Parâmetros Jurídicos ao Uso de Dados Pessoais Como Estratégias de Negócios

Legal Parameters for the Use of Personal Data As Business Strategies

DANILO HENRIQUE NUNES[1]
Centro Universitário Estácio de Ribeirão Preto, Ribeirão Preto, São Paulo, Brasil.
Centro Universitário da Fundação Educacional de Barretos, São Paulo, Brasil.

LUCAS SOUZA LEHFELD[2]
Universidade de Ribeirão Preto, Ribeirão Preto, São Paulo, Brasil.

DIRCEU PEREIRA SIQUEIRA[3]
Centro Universitário Cesumar de Maringá, Paraná, Brasil.

RESUMO: A utilização de dados pessoais como estratégia de negócios é tema difundido e controverso que tem gerado uma série de discussões em face de acontecimentos recentes, devido ao fato de que a maior parte das empresas modernas nacionais e estrangeiras aposta no uso destas ferramentas para potencializar seus negócios. O estudo, a partir do método hipotético-dedutivo e de revisão de literatura, analisa os parâmetros para captação, uso, manejo, tratamento e conservação de dados, reconhecendo a proteção deles como direito fundamental.

PALAVRAS-CHAVE: Proteção de dados; direito fundamental; limitações jurídicas.

ABSTRACT: The use of personal data as a business strategy is a widespread and controversial topic that has generated a lot of discussion in the face of recent events, due to the fact that most modern domestic and foreign companies are betting on the use of these tools to enhance their business. The study, based on the hypothetical-deductive method and literature review, analyzes the parameters for data collection, use, management, treatment and conservation and recognizing their protection as a fundamental right.

KEYWORDS: Data protection; fundamental right; legal limitations.

1 Orcid: <http://orcid.org/0000-0001-9162-3606>.
2 Orcid: <http://orcid.org/0000-0002-1021-0891>.
3 Orcid: <http://orcid.org/0000-0001-9073-7759>.

estratégia de negócios; 4.1 A captação de dados pessoais, seu tratamento e manejo no corporativo para fins comerciais; 4.2 O uso de dados dos usuários de serviços públicos na era da vigilância governamental; 4.3 Da Autoridade Nacional de Proteção de Dados e a possível insegurança jurídica na sua implantação; Considerações finais; Referências.

INTRODUÇÃO

Em tempos em que a internet e os serviços digitais passaram a fazer parte do cotidiano dos seres humanos ao redor de todo o globo, as discussões envolvendo a utilização dos dados pessoais dos usuários como estratégias de negócios vêm ganhando mais corpo e provocando série de discussões que contam com a participação de juristas e de especialistas e autoridades em proteção de dados.

O presente estudo tem, a partir dos métodos hipotético-dedutivos e de revisão de literatura, como objetivo geral aprofundar os parâmetros jurídicos referentes à utilização dos dados pessoais como estratégias de negócios. Tem, ainda, como objetivos específicos perpassar pelo reconhecimento da proteção de dados como um direito fundamental (PEC 17/2019), pelo advento da Lei Geral de Proteção de Dados (LGPD), da Autoridade Nacional de Proteção de Dados (a partir da MP 869/2018) e de outros pressupostos e parâmetros legais sobre o tema que fomentam discussões na contemporaneidade. Os objetivos específicos, no mesmo sentido, foram delimitados na seguinte disposição: apresentar os conceitos fundamentais que delimitam o entendimento sobre a proteção de dados pessoais na internet; analisar as questões que envolvem a proteção de dados pessoais como um direito fundamental na medida de sua inclusão em dispositivos do Diploma Constitucional de 1988, partindo da doutrina e da PEC 17/2019; apresentar a Lei Geral de Proteção de Dados (LGPD), que entra em vigor em 2020 e versa sobre seus mecanismos e sua aplicabilidade e abordando a influência de legislações europeias recentes para sua fundamentação; além disso, abordar os dados pessoais como estratégias de negócios, versando sobre a captação e o uso de dados no cenário corporativo para fins comerciais e o uso de dados de usuários dos serviços públicos na era da vigilância governamental, além de abordar a Autoridade Nacional de Proteção de Dados e a possível insegurança jurídica em sua implementação a partir da MP 869/2018.

A justificativa para a realização do presente estudo parte justamente da relevância dos estudos jurídicos sobre o uso e a proteção de dados, posto que as informações pessoais dos usuários na internet são revestidas por grande valiosidade, sendo utilizadas para diferentes fins, sobretudo enquanto estratégias de negócio, de modo que se torna indispensável aprofundar

conhecimentos sobre os aspectos legais discutidos à luz da doutrina e da legislação sobre o tema em questão.

1 CONCEITOS INTRODUTÓRIOS À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Com a evolução e o desenvolvimento da rede mundial de computadores e com o surgimento de mecanismos sofisticados como as redes sociais, surgiram grandes preocupações sobre a privacidade, de modo que é importante que os internautas estejam alerta sobre os perigos de se fornecer informações de cunho íntimo que podem ser utilizadas indevidamente, pela ação de *hackers*, *crackers* e de outras figuras que permeiam a internet com o intuito de fazer uso malicioso dos dados pessoais (Hirata, 2014).

Para Eduardo Steffenello Ghisleni (2015:4), o "surgimento da internet determinou uma transformação nos mecanismos de coleta e difusão de informações", de modo que a coleta de dados pessoais na rede (seja com interesse públicos, seja com interesses privados) se tornou algo bastante difundido. O acesso à rede mundial é, na contemporaneidade, considerado um direito fundamental, o qual contempla que a célere evolução tecnológica possibilitou uma coleta massiva e sistemática de informações através das redes de comunicação, promovendo a violação dos dados pessoais dos usuários.

De acordo com Danilo Doneda (2011), os dados pessoais são indissociáveis da própria internet, de modo que sua utilização (para identificação, classificação, autorização, dentre outras) torna esses dados vitais para que a pessoa possa se "mover" com autonomia e liberdade no ambiente permeado pela Sociedade da Informação, sendo que estes tornam inclusive a presença física da pessoa desnecessária para ações que outrora seriam inimagináveis. Um exemplo dessa dispensabilidade de presença física se dá na realização de transações financeiras pelo celular: fazendo uso de seus dados pessoais, o usuário consegue realizar a maior parte das operações sem a necessidade de se deslocar para a instituição financeira. Desse modo, é indispensável considerar que os dados pessoais funcionam como "a identidade" das pessoas que permeiam o ambiente virtual. Contudo, conforme já apontado pelo presente estudo, a proteção desses dados se faz fundamental, uma vez que eles podem ser utilizados por terceiros mal-intencionados.

Alguns conceitos fundamentais devem ser concebidos nessa análise, como os metadados, os algoritmos, *big data* e *bots*, os quais serão apresentados de modo sintetizado a seguir: a) Luiz Fernando de Barros Campos (2007) leciona que os metadados digitais (dados sobre dados ou

dados descrevendo outros dados) são considerados informação sobre objetos presentes na internet e que podem ser compreendidos e interpretados por máquinas, tendo ênfase no processamento automático. Basicamente se trata de dados associados com objetos que dispensam os usuários potenciais do conhecimento completo da existência e característica de um determinado objeto; b) quanto aos algoritmos, Fabricio Ferrari e Cristian Cechinel (2008:14) apontam que o "algoritmo pode ser definido como uma sequência finita de passos (instruções) para resolver um determinado problema", estando associado com o padrão de comportamento que deve ser seguido (norma de execução de ações) visando ao alcance do resultado de um problema; c) sobre o conceito de *big data*, Priscila Basto Fagundes (2018) *et al.* conceituam-no como um setor voltado para a análise, processamento e armazenamento de grandes *datasets* (coleções ou agrupamentos de dados relacionados), com soluções práticas que se revelam fundamentais quando as tradicionais se mostram insuficientes para executar a atividade. *Big data* não é necessariamente apenas uma tecnologia, mas também uma noção sobre como as tecnologias podem impulsionar uma organização a partir das enormes quantidades de dados oriundos de fontes distintas e de diversas maneiras, demandando um processo de gestão específico para assegurar a qualidade da informação; e, d) por fim, os *bots* são caracterizados por Ricardo Murer (2017) como aqueles baseados em inteligência artificial ao realizarem a tarefa de selecionar, coletar, classificar e filtrar os dados, atribuição que outrora era dos especialistas em programação e tecnologia.

Na internet (sobretudo considerando o contexto das mídias sociais), o *big data* é uma das áreas de maior relevância para a análise que se pretende no presente estudo, visto que, a partir do uso de algoritmos e *bots*, dos padrões de comportamento *online*, tais dados são utilizados sobretudo por campanhas publicitárias. Os usuários costumeiramente fornecem os dados de modo voluntário para empresas como o Facebook, Twitter e Google, de modo que tais dados são convertidos para o uso publicitário, oferecendo produtos e serviços que são baseados nos interesses e comportamentos dos internautas a partir dos dados obtidos.

2 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: ASPECTOS CENTRAIS E A PEC 17/2019

Diante de uma melhor compreensão dos conceitos fundamentais relacionados aos dados no contexto da internet, torna-se possível aprofundar a proteção de dados pessoais como um direito fundamental, partindo das questões envolvendo a liberdade *versus* a privacidade. Danilo Doneda

(2011) aponta que toda a legislação (em âmbito nacional e internacional) produzida para a proteção de dados versa sobre ela como um direito fundamental, assegurando que o direito à liberdade não deve ferir o direito à privacidade do usuário.

Conforme apontado por Daniel Piñeiro Rodriguez (2010), o direito fundamental à privacidade tem origem no século XIX, com acepções no cenário norte-americano, de modo que ela não pode ser concebida de modo delimitado, posto que grandes transformações sociais e tecnológicas ocorreram durante esse período em todo o mundo, versando, sobretudo, ao acesso à rede. A partir de esforços realizados na Europa, houve a inserção em diversos documentos internacionais, como o art. 8º do Convênio Europeu para Proteção de Direitos Humanos e Liberdades Fundamentais (pactuado em 1950, em Roma) e a Carta dos Direitos Fundamentais da União Europeia (2000), que assegurou a privacidade e, por conseguinte, a própria proteção de dados como um direito fundamental do indivíduo. Nesse sentido Larissa Britto Florenço:

> Sob as modernas condições de processamento de dados, a inviolabilidade da intimidade e da vida privada pressupõe a proteção do indivíduo contra a coleta, o armazenamento, o uso e a transmissão irrestrita de seus dados pessoais. Essa proteção é abrangida pelo direito fundamental do art. 5º, X, c/c o art. 5º, LXXII, da Constituição Federal (CF/1988), à luz do princípio da dignidade da pessoa humana, de modo que atribui ao cidadão de controlar livremente a divulgação, transmissão e uso de seus dados pessoais, bem como garante o tratamento leal e lícito dos seus dados, conforme o princípio da boa-fé objetiva e da proteção das suas legítimas expectativas. (Florenço, 2016:168)

A autora supracitada aponta ainda que a tutela da proteção de dados detém fundamento constitucional, de modo que ela é assumida como um direito fundamental destinado à proteção do indivíduo perante interesses oriundos de diversas fontes (tanto na esfera pública quanto na esfera privada) se projetando na contemporaneidade como um direito autônomo, necessitando tutela ampla. No mesmo sentido, Danilo Doneda (2011) defende que os dados pessoais na atualidade são considerados como valiosas mercadorias, de modo que tais informações passam a ser consideradas como bens jurídicos e/ou econômicos. Os ordenamentos jurídicos, nesse sentido, dão *status* de direito fundamental aos dados pessoais na atualidade, funcionando como uma chave para efetivar a liberdade individual nos meandros da Sociedade da Informação.

Regina Linden Ruaro, Daniel Piñeiro Rodriguez e Brunize Finger (2011) também reconhecem a proteção de dados como um direito funda-

mental, sendo tal proteção necessária para que o usuário possa permanecer no ambiente digital exercendo seu direito à liberdade sem colocar em risco seu direito à intimidade e à privacidade. Assim:

> Promulgada em 1988, a Constituição Federal apresentou técnica mais apurada e inovou ao reconhecer diversos direitos e garantias específicas. Em seu corpo normativo, abordou tanto a proteção dos direitos referentes ao cidadão como aqueles concernentes ao próprio Estado. Assim, o seu art. 1º, III, *ao reconhecer o princípio da dignidade humana, protegeu de imediato todos os direitos da personalidade, além de positivar garantias como a do direito à liberdade de expressão (art. 5º, IX) e do direito à informação (art. 5º, XV)*, a inviolabilidade da vida privada e da intimidade (art. 5º, X), a garantia do *habeas data* (art. 5º, LXXII), a proibição da invasão de domicílio (art. 5º, XI) e violação de correspondência (art. 5º, XII). (Ruaro; Rodriguez; Finger, 2011:323 – grifos nossos)

Há consenso dentre os autores utilizados para a elaboração do presente capítulo quanto ao reconhecimento da proteção de dados (sobretudo considerando ambientes digitais – plataformas e mídias sociais) como um direito fundamental do indivíduo. Questões como a proteção da honra e a vida privada sempre são concebidas nessa discussão, bem como impasses entre a liberdade de expressão e direito à informação, dentre outras que serão aprofundadas mais adiante no presente estudo. Dito isso, torna-se possível aprofundar a Lei nº 13.709/2018, versando sobre suas aplicações e mecanismos.

Antes de abordar os aspectos relacionados a essa legislação, contudo, torna-se indispensável versar sobre a PEC 17/2019, a qual busca acrescer ao inciso XII-A do Diploma Constitucional de 1988, ao art. 5º e inciso XXX e ao art. 22 da Lei Máxima do país a inclusão da proteção de dados pessoais entre os direitos fundamentais do cidadão, fixando a competência privativa da União para legislar sobre tal matéria. Trata-se de uma PEC em trâmite, até o momento da elaboração do presente estudo, que busca transformar a proteção de dados em um direito fundamental em caráter objetivo, incluindo-a no rol de direitos fundamentais dispostos em nossa Carta Magna.

Nota-se que há uma grande preocupação dos legisladores brasileiros como um todo para a inclusão da proteção de dados como um direito fundamental dos cidadãos brasileiros, de modo que a PEC 17/2019 é contemplada como o instrumento indispensável para que a legislação brasileira esteja alinhada aos pressupostos fundamentados na doutrina jurídica dos novos tempos.

3 DADOS PESSOAIS & INTERNET: DA LEI Nº 13.709/2018, SUAS APLICAÇÕES E MECANISMOS

De acordo com Zeca Berardo, Paulo Lilla e Elen Zilas (2019), a Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), é um marco legal que dispõe acerca da proteção da privacidade de dados pessoais no território brasileiro, prevendo uma proteção específica à privacidade e aos dados pessoais dos cidadãos, além de determinar como as empresas, organizações e o próprio Poder Público deverão coletar, utilizar, processar e armazenar esses dados em seu cotidiano de atividades. Essa nova legislação brasileira, contudo, é baseada na *General Data Protection Regulation* – GDPR em vigor na União Europeia.

Antes de aprofundar as aplicações e os mecanismos dessa legislação, é indispensável tomar conhecimento sobre a GDPR. Segundo Colin J. Bennet (2018), trata-se de um complexo instrumento que gerou uma série de volumes de material interpretativo por especialistas do Direito e da proteção de dados, consagrando uma série de direitos fundamentais para o indivíduo (ou seja, o titular dos dados), impondo obrigações significativas às organizações públicas e privadas (responsáveis pelo tratamento dos dados) e às partes contratantes (os processadores de dados). Tal instrumento incorpora princípios essenciais da privacidade das informações, como licitude, equidade e transparência do tratamento; limitações de finalidade; minimização de dados; precisão; limitação de armazenamento; integridade e confidencialidade; e prestação de contas – os quais foram reforçados e ampliados de diversas maneiras.

Para Fabrício Bertini Pasquot Polido (2019) *et al.*, esse Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (tradução dos autores para a GDPR), que entrou em vigor em maio de 2018, representou um novo paradigma de proteção de dados pessoais, o qual não se restringe apenas ao continente europeu:

> Sua abrangência, ambição legislativa e maturidade conceitual corroboram a ideia de que esse é um autêntico regulamento-modelo, no qual diversas outras iniciativas nacionais, regionais e intracomunitárias também serão espelhadas em busca de padrões normativos uniformes na proteção de dados pessoais. Não seria exagero afirmar que o GDPR nasce como "monstro normativo", um Leviatã a induzir condutas de conformidade ("*compliance*") por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais e especialmente identificáveis nos ambientes informacional e digital. (Polido, 2019:23)

Rafael A. F. Zanatta (2017) aponta que, a partir de sua elaboração, a GDPR passou a ser concebida como a legislação mais avançada para a proteção dos titulares de dados pessoais, estabelecendo uma série de mudanças na legislação europeia e representando significados para o direito como um todo. O autor defende que justamente por essa sofisticação desse instrumento jurídico aplicado no cenário europeu, mitigando os riscos e estabelecendo normas claras e bem definidas, promoveu uma influência em todo o campo jurídico, o que acaba culminando no surgimento da Lei nº 13.709/2018.

Em posse desses conhecimentos, torna-se possível aprofundar os princípios da Lei nº 13.709/2018 para o tratamento de dados, os quais são elencados na publicação de Zeca Berardo, Paulo Lilla e Elen Lizas (2019) nos seguintes pontos: a) *finalidade*: impõe que os dados pessoais tão somente podem ser tratados para atender a propósitos legítimos, específicos, explícitos e informados ao titular, vetando tratamento posterior desalinhado a essas finalidades; b) *adequação*: o tratamento de dados sempre deve ser compatível com as finalidades informadas ao titular; c) *necessidade*: ele deve ser limitado ao mínimo necessário para atender aos objetivos; d) *livre acesso*: os titulares dos dados sempre poderão consultar, de modo simplificado e gratuito, a forma e duração do tratamento e a integralidade de seus dados pessoais; e) *qualidade dos dados*: trata-se das garantias oferecidas aos titulares de dados envolvendo exatidão, clareza, relevância e atualização dos dados; f) *transparência*: também deve ser assegurada aos titulares a prestação de informações claras, precisas e de fácil acesso sobre a realização do tratamento; g) *segurança*: devem ser empregadas medidas técnicas e administrativas que visem à proteção dos dados pessoais de acessos não autorizados e de incidentes ou ilicitudes que levam à destruição, perda, alteração, comunicação ou difusão de dados; h) *prevenção*: devem ser adotadas medidas preventivas para evitar prejuízos ou danos decorrentes do tratamento de dados; i) *não discriminação*: é o veto ao tratamento de dados para fins discriminatórios, ilícitos ou abusivos; j) *responsabilização e prestação de contas (accountability)*; e, por fim, f) o agente de tratamento deve sempre comprovar a adoção de medidas eficazes e capazes para demonstrar a observância e o cumprimento das normas de dados pessoais.

A partir desses princípios, torna-se possível evidenciar uma clara intenção do legislador em aumentar a segurança e a privacidade dos cidadãos brasileiros (em consonância ao praticado pelos legisladores europeus com o GDPR), evitando práticas abusivas e o uso irrestrito dos dados e informações pessoais obtidos por terceiros em relação ao cidadão, quer se fale em

empresas privadas, organizações como um todo ou mesmo no uso de tais informações por parte do Poder Público.

De acordo com Adriana Espíndola Corrêa (2019), antes da promulgação dessa legislação em agosto de 2018, a tutela dos dados tinha como fundamentos tão somente o direito à vida privada e à intimidade, com fulcro no art. 5º, X, da CRFB/1988 e no art. 21 do Diploma Civil. Assim, a Lei Geral de Proteção de Dados (LGPD) estabeleceu, a partir de seu art. 2º, como preceitos fundamentais respeito à privacidade, autodeterminação informativa, liberdade de expressão, informação, comunicação e opinião, inviolabilidade da intimidade, da honra e da imagem, direito ao livre desenvolvimento da personalidade, desenvolvimento econômico e tecnológico, livre iniciativa, livre concorrência e defesa do consumidor.

Segundo Renato Leite Monteiro, a LGDP

> complementa, harmoniza e unifica um ecossistema de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil. Foi inspirada nas discussões que culminaram na GDPR europeia e tem por objetivo não apenas conferir às pessoas maior controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. Isso inclui modelos de negócio que se valem de algoritmos para auxiliar na tomada de decisões automatizadas. A LGPD também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos nesse processo, por meio da diminuição da assimetria de informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado. (Monteiro, 2018:9)

Para o autor supramencionado, essa legislação foi idealizada para garantir aos indivíduos o direito de ter acesso às informações referentes aos tipos de dados pessoais que são utilizados para alimentar os algoritmos responsáveis por decisões automatizadas, de modo que, caso o processo automatizado tenha por intuito formar perfis comportamentais para tomar uma decisão subsequente, devem ser incluídos dados anônimos para o enriquecimento de tais perfis, estabelecendo que o titular dos dados possa conhecer os critérios utilizados para tomar a decisão automatizada e de solicitar a revisão por um ser humano quando esta afetar os interesses do titular dos dados.

Já nos estudos da autora Monteiro (2019), ela versa sobre a aplicabilidade da LGPD nos termos do art. 3º (incisos I, II e III) da legislação, apontando que ela é aplicável a qualquer pessoa natural ou jurídica de

direito público ou privado, independente do meio, país ou sede do país no qual estejam localizados os dados, desde que sejam atendidos aos seguintes critérios: a operação de tratamento de dados deve ser realizada no território brasileiro; tal atividade deve ter por objetivo a oferta ou o fornecimento de bens ou serviços ou tratamento de dados de indivíduos localizados no território brasileiro; os dados pessoais do tratamento tenham sido coletados de modo direto ou indireto no território brasileiro.

4 DADOS PESSOAIS COMO ESTRATÉGIA DE NEGÓCIOS

4.1 A captação de dados pessoais, seu tratamento e manejo no corporativo para fins comerciais

Diante do exposto até o então, tem-se que os dados pessoais dos usuários se constituem como informações valiosas, as quais podem ser exploradas seguindo o mais moderno das legislações recentes. Segundo Francieli Puntel Raminelli e Letícia Bodanese Rodegheri (2016), as questões que envolvem a captação, o tratamento e o manejo dos dados pessoais no contexto da utilização corporativa para fins comerciais são uma questão fundamental a ser analisada nessa discussão, posto que, ainda que existam possibilidades para o uso comercial dos dados pessoais, quando tal utilização se dá de modo indiscriminado ou irrestrito, ela pode ser extremamente maléfica para os titulares das informações (e, por conseguinte, dos direitos).

Salete Oro Boff e Vinícius Borges Fortes (2014) realizaram um estudo versando sobre a privacidade e proteção dos dados pessoais no ciberespaço como um direito fundamental, apontando que os marcos regulatórios a serem produzidos no Brasil (o que se confirmou com o decorrer dos anos) deveriam se ocupar de questões relacionadas à violação de privacidade, publicação deliberada de dados e mesmo para a comercialização dos dados pessoais.

No mesmo sentido, Luiz Ernani Bonesso de Araujo e Larissa Nunes Cavalheiro (2014) apontam que, em tese, não deveria ser permitida a formação de bancos de dados com o tratamento de dados sensíveis (como origem étnica, convicções religiosas, dentre outros aspectos) para fins comerciais, salvo em casos para a indispensabilidade para finalidades de pesquisa. Contudo, os aspectos envolvendo fins comerciais passam diretamente pela publicidade comportamental, sendo um exemplo desta a disposição de anúncios em páginas de conta de *e-mail* do usuário, de acordo com seus hábitos e preferências e se configurando como invasão de privacidade, uma vez

que levanta dados pessoais através das informações da conta do titular das informações.

É complexa, portanto, a questão dos dados pessoais sendo utilizados para fins comerciais. Um importante estudo nesse sentido foi produzido por Ana Cláudia Hostert (2018), que abordou casos como o da empresa Google e do Facebook na captação, tratamento e manejo de dados pessoais dos usuários para fins comerciais: o Google, inicialmente uma ferramenta de busca, foi uma empresa que se reorganizou de modo que os serviços de anúncios se tornaram sua principal fonte de renda com a criação do *AdWords*, a ferramenta que disponibiliza a publicidade para os anunciantes em razão do aumento dos dados pessoais de diversos serviços oferecidos pelo Google[4], os quais combinam o comportamento *online* dos usuários com as oportunidades de publicidade. O sistema adotado por essa empresa para conduzir suas publicidades faz uso de um algoritmo que calcula a relevância de uma determinada publicidade para cada usuário, de modo que o Google alega que os dados pessoais coletados e tratados são utilizados apenas para os propósitos publicitários, não sendo comercializados para terceiros e sem o envolvimento de pessoas no tratamento de dados, o qual ocorre de modo automatizado.

Essa mesma perspectiva é válida para a empresa Facebook, a qual dispõe de uma série de serviços considerados essenciais para os usuários modernos, como o WhatsApp e o Instagram. Contudo, tal empresa se envolveu em uma polêmica recente, posto que foram descobertas parceiras de dados com ao menos sessenta empresas[5], sendo que o Facebook foi apontado como uma ameaça à segurança nacional por agências de inteligência:

> Isso significa que o Facebook dispõe às empresas parceiras os dados pessoais colhidos de seus usuários – que supostamente concordam com alguns termos de privacidade – e dos amigos de seus usuários. Ainda, confirmou-se que os referidos acordos datam do ano de 2007, há mais de uma década. Por fim, já que muitos aparelhos eletrônicos e celulares não conseguiam executar perfeitamente o aplicativo do Facebook, a justificativa dada pela empresa de mídia social foi que os acordos celebrados se deram a fim de possibilitar o pleno funcionamento do seu serviço em forma de aplicativos nos mais varia-

4 Além dos mecanismos de busca, a empresa conta com importantes ferramentas e serviços disponibilizados ao usuário como o servidor de *e-mail* Gmail e o principal *site* de conteúdos em vídeo da internet, o YouTube. Há ainda o Google Play, loja de aplicativos e jogos voltada para os usuários de *smartphones* com o sistema operacional (SO) Android, o mais popular no Brasil, estando disponível em dispositivos utilizados por usuários de todas as classes sociais.

5 Dentre as empresas citadas no estudo, destacam-se *Lennovo*, *Amazon*, *Apple*, *Blackberry*, *Samsung* e *Huawei*.

> dos produtos – todos os tipos de celulares, *smart Tvs* e videogames. (Hostert, 2018:34)

Há, nesse sentido, uma série de controvérsias no tocante à coleta, tratamento e manejo de dados pessoais dos usuários, sobretudo envolvendo essas gigantes empresas da internet, as quais contam com uma facilidade de acesso que seria irrestrita sem a existência dos marcos legais que versam sobre a privacidade e proteção dos dados.

4.2 O uso de dados dos usuários de serviços públicos na era da vigilância governamental

Assim como a abrangência e a complexidade que gira em torno da utilização comercial dos dados pessoais de usuários no século XXI, outro ponto a ser abordado parte da utilização dos dados os usuários de serviços públicos na era da vigilância governamental. Segundo Yuri Monnerat Lott e Regina de Barros Cianconi (2018:125), a "grande questão que move as empresas e os governos para o *big data* é a (nova) possibilidade de encontrar relações entre pontos distantes de um sistema complexo e sem necessariamente entender suas causas, podendo fazer previsões para o futuro", sendo que a relação entre o uso de serviços públicos e de dados pessoais se confirma a partir de tecnologias que permitam o processamento e aproveitamento dos dados para a melhoria dos serviços públicos.

Segundo Ana Cláudia Hostert (2018), também é verificada uma utilidade dos dados pessoais na manipulação dos governos, a partir do fenômeno denominado *surveillance*[6], o qual envolve a previsão de comportamentos futuros em que o Poder Público pode, por exemplo, prever atitudes terroristas, no mesmo sentido em que pela iniciativa privada se buscam melhores formas de lucrar com anúncios, nos termos já apresentados no presente estudo. Os governos ao redor de todo o mundo também almejam a utilização dos dados pessoais dos usuários; contudo, assim como ocorre com as empresas pertencentes à iniciativa privada, os governos também devem obedecer às normas pertinentes à proteção de dados e ao reconhecimento dessa proteção como um direito fundamental. Destaca-se que, na atualidade, há uma escassez generalizada de estudos produzidos em âmbito nacional sobre esse fenômeno, de modo que o presente tópico buscou apenas comprovar a relação entre os dados pessoais dos usuários na era da

6 Embora o termo possa ser traduzido literalmente para "vigilância" na Língua Portuguesa, o seu significado engloba uma série de outros aspectos que trazem o novo entendimento do *new surveillance*, envolvendo a previsão de comportamentos futuros.

vigilância governamental, destacando que tais dados podem ser utilizados de modo positivo ou negativo pelos agentes públicos, desde que respeitados os limites da lei e a proteção aos direitos fundamentais dos cidadãos.

4.3 Da Autoridade Nacional de Proteção de Dados e a possível insegurança jurídica na sua implantação

Segundo Coelho (2019), dentre os inúmeros aspectos controversos que abrangem a LGDP, um consiste na criação de uma Autoridade Nacional de Proteção de Dados a qual será incumbida da fiscalização do cumprimento da legislação e da aplicação de sanções em caso de violação. Essa Autoridade poderá também dispor sobre os padrões técnicos mínimos para aplicar padrões de segurança e governança, em especial para o tratamento de dados pessoais sensíveis, os quais já foram contextualizados no presente estudo. Basicamente, a Autoridade Nacional seria o

> [...] órgão da Administração Pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta lei. Peça essencial do marco normativo em questão, com competências de promoção de estudos e da cultura de proteção de dados, cooperação com as demais autoridades nacionais e internacionais, edição de regulamentos, fiscalização, sancionamento, entre outros. A experiência internacional reforça a necessidade de criação de tal instância reguladora, com *características de independência, especialização técnica* e poderes efetivos de *enforcement*. Espera-se que tal Autoridade seja estabelecida por lei ou medida provisória que reproduza os artigos que foram objeto de veto da LGPD. (Coelho, 2019:17)

Sergio Paulo Gomes Gallindo e Daniel T. Stivelberg (2019) apontam que, dentre os objetivos da criação da MP 869/18, encontram-se alterações na Lei nº 13.709/2018, para criar a Autoridade Nacional de Proteção de Dados (ANPD), além de outras providências. De acordo com os autores, é esperado que a ANPD harmonize, a partir da regulação, a centralidade protetiva com o desenvolvimento da economia de dados, orientando o cumprimento da LGDP, interagindo com os regulados do setor público e privado e induzindo novos modelos de negócio no tocante ao tratamento, captação e manejo de dados pessoais.

Juliana Falci Sousa Rocha Cunha (2019) leciona que essa MP é uma norma com força de lei editada pelo Presidente da República em situações de relevância e/ou urgência, com efeitos jurídicos imediatos, além da apreciação pelas duas Casas do Congresso Nacional (CN) para conversão em lei ordinária. Ao versar sobre a ANPD e suas competências, a MP 869 dis-

põe sobre a edição de normas e procedimentos sobre a proteção de dados pessoais, requisição de informações aos agentes de tratamento de dados, deliberação administrativa sobre a interpretação da LGPD, fiscalização e aplicação de sanções nos casos de tratamento de dados em descumprimento da legislação, além da promoção de ações cooperativas com Autoridades de Proteção de Dados de países estrangeiros e a difusão na sociedade sobre o conhecimento das normas e políticas públicas relacionadas à proteção dos dados pessoais e medidas de segurança.

A MP 869 foi convertida em lei no mês de maio de 2019, originando a Lei nº 13.853, de julho de 2019, alterando dispositivos da LGDP. Nesse ponto, o art. 55-A dispõe sobre a criação da ANPD como órgão da Administração Pública federal integrante da Presidência da República, de modo que, em seu § 1º, sua natureza jurídica é transitória e pode ser transformada em entidade da Administração Pública federal indireta, com submissão a regime autárquico especial e vinculação à Presidência da República (em até dois anos da entrada em vigor da estrutura regimental da ANPD).

As questões envolvendo uma possível (e provável) insegurança jurídica são abordadas nos estudos de Pedro Nachbar Sanches e Eduardo Salim Curiati (2019) a partir do veto presidencial da criação da ANPD, o que fez com que 39 entidades subscrevessem um manifesto cobrando o Congresso Nacional para a avaliação dos vetos impostos pelo então Presidente Michel Temer nesse sentido. Há, assim, uma necessidade de mobilização do setor público e privado para a criação da referida autoridade para efetivar a aplicação da LGPD.

A segurança jurídica é fundamental para as empresas que trabalham com o tratamento de dados, de modo que, sem a existência de uma autoridade nesse sentido, não existe o órgão regente para a aplicação da legislação de modo prático, instaurando, assim, um grande nível de insegurança jurídica. Os juristas que se manifestam sobre o tema, nesse sentido, apontam para a insegurança jurídica envolvendo a implantação da ANPD, de modo que tais discussões vêm permeando um ambiente consolidado de discussão envolvendo a utilização dos dados pessoais e o seu reconhecimento como um direito fundamental dos indivíduos no sentido da previsão de sua proteção no Diploma Constitucional de 1988.

CONSIDERAÇÕES FINAIS

Vivemos atualmente na era da informação, de modo que não tão somente as pessoas vêm se adaptando de modo célere à incorporação das

tecnologias e dos serviços inovadores em seu cotidiano, como também as organizações que compõem o segmento público e privado e o próprio Direito vêm se ocupando de alinhar os pressupostos fundamentais para que tal adaptação não seja nociva ao funcionamento dos sistemas, sem que as informações de usuários sejam exploradas de modo irrestrito e prejudicial.

Os dados pessoais dos indivíduos se tornaram, na contemporaneidade, informações valiosas, de modo que o Direito vem se ocupando da criação de legislações importantes nesse sentido, buscando assegurar a proteção aos dados pessoais como um direito fundamental de previsão constitucional e estabelecendo uma série de limites para a captação, tratamento e manejo de dados pessoais. No presente estudo, foi apresentada a Lei Geral de Proteção de Dados (LGPD) e seus principais mecanismos e aplicações, posto que ela fora elaborada com base na *General Data Protection Regulation* – GDPR – legislação europeia que versa sobre o tema.

No mesmo sentido em que o Direito em todo o mundo vem buscando estabelecer parâmetros legais para a utilização dos dados pessoais como estratégias de negócios, surge uma série de congruências que vem se tornando objeto de pesquisa dos juristas e de análise dos legisladores. No Brasil, um dos grandes exemplos se dá na criação da Autoridade Nacional de Proteção de Dados (ANPD). Para que haja segurança jurídica para as empresas que operam no segmento de tratamento de dados, é indispensável o estabelecimento da ANPD como um órgão que rege a aplicação da LGPD no sentido prático. Sem o estabelecimento do órgão, contudo, se estabelece um alto nível de insegurança jurídica, colocando em risco todos os aspectos relacionados ao uso de dados pessoais como estratégias de negócios.

Cumpre-se destacar que o presente estudo não buscou esgotar completamente o tema, posto que, no momento da realização de sua pesquisa e redação, uma série de alterações na legislação vem sendo promovidas, inclusive com o trâmite da PEC 17/2019, a qual versa sobre a inclusão da proteção fundamental no rol de direitos fundamentais. Porém, tornou-se possível apresentar os principais parâmetros jurídicos envolvendo o uso de dados pessoais como estratégias de negócio à luz do advento tecnológico e dos avanços legais nesse sentido.

REFERÊNCIAS

ARAUJO, Luiz Ernani Bonesso de; CAVALHEIRO, Larissa Nunes. A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do

internauta. *Revista Do Direito Público*, Londrina, v. 9, n. 1, p. 209-226, jan./abr. 2014.

BENNET, Colin J. The European General Data Protection Regulation: an instrument for the globalization of privacy standards? *Information Polity*, 23 (2018) 239-246.

BERARDO, Zeca; LILLA, Paulo; LIZAS, Elen. Promulgada a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD). 15 ago. 2018. Disponível em: <https://www.lefosse.com/Promulgada_Lei_n_13.709_2018_Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_LGPD.pdf>. Acesso em: jul. 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Sequência*, Florianópolis, n. 68, p. 109-127, jun. 2014.

CAMPOS, Luiz Fernando de Barros. Metadados digitais: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. In: *Encontros Bibli – Revista Eletrônica de Biblioteconomia e Ciência da Informação*, Florianópolis, n. 23, 1º sem. 2007.

COELHO, L. V. (Coord.). LGDP – Lei Geral de Proteção de Dados. FIESP, 2018. Disponível em: <https://www.fiesp.com.br/arquivo-download/?id=252615>. Acesso em: jul. 2019.

CORRÊA, Adriana Espíndola. Lei de proteção de dados e a identificação nacional: há antinomias? In: *Conjur*, fev. 2019. Disponível em: <https://www.conjur.com.br/2019-fev-18/direito-civil-atual-lei-protecao-dados-identificacao-nacional-antinomias>. Acesso em: jul. 2019.

CUNHA, Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. In: *PIDCC*, Aracaju/SE, a. VIII, v. 13, n. 02, p. 115 a 145, jul. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. In: *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FAGUNDES, Priscila Basto; MACEDO, Douglas Dyllon Jeronimo de; FREUND, Gislaine Parra. A produção científica sobre qualidade de dados em *big data*: um estudo na base de dados web of science. *RDBCI – Revista Digital. Bibliotecon. Cienc. Inf.*, Campinas, v. 16, n. 1, p. 194-210, jan./abr. 2018.

FERRARI, Fabricio; CECHINEL, Cristian. Introdução a algoritmos e programação. Bagé, Universidade Federal do Pampa, abril de 2008, versão 2.0.

FLORENÇO, Larissa Britto. A proteção de dados pessoais nas relações de consumo como um direito fundamental: perspectivas de um marco regulatório para o Brasil. *Revista da ESMESC*, v. 23, n. 29, p. 165-182, 2016.

GALLINDO, Sergio Paulo Gomes; STIVELBERG, Daniel T. Questões sobre a nova Autoridade Nacional de Proteção de Dados da MP 869/2018. In: *Conjur*, jan. 2019. Disponível em: <https://www.conjur.com.br/2019-jan-24/opiniao-questoes-anpd-mp-8692018>. Acesso em: jul. 2019.

GHISLENI, Eduardo Steffenello. Vigilância na sociedade em rede: a coleta de dados pessoais na internet e suas implicações ao direito à privacidade. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Maria, Santa Maria, 2015.

HIRATA, Alessandro. O Facebook e o direito à privacidade. *Revista de Informação Legislativa*, a. 51, n. 201, jan./mar. 2014.

HOSTERT, Ana Cláudia. Proteção de dados pessoais na internet: a necessidade de lei específica no ordenamento jurídico brasileiro. Monografia apresentada à Universidade Federal de Santa Catarina para obtenção do título de Bacharel em Direito, Florianópolis, 2018.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do *big data* e dados pessoais: análise da produção da Ciência da Informação no Brasil. In: *Perspectivas em Ciência da Informação*, v. 23, n. 4, p. 117-132, p. 125, out./dez. 2018.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? In: *Instituto Igarapé*, artigo estratégico nº 39, dez. 2018.

MONTEIRO, Y. S. A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018. Artigo científico apresentado como requisito para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB), Brasília, 2019.

MURER, Ricardo. *Big data* e a ascensão dos *bots* nas mídias sociais. Escola Superior de Propaganda e Marketing – ESPM, 8 de outubro de 2017.

POLIDO, Fabrício Bertini Pasquot et al. GDPR e suas repercussões no Direito brasileiro. In: *IRIS – Instituto de Referência em Internet e Sociedade*, 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf>. Acesso em: jul. 2019.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A proteção de dados pessoais na internet no Brasil: análise de decisões proferidas pelo Supremo Tribunal Federal. In: *Cadernos do Programa de Pós-Graduação da UFRGS*, v. XI, n. 2, 2016.

RODRIGUEZ, Daniel Piñeiro. O direito fundamental à proteção de dados pessoais: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado) – Faculdade Direito, Pós-Graduação em Ciências Criminais, PUCRS, Porto Alegre, 2010.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito – UFPR*, Curitiba, n. 53, 2011.

SANCHES, Pedro Nachbar; CURIATI, Eduardo Salim. A imprescindibilidade da criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). In: *Migalhas*, jan. 2019. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI293587,81042-A+imprescindibilidade+da+criacao+da+Autoridade+Nacional+de+Protecao>. Acesso em: jul. 2019.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? Artigos Selecionados Rede 2017. I Encontro da Rede de Pesquisa em Governança da Internet Rio de Janeiro, 14 de novembro de 2017.

Sobre os autores:

Danilo Henrique Nunes | *E-mail:* dhnunes@hotmail.com
Doutorando e Mestre em Direitos Coletivos e Cidadania Universidade de Ribeirão Preto – Unaerp, Ribeirão Preto/SP, Advogado, Jornalista, Professor Universitário.

Lucas Souza Lehfeld | *E-mail:* lehfeldrp@gmail.com
Pós-Doutor em Direito pela Universidade de Coimbra, Portugal, Doutor em Direito pela PUC/SP, Professor Orientador do Programa de Doutorado e Mestrado em Direitos Coletivos e Cidadania Universidade de Ribeirão Preto – Unaerp, Ribeirão Preto/SP, Advogado, Professor Universitário.

Dirceu Pereira Siqueira | *E-mail:* dpsiqueira@uol.com.br
Coordenador e Professor Permanente do Programa de Pós-Graduação *Stricto Sensu* (Doutorado e Mestrado) em Direito no Centro Universitário de Maringá/PR (UniCesumar), Pós-Doutor em Democracia e Direitos Humanos pelo Ius Gentium Conimbrigae da Faculdade de Direito da Universidade de Coimbra e pelo Centro de Estudos Interdisciplinares do Séc. XX da Universidade de Coimbra, sob orientação do Prof. Doutor Jónatas Eduardo Machado (2014), Doutor (2013) e Mestre (2008) em Direito Constitucional pela Instituição Toledo de Ensino – ITE/Bauru, Especialista (2006) Lato Sensu em Direito Civil e Processual Civil pelo Centro Universitário de Rio Preto (UNIRP), Graduado em Direito (2002) pelo Centro Universitário de Rio Preto (UNIRP), Professor nos Cursos de Graduação em Direito do Centro Universitário de Bebedouro (UNIFAFIBE) e da Universidade de Araraquara (UNIARA), Professor Pesquisador do Núcleo de Pesquisa em Direito da Universidade de Araraquara (UNIARA).

Data de submissão: 12 de setembro de 2019.

Data do aceite: 11 de maio de 2020.