidade do Rio de Janeiro. São Paulo: Atlas, 2008.

PERLINGIERI, Pietro**. O direito civil na legalidade constitucional**. Trad. de Maria Cristina de Cicco. Rio de Janeiro: Renovar, 1999.

PINHEIRO, Patrícia Peck. **Direito Digital Aplicado 3.0**. São Paulo: RT, 2018.

_____. **Proteção de dados pessoais: comentários à Lei n. 13.709/18 (LGPD).** Saraiva Educação: São Paulo, 2018.

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

ROSENVALD, Nelson. **Dignidade humana e boa-fé no Código Civil**. São Paulo: Saraiva, 2005.

SANDEL, Michael. **O que o dinheiro não compra**. Os limites morais do mercado. Rio de Janeiro: Civilização Brasileira, 2012.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento Civil-Constitucional brasileiro. In TEPEDINO, Gustavo. **Temas de Direito Civil**. 4ª Ed. Rio de Janeito: Renovar, 2008.

_____. Do sujeito de direito à pessoa humana. In TEPEDINO, Gustavo. **Temas de Direito Civil, Tomo II**. Rio de Janeito: Renovar, 2006.

_____. O Direito Civil-Constitucional e suas perspectivas atuais. *In:* TEPEDINO, Gustavo (Org.) **Direito civil contemporâneo: novos problemas à luz da legalidade**

constitucional: anais do congresso nacional de Direito Civil. Constitucional da Cidade do Rio de Janeiro. São Paulo: Atlas, 2008.

TORRES, Ricardo Lobo. A jurisprudência dos valores. In: SARMENTO, Daniel (org.). **Filosofia e teoria constitucional contemporânea.** Rio de Janeiro: Livraria e Editora Lumen Juris, 2009.

VIANNA, Tulio. (2014). **Transparência pública, opacidade privada: o direito como instrumento de limitação do poder na sociedade de controle.** oai:ufpr.br:222407. 10.13140/2.1.3170.4002.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity Versus Liberty. **YALE Law Journal.** Vol. 113 (2004). Disponível em: http://www.yalelawjournal.org/images/pdfs/246.pdf. Acesso em 03 dez. 2019.

ZITTRAIN, Jonathan. **The future of Internet and how to stop it.** New Haven/London: Yale University Press, 2008.

6.10. O impacto da Lei Geral de Proteção de Dados nos contratos de prestação de serviços educacionais – *Luiz Fernando Salles Giannellini*[165] *& Renata Mota Maciel*[166]

Resumo

Os contratos de prestação de serviços educacionais serão analisados no presente artigo com vistas a recém sancionada Lei n.º 13.709/18, que dispõe sobre a proteção de dados pessoais. O objetivo enfocado neste trabalho será revelar quais serão os principais impactos que a novel legislação imporá a esses contratos. A metodologia utilizada ancorou-se, no método indutivo, já que este artigo parte do exame de premissas necessárias para revelar uma nova realidade que, eventualmente, poderá advir da aplicação desse novo marco legal. Conclui-se que a aplicação da nova legislação, ao conferir segurança e proteção ao direito fundamental da privacidade, além de ampliar ainda mais os direitos outrora reconhecidos pelo Código de Defesa do Consumidor, destinou-se a aprimorar o ferramental jurídico já existente, a fim de

[165] Mestrando em Direito pela Universidade Nove de Julho – UNINOVE.

[166] Professora Permanente do Programa de pós-graduação stricto sensu em Direito da Universidade Nove de Julho – UNINOVE.

coibir abusos cometidos pelos detentores do poder econômico, numa sociedade massificada onde o acesso à informação tem o poder de criar ou revolucionar novos modelos de negócio.

Palavras-Chave: Contratos; Serviços; Educação; Proteção de Dados; Abusos.

Abstract

The contracts for the provision of educational services will be analyzed in this article with a view to the recently enacted Law No. 13,709 / 18, which provides for the protection of personal data. The objective focused on this work will be to reveal the main impacts that the novel legislation will impose on these contracts. The methodology used was anchored in the inductive method, since this article starts from the examination of premises necessary to reveal a new reality that, possibly, could arise from the application of this new legal framework. It is concluded that the application of the new legislation, by granting security and protection to the fundamental right of privacy, in addition to further expanding the rights once recognized by the Consumer Protection Code, was aimed at improving existing legal tools in order to curb abuses committed by the holders of economic power in a mass society where access to information has the power to create or revolutionize new business models.

Keywords: Contracts; Services; Education; Data Protection; Abuses.

Introdução

A proteção da privacidade das pessoas é, sem dúvida alguma, um dos pilares mais importantes da Democracia. É através da proteção da privacidade que se reconhece a dignidade da pessoa humana como fundamento indissociável da liberdade, da justiça e da paz. Tanto por isso, a Declaração Universal dos Direitos Humanos consagra em seu artigo 12º que:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.[167]

Parece evidente, nos dias atuais, que a privacidade deva receber disciplina jurídica e tutela do Estado.

[167] Disponível em: <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>

Ocorre que, a realidade nem sempre foi assim, inclusive nos países ocidentais, onde as liberdades públicas sempre tiveram enorme relevo na ordem jurídica nacional. O próprio Brasil, em passado não tão longínquo, foi regido por uma ordem jurídica caracterizada, dentre outras mazelas, pela censura, pelo autoritarismo, pela centralização do poder e, também, pela cassação de direitos políticos, nada obstante houvesse previsão de proteção, em todas as constituições anteriores, dos direitos individuais.

Numa verdadeira demonstração da importância do tema dada pelo legislador constituinte, a Constituição Federal de 1.988 consagrou, logo após o título I dedicado aos princípios fundamentais, a proteção dos direitos e garantias fundamentais, alterando a sua localização topológica no texto constitucional.

Passados mais de 30 (trinta) anos da promulgação da Carta Política, a proteção da privacidade, que nesse período de tempo jamais se esmoreceu, tornou-se tema de frequentes e intensos debates, seja na mais alta Corte do país - em célebres julgamentos, como por exemplo, no caso da autorização de publicação de biografias não autorizadas[168] - seja nas conversas entre amigos, nas ruas, no ambiente familiar e, especialmente, nas instituições de ensino.

A relevância do tema foi exponencialmente aumentada em razão de 02 (dois) fatores principais: (i) **o da globalização**, que nada mais é do que um processo de integração entres as várias partes do mundo, especialmente nos campos político, econômico, social e cultural, com vistas a formar um espaço internacional comum, dentro do qual bens, serviços e pessoas circulem da maneira mais desimpedida possível[169] e (ii) **do incremento do avanço tecnológico**, em especial da internet e suas aplicações, e dos ferramentais de veiculação de informações (smartphones, tablets e outros dispositivos).

Decorreu disso, logicamente, a necessidade de se estabelecer normas legais que pudessem dar efetiva concretude à proteção da privacidade, tal como consagrado na Carta Política. E, nesse sentido, muito diplomas normativos tiveram o condão de, ainda que superficialmente, cumprir esse desiderato.

No entanto, o mundo globalizado que estreita fronteiras permitindo a circulação de riqueza, pessoas e informações é o mesmo que exigiu que o Brasil, para se manter competitivo no cenário econômico global, proporcionando o mínimo de segurança jurídica, editasse um diploma normativo específico, através do qual se pudesse disciplinar em minúcias o modo pelo qual a privacidade das pessoas seria, concretamente, protegida.

[168] STF, ADI 4815, Relatora: Min. CÁRMEN LÚCIA, Tribunal Pleno, julgado em 10/06/2015, Processo Eletrônico DJE-018. Divulg. 29-01-2016. Public. 01-02-2016.

[169] PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado,* 8ª edição, p. 35.

Adveio, então, a Lei n.º 13.709, de 14 de agosto de 2018, que objetivou estabelecer normas legais para disciplinar tais relações (velocidade em que novas tecnologias são desenvolvidas para a comunicação com as pessoas), especialmente para dar proteção à individualidade e a privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação.

É inegável, por outro lado, que o ambiente escolar constitui-se num dos pilares sobre os quais se assenta um Estado Democrático de Direito, já que o atingimento e a consagração das liberdades públicas - seu maior primado – somente pode ser alcançado através da *Educação,* meio através do qual se ultimará o pleno desenvolvimento da pessoa, tornando-a apta ao exercício da cidadania e para o mercado de trabalho.

Nesse contexto, a justificativa para o presente trabalho pode ser referendada não somente pela crescente e complexa dimensão da futura aplicação da novel legislação a todas as situações em que haja necessidade de proteção de dados, inclusive nos contratos de prestação de serviços educacionais, que por sua própria natureza, apresentam diversos caracteres contemplados no inovador diploma normativo, seja de ordem pessoal ou financeira.

1. Educação

A Educação, que de acordo com o Ministro Celso de Mello, citado pelo também Ministro Alexandre de Moraes[170], é o "meio pelo qual se objetiva propiciar formação necessária ao desenvolvimento das aptidões, das potencialidades e da personalidade do educando", evidencia-se como a principal ferramenta, não apenas de instrução destinada a preparar alguém para o trabalho, mas de verdadeira transformação social.

Não é de hoje que a educação é um dos pilares da sociedade moderna. No Brasil, sua importância sempre foi reconhecida, embora somente na vigente Carta Política de 1988, conhecida como Constituição Cidadã, tenha passado a ter *status* constitucional de direito social[171], que José Afonso da Silva define como *"as prestações positivas pelo Estado direta ou indiretamente, enunciadas em normas constitucionais, que*

[170] DE MORAES, Alexandre. *Direito Constitucional.* Ed. Gen/Atlas. 35ª edição. São Paulo: 2019, p. 911.

[171] Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição (Redação dada pela Emenda Constitucional nº 90, de 2015).

possibilitam melhores condições de vida aos mais fracos"[172]. Não por outra razão, o próprio texto constitucional consagra que a educação é direito de todos e dever do Estado e da família[173].

Todavia, como adverte o Ministro Gilmar Mendes[174] do Supremo Tribunal Federal, a importância dada à *Educação* pela Constituição da República, lamentavelmente, não decorre das experiências e dos valores culturais da sociedade, mas sim do descaso do próprio Estado na execução dessa elementar política pública.

2. Contrato de Prestação de Serviços Educacionais

2.1. Conceito preambular de contrato

Antes da apresentação da ideia que está por trás deste subtítulo, convém destacar o conceito de contrato apresentado pela doutrina de escol.

Nesse sentido, Caio Mário da Silva Pereira apresenta o seguinte conceito para contrato:

> É um acordo de vontades, na conformidade da lei, e com a finalidade de adquirir, resguardar, transferir, conservar, modificar ou extinguir direitos.[175]

Ao referir que o acordo de vontades deve se dar na conformidade da lei, o citado autor fez questão de ressalvar que a comunhão de vontades deve obedecer aos requisitos subjetivos, objetivos e formais para ser válida[176]. No entanto, como advertem Pablo Stolze Gagliano e Rodolfo Pamplona Filho[177], a validade do negócio jurídico também é limitada pelos princípios constitucionais da teoria contratual,

[172] DA SILVA, José Afonso. *Curso de Direito Constitucional Positivo.* 22ª edição. Ed. Malheiros. São Paulo: 2003, p. 285.

[173] Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho.

[174] MENDES, Gilmar Ferreira. Branco. Paulo Gustavo Gonet. *Curso de Direito Constitucional.* 12ª edição, Ed. Saraivajur, São Paulo: 2017, p. 686.

[175] SILVA PEREIRA, Caio Mário da. Instituições de Direito Civil. Vol. III. CONTRATOS – Declaração Unilateral de Vontade – Responsabilidade Civil. 16ª edição. Ed. Gen/Forense, Rio de Janeiro: 2012, p. 7.

[176] Art. 104. A validade do negócio jurídico requer:
I - agente capaz;
II - objeto lícito, possível, determinado ou determinável;
III - forma prescrita ou não defesa em lei.

[177] GAGLIANO, Pablo Stolze. Pamplona Filho, Rodolfo. Novo Curso de Direito Civil. Contratos: teoria geral. Vol. IV. Tomo I. Ed. Saraiva. 7ª edição, São Paulo: 2011, p. 47-48.

assim como pela boa fé objetiva e por sua função social, vale dizer: tanto na conclusão quanto na execução.

2.2. Contrato de Prestação de Serviços Educacionais

Superada essa ideia inicial, a conceituação do que viria a ser contrato de prestação de serviços educacionais transpassa pelo conceito propriamente dito do que a lei define como serviço. E o Código de Defesa do Consumidor, assim o faz no parágrafo 2º do artigo 3º, estabelecendo que "serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista."

Soma-se à exceção trazida pela própria lei, os serviços que assumem caráter público, assim definidos por Odete Medauar[178] como as "atividades que propiciam diretamente benefícios e bens, aos administrados, não se incluindo aí as de preparação de infraestruturas (...)"

Assim, à luz dos ensinamentos do Ministro Celso de Mello e considerando o conceito clássico de contrato, pode-se concluir que contrato de prestação de serviços educacionais é aquele por meio do qual a instituição de ensino se obriga a ministrar formação acadêmica, transmitindo conhecimento e desenvolvendo aptidões, que dotarão o educando de capacidades para se desenvolver e qualificar para o mercado de trabalho.

2.3. Incidência do Código de Defesa do Consumidor nos Contratos de Prestação de Serviços Privados e Inaplicabilidade nos Contratos de Prestação de Serviços Públicos

A partir das afirmações acima deduzidas, intuitivamente, se conclui que a prestação de serviços educacionais privadas, evidentemente, sofre a incidência da legislação do consumidor.

Isso porque, tal como adverte o jurista Newton De Lucca[179], pouco ou nada importa perquirir o sentido etimológico do vocábulo "serviço" se a própria lei a define como a atividade fornecida no mercado de consumo, mas sim a exata compreensão do que seriam ***atividade*** e ***mercado de consumo***. Enquanto aquela se consubstancia numa "sucessão repetida de atos, praticados de maneira organizada, de molde a caracterizar-se numa constante oferta de bens e serviços à coletividade"[180], este deve ser entendido como a "cadeia das relações de troca de bens e prestação de serviços, realizadas pelos diversos agentes econômicos"[181].

[178] MEDAUAR, Odete. Direito Administrativo Moderno. 4ª edição, Ed. RT, São Paulo: 2000, p. 369.

[179] DE LUCCA, Newton. *Direito do Consumidor – Teoria Geral da Relação Jurídica de Consumo.* Ed. Quartier Latin. 2ª edição. São Paulo: 2008, p. 152.

[180] DE LUCCA, Newton. *Direito do Consumidor – Aspectos Práticos – Perguntas e Respostas.* Edipro. 2ª edição. São Paulo: 2000, p. 182.

[181] DE LUCCA, Newton. *Direito do Consumidor* ... ob. cit., p. 153.

Engana-se, porém, quem, induzido pela literalidade da norma, acredita que para qualificar uma atividade posta no mercado de consumo como serviço se exija remuneração (contraprestação) por parte do consumidor. Com efeito, a remuneração referida pela lei não é relacionada à figura do consumidor, mas sim ao serviço em si, o que torna evidente que a remuneração preconizada na lei pode ser direta ou indireta.

Nas palavras de Cláudia Lima Marques:

> "Na prática só existem três possibilidades: a) ou o serviço é remunerado diretamente pelo consumidor; b) ou o serviço não é oneroso para o consumidor, mas remunerado indiretamente, não havendo enriquecimento ilícito do fornecedor, pois o sem enriquecimento tem causa no contrato de fornecimento de serviço, causa esta que é justamente a remuneração indireta do fornecedor; c) ou o serviço não é oneroso de maneira nenhuma (serviço gratuito totalmente) nem o fornecedor remunerado de maneira nenhuma, pois se ele fosse 'remunerado' indiretamente haveria enriquecimento sem causa de uma das partes".

A jurisprudência dos tribunais pátrios, em especial do Superior Tribunal de Justiça, é uníssona no sentido da plena aplicabilidade das disposições do Código de Defesa do Consumidor à prestação de serviços de educação exploradas, mediante autorização do Poder Público[182], pela iniciativa privada, conforme se infere do excerto abaixo transcrito:

> "ADMINISTRATIVO E PROCESSUAL CIVIL. INSTITUIÇÃO DE ENSINO SUPERIOR. EXPEDIÇÃO DE DOCUMENTOS CONCERNENTES À VIDA ACADÊMICA DO ALUNO. COBRANÇA. ALEGAÇÃO DE OFENSA AOS ARTS. 1º, § 5º, DA LEI N. 9.870/99, 39, V, E 51, IV, DO CDC. NECESSIDADE DE INTERPRETAR ATO NORMATIVO QUE NÃO SE ENQUADRA NO CONCEITO DE TRATADO OU LEI FEDERAL. 1. Em que pese ter a parte recorrente alegado ofensa aos arts. 1º, § 5º, da Lei n. 9.870/99; 39, V, e 51, IV, do CDC, verifica-se que o exame da controvérsia, tal como enfrentada pela Corte de origem, demanda a interpretação da Portaria Normativa n. 40/2007 do MEC e

[182] Art. 209. O ensino é livre à iniciativa privada, atendidas as seguintes condições:
I - cumprimento das normas gerais da educação nacional;
II - autorização e avaliação de qualidade pelo Poder Público.

> do Parecer CNE/CES n. 164/2009, atos normativos estes que não se enquadram no conceito de "tratado ou lei federal" de que cuida o art. 105, III, a, da CF. 2. Agravo interno desprovido."[183]

No entanto, igual raciocínio, s.m.j., não se aplica quanto aos serviços de educação públicos, isto é, aqueles prestados pela Administração Pública Direta, porque estes se encontram fora do conceito de mercado, não são explorados por agentes econômicos e não se destinam à exploração de atividade econômica com interesses voltados à obtenção de lucro. Nesse sentido, aliás, é o escólio de Alberto Canellas Neto, para quem

> "Em suma: o MERCADO capitalista (neoliberal), caracterizado pelo intuito lucrativo e pela "concorrência", É O ESPAÇO ("inconfundível com os da ordem exclusivamente social") ONDE O CONSUMIDOR PROMOVE SUAS RELAÇÕES COM OS FORNECEDORES, TANTO QUE SE PRETENDEU PROTEGÊ-LO (CRFB/1988, ART. 170, V).[184]

Deve ser ressalvada, no entanto, a possibilidade de incidência da legislação consumerista aos serviços públicos de educação prestados pela Administração Indireta, *v.g.*, no caso das autarquias municipais e/ou estaduais, que diante do permissivo constitucional do artigo 242[185], podem auferir receita, tornando tais instituições fornecedoras de serviços. Nesse sentido, confira-se os arestos do Tribunal de Justiça bandeirante, cujas ementas estão abaixo transcritas:

> "CIVIL - PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS - REPETIÇÃO DE INDÉBITO - MULTA MORATÓRIA - REGRA DE ORDEM PÚBLICA - INCIDÊNCIA DO CDC - REDUÇÃO -ADMISSIBILIDADE - ATUALIZAÇÃO MONETÁRIA TABELA PRÁTICA - DEVOLUÇÃO EM DOBRO MÁ-FÉ - COMPROVAÇÃO - INOCORRÊNCIA - SENTENÇA MANTIDA. 1. O princípio da força vinculante das convenções cede passo à regra de ordem pública do Código de Defesa

[183] AgInt no REsp 1490498/RS, Rel. Ministro SÉRGIO KUKINA, PRIMEIRA TURMA, julgado em 14/08/2018, DJe 23/08/2018.

[184] CANELLAS NETO, Alberto. (In)aplicabilidade do CDC aos serviços de saúde e educação públicas. Enfoque: o objeto de consumo. *Revista da AGU*, Brasília-DF, ano XIII, n. 41, p. 85-116, jul./set.2014.

[185] Art. 242. O princípio do art. 206, IV, não se aplica às instituições educacionais oficiais criadas por lei estadual ou municipal e existentes na data da promulgação desta Constituição, que não sejam total ou preponderantemente mantidas com recursos públicos.

> do Consumidor, que limita a multa moratória ao patamar de 2% - 2. A ausência de índice de atualização monetária determinado, torna plenamente cabível a aplicação da Tabela Prática do Egrégio Tribunal de Justiça de São Paulo. 3. A adoção de percentagem por perspectiva da prestadora do serviço não implica, necessariamente, em cobrança indevida em detrimento da tomadora do serviço, sobremodo se os contratantes ajustaram acordos para pagamento das mensalidades escolares vencidas, circunstância que infirma a repetição em dobro do valor pago pelo autor. 4. Recursos improvidos."[186]

> Mensalidade escolar — Cobrança - Procedência parcial - Mensalidades cobradas de fevereiro a dezembro de 2000, com ação ajuizada em 28/11/01 - Redução da multa de 6% para 2% - Maioria que entendeu inaplicável o disposto no art. 52, § Io, do CDC - Incidência de correção monetária e juros moratórios a partir do vencimento de cada parcela - Apelação provida."[187]

3. Lei Geral de Proteção de Dados

De acordo com a exposição de motivos constante do Projeto de Lei 4060/2012 (PL 53/18 do Senado Federal), de relatoria do Deputado Federal Milton Monti, convertido na Lei n.º 13.709/2018 objeto de exame neste subcapítulo, percebe-se que o objetivo do citado diploma legal foi o de dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, de acordo com a Constituição da República Federativa do Brasil.

É bem verdade que diversas leis já vigentes no país já tiveram o condão de tratar, ainda que superficial e indiretamente, do mesmo tema, veiculando uma proteção de dados umbilicalmente vocacionadas ao objeto fulcral de cada um dos diplomas legais.

[186] TJSP; Apelação Cível 9174162-45.2005.8.26.0000; Relator (a): Artur Marques; Órgão Julgador: 35ª Câmara de Direito Privado; Foro de Taubaté - 4ª. Vara Cível; Data do Julgamento: 15/08/2011; Data de Registro: 15/08/2011.

[187] TJSP; Apelação com Revisão 9150499-67.2005.8.26.0000; Relator (a): Romeu Ricupero; Órgão Julgador: 36ª Câmara do D.OITAVO Grupo (Ext. 2° TAC); Foro de São Caetano do Sul - 4ª. Vara Cível; Data do Julgamento: 31/05/2007; Data de Registro: 03/07/2007.

A guisa de exemplos, podem ser citadas, além da própria Carta Política, (i) o Código de Defesa do Consumidor (L. 8078/90), (ii) o Código Civil (L. 10406/02), (iii) a Lei Geral de Telecomunicações (L. 9472/97), (iv) a Lei de Interceptações (L. 9296/96), (v) MP 2.200-2/2001 que instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, (vi) a Lei do Cadastro Positivo (l. 12414/11), (vii) a Lei de Acesso à Informação (L. 12527/11), (viii) o Estatuto da Criança e do Adolescente (L. 8069/90), (ix) a lei que dispôs sobre a tipificação criminal de delitos informáticos (L. 12.737/12, conhecida como lei Carolina Dieckmann) e, (ix) o Marco Civil da Internet (L. 12965/14) e seu decreto regulamentador (Decreto 8.771/16).

No entanto, nenhum dos diplomas normativos retro-mencionados tiveram como foco central e determinante a privacidade dos cidadãos, através da proteção de seus dados pessoais.

Por isso, impulsionada pelo escândalo de vazamento de dados de milhões de usuários da rede social Facebook, que tinham sido coletados pela consultoria política do então candidato à Presidência da República Donald Trump, Cambridge Analytica, a LGPD foi sancionada pelo então Presidente da República, Michel Temer, no último dia 14/8/18.

3.1. Notas introdutórias da LGPD

Apenas a título introdutório, é necessário observar que a LGPD, como ficou conhecida a Lei 13.709/2018, destina-se à proteção de dados pessoais de qualquer pessoa natural[188], que sejam ou venham a ser objeto de tratamento por qualquer pessoa, natural ou jurídica de direito público e/ou de direito privado, *on-line (online)* ou *off-line*.

Sua abrangência territorial para incluir empresas que, embora não tenham estabelecimento no Brasil, ofereçam serviço ao mercado consumidor interno e que coletem e tratem dados pessoais em território nacional, de brasileiro ou estrangeiro.[189]

A importância da inovação legislativa, do ponto de vista puramente empresarial, é a de que insere o país dentre aqueles que contam com legislação específica e avançada sobre a proteção de dados pessoais, circunstância que proporciona um ambiente de negócios mais seguro e previsível, para captação de recursos econômicos estrangeiros que, em última análise, visam fomentar a ordem econômica, através da livre iniciativa e da valorização do trabalho humano, conforme preconizado no artigo 170 da Carta Política[190].

[188] Vainzof, Rony. *LGPD – Lei Geral de Proteção de Dados Comentada.* Ed. RT, São Paulo: 2019, p. 19.

[189] Albani Siqueira, Antônio Henrique. *In Comentários à Lei Geral de Proteção de Dados.* Ed. RT. São Paulo: 2019, p. 48-49.

[190] Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:

São inúmeros os dados não sujeitos a tratamento e, portanto, imunes à aplicação da LGPD, tais como, mas não exclusivamente, (i) os dados relativos à pessoas jurídicas, (ii) os documentos sigilosos/confidenciais, (iii) os segredos de negócios, (iv) os planos estratégicos, (v) os algoritmos, (vi) fórmulas, (vii) softwares, (viii) patentes, entre outros, mesmo porque alguns deles apresentam disciplina e legislação próprias.

Enquanto os conceitos trazidos pela LGPD estão arrolados no artigo 5º[191], a forma de tratamento dos dados está relacionada no seu artigo 7º[192].

Para o escopo deste trabalho, que revelar o impacto da aplicação da LGPD nos contratos de prestação de serviços educacionais, se afigura-nos suficiente trazer o conceito de dados pessoais e dados sensíveis em relação ao primeiro dispositivo, e o consentimento como a forma de tratamento mais importante, embora não a única, quanto ao segundo dispositivo legal.

3.2. Conceitos e forma de tratamento

A própria LGPD conceitua como:

> I - dado pessoal: a informação relacionada a pessoa natural identificada ou identificável e;
>
> II - dado pessoal sensível: o 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.

Dentre as inúmeras formas de tratamento relacionadas no artigo 7º da LGPD, certamente a que mais causará celeuma será aquela relacionada ao **consentimento**, exatamente em virtude do que dispõe o *caput* do artigo 8º e os parágrafos 1º a 4º[193] da LGPD.

[191] Art. 5º Para os fins desta Lei, considera-se:

[192] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

[193] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Isso porque, ao que se depreende da leitura dos comandos legais em questão, além da obtenção do consentimento dever ser, necessariamente, por escrito ou outro meio que demonstre a vontade do titular, deverão ser observadas certas formalidades que exigem atenção redobrada e cuidados especiais.

Dentre elas, a obtenção de consentimento por escrito por meio de cláusula contratual destacada das demais, que além de indicar, precisamente, a finalidade para a qual é outorgado, sendo nulas as autorizações genéricas, deverá ser imune a qualquer vício de consentimento, cujo ônus da prova quanto à obtenção em conformidade com o disposto na Lei, incumbirá ao controlador, que nos termos da legislação, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

4. Aplicabilidade da LGPD aos contratos de prestação de serviços educacionais: impactos

Esses conceitos se mostram deveras importantes, justamente, porque compõem a base fundamental da celebração de qualquer contrato, especialmente de um contrato de prestação de serviços educacionais.

Pois, com efeito, na celebração de um contrato de serviços educacionais são colhidos dados pessoais tanto do contratante, que não raramente, é o responsável legal de um terceiro, a quem efetivamente, serão prestados os serviços educacionais, isto é: ao *educando*. Como, na maioria dos casos, o *educando* é um menor de idade – circunstância que atrai a aplicação do Estatuto da Criança e do Adolescente – tem-se a conjugação do tratamento de dados de 02 (dois) titulares[194].

Além disso, como a aplicação da lei, por expressa dicção do *caput* do artigo 3º[195], se aplica à pessoas físicas ou jurídicas, de direito público ou de direito privado, forçosamente se conclui que a LGPD abarcará todos os contratos de serviços educacionais. As próprias formalidades determinadas pela lei para obtenção do consentimento convergem com as exigências legais do Código de Defesa do Consumidor, quanto à sua obtenção por escrito por meio de cláusula contratual destacada das demais, e do Código Civil, quanto à ausência de quaisquer vícios a manifestação volitiva, diplomas legais que são, igualmente, aplicados aos contratos de serviços educacionais.

Veja-se que a dinâmica da prestação dos serviços educacionais ou do modelo de negócios impõe obediência à LGPD, já que são frequentes, para não dizer constantes, a realização:

(i) de parcerias institucionais das mais variadas formas e espécies, como por exemplo: (a) com outras instituições de ensino em relação à programação curricular, (b) como critério para obtenção de descontos e bolsas (vide os programas sociais do próprio Estado, destinados ao fomento da Educação, como por

[194] Art. 5º, V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

[195] Art. 3º Esta Lei 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 (...)

exemplo, o Prouni[196] e o Fies[197], e das próprias instituições de ensino, como o PRIUNI[198] da Universidade Nove de Julho – UNINOVE), (c) seja em relação a abertura de ativos financeiros em instituições financeiras;
(ii) de hospedagem de banco de dados em nuvem, circunstância que imporia a necessidade de transferência dos dados pessoais, inclusive, dos sensíveis, a terceiros que não o próprio controlador;
(iii) ações e estratégias de marketing digital, como envio de mailing, mala direta, etc.;
(iv) uso de mídias e plataformas de educação digital;
(v) realização de excursões, ranqueamento entre alunos, visando estímulo à competição, divulgação de projetos de científicos em eventos de cooperação acadêmica e etc.

Até mesmo dados pessoais sensíveis são objeto de tratamento pelas instituições de ensino, os quais, por sua vez, tem disciplina própria ainda mais restritiva.

Nesse sentido, exemplificativamente, vale destacar que por força da Lei nº 13.722/2018, que tornou obrigatória a capacitação em noções básicas de primeiros socorros de professores e funcionários de estabelecimentos de ensino públicos e privados de educação básica e de estabelecimentos de recreação infantil, os estabelecimentos de ensino deverão estar integrados à rede de atenção de urgência e emergência de sua região e estabelecer fluxo de encaminhamento para uma unidade de saúde de referência, fato que, inegavelmente, pressupõe, a necessidade de tratamento de dados relativos ao histórico de saúde do *educando*.

Mas não é só. Dados relativos à convicção religiosa também constituem dados sensíveis que também deverão ser tratados pelas instituições de ensino para atendimento da sua grade curricular, tal como acontece, por exemplo, nas escolas confessionais de que trata o inciso III do artigo 20 da Lei de Diretrizes e Bases da Educação Nacional[199].

Tudo isso sem mencionar que as atribuições administrativas e regulatórias das instituições de ensino exige o tratamento de dados pessoais (i) para o cumprimento de obrigação legal ou regulatória pelo controlado, (ii) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais, (iii) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem, (iv) para a proteção da vida ou da incolumidade física do titular ou de terceiro, (v) para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, (vi) quando necessário para atender aos

[196] Disponível em: <http://siteprouni.mec.gov.br/>

[197] Disponível em: <http://fies.mec.gov.br/>

[198] Disponível em: <http://www.priuni.com.br/>

[199] Art. 20. As instituições privadas de ensino se enquadrarão nas seguintes categorias:
III - confessionais, assim entendidas as que são instituídas por grupos de pessoas físicas ou por uma ou mais pessoas jurídicas que atendem a orientação confessional e ideologia específicas e ao disposto no inciso anterior (...)

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 e ainda, (vii) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Conclusão

Em suma, por todos os ângulos que se possa enfocar, a LGPD será de observância obrigatória pelas instituições de ensino, na medida em que, conforme leciona Marcel Leonardi, "o atributo básico do direito à privacidade é, portanto, a capacidade de o indivíduo controlar a circulação de informações a seu respeito"[200].

Sua importância é inegável, na medida em que a proteção à privacidade é um postulado constitucional, especialmente numa era em que "a evolução tecnológica impactou enormemente o cotidiano de grande parte da população mundial e alterou os paradigmas da economia, que migrou para um formato muito mais intangível, especialmente digital"[201].

Pelas razões expostas no decorrer do presente trabalho, não se reputa possível que as instituições de ensino, públicas ou privadas, possam se furtar ao cumprimento dessa novel legislação. Especialmente, porque destinando-se a *Educação* a desenvolver as potencialidades do indivíduo, certamente também o fará com vistas a torna-lo apto ao exercício da cidadania.

Sujeitos ou não à incidência das disposições de outros diplomas normativos, especialmente do Código Civil e do Código de Defesa do Consumidor, a proteção de dados preconizada na LGPD, mesmo no período de *vacatio legis,* já é uma realidade da nova era da sociedade do espaço virtual.

Logo, a inobservância dos ditames da LGPD, ensejarão a aplicação de severas penalidades, dentre as quais, (i) advertência, (ii) multa simples, (iii) multa diária, (iv) publicização da infração, (v) bloqueio dos dados pessoais, (vi) eliminação dos dados pessoais a que se refere a infração, tudo isso, sem prejuízo da adoção de outras penalidades administrativas, civis ou penais definidas em legislação específica.

Isso significa que caberá ao controlador, aqui enquadrado como empresário unicamente sob uma perspectiva de análise econômica do direito, avaliar quais cautelas serão adotadas para evitar o cometimento de ilícitos, que irremediavelmente, conduzirão à sua responsabilização, principalmente na esfera civil, circunstância que, como advertem Renata Dezem e Marcelo Sacramone, "é urgente e

[200] DE LUCCA, Newton; Simão Filho, Adalberto e Lima, Cíntia Rosa Pereira de (coords). *In Direito & Internet III – Marco Civil da Internet Lei 12.965/2014.* Tomo I. Ed. Quartier Latin, São Paulo: 2015, p. 518.

[201] COTS, Márcio. Lei Geral de Proteção de Dados Comentada. Ed. RT, São Paulo: 2018, p. 29.

altamente produtiva na busca da melhor acomodação dos riscos"[202], ainda mais na era da velocidade das informações.

Referências bibliográficas

BENACCHIO, Marcelo; GUERRA, Alexandre Dartanhan de Mello (coords). **Responsabilidade civil.** São Paulo: Escola Paulista da Magistratura, 2015.

BLUM, Renato Ópice; MALDONADO, Viviane Nóbrega (coords). **LGPD – Lei Geral de Proteção de Dados Comentada.** São Paulo: RT, 2019.

CANELLAS NETO, Alberto. (In)aplicabilidade do CDC aos serviços de saúde e educação públicas. Enfoque: o objeto de consumo. **Revista da AGU**, Brasília-DF, ano XIII, n. 41, p. 85-116, jul./set.2014.

COTS, Márcio. **Lei Geral de Proteção de Dados Comentada.** São Paulo: RT, 2018.

DA SILVA, José Afonso. **Curso de Direito Constitucional Positivo.** 22ª edição. São Paulo: Malheiros, 2003.

_____. A aplicabilidade das normas constitucionais. 7ª edição. Ed. Malheiros. São Paulo: 2009, apud PASSOS, Daniel Silva. Intervenção Judicial nas Políticas Públicas. **O Problema da Legitimidade.** São Paulo: Saraiva, 2014.

DE LUCCA, Newton. **Direito do Consumidor** – Teoria Geral da Relação Jurídica de Consumo. 2ª edição. São Paulo: Quartier Latin, 2008.

_____. **Direito do Consumidor** – Aspectos Práticos – Perguntas e Respostas. 2ª edição. São Paulo: Edipro, 2000.

De LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords). **Direito & Internet III – Marco Civil da Internet Lei 12.965/2014.** Tomo I. São Paulo: Quartier Latin, 2015.

DE MORAES, Alexandre. **Direito Constitucional.** 35ª edição. São Paulo: Atlas, 2019.

GAGLIANO, Pablo Stolze. PAMPLONA FILHO, Rodolfo. Novo Curso de Direito Civil. Contratos: teoria geral. Vol. IV. Tomo I. 7ª edição. São Paulo: Saraiva, 2011.

MEDAUAR, Odete. **Direito Administrativo Moderno,** 20ª ed. São Paulo: Editora Revista dos Tribunais, 2016.

_____. **Direito Administrativo Moderno.** 4ª edição. São Paulo: RT, 2000.

[202] GUERRA, Alexandre Dartanhan de Mello; BENACCHIO, Marcelo (coords). *Responsabilidade Civil.* São Paulo: Escola Paulista da Magistratura, 2015, p. 335.

MELLO FILHO, José Celso. Constituição Federal Anotada. 2ª edição. Saraiva, São Paulo: 1986 *apud* Moraes, Alexandre. **Direito Constitucional.** 7ª edição. São Paulo: Ed. Jurídico Atlas, 2000.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 12ª edição. São Paulo: Ed. Saraivajur, 2017.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil.** Vol. III. Contratos – Declaração Unilateral de Vontade – Responsabilidade Civil. 16ª edição. Ed. Gen/Forense, Rio de Janeiro: 2012.

SIQUEIRA, Antônio Henrique Albani. *In:* **Comentários à Lei Geral de Proteção de Dados.** São Paulo: Editora RT, 2019.

6.11. Personal Data Protection and multi-side Internet market regulation: an analysis on the limits of profiling – *José Luiz de Moura Faleiros Júnior & Pietra Daneluzzi Quinelato*

Abstract

The original concept of multi-sided markets has been developed to operate the interests of distinct groups through a platform, generating profitability from the massive volume of interconnected participants in order to enable the economic desires of one another in alignment with the usual consumer interests of others. With a transposition of daily activities into the virtual environment, and with Internet being the basis of professional and recreational activities, some disturbing practices of placidity may be questionable not only in terms of civil liability but also because of the lack of specific regulation for whoever extrapolates its reasonable limits, being this the problem-theme of this research. Such scenario is aggravated by the implementation of deep machine learning practices that aggregates big data in structured forms for the construction of users profiles for predictive behavioral purposes. The pursued hypothesis consists on the (in)sufficiency of the State's regulatory labor force for social pacification of such situations in light of recent efforts put forth from a legal framework standpoint. The research will use the deductive method, with the bibliographical analysis, at the end, aiming for final considerations with the objective of extracting a more assertive understanding of the problematic investigated.

Keywords: Personal Data. Multi-sided markets. Profiling.

Introduction

Unsurprisingly, the pace of technological innovation is at odds with the State's ability to provide adequate legal solutions on all fronts of its operations, including economic ones, which consequences

reverberate effects on the social environment.

In this context, important regulations were issued in Brazil, the first of which was Law No. 12965, of April 23, 2014 (the so-called "Internet Civil Framework") and, subsequently, Decree No. 8771/2016, that regulated it. More recently, Law No. 13709 of August 14, 2018 (the so-called "General Data Protection Law"), subsequently amended by Provisional Measure 869 of December 27, 2018, which was consolidated by the text of the Law No. 13853, of July 8, 2019, was the second and utmost installment of this increasing regulatory effort.

The fact is that law and justice go out of step with new technologies and certain contingencies now demand this regulatory intervention, notably in the economic front, in order to avoid illicit acts—with emphasis on those driven by the operationalization of business models implemented on the Internet.

Add to that the fact that the propulsion of new inter-relational dynamics, from the outbreak of the globalizing phenomenon and the rise of Internet, led to the colossal increase of information capture, structured or not, which enabled the configuration of what is conventionally called big data. This modern phenomenon, which is one of the preponderant marks of the so-called information society, makes it increasingly plausible to migrate acts once practiced on the physical, real, material world, to the virtual, immaterial, digitally driven cyberspace, backed by increasingly reliable projections of characters that essentially form the personality of the practitioner. All this thanks to the presence of technology in everyday life.

The research hypothesis revisits the essential nuclei of State regulatory dynamics that, for the purposes of the research, cannot be limited to the edition of regulatory frameworks, always in lack of tune with technological innovation; rather, the State must be able to regulate and monitor activities that are potentially contrary to the economic order through the settingof preventive duties in an ecosystem in which governments, companies, programmers, data scientists, stakeholders, legal operators and users can work best on good big data applications to promote economic development with inexorable respect for fundamental rights, especially the protection of personal data and the prevention of discriminative practices like profiling.

The research will use the deductive method, investigating conceptual nuances of the incidence of technology in such scenarios, based on bibliographic-doctrinal analysis to, finally, present the final considerations, which will seek to extract a more assertive understanding of the explicit problem.

1. Multi-sided markets and personal data protection

Privacy gains a critical conceptualization from the perspective of Helen Nissenbaum (2010, p. 127), to whom, in the current context, the transit of personal information has a very important social value, which

should be analyzed according to the context in which it is inserted, thus revealing whether the use of data will be appropriate or not. In other words, privacy must be conceptualized nowadays as contextual integrity, that is, it must be oriented according to social contexts.

Thus, the violation of privacy, from this perspective, demands the analysis of several criteria, such as the social context, the participating actors, the purpose, the forms of transmission, among others. For instance, the use of a patient's personal and sensitive data by his/her physician cannot be considered a breach of privacy. (CORREIA, 2018, p. 52-56) However, this same data, if handed over to specific companies for health plan marketing and selling purposes, shall indicate a violation of consumer intimacy and, ultimately, a disrespect to a dimension of personal dignity. In this context, it might be asserted that life in the information society is changing—including from a philosophical point of view—the way by which human beings perform acts and relate to each other in the various circumstances of life. Commenting on Don Ihde's views regarding such theme, Peter-Paul Verbeek (2001, p. 120) points out that:

> Classical philosophy of technology tended to reify technology, treating it as a monolithic force, "Technology". Ihde, by contrast, shuns general pronouncements about Technology, fearing to lose contact with the role that concrete Technologies play in our culture and in people's everyday lives. He sets himself the task of exploring this very role of technologies. Ihde does so from within the phenomenological tradition, which he has helped to connect to the philosophy of technology.

Clearly, there is a new perception of man about himself that contributes to the formation of personality archetypes, projected to a new 'universe' (and, naturally, to new markets). This demands great accuracy in the analysis of the dialogue between the spheres of individual, social and state interests—as a result of the depatrimonialization of private law, which stems from the mismatch between essential concepts of civilism in light of new contexts and realities. (FLORIDI, 2014, p. 118-119)

Stefano Rodotà (2005, p. 120-121), for instance, describes the formation of an electron body ('*corpo elettronico*'), a new aspect of the natural person that not only bears physical mass, or a *corpus*, but also a digital dimension. A similar concept is that of Roger Clarke (1993, p. 403) regarding the formation of a 'digital persona'. Both are models for the digital portrayal of an individual and, therefore, a simplified representation of only a few aspects of reality.

To that end, a specific concern is analyzed by Danilo Doneda (2006, p. 2):

> To this "classical" problem of privacy we can now add another element: the fact that we are, before various instances, represented—and judged—

> through this data. This opens up another possibility to focus on the issue, whereby privacy resonates with a host of other questions concerning our personality. This can mean the loss of part of our autonomy, our individuality, and ultimately our freedom. Our data, structured to mean for a given subject our virtual the judgment of granting a credit line, a health plan, obtaining a job, free passage through a country's customs, and so many other assumptions. (freely translated)[1]

That sets the basis of what Nobel Memorial Prize in Economic Sciences award winner French economist Jean Tirole (2016) described as 'two-sided markets' in platform competition for what he regarded as a much-needed review towards a new economics theory for the common good. Along with Jean-Charles Rochet, Tirole had previously already pointed out, in a paper published in 2003, the mathematics behind said business models:

> Yet thinking of the markets discussed in this paper as one-sided markets just runs counter to evidence. First, the platform owners in all these industries devote much attention to their price allocation business model: Is it more important to woo one side or the other? The quest for "getting both sides on board" makes no sense in a world in which only the total price for the end user interaction, and not its decomposition, matters. And the trade press would not contain so many descriptions of "chicken-and-egg" problems. Second, the end users themselves are also very sensitive to the allocation of cost between them, indicating that some actual redistribution is taking place. Merchants vocally object to increases in interchange feed, and website operators will do so if settlement charges are introduced in the Internet. (ROCHET; TIROLE, 2003, p. 1018-1019)

The effectiveness of the model depends on the extent to which it captures the characteristics of reality that are relevant to the use of the model. As with any modeling activity, it suffers from the weaknesses of the reductionist approach: individuals are treated not holistically, but as if a relatively simple set of data structures were adequate to represent their pertinent characteristics. These representations (true "avatars"), formed from a true data set, are given legal treatment. (INIESTA; SERNA, 2015, p. 184)

Therefore, human personality, in general, is undergoing strong changes due to the social deviations promoted by the expansion of technological use. In fact, this mutation demands new legal studies, especially in order to understand the legal situations derived from such practices and that demand protection.

2. Profiling practices in data-rich multi-sided markets

Whereas this new markets set the tone for real domination—or the formation of monopolies—it is undeniable that a few huge companies have been reigning on the Internet over the past decades. Stephen Hannaford (2007) has long been explaining key expressions like monopoly and the new oligopoly. He argues that there has always been an urge for companies to merge, but this urge has never been as strong as it is nowadays. Companies have the possibility to merge or acquire other companies, as long as it is within legal boundaries. In order to measure concentration, two methods are explained, namely the concentration ratio and the Herfindahl–Hirschman index, where the last one is often used in courts concerning antitrust cases. In addition, in antitrust cases, market-definition, narrow or broad, can also be determining for the outcome of a process. Moreover, companies strive to be number one or two in the market, resulting in the fact that they often define a narrow market leading to more oligopolies. The second chapter describes the complication of oligopolies and oligopsonies, hence situations in which there are only a small number of sellers or a small number of buyers respectively.

In reality, combinations of oligopolies and oligopsonies, called oligonomies, often take place. Oligonomies are oligopolies in one direction and oligopsonies in the other. The author gives several examples of this phenomenon, such as the couple of major book publishers, being an oligopsony to authors and an oligopoly to readers. Also, he is of the opinion that this is actually justified, since only big corporations can serve the large number of transactions.

It's also important to point out that the rise of a few large companies whose businesses on the Internet elevates them to the status of "communication empires" was pioneered by Tim Wu, who in "The Curse of Bigness" (2018) argues that Governments must stop self-regulation and intervene, through antitrust laws, to split technology giants like Google, Facebook and Amazon in order to restore dynamism and foster innovation.

Tim Wu (2016, p. 267) has also been a vocal force in terms of user attention being considered the main input for the content delivery industry in line with the prospection of users' personal data, forming a data-rich market that becomes the preponderant factor of a new economy,as narrated by Viktor Mayer-Schönberger and Thomas Ramge (2018, p. 6):

> Conventional markets have been highly useful, but they simply can't compete with their data-driven kin. Data translates into too much of an improvement in transactions and efficiency. Data-rich markets finally deliver what markets, in theory, should always have been very good at—enabling optimal transactions—but because of informational constraints really weren't. (...) The promise of data-rich markets is not that we'll eradicate these market

> failures completely, but that we'll be able to greatly reduce their frequency and the resulting financial devastation.[203]

This new reality is permeated by contemporary propaganda techniques, especially consumer-directed behaviorally profiled advertising that advances over lands previously unexplored by marketing of products and services, such as influence and personalization. That sets the field for a series of marketing strategies for Law and Economics studies, since, according to Robert Cooter and Thomas Ulen (2012, p. 3), "[t]he response of people is always relevant to making, revising, repealing, and interpreting laws."

Cass Sunstein (2014, p. 2-3) also has important studies regarding this matter, as "behavioral insights units"—the so-called "nudges"—are capable of conducting decision-making behavior, which then provide a "choice architecture". Similar studies have been showcased by van Ooijen and Vrabec (2019), with a special glance on the impacts of the European General Data Protection Regulation (GDPR)—Regulation (EU) 2016/679—and its capabilities in terms of enhancing consumers' control over personal data.

That's a question of the utmost interest for countries all around the globe, because unregulated data harvest may lead to unwanted consequences in various fields, not only for privacy violations, but also for company undue empowerment (VAIDHYANATHAN, 2011, p. 136), dissemination of fake news (GERBAUDO, 2019, p. 177), threats to reputation (SOLOVE, 2007, p. 189) and algorithmic secrecy (PASQUALE, 2015, p. 3-8).

Jean Tirole, once again, alongside Bengt Holmström (2013), not only to cast some light on the problem, but also ask questions like why do financial institutions, industrial companies, and households hold low-yielding money balances, Treasury bills, and other liquid assets? When and to what extent can the State and international financial markets make up for a shortage of liquid assets, allowing agents to save and share risk more effectively? These questions are at the center of all financial crises, including the current global one. In a slight, but important, departure from the standard theory of finance, the authors show how imperfect pledgeability of corporate income leads to a demand for as well as a shortage of liquidity with interesting implications for the pricing of assets, investment decisions, and liquidity management.

[203] In the original work: "*A esta problemática "clássica" da privacidade podemos acrescentar atualmente um outro elemento: o fato de sermos, perante diversas instâncias, representados – e julgados – através destes dados. Tal fato abre uma outra possibilidade de enfocar a questão, pela qual a privacidade faz ressoar uma série de outras questões referentes à nossa personalidade. Isso pode significar a perda de parte de nossa autonomia, de nossa individualidade e, por fim, de nossa liberdade. Nossos dados, estruturados de forma a significarem para determinado sujeito uma nossa representação virtual – ou um avatar –, podem ser examinados no julgamento de uma concessão de uma linha de crédito, de um plano de saúde, a obtenção de um emprego, a passagem livre pela alfândega de um país, além de tantas outras hipóteses.*"

When it comes to big data, its commercial value and uses, specially in terms of profiling practices, an urgency for regulation emerges.

3. Perspectives for specific regulation in light of the Brazilian framework

Brazilian legislation still hasn't specifically tackled themes like profiling and its consequences, but the General Data Protection Law appears to be the main framework for such matters, as its large scope seems adequate enough as a starting point on the matter.

By unfolding the right to personal data protection, it's to be expected that a substantial change in the social landscape, from new technologies that become more and more neuralgic to the structure of the order, would have enormous impacts and impose a need to rethink the risks arising from it.

The importance of regulating the protection of privacy and data collection, processing and storage operations is essential in light of this new reality. In that sense, Richard Warner (2011, p. 1084) warns of the risk of understanding some privacy developments, which ultimately requires behavior that most individuals simply do not see as viable, given that the perceived benefits are simply too low, leading to a slight disregard for the data itself, which is easily handled in trivial operations such as creating an account on any platform (a social network, a virtual retail portal, an email provider, a news feed, etc.).

Europe has taken the lead with the aforementioned Regulation 2016/679, widely known as the "General Data Protection Regulation" (GDPR), aimed at reinforcing and bringing closer to reality institutes such as the right to data deletion, the right to be forgotten, and contain rules that go beyond the already established data protection authorities in each country, disciplining the European Data Protection Committee.

The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

According to Paul Voigt and Axel von dem Bussche (2017, p. 27):

> According to Art. 3 Sec. 2 lit. b GDPR, data processing that is related to the monitoring of EU customers' behaviour, as far as their behaviour takes place within the Union, falls within the territorial scope of application. In order to determine if behavior qualifies as 'monitoring' under this article, it should be ascertained whether individuals are tracked on the Internet, including potential subsequent use of personal data processing techniques that consist

> of profiling an individual. This is particularly the case if processing takes place in order to take decisions concerning that individual or for analysing or predicting the persons' preferences, behaviours and attitudes.

In Germany, for instance, the *Bundesverfassungsgericht* has paid a lot of attention in personality profiles. From a legal point of view, "profiling differs from other extensive data collections like data warehouses. Within a profile, the data is to be linked purposefully to gather additional information which goes beyond that which can be obtained from the original data." (HORNUNG; SCHNABEL, 2009, p. 86-87)

Brazil acted months after, having approved in 2018 the General Data Protection Law (Law No. 13.709, of 14 August 2018, commonly identified by the acronym LGPD), with validity initially delayed until August 2020. The new law specifically regulated compliance and good practices on Articles 50 and 51, although not cogently.

In this new context, a wide field emerges for the proliferation and propagation of new extraregulatory modalities capable of generating legal impacts on all branches of law, even for the implementation of the General Data Protection Law and, in particular, for the protection broadly applicable to the relations between law and technology.

Governance (commonly taken as a synonym to "compliance") has been taken by André-Jean Arnaud (2014, p. 214-223) based on the construction of a perfect definition that is capable of acting by the coordination of actors, social groups and institutions, in public-political action, with the scope of defining their own objectives, discussed and collectively defined. All of this is in line with the motivation and responsiveness parameters expected from a sound and effective compliance policy framework, especially so as not to create empty programs (which only exist on paper) and to substantiate a "regulated self-regulation", serving as an expedient for "evasion of responsibility". (AYRES; BRAITHWAITE, 1992, p. 158-162)

That said, it seems that compliance might be one of the applicable solutions to said lag between innovation and regulation, which, for the Brazilian legal framework, is something completely new and able to open up a broad range of interesting possibilities for self-regulation and tort prevention.

Conclusion

In conclusion, after a very brief analysis of the current impacts of multi-sided markets in light of the State's lack of regulatory capacity to overcome the challenges of new Internet contingencies, profiling has been elected as the main object for the purposes of this study, even though there are many more specific cases worthy of analysis.

The inexorable path to this new reality is, without a doubt, dependent on the implementation of compliance policies, even though the Brazilian legislation does not conceive it as an obligation. Many companies are still searching for answers as to how this implementation should take place whilst the regulatory agency, that will be responsible for enforcing the new law, is still not operational.

In light of such factor, Jean Tirole's description of multi-sided markets has set the tone for new ways of understanding new data-rich markets that, after all, are the core nexus of a large set of practices derived from big data and behavioral analysis that demand urgent regulation. In its absence, however, compliance emerges as a feasible solution, at least for the time being.

References

AYRES, Ian; BRAITHWAITE, John. **Responsive regulation**: transcending the deregulation debate. New York: Oxford University Press, 1992.

CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. **Journal of Law, Information and Science**, Sydney, v. 4, n. 2, dec. 1993.

COOTER, Robert; ULEN, Thomas. **Law & Economics**. 6. ed. Boston: Addison-Wesley, 2012.

CORREIA, Victor. **Da privacidade**: significado e valor. Coimbra: Almedina, 2018.

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

FLORIDI, Luciano. **The Fourth Revolution**: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014.

GERBAUDO, Paolo. **The digital party**: political organization and online democracy. London, Pluto Press, 2019.

HANNAFORD, Stephen G. **Market domination!** The impact of industry consolidation on competition, innovation, and consumer choice. Westport: Praeger Publishers, 2007.

HOLMSTRÖM, Bengt; TIROLE, Jean. **Inside and outside liquidity**. Cambridge: The MIT Press, 2013.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: the population census decision and the right to informational self-determination. **Computer Law & Security Report**, United Kingdom, v. 25, n. 1, p. 84-88, 2009.

INIESTA, Javier Belda; SERNA, Fracisco José Aranda. El paradigma de la identidad: hacia una regulación del mundo digital. **Revista Forense**, Rio de Janeiro, v. 422, jul./dec, p. 181-202, 2015.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing capitalism in the age of Big Data**. New York: Basic Books, 2018.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

ROCHET, Jean-Charles; TIROLE, Jean. Platform competition in two-sided markets. **Journal of the European Economic Association**. v. 1, n. 3, pp. 990-1029, jun. 2003.

RODOTÀ, Stefano. **Intervista su privacy e libertà**. Rome/Bari: Laterza, 2005.

SOLOVE, Daniel J. **The future of reputation**: gossip, rumor, and privacy on the Internet. New Haven: Yale University Press, 2007.

SUNSTEIN, Cass. Nudge: a very short guide. **Journal of Consumer Policy**, Berlin/Heidelberg: Springer-Verlag, v. 37, p. 583-589, set. 2014.

TIROLE, Jean. **Économie du bien commun**. Paris: PUF, 2016.

VAIDHYANATHAN, Siva. **The googlization of everything (and why should we worry)**. Berkeley, University of California Press, 2011.

VAN OOIJEN, Iris; VRABEC, Helena U. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. **Journal of Consumer Policy,** Berlin/Heidelberg: Springer-Verlag, v. 42, p. 91-107, 2019.

VERBEEK, Peter-Paul. Don Ihde: the technological lifeworld. *In:* ACHTERHUIS, Hans (Ed.). **American philosophy of technology**: the empirical turn. Translated from german to english by Robert P. Crease. Indianapolis: Indiana University Press, 2001.

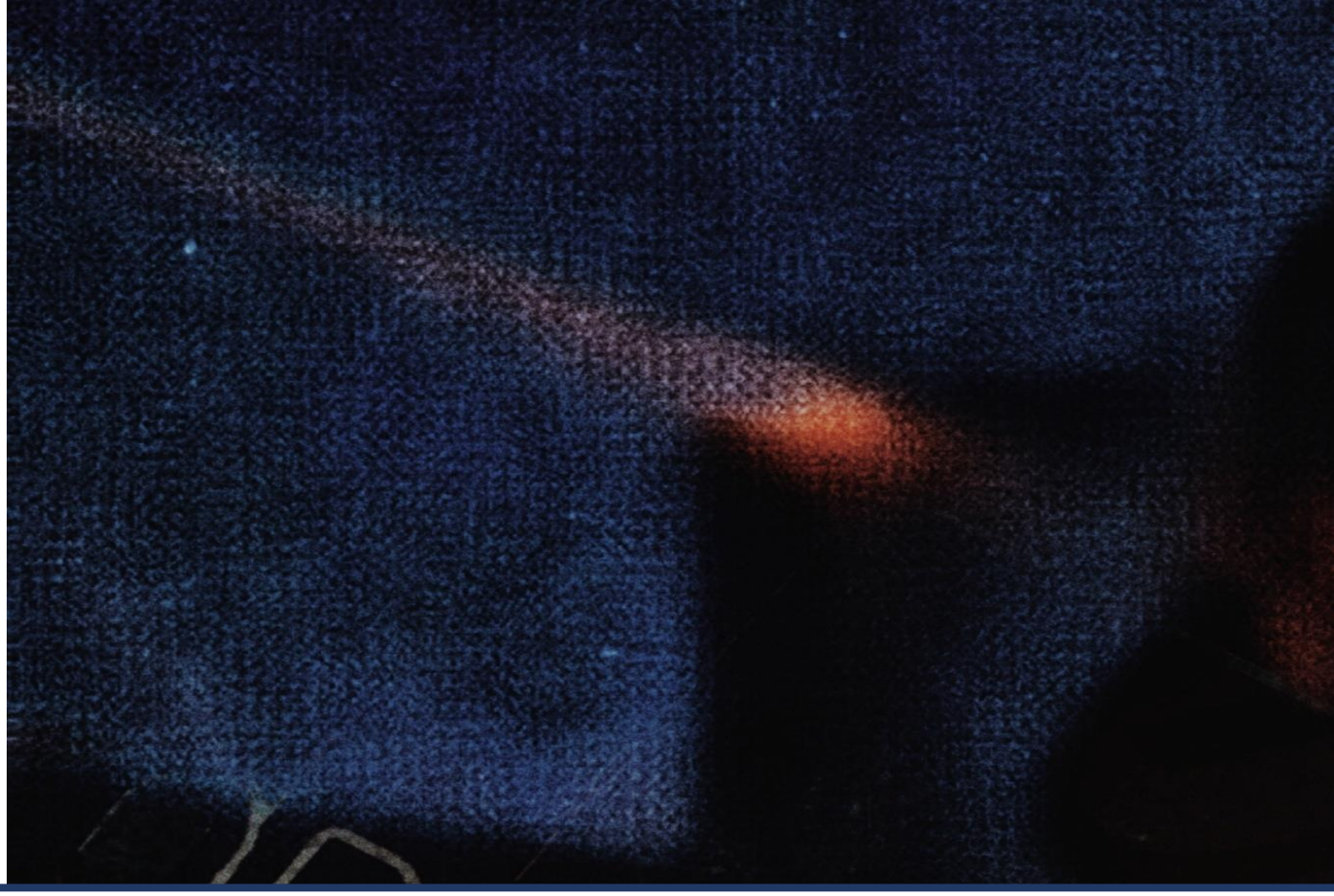
VOIGT, Paul; VON DEM BUSSCHE, Axel. **The EU General Data Protection Regulation (GDPR)**: a practical guide. Cham/Basel: Springer, 2017.

WARNER, Richard. Undermined norms: the corrosive effect of information processing technology on informational privacy. **Saint Louis University Law Journal**, Saint Louis, v. 55, p. 1047-1086, 2011.

WU, Tim. **The attention merchants**: the epic scramble to get inside our heads. New York: Vintage, 2016.

WU, Tim. **The curse of bigness**: antitrust law in the new Gilded Age. Nova Iorque: Columbia Global Reports, 2018.

WU, Tim. **The master switch**: the rise and fall of information empires. Nova Iorque: Vintage, 2010.



Universidade de São Paulo

