PRIM@ FACIE

v. 19, nº. 42, 2020

Proteção de Dados na América Latina e os Desafios do COVID-19

Giovani Saavedra*
Universidade Presbiteriana Mackenzie, Programa em Pós-Graduação em Direito Econômico e Político, São Paulo-SP, Brasil.
https://orcid.org/0000-0002-5269-3844

Daniel Nagao Menezes**
Universidade Presbiteriana Mackenzie, Programa em Pós-Graduação em Direito Econômico e Político, São Paulo-SP, Brasil.
https://orcid.org/0000-0001-9151-5699

Resumo: O artigo trata de um tema relevante para o seu momento histórico que é a necessidade do uso de dados pessoais pelas autoridades públicas no combate à pandemia mundial da COVID-19. Esta necessidade de acesso às mais diversas informações no enfrentamento da pandemia global acarreta diversos conflitos éticos, políticos e jurídicos. A partir deste problema o texto busca analisar a estrutura legal dos países latino americanos referente à proteção e acesso de dados e como isso se relaciona com a necessidade de acesso pelas autoridades sanitárias. Conclui que possuem estruturas jurídicas e institucionais mais avançadas de proteção de dados que têm condições de compartilhamento das informações sem a exposição indevida de informações do cidadão. A método utilizado foi a hipotético dedutivo com uso da revisão bibliográfica como procedimento metodológico.

Palavras-chave: Acesso à informação; Crise Sanitária; COVID-19; Proteção de Dados.

* Doutor em direito e em filosofia pela Johann Wolfgang Goethe - Universität Frankfurt am Main. Professor de graduação e pós-graduação (especialização, mestrado e doutorado) na faculdade de direito da Universidade Presbiteriana Mackenzie. E-mail: giovani.saavedra@me.com

** Doutor em Direito Político e Econômico (Universidade Presbiteriana Mackenzie), Pós-Doutor em Direito (USP). Pós-Doutorando em Economia (UNESP-Araraquara). Professor do Programa de Pós-Graduação em Direito Político e Econômico da Faculdade de Direito da Universidade Presbiteriana Mackenzie. Membro do CIRIEC-Brasil. E-mail: nagao.menezes@gmail.com

UNIVERSIDADE FEDERAL DA PARAÍBA

Programa de Pós-Graduação em Ciências Jurídicas

DOI: https://doi.org/10.22478/ufpb.1678-2593.2020v19n42.54590

Proteção De Dados Na América Latina E Os Desafios Do Covid-19

Giovani Saavedra

Daniel Nagao Menezes

1 INTRODUÇÃO

Na chamada era digital, a circulação de dados tornou-se um aspecto nevrálgico. Os dados, por si só, são reconhecidos "o petróleo da era digital". No entanto, os dados são mais abrangentes, pois, em vez de serem extintos com o uso, têm a vocação de enriquecer a si mesmos – o chamado efeito multiplicador-; portanto, se os dados não podem circular, não podem alimentar os sistemas de informação. E, toda a cadeia que foi construída em torno dos dados enfraquece, perde sua utilidade e importância. A circulação e o tratamento de dados são, então, o núcleo central da lei de dados. Daí o interesse manifestado pelos apoiadores de movimentos como governo aberto, tecnologia cívica, cidades inteligentes, entre os mais conhecidos.

Os dados têm proprietários, esses são os titulares dos dados. A tendência relativa à proteção legal dos dados tem sido, por um lado, seu reconhecimento como um direito de personalidade, bem como nome, nacionalidade, etc, e; por outro lado, como um direito relacionado ao direito à privacidade ou intimidade. Esses dados foram chamados de "dados pessoais", mas também existem outras categorias de dados, como dados públicos, como dados meteorológicos, dados de tráfego automotivo; dados corporativos em desenvolvimento, como capital de uma empresa, decisões de negócios, número de toneladas de carga transportada, algumas delas classificadas como protegidas por

"sigilo profissional". Além desses dados, existem outros dados que podem ser chamados de "derivativos" e que são extraídos dos sistemas de informação, como resultado da implementação de algoritmos ou, da chamada inteligência artificial, ou ainda, dados produzidos simplesmente cruzando-os com outros dados, conhecidos como "mega dados" e, finalmente, os dados resultantes de atividades científicas ou acadêmicas, que foram denominados "dados de pesquisa".

Com isso surge a questão de fundo: existem limites para esta circulação dos dados? E, sendo positiva a resposta, quais são esses limites? Essas questões voltaram à agenda acadêmica e política com a pandemia global de COVID-19 em que, para se criar conhecimento de enfrentamento ao Corona Vírus e sua circulação no planeta, é necessário o acesso aos dados pessoais da população (especialmente as pessoas contaminadas) pelas autoridades sanitárias de todos os países.

O artigo pretende analisar a situação jurídica na América Latina através da análise da legislação de alguns países chave, buscando compreender a situação jurídica no continente. Para isso foi realizada a revisão bibliográfica do assunto, valendo-se do método hipotético dedutivo.

2 PANORAMA DA PROTEÇÃO DE DADOS NA AMÉRICA LATINA

Nos países da América Latina (PATIÑO; POVEDA, 2018), se investe no desenvolvimento de redes de telecomunicações para garantir o chamado "serviço universal" de acesso às redes de comunicação, no entanto, de acordo com o último relatório do BID, há um atraso na inovação dos negócios e as empresas da região adotam novas tecnologias em um ritmo mais lento (CAVALLO; POWELL, 2018). Um elemento necessário para desenvolver a economia digital,

que, como demonstrado (CARLSSON, 2004, p. 245-264,) vem mudando paradigmas (BABINET, 2014), tornando a "inovação" um elemento essencial para o crescimento das empresas, tornando obsoletas algumas práticas comerciais tradicionais. É assim que os dados são uma fonte essencial desse tipo de práticas comerciais, pois também são atividades do Estado.

Uma questão fundamental que emerge desse tema é qual é o interesse dessa análise? Para responder a essa pergunta, pode-se observar as taxas de crescimento do mercado digital latino-americano. Nesse sentido, verifica-se que entre 31 de dezembro de 2017 e junho de 2018, o crescimento foi de 2.325,4% (INTERNET WORLD STATS, 2020). Em maio de 2020, o mundo possuía 4.648.228.067 (INTERNET WORLD STATS, 2020) usuários da Internet. Na América Latina, na mesma data, são 453.702.292 usuários conectados à Internet, com 69% a população com acesso à Internet (INTERNET WORLD STATS, 2020). Ou seja, além de ser um mercado amplo, há perspectivas de crescimento mais do que o dobro nos próximos anos. Esses números vislumbram claramente o espectro social e econômico que é chamado a desenvolver e as políticas que devem ser adotadas para responder a eles (ROSE; RHESE; RÖBER, 2012).

Para limitar o assunto exposto, em uma primeira parte, será apresentado o panorama jurídico da proteção de dados na América Latina, a fim de observar qual é o status jurídico atual nesse assunto e, em uma segunda parte, uma análise reflexiva Perspectiva dos desafios enfrentados por essa estrutura legal. Para realizar essa análise, foram considerados os 19 países latino-americanos que compõem a Rede Ibero-Americana de Proteção de Dados Pessoais - RPDP -, formada em junho de 2003, para compilar os elementos legais essenciais que foram desenvolvidos até o momento.

No Encontro Ibero-Americano de Proteção de Dados, organizado em 2002 pela Agência Espanhola de Proteção de Dados, realizada em San Lorenzo de El Escorial, Espanha, foi criada a Rede Ibero-Americana de Proteção de Dados Pessoais, tendo os países fundadores (Argentina, Brasil, Costa Rica, Espanha, México, Paraguai,

Peru e Uruguai) declarado o seguinte: “respeito à intimidade e privacidade e, em particular, à livre disposição de seus dados pessoais, é um direito fundamental dos povos”.

O Direito latino-americano de inspiração romano-germânica, em termos de dados, tem influenciado e sido influenciado pelo direito europeu. Nesse sentido, intercâmbios em torno da Rede RIPDP, como em outros cenários, como a Cúpula União Europeia-América Latina e Caribe, o processo de negociação da União Europeia e Mercosul, os acordos de livre comércio firmados entre a União Europeia com alguns países latino-americanos, fortaleceram os laços e defenderam um intercâmbio ativo entre a América Latina e a União Europeia.

Na ausência do arcabouço legal estabelecido por esse grupo de países, pode-se apontar, em primeiro lugar, que os dados sujeitos ao maior desenvolvimento jurídico são “dados pessoais”, sendo os dados públicos desenvolvidos através dos números de “habeas data”, e a “transparência da administração pública”. Em segundo lugar, não é supérfluo especificar que a consagração legal no sistema jurídico de um Estado não determina sua eficácia e observância. Ou seja, a extensão de um regulamento - lato senso - não implica, por si só, uma proteção mais efetiva, mas denota a vontade política favorável ao desenvolvimento de um arcabouço legal devido a diferentes razões. Depois de revisar a legislação dos países latino-americanos que são membros da Rede Ibero-americana de Proteção de Direitos Pessoais, dois níveis de legislação são observados. O primeiro corresponde a países com um amplo regime jurídico, que chamaremos de lei de dados com um regime jurídico desenvolvido, e o segundo, com um regime jurídico escasso, que chamaremos de Lei de Dados com um regime jurídico limitado.

Os sistemas reguladores com regulamentos abrangentes sobre a proteção de dados pessoais foram classificados nesta categoria. Este grupo pode ser subdividido em dois subgrupos. O primeiro, constituído por sistemas que possuem desenvolvimento constitucional, legislativo e até regulatório, mas sem a existência de

uma autoridade específica para sua observância. E no segundo subgrupo, composto por países que também possuem uma autoridade especializada para garantir o cumprimento da legislação sobre proteção de dados pessoais. Nos dois grupos, os direitos fundamentais relacionados são encontrados na Constituição, como privacidade ou privacidade, inviolabilidade das comunicações e, em alguns casos, consagração expressa da proteção de dados pessoais como um direito fundamental.

Chamaremos as estruturas normativas que não possuem uma entidade pública ou que cumprem funções públicas para garantir a aplicação da estrutura legal em questões de dados, acéfalas ou inorgânicas. Vale ressaltar que a ausência de um órgão especializado não implica uma falta de preocupação política em relação a um setor específico. Isso é explicado funcional e organicamente na distribuição das três funções em torno das quais as estruturas legais se desenvolvem e evoluem. Ou seja, a existência da divisão de poderes implica a distribuição dos poderes de criação, modificação (legislativa); execução (executivo) e sanção em caso de não observância deles (judicial). Funções que podem ser reforçadas por entidades ainda mais especializadas, como as comissões reguladoras em relação à primeira função.

Paraguai e Chile estão neste primeiro subgrupo. O Paraguai[1], em 2001, promulgou o chamado "Regulamento de Informação Privada", esta norma contém o quadro normativo sobre a proteção dos direitos pessoais. Da mesma forma, em 2011, mediante a Lei nº 4.439, foram incluídos os seguintes tipos criminais: acesso inadequado a dados pessoais, interceptação de dados, preparação (tentativa) de acesso inadequado à interceptação de dados, acesso inadequado a sistemas de computadores, sabotagem de sistemas de computadores. No entanto, apesar de não ter inicialmente fornecido uma autoridade independente sobre o assunto, em 3 de julho de 2018, o Parlamento

[1] República del Paraguay. Ley nº 1.682, de 16 de enero de 2001.

criou o Conselho de Transparência para Dados Pessoais, ou seja, este país está em transição para o segundo subgrupo.

O Chile, por sua vez, emitiu uma lei sobre a proteção da privacidade em 1999[2], com a particularidade de um regime mais rigoroso quando aquele que processa dados pessoais é o Estado ou quem exerce funções públicas. Por outro lado, também estabeleceu um organismo de registro denominado "Banco de Dados Pessoais" mantido no Serviço de Registro e Identificação Civil; no entanto, o consentimento do proprietário não é necessário para o uso de dados para marketing direto, entre outras exceções ao requisito de consentimento (VIOLLIER, 2017), nem possui uma autoridade e sanções que permitam maior proteção dos dados pessoais.

Esses países têm a consagração dos direitos fundamentais nas respectivas Constituições, como é o caso dos chamados "direitos ARCO", ou seja, o direito de acesso, retificação, cancelamento, oposição à informação. Esses direitos desenvolvem o princípio da "autodeterminação da informação" (PÉREZ ROYO, 1999, p. 19-34, p. 22). Este subgrupo é formado pela Argentina, Colômbia[3], México, Nicarágua, Peru[4], Uruguai e República Dominicana[5]. Esses países estabeleceram um novo órgão de controle que busca garantir o Regime de Propriedade de Dados Pessoais. Os órgãos foram criados como um novo ou como anexados ou derivados de um já existente. No primeiro

[2] República de Chile. Ley 19.628 de 1999.
[3] Constituição Política de 1991, o artigo 15 estabeleceu o direito à privacidade pessoal e ao habeas data. No nível legislativo, foi promulgada a Lei 1.581, de 17 de outubro de 2012, relativa à proteção de dados pessoais, regulamentada pelo Decreto 1.377, de junho de 2013, e pelo Decreto 886, de 14 de maio de 2014, e pela Lei de Habeas Data, Lei 1.266, de 31 de dezembro de 2008, regulamentada pelo Decreto 2.952, de 6 de agosto de 2010, da mesma forma, a Lei 1.273 de 2009 modifica o código penal e cria um novo ativo jurídico protegido para a proteção de informações e dados.
[4] Art. 2 num. 6 da Constituição. Lei 3 de julho de 2011 regulamentada em março de 2013. Estabelece que a Autoridade Nacional para a Proteção de Dados Pessoais pertence à Diretoria Geral de transparência e acesso público que por sua vez está vinculado ao Ministério da Justiça e Direitos Humanos.
[5] Constituição Art. 44 - Direito de acesso à informação e princípios, art. 70 Habeas Data. É estabelecido um órgão específico para dados de crédito, a Superintendência de Bancos, art. 81 da Lei 172 de 2013, finalmente. Também há a Lei Geral de Livre Acesso à Informação Pública, Lei 200, de 28 de julho de 2004.

caso, o Uruguai[6], que criou a AGESIC, a Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, como um órgão descentralizado emanado da Presidência da República (2009). No segundo caso, existem organizações ligadas a um ministério. No caso da Argentina[7] e do Peru[8], ao Ministério da Justiça, na Colômbia[9], vinculado ao Ministério da Indústria e Comércio e, da Nicarágua[10], vinculado a dois ministérios, Ministério da Justiça e Ministério das Finanças e Crédito Público e, o México, vinculado ao Congresso Nacional[11]. Por seu turno, a Nicarágua possui duas autoridades, a pessoa responsável pelo registro de arquivos de dados[12] e a Diretoria de Proteção de Dados Pessoais.

Os sistemas regulatórios nos quais o desenvolvimento legislativo é inexistente ou escasso são encontrados nessa categoria. No entanto, eles mencionam, mesmo que apenas brevemente, os direitos fundamentais relacionados à proteção de dados pessoais. Nesse grupo, podemos identificar dois subgrupos. A primeira caracterizou-se por estabelecer um amplo desenvolvimento constitucional, uma categoria chamada pelos constitucionalistas como o "novo constitucionalismo" (WOLKMER; FAGUNDES, 2012, p.371-408). Por seu lado, o segundo subgrupo inclui sistemas legais que possuem uma estrutura constitucional muito menos desenvolvida.

---

[6] República do Uruguai, art. 72 da Lei n ° 17.930, de 19 de dezembro de 2005, cria como órgão descentralizado da Presidência da República a "Agência para o Desenvolvimento do Governo de Gerenciamento Eletrônico e da Sociedade da Informação e do Conhecimento" [tradução dos autores].

[7] Argentina, Ministério da Economia, Decreto Regulamentar 1.658, de janeiro de 2001 cria a Dirección Nacional, sob o controle do Ministério de Justicia.

[8] A Direção Geral de Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais é o órgão responsável pelo exercício da Autoridade, subordinando-se hierarquicamente ao Despacho Viceministerial de Justicia.

[9] República da Colômbia. O Decreto 4.866 de 2006 cria o Escritório para a proteção de dados pessoais em 2011. A Lei 1.266 de 2008 a inclui sob a direção da Superintendência da Indústria e Comércio, que tem, entre outras funções, analisar solicitação para corrigir, atualização ou remoção de bancos de dados.

[10] Nicarágua - Lei de proteção de dados pessoais, Lei nº 787, aprovada em 21 de março de 2012.

[11] Art. 39, VIII da Lei Federal de Proteção de Dados Pessoais de Indivíduos.

[12] Ley nº 787, Ley de Protección de Datos Personales.

Os regimes legais localizados nesse grupo são caracterizados por um amplo catálogo de direitos constitucionais, garantias e liberdades, que alguns deles até se desenvolvem dentro da estrutura constitucional. Bolívia e Venezuela estão neste subgrupo. Na Bolívia, além de incluir a proteção de dados pessoais em nível constitucional, o Presidente emitiu o "Decreto Supremo"[13] que aprova o regulamento de proteção de dados pessoais[14]. Em sua leitura, vale ressaltar duas particularidades em relação à autodeterminação informativa, a primeira é a necessidade de justificativa para retirar o consentimento no tratamento de dados pessoais, o que limita o direito à oposição e, por outro lado, a impossibilidade de uso para outros fins, ainda mais protetor.

A Venezuela, por sua vez, estabelece em sua Constituição Política a proteção de dados pessoais, ou seja, como princípio de ordem constitucional, estabelecendo o sigilo profissional e jornalístico como exceções, ou seja, como um direito não absoluto, a proteção que pode ser solicitada pelo Provedor Geral de Justiça (Defensor del Pueblo) por meio de proteção constitucional ou perante jurisdições comuns, denominada "rota autônoma" (processos individuais como chamamos no Brasil).

Dentro deste grupo estão Equador, Guatemala, El Salvador, Honduras, Panamá e Haiti. O Haiti estabeleceu em sua Constituição Política de 1987 o direito à informação[15], um direito que tem conotações duplas, o direito de acesso e o direito de comunicar as informações que são conhecidas. No caso do Equador, o direito à proteção dos direitos pessoais foi incluído na Constituição Política Nacional como um direito fundamental. A Guatemala e o Panamá estabelecem em suas Constituições a inviolabilidade das

[13] Bolivia. Decreto Supremo da Presidência da República nº 1.793 de 13 de novembro de 2013.
[14] Reglamento a la Ley nº 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación.
[15] Constituição de 1987, art. 40. Porém não menciona dados pessoais, apenas fala sobre liberdade de informação escrita e oral sobre informação pública, exceto aquelas relativas à segurança nacional.

comunicações e o acesso à informação pública, direitos relacionados a Lei de Proteção de Dados. Na Guatemala, um código de crimes de informática foi inserido no Código Penal[16], incluindo: destruição de registros de computador (art. 274 A), alteração de programas, registros proibidos (art. 274D), manipulação informação (art. 274E). Em Honduras e Panamá, o habeas data foi consagrado nas Constituições e foi promulgada no Panamá em 202, uma Lei de Transparência que desenvolve o direito de acesso à informação pública e; em Honduras promulgado em 2006[17]. El Salvador, por sua vez, não é muito explícito no nível constitucional[18], mas incluiu a confidencialidade de dados pessoais não públicos na Lei de Telecomunicações[19].

3 PROTEÇÃO DE DADOS NO BRASIL

No Brasil, o tema da proteção de dados ocupa um lugar de destaque no debate da esfera pública, em especial pela recente promulgação da Lei Geral de Proteção de Dados (Lei 13.709 de 14 de agosto de 2018), atualizada pela Lei 13.859 de 14 de agosto de 2019, com evidência para a Autoridade Nacional de Proteção de Dados (ANPD). O tema da proteção de dados é também reforçado por uma série de dispositivos constitucionais, que estabelecem: a) a inviolabilidade da vida privada e da intimidade (Art. 5º., Inc. X) e do "sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas" (Art. 5º., Inc. XII). Além disso, no art. 5º, inciso X, a Constituição Federal determina a inviolabilidade da

[16] República de Guatemala. Código Penal, Decreto nº 17-73, 27 de julho de 1973.
[17] República do Panamá. Lei 6 de 22 de janeiro de 2002, que determina regras de transparência na administração pública, estabelece a ação de habeas data e determina outras disposições.
[18] A Constituição estabelece o direito à liberdade, propriedade e propriedade em nível geral.
[19] Decreto Legislativo 911 de 14 de dezembro de 2005.

"*intimidade, a vida privada, a honra e a imagem das pessoas*", resguarda a possibilidade de indenização, tanto por danos morais quanto materiais, bem como institui ação de *habeas data* (Art. 5º., LXXII)[20]. Há um debate acerca da existência de um direito fundamental à proteção de dados[21]. Esse debate foi reforçado recentemente pelo projeto de emenda constitucional (PEC-17). Hoje, Sarlet registra poder-se afirmar que há um forte consenso na doutrina brasileira no sentido de a Constituição Federal ter consagrado um direito fundamental implicitamente positivado à proteção de dados pessoais[22].

O Código Civil, de 2002 concretiza as normas constitucionais nas relações privadas, à medida que reforça ser a proteção à vida privada inviolável. Ainda na esfera infraconstitucional o Código de Defesa do Consumidor também trouxe elementos de proteção às informações de seus cadastros, ampliando a proteção trazida, até então para a esfera pública, sob o instituto do Habeas Data, para a esfera privada, determinando, não apenas o acesso, mas trazendo critérios acerca de seu formato e possível correção (art. 43, Lei nº 8078/90).

Já com o avanço da tecnologia, o reconhecimento da informação como fomento importante para o desenvolvimento econômico, foi promulgada em 2011 a Lei de Cadastro Positivo (Lei n.º 12.414/2011), a qual determina as condições de armazenamento de histórico de informações de adimplemento do indivíduo, com a finalidade de avaliar a situação econômica do cadastro. A Lei do

---

[20] Sobre um panorama da evolução da proteção de dados no direito brasileiro, em especial, no direito constitucional, ver: DONEDA, Danilo. Da Privacidade à Proteção dos Dados Pessoais. Fundamentos da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019. p. 259 e ss.

[21] Ver, a esse respeito: DONEDA, Danilo. A proteção de Dados Pessoais como um Direito Fundamental. In: Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 91-108.

[22] Sarlet desenvolve essa tese em artigo ainda não publicado: Sarlet, Ingo Wolfgang. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais (ainda não publicado), p. 9. Agradeço ao Prof. Ingo por ter-me franqueado acesso ao texto ainda antes da publicação. Ver, também: BIONI, Bruno. Proteção de Dados Pessoais. A função e os limites do consentimento. Rio de Janeiro: Forense, 2020. p. 90 e ss.

Cadastro Positivo destaca como princípio do tratamento dos dados a transparência e o respeito "à intimidade, vida privada, honra e imagem das pessoas", limitando sua divulgação à previsão legal ou consentimento expresso. Contudo, a Lei de Acesso à Informação (Lei nº 12.527/2011), já traz exceções à garantia do consentimento expresso para utilização do cadastro positivo quando necessários os dados para fins de (i) prevenção e diagnóstico médico; (ii) realização de estatísticas e pesquisas cientificas de evidente interesse púbico ou geral, previstos em lei, vedando a identificação pessoal; (iii) cumprir ordem judicial; (iv) proteção do interesse público e geral preponderante (art. 31, 3º e incisos).

Em 2014, foi aprovada a Lei nº 12.965/2014, o Marco Civil da Internet, que estabeleceu os direitos dos usuários na rede preservando em um único arcabouço legislativo: (i) inviolabilidade da intimidade e da vida privada, (ii) a preservação do sigilo das comunicações privadas transmitidas ou armazenadas; (iii) a proteção contra o fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do titular; (iv) o direito a informações claras e completas sobre o tratamento de dados pessoais e (v) a prerrogativa do consentimento expresso e destacado sobre o tratamento dos dados (art. 70 e incisos).

No dia 14 de agosto de 2018 foi promulgada a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). O período de vigência da lei já passou por diversas modificações, mas com a imposição da quarentena em razão da pandemia do Corona vírus (COVID-19) a situação de insegurança jurídica se agravou: o Senador Anastasia apresentou o Projeto de Lei nº1179/2020, que propunha a postergação da vigência da LGPD por mais 18 (dezoito) meses. Por tratar de medidas emergenciais de contingência diante da pandemia, o PL ganhou regime de urgência na tramitação, tendo sido aprovado no Senado em 04 de abril de 2020, seguindo para a Câmara dos Deputados com a proposta de início da vigência da LGPD para 1º de janeiro de 2021 e da aplicação das sanções somente s partir de 1º de agosto de 2021. Em 29 de abril de 2020 foi editada a Medida Provisória

959/2020, com eficácia imediata, que propôs o adiamento da LGPD para o dia 03 de maio de 2021. Dia 25 de Agosto de 2020, a Câmara dos Deputados editou a MP mudando a entrada da lei para o dia 31 de dezembro de 2020. A MP foi enviada para ao Senado e tudo se encaminhava para uma confirmação da decisão da Câmara, mas o Senado retirou o artigo do texto, que tratava da vigência da Lei Geral de Proteção de Dados. Subsistiu, ainda, um debate sobre a entrada em vigor da lei, tendo em vista que o artigo foi retirado do texto, logo, em regra, valeria o artigo anterior, mas, o fato é que no dia 18 de setembro de 2020, com a sanção presidencial da lei, que não tinha nenhuma linha sobre a Lei Geral de Proteção de Dados, o debate acabou, a partir de então não havia mais dúvidas, a lei entrou em vigor.

4 PROTEÇÃO DE DADOS EM TEMPOS DE EMERGÊNCIA SOCIAL: COVID-19, DEMOCRACIA, INOVAÇÃO E REGULAÇÃO NA AMÉRICA LATINA

A América Latina é a região com maior envolvimento em redes sociais em nível global, ou seja, uma média de 6 horas menal por visitante (INTERNET WORLD STATS, 2020). Entre as principais dificuldades relacionadas à circulação de dados está o cibercrime. É assim que, por exemplo, no México quase metade dos usuários da Internet sofreu ataques cibernéticos. Das 71 milhões de pessoas conectadas no país, 33 milhões tiveram seus equipamentos ou informações violadas. Assim, sem segurança, os níveis de confiança caem, nesse sentido, Basdenvand e Mignard (2018) apontaram que *"le numérique sera un réel progrès lorsque la sécurité et la confiance auront éliminé les dangers"*. Por outro lado, a obsolescência das normas é um dos temas a serem enfrentados. Bem como a aplicação

de regras relacionadas à proteção de dados pessoais em situações regidas por regras estabelecidas sob outros objetivos. De fato, essas situações têm impacto nos direitos fundamentais relacionados à circulação de dados e na democracia.

Os direitos fundamentais podem ser limitados, são reconhecidos dois tipos de limites (GHEVONTIAN; FAVOREU; GAÏA, 2015). Os primeiros são aqueles que emergem da necessidade de respeitar outro direito fundamental ou de respeitar objetivos de interesse geral. Em relação aos direitos fundamentais relacionados à proteção de dados pessoais, existe o direito à privacidade ou o direito à intimidade. Este direito, com a era digital foi diminuído devido à obsolescência das normas legais. De Filippi (2016), sobre esse tema, explica a dificuldade de garantir o direito ao esquecimento[23], considerando que na era digital, uma vez publicada, as informações podem ser recuperadas (WEBER, 2011, p. 120-130), e também são de conhecimento público. O fato do link que leva à referida informação ser excluído não será mais tão relevante, pois há possibilidade de recuperação da informação.

Tecnicamente, o anonimato dos dados pode ser revertido, através do uso de software e do cruzamento de bancos de dados, reconstituindo a identificação das pessoas que dizem respeito aos dados que foram anonimizados, por meio de mecanismos de engenharia reversa (ENISA, 2012). Conforme analisado por Oboler, Welsh e Cruz (2012) a maioria dos usuários da Internet concorda com o processamento de seus dados para acessar um serviço mais personalizado que não poderia ser fornecido de outra forma ou que está sujeito ao consentimento para a prestação do serviço. No final, os internautas aceitam por indiferença ou por necessidade, porque é aborrecedor e confuso ler todos os termos das condições gerais de uso ou, em algumas ocasiões, com a intenção de receber prospecção de bens e serviços de seu interesse (THOMPSON, 2013, p. 199-223).

---

[23] Sobre o direito ao esquecimento no âmbito do direito brasileiro, ver: SARLET, Ingo Wolfgang; NETO, Arthur Ferreira M. *O "Direito ao Esquecimento" na Sociedade da Informação*. Porto Alegre: Livraria do Advogado, 2018.

A observância da autodeterminação dos dados ou o respeito pelo consentimento para o processamento dos dados são violados pelo uso de cookies e pela captura de dados pessoais por meio de publicações de terceiros que deixam vestígios nos sistemas de informações, conhecidas como data shadows (KOOPS, 2011). A proliferação de informações acessíveis de acordo com o perfil digital ou, que responde à vontade dos grupos de poder, são situações enquadradas "de risco" como manipulação em massa, engenharia social (MITNICK, K.; SIMON, 2003), vigilância eletrônica, acesso à saúde (HARARI, 2016). Por outro lado, o direito à liberdade de expressão e o direito à informação, que podem ser violados nas chamadas comunicações eletrônicas, principalmente devido à falta de observância dos princípios da neutralidade da rede e do princípio do serviço universal.

Diante dos direitos fundamentais e da adaptação da lei a situações de fato, vale a pena levantar a teoria canadense, chamada "acomodação razoável"[24], que foi aceita pela jurisprudência na Europa - Tribunal de Direitos Humanos -, através da qual procura evitar, tanto quanto possível, a discriminação indireta contra minorias e também com maiorias, revendo novos tópicos como soberania nacional e democracia. A pesquisa jurídica sobre direitos fundamentais requer a necessidade de estruturas legais que respondam às realidades e aos avanços tecnológicos, levando em consideração a extraterritorialidade da circulação de dados, evitando a proliferação de exceções e um regime de sanções acessível a cidadãos, isto é, regimes que lhes permitem ir aos tribunais de justiça que garantem a observância dos direitos fundamentais que foram violados.

[24] A obrigação de acomodar ou ajustar é a obrigação que, por lei, cabe aos gerentes de instituições e organizações públicas e privadas de evitar qualquer forma de discriminação indireta contra minorias e maiorias, adotando diferentes meios de harmonização. A aplicação de certas leis ou regulamentos, torna a norma mais flexível ou a adapta em sua aplicação. ITXASO, M. E. El concepto jurisprudencial de acomodamiento razonable. El Tribunal Supremo de Canadá y el Tribunal Europeo de Derechos Humanos ante la gestión de la diversidad cultural y religiosa en el espacio público. Anuario de Filosofia del Derecho, vol. XXX, 2014, p. 69-96.

Essa realidade se impõe de maneira mais forte ainda em períodos de emergência social. Nesse sentido, é sintomática a "Nota Conjunta" (PFDC & Câmara Criminal) da Procuradoria Geral da República do Brasil, que destacou a importância da entrada em vigor da Lei Geral de Proteção de Dados (LGPD) mesmo num contexto de emergência em função da pandemia do COVID-19, dado que a lei geral de proteção de dados "*normatiza os procedimentos para assegurar as garantias desses direitos, estrutura o marco regulatório, cria o sistema administrativo e define o regime sancionatório, vem dar maior segurança aos indivíduos e a setores por ela abrangidos*". A nota destaca ainda o risco da falta de proteção jurídica de dados, dado que a políticas sanitárias poderiam ser centradas "*na questão de coleta de dados e de seu uso indiscriminado, sem que os usuários(...)"* tivessem *"(...) ideia do que é feito com seus dados pessoais, que são o grande ativo desta época, servindo até a experimentos sociais com os indivíduos, que os ignoram por completo"* (MPF, 2020)

E, de fato, esse risco se concretizou: como uma das medidas de política de saúde, o Governo Federal editou a Medida Provisória nº 954/2020, que determinava o compartilhamento de dados pessoais de consumidores (nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas), por empresas de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE). A constitucionalidade dessa medida foi questionada no Supremo. A relatora, Ministra Rosa Weber, concedeu liminar suspendendo a eficácia da Medida Provisória 954/2020, que foi confirmada pelo Plenário do Supremo Tribunal Federal. Em sua decisão, a Ministra reconheceu o direito à proteção de dados e a necessidade de o estado apresentar uma "justificativa consistente e legítima":

> No clássico artigo The Right to Privacy, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, **já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e**

> **extensão da proteção à privacidade do indivíduo**. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, **permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima**. Em seus dizeres, "a invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida" (g.n).

A relatora embasou a decisão também no direito à autodeterminação informativa e, conforme ressalta Sarlet, demonstra que política de monitoramento estabelecida na referida medida provisória seria inconsistente com as exigências da proporcionalidade e razoabilidade:

> [...] no julgamento, pelo Plenário do STF, em 07.05.2020, que confirmou o deferimento, em sede de decisão monocrática proferida em 17.04.20, pela relatora da ADIn 6387, Ministra Rosa Weber, de medida liminar suspendendo a eficácia da Medida Provisória nº 954, que determinava às empresas de telefonia a fornecer ao IBGE os nomes, endereços e telefones de mais de cem milhões de brasileiros, mediante o argumento de que tal medida representaria uma restrição constitucionalmente ilegítima dos direitos à privacidade, intimidade e sigilo dos dados pessoais, porquanto inconsistente com as exigências da proporcionalidade e razoabilidade . De acordo com a decisão, o direito fundamental à proteção de dados pessoais representa direito autônomo e com âmbito de proteção distinto ao do direito à privacidade[25].

Conectando a análise desse caso específico ao que se demonstrou sobre a realidade de proteção de dados na América Latina, resta clara a tese de que os países que tem estrutura jurídicas mais frágeis ficam mais expostos a violações de proteção de dados, criando Ciberculturas e até mesmo democracias mais frágeis (UELZE; BARRETO JÚNIOR, 2020). De fato, o COVID-19 impacta questões como exposição dos dados do infectado, do direito ao esquecimento, do mau uso dos dados públicos etc. E a fragilidade institucional na proteção de dados contribui para gerar confusão e exposição

[25] SARLET, Ingo Wolfgang. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais (manuscrito ainda não publicado), p. 9.

desproporcional de informações pessoais. E essa não é apenas uma realidade brasileira: a) na China estão sendo utilizados drones com "tecnologia de reconhecimento facial, scanners infravermelhos, além da implementação de aplicativo para classificar as pessoas de acordo com o risco do contágio, sendo essa informação transmitida às autoridades competentes" (REQUIÃO, 2020, p.201); b) na Coreia do Sul são rastreados celulares dos usuários para "criar mapa que fica disponível publicamente para que todos os cidadãos possam consultar por onde passaram as pessoas infectadas" (REQUIÃO, 2020, p.202) e c) medidas de monitoramento como essas "já foram adotadas também no Irã, Israel, Taiwan, Áustria, Polônia, Bélgica, Alemanha e Itália" (REQUIÃO, 2020, p.202).

Na prática, o que se está vendo é que a situação de pandemia tem reforçado a necessidade de consolidação global de um "constitucionalismo digital" (SAMPAIO, 2020, p. 162-176), que seja construído sobre a base de direitos fundamentais digitais, que vão definir as bases normativas da limitação material da ação do Estado e das empresas sobre os dados pessoais. Além disso, mister que se consolidem também direitos de privacidade na internet, bem como haja política públicas de acesso e educação digital. Somente assim será possível se proteger uma cidadania integral e digital dos cidadãos.

5 CONCLUSÃO

Ficou claro na exposição do presente artigo que os países que têm estruturas jurídicas mais frágeis ficam mais expostos a violações de proteção de dados. De fato, o COVID-19 impacta questões como exposição dos dados do infectado, do direito ao esquecimento, do mau uso dos dados públicos etc. E a fragilidade institucional na proteção de dados acaba por facilitar a exposição desproporcional de informações pessoais. Portanto, a situação de emergência social oriunda da pandemia do COVID-19 torna evidente a necessidade de consolidação

de um "constitucionalismo digital" na América Latina. Como o presente estudo mostrou, esse processo está em curso, porém não é uniforme, o que gera dúvidas sobre a capacidade de os países da América Latina de protegerem os dados pessoais de seus cidadãos de maneira efetiva, especialmente neste momento de emergência social decorrente do COVID-19.

Assim, podemos concluir que o subcontinente possui uma estrutura jurídica suficiente para proteger – em maior ou menor grau – as informações pessoais dos cidadãos mesmo diante do quadro de excepcionalidade decorrente da pandemia global, porém, cabendo ajustes em todas as legislações nacionais, recomendando-se a aproximação das legislações na região.

Data de Submissão: 16/08/2020
Data de Aprovação: 28/08/2020
Processo de Avaliação: *double blind peer review*
Editor Geral: Jailton Macena de Araújo
Editor de Área: Jailton Macena de Araújo
Assistente Editorial: Jaqueline Rosario Santana

REFERÊNCIAS

BABINET, G. **L'ère numérique, un nouvel âge de l'humanité. Cinq mutations qui vont bouleverser notre vie.** Paris: Le Passeur, 2014.

BASDENVAND, A.; MIGNARD, J-P. **L'empire des données, essai sur la société, les algorithmes et la loi**. Paris: Don Quichotte, 2018.

BIONI, Bruno. **Proteção de Dados Pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2020. p. 90 e ss.

CARLSSON, B. **The Digital economy: what is new and what is not?** Structural Change and Economic Dynamics, vol. 15, issue 3, set. 2004, p. 245-264.

CAVALLO, E.; POWELL, A. **Informe macroeconómico de América latina y el Caribe**, La hora del crecimiento. Washington: Banco Interamericano de Desarrollo, 2018.

DE FILIPPI, P. **Gouvernance algorithmique**: Vie privée et autonomie individuelle à l'ère des Big Data. Paris: Mare & Martin, 2016.

DONEDA, Danilo. **Da Privacidade à Proteção dos Dados Pessoais**. Fundamentos da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

ENISA. European Network and Information Security Agency. **The right to be forgotten, between expectations and practice.** 2012.

FLORIMOND, G. **Droit et Internet**, De la logique internationaliste à la logique realiste. Paris: Mare & Martin, 2016.

GHEVONTIAN, R.; FAVOREU, L.; GAÏA, P. **Droit des libertés fondamentales**. 6. ed. Paris: Dalloz, 2015.

HARARI, Y. N. **Homo Deus**: A Brief History of Tomorrow. London: Harvill Secker, 2016.

INTERNET WORLD STATS. **World Internet Users Statistic and 2020 World Population Stats**. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: 11.jun.20.

ISAAC, H. La donnée numérique, bien public ou instrument de profit. **Revue Pouvoirs**, n° 164, ed. Seuil, France, p. 75-86, 2018.

ITXASO, M. E. El concepto jurisprudencial de acomodamiento razonable. El Tribunal Supremo de Canadá y el Tribunal Europeo de Derechos Humanos ante la gestión de la diversidad cultural y religiosa en el espacio público. **Anuario de Filosofia del Derecho**, vol. XXX, 2014, p. 69-96.

KOOPS, B.-J. Forgetting Footprints, Shunning Shadows: A Critical Analysis of the Right to be forgottenn in Big Data practice. **SCRIPTed**, vol. 18, nº 3, p. 229-256, 2011.

MITNICK, K.; SIMON, W. L. **The Art of Deception, Controlling the Human Element of Security.** New Jersey: John Wiley & Sons, 2003.

MPF. Ministério Público Federal. **Nota Técnica Conjunta**. PFDC & Câmara Criminal.
Disponível em:
http://www.mpf.mp.br/pgr/documentos/PRSP00039100.2020.pdf. Acesso em: 01 jul. 2020.

OBOLER, A.; WELSH, K.; CRUZ, L. The danger of big data: Social media as computational social science. **First Monday**, vol 17, n. 2, jul. 2012. Disponível em:
http://firstmonday.org/ojs/index.php/fm/article/view/3993/3269. Acesso em: 11 jun. 2020.

PATIÑO, J. A.; POVEDA, L. **Monitoreo de la Agenda Digital para América Latina y el Caribe eLAC2018**. Santiago: CEPAL, 2018.

PÉREZ ROYO, F. J. Derecho a la información. **Revista Boletín de la ANABAD**. Tomo 49, Nº 3-4, 1999, p. 19-34, p. 22.

REQUIÃO, Maurício. COVID-19 e Proteção de Dados Pessoais: o antes, o agora e o depois. In: Bahia, Saulo José Casali. **Direitos e Deveres Fundamentais em Tempos de Coronavírus.** vol. 1. São Paulo: IASP, 2020. p. 200-208.

ROSE, J.; REHSE, O; RÖBER, Björn. **The Value of Our Digital Identity**. 2012 Disponível em: https://www.bcg.com/pt-br/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity. Acesso em: 11 jun.2020.

SARLET, Ingo Wolfgang; NETO, Arthur Ferreira M. **O "Direito ao Esquecimento" na Sociedade da Informação.** Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. **Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais** (manuscrito ainda não publicado).

SAMPAIO, Marcos. O Constitucionalismo Digital e a COVID-19. In: Bahia, Saulo José Casali. **Direitos e Deveres Fundamentais em Tempos de Coronavírus**. vol. I. São Paulo: IASP, 2020. p. 162-176.

THOMPSON, D. I agreed to what? A call for enforcement of Clarity in the Presentation of Privacy Policies. **UC Hastings Communications and Entertainment Law Journal**, vol. 35, nº 1, 2013, p. 199-223.

UELZE, Hugo Barroso; BARRETO JÚNIOR, Irineu Francisco. Cibercultura e o Poder Informacional na Esfera Pública: Crise do Paradigma Positivista no Direito Tributário. **Prim@ Facie**, v. 19, n. 40, 2020, p. 01-29. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/51047. Acesso em: 27. ago. 2020.

VIOLLIER, P. **Derechos Digitales América Latina**, 2017. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf. Acesso em: 11 jun.2020.

WEBER, R. H. The right to be forgotten: more than a Pandora's box? **Journal of intellectual property, information technology and e-commerce law.** nº 2, 2011, p. 120-130.

WOLKMER, A. C.; FAGUNDES, L. M. Tendências contemporâneas do constitucionalismo latino-americano: estado plurinacional e pluralismo jurídico. **Pensar**: Revista de Ciências Jurídicas, v. 16, n. 2, p.371-408, 2012.

Data Protection In Latin America And The Challenges Of Covid-19

Giovani Saavedra

Daniel Nagao Menezes

Abstract: The article deals with a relevant topic for its historical moment, which is the need for the use of personal data by public authorities in the fight against the global pandemic of COVID-19. This need for access to the most diverse information in the face of the global pandemic causes several ethical, political and legal conflicts. Based on this problem, the text seeks to analyze the legal structure of Latin American countries regarding data protection and access and as this relates to the need for access by health authorities. It concludes that they have more advanced legal and institutional data protection structures have conditions for sharing information without undue exposure of citizen information. The hypothetical deductive method was used, using the literature review as a methodological procedure.

Keywords: Access to information; COVID-19; Data Protection; Sanitary Crisis.

DOI: https://doi.org/10.22478/ufpb.1678-2593.2020v19n42.54590