Proteção de Dados e o Acordo de Livre Comércio Mercosul-União Europeia: Notas sobre a Adequação da Autoridade Nacional de Proteção de Dados no Brasil

Data Protection and the Mercosur-European Union Free Trade Agreement: Notes on the Adequacy of the National Data Protection Authority in Brazil

REGINA LINDEN RUARO[1]
Pontifícia Universidade Católica do Rio Grande do Sul (PUC – RS). Porto Alegre (RS). Brasil.

CECÍLIA ALBERTON COUTINHO SILVA[2]
Pontifícia Universidade Católica do Rio Grande do Sul (PUC – RS). Porto Alegre (RS). Brasil.

RESUMO: O avanço das novas tecnologias, impulsionado pelos influxos disruptivos da Revolução 4.0, proporcionou a criação e o aperfeiçoamento das legislações de proteção de dados pessoais ao redor do mundo. Neste contexto, as autoridades de proteção de dados passaram a assumir papel de grande relevância para orquestrar as trocas comerciais internacionais e o fluxo transnacional de dados. Dito isso, o trabalho busca responder à seguinte hipótese: De que forma as legislações na União Europeia ("UE") e na América Latina vêm regulamentando a proteção de dados pessoais, especialmente no que toca à independência e à autonomia das autoridades de proteção de dados? O objetivo geral da pesquisa consiste em evidenciar tal contexto internacional na matéria de proteção de dados pessoais na UE e na América Latina. Partindo do cenário delimitado, os objetivos específicos são (i) identificar as principais características das legislações de proteção de dados, notadamente do Regulamento Europeu de Proteção de Dados ("RGPD") e das leis locais de proteção de dados na América Latina; (ii) verificar a forma com a qual as autoridades de proteção de dados foram estruturadas nesses locais; e (iii) a partir da apresentação do Acordo de Livre Comércio entre a União Europeia e o Mercosul, analisar o caso da Autoridade Nacional de Proteção de Dados brasileira ("ANPD"). Ao final, conclui-se-á no sentido de que as presentes e futuras relações comerciais, especialmente aquelas que impliquem transferência internacional de dados, dependerão do cumprimento de parâmetros de proteção de dados. A pesquisa foi realizada a partir do método de abordagem hipotético-dedutivo, com procedimento comparativo e histórico e interpretação sistemática. A natureza da pesquisa foi teórica, o objetivo foi exploratório e explicativo e, quanto ao objeto, a pesquisa foi bibliográfica.

PALAVRAS-CHAVE: Proteção de dados; União Europeia; América Latina; autoridades de proteção de dados; Acordo de Livre Comércio.

1 Orcid: <https://orcid.org/0000-0003-1144-9383>.
2 Orcid: <https://orcid.org/0000-0001-8357-3557>.

ABSTRACT: The rise of new technologies, driven by the disruptive inflows of Revolution 4.0, led to the creation and improvement of personal data protection laws around the world. In this context, the national data protection authorities started to play a very important role in orchestrating international trade and the transnational flow of data. That said, the paper seeks to answer the following hypothesis: How the legislation in the European Union ("EU") and in Latin America have been regulating the protection of personal data, especially with regard to the independence and autonomy of the data protection authorities? The general objective of the research is to highlight this international context in the field of personal data protection in the EU and Latin America. Within this scenario, the specific objectives are to (i) identify the main characteristics of data protection legislation, notably, the General Data Protection Regulation ("GDPR") and local data protection laws in Latin America; (ii) verify the way in which data protection authorities were structured in those places; and (iii) after the presentation of the Free Trade Agreement signed between the European Union and Mercosur, analyze the case of the Brazilian National Data Protection Authority ("ANPD"). Lastly, the research concludes in the sense that present and future commercial relations, especially those involving the international transfer of data, will depend on compliance with data protection standards. The research was carried out thorough a hypothetical-deductive approach method, with comparative and historical procedure and systematic interpretation. The nature of the research was theoretical, the objective was exploratory and explanatory and, as for the object, the research was bibliographical.

KEYWORDS: Data protection; European Union; Latin America; data protection authorities; Free Trade Agreement.

INTRODUÇÃO

As formas de coleta e tratamento de informações provocaram a necessidade de rediscutir-se o contexto da privacidade e, com isso, novas estratégias para regulamentar a matéria, especialmente a proteção de dados pessoais. Nesse estado das coisas, atualmente, tomou importância, ademais da privacidade em si, tratar-se da proteção de dados pessoais e outros direitos de personalidade, porque a utilização dos instrumentos já existentes não é suficiente para promover suas condições mais básicas, motivo pelo qual é necessária a criação de novas categorias para a proteção da esfera privada do indivíduo e, da mesma forma, da esfera pública do indivíduo, a dos dados pessoais. A proteção de dados pessoais tornou-se um direito fundamental autônomo.

A discussão atinente à proteção da esfera privada, como se sabe, vem de longa data, a exemplo do julgado *Boyd v. United States*, caso em que a

Suprema Corte norte-americana considerou inconstitucional a exposição de documentos fiscais, com base na Quarta Emenda (Ruaro; Rodrigues; Finger, 2011). Hoje, sob outro viés, as novas tecnologias de inteligência artificial[3] e *big data* deram outro tom à necessidade de preservar a privacidade, desafiando os limites anteriormente traçados.

Nesse sentido, a referida evolução tecnológica, cada vez mais rápida, conjuntamente com a integração econômica e social, fenômenos identificáveis tanto na UE quanto no Mercosul, criaram novos desafios em matéria de proteção de dados, inclusive pelo aumento do intercâmbio de informações entre entes públicos e privados. Assim, percebe-se que a proteção de dados pessoais, hoje, está diretamente ligada ao comércio e à troca de bens e serviços, motivo pelo qual é imperativo que a legislação promova segurança e previsibilidade[4] (UNCTAD, 2016).

Por conta disso, as informações pessoais[5] são cada vez mais públicas em nível global, o que exige uma posição afirmativa das autoridades competentes, externalizadas por meio de normas: na União Europeia, com o Regulamento nº 2016/679 do Parlamento Europeu ("RGPD"), que revogou a Diretiva nº 95/46/CE; e no Mercosul, com os regulamentos internos de cada integrante, com destaque para os *Estándares de Protección de Datos Personales* da *Red Iberoamericana de Protección de Datos*; e, no Brasil, a Lei nº 13.709/2018 ("LGPD").

Na América Latina, diversos países já possuem legislações de proteção de dados, nos quais há especial interesse na proteção dos direitos do titular e sobre o armazenamento e a transferência de informações; contudo, nem todos preveem a criação de uma autoridade nacional de proteção, como se verá adiante, o que dificulta a proteção de dados no contexto da sociedade de vigilância (Rodotá, 2008).

---

3 Nesse aspecto, Klaus Schwab refere que a inteligência artificial é uma nova forma de produção, que revoluciona as relações de trabalho, associando tarefas de reconhecimento de padrões e processamento de informações complexas (2016, p. 50).

4 *Data protection is directly related to trade in goods and services in digital economy. Insufficient protection can create market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the internet*.

5 Danilo Doneda entende que há uma utilização, por vezes equivocada, ao utilizar-se informação pessoal como dado pessoal, é nesse sentido que acompanhamos o autor (2019, p. 135-136).

Assim, o presente estudo questiona de que forma as legislações vêm regulamentando a proteção de dados pessoais na UE e América Latina[6], especialmente no que toca à independência e à autonomia das autoridades de proteção de dados. Isso porque as estratégias regulatórias constituem verdadeira defesa do indivíduo que passará a ter controle significativo sobre seus dados, restringindo os interesses econômicos e preservando a dignidade da pessoa humana, anteriormente reduzidos às fronteiras tradicionais da privacidade, da dicotomia "recolhimento" e "exposição".

Para fins de responder ao problema apontado, o objetivo geral da pesquisa consiste em evidenciar o contexto internacional na matéria de proteção de dados pessoais na UE e na América Latina. Partindo desse cenário delimitado, os objetivos específicos são (i) identificar as principais características das legislações de proteção de dados, notadamente do Regulamento Europeu de Proteção de Dados ("RGPD") e das leis locais de proteção de dados na América Latina; (ii) verificar a forma com a qual as autoridades de proteção de dados foram estruturadas nesses locais; e, (iii) a partir da apresentação do Acordo de Livre Comércio assinado entre a União Europeia e o Mercosul, analisar o caso da Autoridade Nacional de Proteção de Dados brasileira ("ANPD"), no esforço de entender se a forma com a qual a ANPD foi criada poderia criar um entrave às futuras trocas comerciais potencializadas pelo Acordo de Livre Comércio.

Nessa linha, a pesquisa partiu do método de abordagem hipotético-dedutivo, com procedimento comparativo e histórico e interpretação sistemática. A natureza da pesquisa foi teórica, o objetivo foi exploratório e explicativo e, quanto ao objeto, a pesquisa foi bibliográfica. Por fim, a presente pesquisa se insere no Grupo de Pesquisa cadastrado no CNPq, "Proteção de Dados no Estado Democrático de Direito", do Programa de Pós-Graduação em Direito da PUCRS, na linha de pesquisa "Direito, Tecnologia e Inovação".

Dito isso, passar-se-á à análise das recentes legislações na matéria de proteção de dados, no Brasil, na América Latina e na União Europeia, iniciando-se pelo RGPD, e das autoridades de proteção de dados no Bloco Europeu, partindo-se da premissa de que a proteção de dados pessoais, atu-

6 No âmbito da América Latina, serão analisados os casos dos seguintes países: Argentina, Colômbia, Chile, Brasil e Uruguai.

almente, integra o rol dos direitos fundamentais do cidadão, como decorrência do princípio da dignidade humana.

1 O REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS E AS AUTORIDADES DE PROTEÇÃO DE DADOS

O Regulamento Europeu de Proteção de Dados consolida o posicionamento de vanguarda do Continente no sentido de conferir especial proteção à esfera dos dados pessoais de seus membros. Quer dizer, desde as primeiras normatizações, sabidamente do movimento contra a Lei do Estado de Hesse, na Alemanha, até o atual Regulamento nº 2016/679, a União Europeia vem ditando os padrões a serem seguidos nessa matéria.

Por conta disso, e tendo em vista as parcerias comerciais havidas entre a União Europeia, o Mercosul e, em última análise, com o Brasil, o nível conferido à proteção de dados passou a ser elemento relevante de observação nas tratativas de novos acordos econômicos, sem prejuízo da revisão daqueles já firmados. Aqui é indispensável referir que as novas tecnologias aceleraram em grande medida o processo de trocas comerciais, de forma que, mais do que nunca, os países devem se posicionar de forma afirmativa, para a regulamentação e para a proteção nacional (e internacional) de dados.

É que, apesar do caráter transnacional da Internet e da crescente economia global, os direitos aos dados e os regulamentos de proteção de dados são ainda muito fragmentados (Schwab, 2016, p. 50), apesar do potencial impacto positivo da tecnologia no crescimento econômico (Fincato; Silva, 2020, p. 26). Daí decorre a relevância da atuação das Autoridades Nacionais de Proteção de Dados (ou *Data Protection Authorities*, "DPA"), entidades que buscam garantir o direito de todos à privacidade e proteção de seus dados.

Assim, desde já, pode-se inferir que há uma clara tendência, resultante de uma "força expansiva" da proteção de dados pessoais, de que a privacidade seja mais do que uma mera característica congênita dos chamados "novos direitos"; verifica-se uma verdadeira mutação do ambiente no qual circulam os dados e nos quais se manifestam os interesses ligados à privacidade (Doneda, 2006, p. 15).

Dito isso, antes de adentrar à realidade brasileira e aos reflexos do Acordo de Livre Comércio assinado entre a União Europeia e o Mercosul,

cumpre analisar (*i*) as características gerais do Regulamento Europeu de Proteção de Dados e (*ii*) de que forma as Autoridades Nacionais de Proteção de Dados são estruturadas e atuam no Bloco.

1.1 O Regulamento Europeu de Proteção de Dados

O Regulamento Geral de Proteção de Dados ("RGPD") foi aprovado em 15 de abril de 2016 e implementado em 25 de maio de 2018 pelo Parlamento Europeu. Possui 99 artigos e um longo preâmbulo "Considerandos", o qual estabelece toda a principiologia fundamental para a aplicação da matéria de proteção de dados.

A nova normatização surgiu para regulamentar o tratamento de dados pessoais de todos os indivíduos da União Europeia e do Espaço Econômico Europeu ("EEE"), bem como a exportação de dados pessoais para fora da UE e do EEE – a chamada transferência internacional de dados. Com isso, o RGPD proporcionou novas formas para que os cidadãos controlem seus dados, bem como unificou as normativas até então existentes, revogando a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE).

O RGPD consolida o entendimento de que, na União Europeia, o direito à proteção de dados foi uma construção jurisprudencial, a exemplo da experiência alemã. Então, atualmente, o direito à proteção de dados está alçado à categoria de direito fundamental[7] no direito comunitário europeu, estando localizado ao lado do direito à privacidade (Zanon, 2013, p. 81-82), considerando, sempre, a aplicação no caso concreto.

Tal fato se deve, em grande medida, à natureza legislativa do regulamento, que, ao contrário da diretiva, é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países do Bloco (Döhmann, 2020, p. 14). Trata-se de uma uniformização que, uma vez aprovada, será imposta a todos e a todas, indiscriminadamente, desde que membros do Bloco. Para Schütze (2017, p. 89-90), o regulamento deve ter aplicação geral, vinculante na sua integralidade e diretamente aplicável, portanto, a

7 Assim, na linha do que já definia a Diretiva nº 45/96, o Regulamento nº 2016/679 da União Europeia trata da proteção de dados pessoais de forma mais específica e mais rigorosa. Refere, inclusive, da proteção de dados genéticos e culturais, conforme art. 4 (1) do GDPR: "*'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, phycological, genetic, mental, economic, cultural or social identity of that natural person*".

todos os membros do Bloco, nos termos do art. 288 do *Treaty on the Functioning of the European Union*[8].

Já a diretiva[9], a título ilustrativo, a exemplo do que era a Diretiva nº 95/46, que anteriormente tratava da proteção de dados na União Europeia, é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo. Assim define Lima Filho (2006, p. 103-104) sobre a natureza dos regulamentos:

> Os Regulamentos constituem atos unilaterais dotados das seguintes características: o caráter geral, a aplicabilidade direta e a obrigatoriedade em todos os seus elementos. Vale dizer: todas as pessoas – singulares ou coletivas, empresas Estados, etc. – que se encontrem no seu âmbito de aplicação – objetivo, subjetivo, temporal e espacial – estão por ele vinculadas, o que faz com que seja obrigatório em todos os seus elementos tendo, portanto, aplicabilidade direta, ou seja, prescinde de qualquer mecanismo de recepção no ordenamento jurídico dos Estados membros incorporando-se automaticamente nesse ordenamento.

Neste contexto, no âmbito na União Europeia, há, em verdade, um sistema de governança em múltiplos níveis e, por isso, a legislação, cada vez mais, vem sendo desenvolvida para ter caráter regulatório, e não redistributivo (Schütz, 2012, p. 87-90). Ou seja, os parâmetros estabelecidos pelo RGPD não comportam relativização de seus termos, justamente para favorecer um ambiente seguro de negociações comerciais[10].

Merece destaque o fato de que os europeus, quando criaram o sistema detalhado de proteção de dados que hoje é o RGPD, estabeleceram uma

---

8 E acrescenta: "*This definition demands four things. First, regulations must be generally applicable. Secondly, they must be entirely binding. Thirdly, they must be directly applicable, and that – fourthly – in all Member States*" (Schütze, 2017, p. 89-90).

9 Diretivas são instrumentos normativos típicos do direito comunitário europeu, recomendações e pareceres. As fontes primárias são os tratados que compõe a União Europeia. Por intermédio de diretivas, a EU busca obter a uniformidade legislativa de seus Países-membros. Uma vez aprovada uma diretiva, cabe a cada um dos Países-membros, dentro de certo espaço de tempo, editar ou adaptar leis internas para que seus respectivos ordenamentos nacionais estejam nos moldes estabelecidos na diretiva. Esse fenômeno é designado de transposição. A força da diretiva deriva do fato de que, excedido o prazo para sua transposição, passa ela própria a ter certa eficácia direta internamente ao país desidioso, ao acréscimo de que este é levado a responder pela mora perante a Corte Europeia de Justiça.

10 Nesse particular, refere Schütze: "*Many provisions are liable to have direct effects and can be enforced by the courts. Other provisions, although they have become part of the domestic legal order as a result of the regulation's direct applicability, are binding for the national authorities only, without granting private persons the right to complain in the courts that the authorities have failed to fulfil these binding obligations*" (2017, p. 91).

regra que passou a ser caracterizada como aplicação extraterritorial da lei; em outras palavras, conforme sustenta Maldonado, empresas em qualquer lugar do mundo, que vierem a oferecer bens para aqueles que estiverem na União Europeia, devem obedecer ao regulamento europeu (Maldonado; Blum, 2019, p. 226) – as normas incidem sobre toda atividade de "tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados", nos termos do art. 2º do RGPD.

Então, hoje, os processos empresariais que tratem dados pessoais, em outras palavras, que manipulem informações dessa natureza, são obrigados a ser desenhados de raiz e por padrão com medidas que respeitem os princípios da proteção de dados por defeito[11] (*privacy by default*) e da proteção de dados desde a concepção[12]. Quer dizer, os dados devem ser armazenados por meio do uso de pseudoanonimização[13] ou anonimização completa[14], com as mais elevadas configurações de privacidade por padrão. O regulamento ainda veda o tratamento de quaisquer dados fora do contexto legal especificado no regulamento, salvo no caso em que quem controle os dados tenha recebido consentimento explícito e *opt-in*[15] do proprietário dos dados. Rije-se que, a qualquer momento, o proprietário ainda tem o direito de revogar essa permissão de uso.

Dito isso, nos termos do art. 3(1), o Regulamento é aplicável ao tratamento de informações pessoais realizado "no contexto das atividades de um estabelecimento" de responsável pelo tratamento ou por operador situado no território europeu, ainda que o tratamento ocorra fora dos limites territoriais da União Europeia[16]. Nesse aspecto, merece destaque o caso *Weltimmo*, no qual a Corte Europeia esclareceu que o conceito de *estabelecimento*

11 A proteção de dados por defeito implica que a sua empresa adote sempre, como definições por defeito, as definições que mais protejam a privacidade. Por exemplo, se forem possíveis duas definições para a proteção da privacidade e uma delas impedir o acesso aos dados pessoais por parte de terceiros, deverá ser essa a definição por defeito.

12 Em outras palavras, as empresas/organizações são incentivadas a aplicar medidas técnicas e organizativas, nas fases iniciais da concepção das operações de tratamento, de forma a garantir os princípios da privacidade e proteção de dados logo desde o início.

13 Pseudoanonimizar é tornar um determinado dado pessoal em um dado que não permita identificar de forma directa o seu titular, mas que o possa tornar identificável, por exemplo, o sistema de controle biométrico.

14 Anonimizar é dissociar definitivamente o dado de seu titular.

15 *Opt-in* é a modalidade de obtenção de conhecimento explícito obtido por meio de caixas de seleção (*checkbox*). Para fins de validade, essas caixas não podem estar previamente assinaladas pelo usuário.

16 Art. 3(1) do GDPR: "O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União".

se "estende a toda atividade real e efetiva – ainda que mínima – exercida mediante uma instalação estável". Construiu-se aí uma concepção flexível – não formalista – do conceito, válida "especialmente para as empresas que se dedicam a oferecer serviços exclusivamente pela Internet". Veja-se o teor do acórdão (European Court of Justice, 2015, p. 7):

> 29. [...] Assim, para determinar se uma sociedade, responsável por um tratamento de dados, dispõe de um estabelecimento, na acepção da Diretiva 95/46, num Estado-membro diferente do Estado-membro ou do país terceiro em que está registada, *há que avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades nesse outro Estado-membro, tendo em conta a natureza específica das atividades económicas e das prestações de serviços em causa*. Este entendimento vale especialmente para as empresas que se dedicam a oferecer serviços exclusivamente na Internet.

Inclusive, nos termos do Regulamento, o local onde se dá o tratamento de dado pessoal é irrelevante se o estabelecimento do responsável é situado na União Europeia. A nova normativa tem evidente pertinência em vista dos avanços da Internet. Alcança, por exemplo, empresas e entidades responsáveis pelo tratamento de dados que utilizam computação em nuvem (*cloud computing*), isto é, se valem de "arranjos pelos quais recursos computacionais são fornecidos de modo flexível e independentemente da localização, que permitem uma rápida e ininterrupta alocação de recursos sob demanda"[17] (Millard; Fosch-Villaronga, 2019, p. 78), nas diferentes modalidades de serviço que podem ser adotadas.

Ainda, a despeito dos elementos de extraterritorialidade do RGPD e efeitos que a normativa europeia pode produzir no sistema jurídico brasileiro ou possíveis conflitos de lei, há ainda a necessidade de se observar as possíveis repercussões em relação à transferência internacional de dados pessoais, disciplinada normativamente nos arts. 44 a 50 do Regulamento Europeu.

Em termos analíticos, uma transmissão transfronteiriça de dados pessoais[18] envolve pelo menos três operações de tratamento: (*i*) a que tornou

17 "[...] *Cloud computing involves the use of computing resources over a network, typically the Internet, scalable according to demand. In addition to the well-established Infrastructure, Platform, and Software as a Service (IaaS, PaaS, and SaaS) service models, cloud providers also provide specialist cloud services such as Machine Learning as a Service (MLaaS) and Blockchain as a Service (BaaS)*" (Fosch-Villaronga; Millard, 2019, p. 78)

18 A respeito do tema, vide trabalho publicado pelo IRIS com comentários ao Projeto de Lei nº 5.276/2016 da Câmara dos Deputados (Cf. Instituto de Referência em Internet e Sociedade, 2017).

disponível as informações pessoais ao agente responsável ou operador (cedente) – *i.e.*, recolhimento ou coleta dos dados; (*ii*) a transmissão dessas informações a receptor sediado ou residente em Estado estrangeiro pelo cedente; e (*iii*) o tratamento que o receptor dos dados pessoais realiza em seu estabelecimento situado em país terceiro (*i.e.*, armazenamento em base de dados) (Giménez, 2015, p. 214).

Em essência, a regra é ancorada em modelo geográfico de regulamentação do fluxo de dados entre fronteiras nacionais, porquanto "objetiva proteger contra riscos gerados pelo país ou localidade para qual os dados serão transferidos"[19] (Kuner, 2011, p. 20). A Comissão Europeia tem a atribuição de analisar o nível de proteção do país terceiro e emitir uma decisão de adequação com base nos critérios apontados no art. 45(2) do Regulamento; com isso, havendo tal decisão – sujeita a revisão quadrienal –, não se demandará prévia e específica autorização para a transmissão internacional de dados.

Por esses motivos, desde já, evidencia-se a relevância da análise da forma com a qual a legislação brasileira, para fins de conformidade com o RGPD e com o disposto na própria Lei Geral de Proteção de Dados, após as alterações promovidas pela Lei nº 13.853/2019, criou a Autoridade Nacional de Proteção de Dados e questionar se, da forma como está sendo implementada, haverá afetação da efetividade do Acordo de Livre Comércio entre o Mercosul e a União Europeia. Contudo, antes, necessário tecer alguns esclarecimentos com relação ao funcionamento das Autoridades de Proteção de Dados na Europa, sob a égide do RGPD.

1.2 Autoridade de proteção de dados na União Europeia

A Autoridade de Controle – ou *Supervisory Authority* – é um ente autônomo do sistema político nacional de cada País-membro do Bloco Europeu, que busca regulamentar e dar efeito aos termos estabelecidos no Regulamento Geral de Proteção de Dados[20]. Destaque-se que tal Autoridade já havia sido criada pela Diretiva nº 46/95/EC, bem como prevista por alguns

19 Tradução livre de: "*Aims to protect against risks posed by the country or location to which the data are to be transferred [...]*" (Kuner, 2011, p. 20).

20 "*Art. 51. Supervisory authority. (1) Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*"

países (levando em consideração que até 2016 a legislação sobre a matéria de proteção de dados era facultativa entre os países do Bloco)[21].

Nos termos do art. 51 do RGPD, cabe aos Estados-membros da União Europeia designar uma ou mais autoridades públicas independentes, ou *Data Protection Authority* ("DPA"), para a fiscalização e aplicação do RGPD. A norma ressalta o papel das autoridades na defesa dos direitos e das liberdades fundamentais das pessoas singulares, relativamente ao tratamento de dados, além de atuar na livre circulação desses dados na União. Ressalta, também, a necessidade de cooperação entre as DPAs para a melhor aplicação do RGPD em todos os Estados-membros (Maldonado; Blum, 2019, p. 227).

Dito isso, Philip Schütz entende que as características da Autoridade de Controle, para serem melhor analisadas, devem ser vistas à luz das *Independent Regulatory Agencies* ("IRA"), as quais podem ser definidas da seguinte forma (Schütz, 2012, p. 5-6):

> *IRAs can be defined as "a body with its own powers and responsibilities given under public law, which is organizationally separated from ministries and is neither directly elected nor managed by elected officials. As the name already suggests, independence from governmental influence plays an essential role in the conception of IRAs.*[22]

Quer dizer, essencialmente, esse tipo de "agência" (por falta de melhor termo para se utilizar em matéria administrativa)[23] deve, para o fiel cumprimento das suas obrigações legais, ser completamente independente de Poderes Públicos – Executivo, Legislativo e Judiciário, na pessoa de seus representantes – e privados, haja vista que tem como função precípua a fiscalização do tratamento de dados por eles realizados.

---

21 É por esse motivo que se justificará a apresentação de alguns julgados do Tribunal Constitucional Europeu anteriores ao GDPR, principalmente no que se refere a (ir)regularidade na atuação de algumas ANPDs.

22 Ou seja, questiona-se se uma Autoridade Nacional de Proteção de Dados, vinculada à Presidência da República, conforme determina o art. 55-A da LGPD cumpre com os níveis de proteção de dados exigidos pelo GDPR, para fins de cumprimento do Acordo de Livre Comércio entre o Mercosul e a União Europeia.

23 A discussão sobre a natureza jurídica da ANPD é extensa, principalmente no Brasil, aonde a Legislação de Proteção de Dados é extremamente recente. Refere-se ao termo "agência", tendo em vista a ausência de estrutura administrativa própria que atenda aos requisitos da Autoridade Nacional de Proteção de Dados dentro do direito administrativo brasileiro. O Centro de Estudos da Fundação Getúlio Vargas do Rio de Janeiro refere que a estrutura mais próxima daquela exigida seria a de uma autarquia, cuja criação se justificaria em função de sua (i) natureza jurídica de direito público; (ii) independência e autonomia; e (iii) possibilidade de exercer poderes de polícia (Moncau; Maciel; Venturini; Luca; Louzada; Foditsch; Mizukami, 2015, p. 45).

Na mesma linha de raciocínio, a DPA deve seguir os mesmos rigores da IRA, conforme define o mesmo autor (Schütz, 2012, p. 2): "*Data protection authorities (DPAs) operate as one of the key actors in the field of privacy regulation, safeguarding civil liberties and consumer rights by monitoring and enforcing the compliance with data protection policies*".

Das definições apresentadas, pode-se extrair que a característica central que a Autoridade de Controle deve apresentar é a de independência no exercício de suas funções. Nesse sentido, Gilardi (2002, p. 880) desenvolveu um índice para apreender a independência formal de IRA, compreendendo quatro indicadores, conforme a seguir: "*The agency's head status, the management board members' status, the general frame of the relationships with the government and the parliament, financial and organizational autonomy, and the extent of delegated regulatory competencies*".

Tendo isso como base, o autor se utiliza de um método quantitativo de aferição da independência da autoridade, buscando medir a independência formal de agentes governamentais. Há outros autores, como Thatcher (2002, p. 956), que, partindo também de uma análise quantitativa, expande sua análise para incluir fontes de influência como política e "*revolving doors*".

Por esses motivos, cabe aos Estados-membros assegurarem às DPAs recursos humanos, físicos, técnicos e financeiros, além de outros que se façam necessários à boa condução dos casos pela autoridade. Um ponto importante a ser salientado é a observação de que caberá aos Estados-membros assegurarem que o orçamento não seja um fator prejudicial à independência das DPAs, ponto que a experiência internacional comprova como relevante em outras autoridades de natureza similar (*i.e.*, autoridades de defesa da concorrência) (Maldonado; Blum, 2019, p. 232).

No que toca ao âmbito empresarial, também objeto desse trabalho, para fins de efetividade do Acordo de Livre Comércio assinado entre representantes da EU e do Mercosul, merece destaque o fato de que o *Data Protection Officer* ("DPO") não se restringe à agência[24] pública de abrangência nacional, porque o RGPD prevê, também, que empresas que tratem

24 Ibidem.

dados, especialmente em grande escala, nomeiem um DPO, conforme os arts. 37[25] e 38[26] do RGPD.

Neste contexto, as empresas deverão considerar cuidadosamente se elas fazem parte do contexto no qual é exigida a designação de um *Data Protection Officer* ("DPO"), considerando que (*i*) as diretrizes contidas no RGPD deixam claro que todas as empresas devem considerar a nomeação voluntária de um DPO; e (*ii*) se uma empresa optar por não nomear um DPO, as diretrizes recomendam que a empresa mantenha registros dos motivos que motivaram a decisão para poder demonstrar que todos os fatores relevantes foram considerados adequadamente.

As empresas que nomeiam um DPO precisam garantir que ele tenha acesso a todos os recursos e apoio necessários para cumprir a função e garantir a sua independência e autonomia. Isso é particularmente importante quando um DPO único é designado para um grupo de empresas, pois os desafios dessa abordagem são muito maiores. Se uma empresa deixar de cumprir suas obrigações com relação à nomeação e ao suporte de um DPO, poderá sofrer multas no âmbito do RGPD até um máximo de 10 milhões de euros ou 2% do faturamento mundial (Gabel; Hickman, 2017).

Feitos tais esclarecimentos, em março de 2010, a Corte Europeia de Justiça entendeu que a Alemanha falhou em cumprir com as suas obrigações, nos termos do parágrafo segundo do artigo 28 (1) da Diretiva nº 95/46/EC, qual seja, assegurar a completa independência da autoridade de proteção de dados:

> *44 And indeed, the ECJ confirmed that some governments of the German Länder had appointed specific "authorities [to be] responsible for monitoring the processing of personal data by nonpublic bodies and undertakings governed by public law which compete on the market (*öffentlich-rechtliche *Wettbewerbsunternehmen)".* (European Court of Justice, 2010)

25 "*Art. 37. Designation of the data protection officer. (1) The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in art. 10*."

26 "*Art. 38. Position of the data protection officer (1). The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data*."

Em outras palavras, o DPO alemão, ou *Federal Comissioner*, representa não somente a diretoria da autoridade de controle, mas também a autoridade em si. Nesse sentido, refere Schütz (2012, p. 13):

> *Though being civil servants, DPA officials are actually working directly for him/her. While the FfDF's basic number of staff amounts to 90,48 the annual budget, which is a part of the Federal Government Budget and therefore determined by both chambers of the legislature, totals around 8.8 million Euros.*

Ainda, em caso recente decidido em outubro de 2015[27], também pela Corte de Justiça Europeia, determinou-se que a independência da autoridade de proteção de dados húngara foi desrespeitada. Em função de uma reforma no sistema de proteção de dados promovida pelo parlamento, o Supervisor da autoridade foi substituído antes do fim de seu mandato de seis anos. O Tribunal considerou que as autoridades não podem estar sujeitas a nenhum tipo de influência externa, e que a alteração da liderança da autoridade seria uma ofensa à independência da instituição[28].

Portanto, o que se buscou demonstrar até aqui é que a *independência* é elemento central para o bom funcionamento da autoridade de controle da proteção de dados, a qual, por sua vez, é um pilar fundamental da estrutura organizacional criada para evitar o verdadeiro varejo de dados pessoais antes existente. O futuro das relações comerciais, principalmente naquelas em que há grande fluxo de dados pessoais, está no fiel cumprimento das legislações nessa matéria, de forma a promover um ambiente de troca seguro e comprometido com o que hoje é considerado um direito fundamental – a proteção de dados, ao lado da privacidade.

Isso posto, passar-se-á a analisar, em linha com os objetivos desse trabalho, a forma com a qual a proteção de dados se dá na América Latina para, após, vincular este contexto à Lei Geral de Proteção de Dados brasilei-

27 Judgment in Case C-288/12 *Commission v. Hungary*.

28 Nesse sentido, fundamentou a Corte: "*[...] the Court points out that the supervisory authorities established in accordance with Directive nº 95/46 must be allowed to perform their duties free from external influence. That requirement implies, on the one hand, that those authorities must not be bound by instructions of any kind in the performance of their duties and, on the other, that their decisiontaking process must be free from political influence, it being necessary to dispel even the risk of such influence. If it were permissible for a Member State to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in that regard by the legislation applicable, that authority might be prompted to enter into a form of prior compliance with political powers. Consequently, the independence of supervisory authorities necessarily covers the obligation to allow them to serve their full term of office and to cause them to vacate office before expiry of the full term only in accordance with the applicable legislation*".

ra e à efetividade do Acordo de Livre Comércio assinado entre o Mercosul e a União Europeia.

2 A PROTEÇÃO DE DADOS NA AMÉRICA LATINA

Frente às conclusões de um futuro previsível, vive-se uma mudança de era, na qual é impossível ignorar os avanços da tecnologia, notadamente da inteligência artificial e seus reflexos na manipulação de dados. Em face da nova revolução, a América Latina, a exemplo da Europa, também viu na uniformização das diretrizes sobre proteção de dados um caminho para maior segurança, tanto a nível individual quando coletivo.

Neste contexto, antes da análise dos aspectos relativos à proteção de dados no Acordo Bilateral assinado entre a União Europeia e no Mercosul, cumpre tecer alguns esclarecimentos com relação às legislações latinas.

2.1 Panorama geral da proteção de dados na América Latina

Diversos países têm legislações de proteção de dados na América Latina, como Chile, Argentina, Uruguai e Colômbia, além do próprio Brasil. Em todos os casos, há especial interesse na proteção dos direitos do titular e sobre o armazenamento e a transferência de dados, mas nem todos os regulamentos fazem menção específica à aplicação territorial, de forma que fica em aberto a abrangência da lei, para fins de comparação com a RGPD. É o que se passa a expor, por partes.

A Lei de Proteção de Dados chilena, Ley nº 19.628[29], de 18 de agosto de 1999, do Ministerio Secretaría General de la Presidencia ("Ley sobre Protección de la Vida Privada" ou "LPVP"), foi a primeira regulamentação na matéria de proteção de dados na América Latina e, assim como as demais, estabelece os parâmetros para o tratamento[30] de dados pessoais e garante aos titulares o direito a acessar as informações de posse de alguma pessoa jurídica ou física, corrigi-la ou eliminá-la, se o armazenamento não respeitar as exigências da lei ou o tratamento for concluído[31]. Todavia, diferentemen-

29 Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599>. Acesso em: 10 maio 2021.

30 Título I – De la utilización de datos personales: "*Art. 4º El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello*".

31 "*Art. 12. Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona,*

te dos outros regulamentos latinos, a LPVP não estabelece um arcabouço principiológico para reger a aplicação da lei.

Ainda, a LPVP prevê a responsabilização de empresas controladoras de dados em caso de prejuízos aos titulares, prevendo a indenização por danos materiais e morais[32], sendo o mecanismo adequado para tanto o recurso ao Judiciário[33]. O texto estabelece algumas diferenças para o Poder Público, limitando o tratamento de dados ao previsto na lei e impedindo divulgação de informações sobre condenações depois de prescreverem[34].

Por fim, a LPVP não determina a criação de alguma autoridade nacional para a execução da lei e administração dos dados. Por isso, não existindo uma autoridade de controle, a legalidade do tratamento de dados pessoais é garantida em razão do regime de sanções e do procedimento de recurso judicial disposto na lei. Em última instância, o ordenamento jurídico chileno tem concedido ao Conselho de Transparência competência para fiscalizar a aplicação da lei.

Na Argentina, a Ley nº 25.326[35], de 30 de outubro de 2000, do Congreso de La Nacion Argentina ("Ley de Proteccion de los Datos Personales" ou "LPDP"), regula o uso de bases de dados públicas e privadas, estabelecendo como princípio o uso limitado à finalidade para a qual foram obtidos. De forma pioneira, a LPDP estabelece que é proibida a transferência de dados pessoais[36] para países ou organismos internacionais ou supranacionais, que não proporcionem níveis de proteção adequados, mas não refere que tal *standard* é requisito para comercialização com outros países. O trata-

---

su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente."

32 "*Art. 23. La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal*."

33 *La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el art. 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los arts. 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez*.

34 "*Art. 21. Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena*."

35 Disponível em: <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto>. Acesso em: 10 maio 2021.

36 "*Art. 12. (Transferencia internacional). 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no propocionen niveles de protección adecuados*."

mento está condicionado ao consentimento do titular[37], que deve ser livre, expresso e informado, sendo que tal autorização não é exigida nos casos de bases públicas, no cumprimento de uma obrigação legal, no exercício de funções próprias do Estado e quando as informações se limitam a nome, identidade, profissão, data de nascimento e endereço[38]. Aliás, é permitido o repasse de dados a terceiros, desde que cumpram um "interesse legítimo" do ente que os estão cedendo. Já órgãos públicos têm regras especiais, como o direito de negar o acesso, a correção e a supressão das informações.

Destaque-se que a LPDP dispõe sobre a criação de órgão de controle ("*Organo de Control*"), que deverá empreender todas as medidas necessárias para o cumprimento dos objetivos indicados na LPDP, podendo, inclusive, solicitar informações às entidades públicas e privadas, que estão obrigadas a fornecer todos os elementos relativos ao tratamento de dados pessoais[39]. Aliás, a autoridade de proteção de dados deverá garantir a segurança e a confidencialidade da informação e dos elementos analisados, podendo impor as sanções administrativas correspondentes em caso de violação às normas legais, bem como se constituir querelante nas ações penais que poderão ser promovidas em função da lei[40].

Por fim, destaca-se que as penalidades previstas na LPDP incluem (i) sanções administrativas, as quais podem variar de uma advertência ("*apercibimiento*") até uma multa de cem mil pesos argentinos; e (ii) sanções penais, as quais foram incluídas no Código Penal argentino por meio da LPDP e que incluem a pena de prisão de 1 (um) mês a 2 (dois) anos em caso de inserção de dados sabidamente falsos em banco de dados[41] e em

37 "*Art. 5º (Consentimiento). 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias*."

38 "*2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 de la Ley nº 21.526*."

39 "*Art. 29. (Organo de Control). 1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: [...]*"

40 "*[...] g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; [...]*"

41 "*Art. 32. (Sanciones penales). 1. Incorpórase como artículo 117 bis del Código Penal, el siguiente: 1º Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales*."

caso de violação de sistemas de confidencialidade e de segurança de dados para invasão de bancos de dados[42]. Para fins de responsabilização do agente de tratamento de dados que venha a descumprir as disposições da LPDP, o requerente deverá ajuizar uma ação de proteção de dados ("*acción de protección de los datos personales*") ou o *habeas data*[43].

No Uruguai, a Ley nº 18.331[44], de 11 de agosto de 2008, do Senado y la Cámara de Representantes de la República Oriental del Uruguay ("Ley de Protección de Datos Personales y Acción de Habeas Data" ou "LPDPA"), é regida de acordo com valores e forças principiológicas, como a veracidade, a segurança de dados e o prévio consentimento informado. A LPDPA é aplicada no âmbito material para as pessoas físicas e, por extensão, para as pessoas jurídicas e, no âmbito objetivo, o regime de proteção de dados se aplica aos dados pessoais registrados em qualquer base de dados que torne os mesmos suscetíveis de tratamento e a toda modalidade de uso posterior de dados por entes públicos ou privados[45].

O manejo de dados nos termos da LPDPA é condicionado ao controle por órgão específico, que poderá aplicar sanções, graduadas em atenção à gravidade, reiteração ou reincidência da infração cometida. Há que se dar especial destaque para o fato de que uma das penalidades previstas em lei é a "clausura da base de dados"[46] respectiva, ante decisão dos órgãos judiciais competentes, desde que comprovada infração ou transgressão da lei.

---

42 "Art. *32. (Sanciones penales). [...] 2. Incorpórase como artículo 157 bis del Código Penal el siguiente: 'Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; [...]*"

43 Capítulo VII – Acción de protección de los datos personales: "*Art. 33. (Procedencia). 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización*".

44 Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 10 maio 2021.

45 "*Art. 3. Ambito objetivo. – El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado*."

46 "*Art. 35 (Potestades sancionatorias). – El órgano de control podrá aplicar las siguientes sanciones a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal, en caso que se violen las normas de la presente ley, las que se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida: [...] 5) Clausura de la base de datos respectiva. A tal efecto se podrá promover ante los órganos jurisdiccionales competentes la clausura de las bases de datos que se comprobare infringieren o transgredieren la presente ley*."

Por sua vez, a lei de proteção de dados da Colômbia, Ley Estatutaria nº 1.581[47], de outubro de 2012 ("Ley Estatutaria para la Protección de Datos Personales" ou "LEPDP"), regulamentada parcialmente pelo Decreto Nacional nº 1.377/2013 e pelo Decreto nº 1.081/2015, é bastante enxuta, possuindo apenas 30 artigos. Dispõe acerca da forma de regulação mediante a apresentação da principiologia básica, do âmbito de aplicação, da categorização de dados, procedimentos, entre outros. A LEPDP possui seção específica para tratar de mecanismos de sanção, que poderá ser aplicada pela Superintendência da Indústria e Comércio[48].

Ressalte-se que entre as medidas punitivas elencadas na lei está a suspensão das atividades relacionadas com o tratamento de dados por até 6 meses e o encerramento imediato e definitivo da operação que envolva o tratamento de dados sensíveis. Não obstante, a LEPDP estabelece que as sanções previstas se aplicam apenas a pessoas de natureza privada; com isso, caso a Superintendência da Indústria e Comércio apure suposta violação por autoridade pública, a ação será encaminhada para o Ministério Público da Colômbia para que este proceda à respectiva investigação[49].

A LEPDP determinou a incorporação da atividade regulatória de proteção de dados à Superintendência de Indústria e Comércio, para realizar a vigilância e garantir que o tratamento de dados respeite os princípios, os direitos, as garantias e os procedimentos previstos em lei[50]. Ainda, criou-se o Registro Nacional de Bases de Dados[51], definido como um diretório

47 Disponível em: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>. Acesso em: 10 maio 2021.

48 Para mais informações, ver: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>. Acesso em: 10 maio 2021.

49 "*Art. 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones: [...] Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva*."

50 "*Art. 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*."

51 Capítulo III – Del Registro Nacional de Bases de Datos: "*Art. 25. Definición. Reglamentado por el Decreto Nacional nº 886 de 2014 el Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley*".

público de bases de dados sujeitas a tratamento, porque operam na Colômbia, vinculado à Superintendência. Por fim, a LEPDP proíbe a transferência de dados pessoais para países que não proporcionem níveis adequados de proteção de dados, que em nenhuma hipótese poderá ser inferior ao da lei colombiana, para fins de circulação de dados colombianos[52].

O Brasil, por sua vez, promulgou a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou "LGPD"), que entrou em vigor em 18 de setembro de 2020, à exceção das sanções administrativas, que passarão a ser exigíveis apenas a partir de 1º de agosto de 2021. A LGPD regulamenta o tratamento das operações envolvendo dados pessoais, seja por meio digital ou não, dentro ou fora da Internet, e abarca, entre outras questões, os direitos dos titulares dos dados, as obrigações dos agentes de tratamento e do encarregado de dados, os parâmetros para segurança da informação, os requisitos para a transferência internacional de dados e, inclusive, as instruções quanto à atuação da Autoridade Nacional de Proteção de Dados ("ANPD"). Com isso, o Brasil passou a ser incluído no grupo de países da América Latina que possui uma Lei Geral de Proteção de Dados.

Ademais, a nível latino-americano, destaquem-se os "Padrões de Proteção de Dados dos Estados Ibero-Americanos", os quais foram aprovados pela Rede Ibero-Americana de Proteção de Dados (RIPD ou a Rede), para cumprir com um objetivo longamente almejado por todas as entidades que a integram, bem como para um dos acordos adotados na XXV Cúpula Ibero-Americana de Chefes de Estado e de Governo, celebrada nos dias 28 e 29 de outubro de 2016, na Colômbia, relacionado com solicitar à Rede a elaboração de uma proposta de cooperação efetiva com a proteção de dados pessoais e a privacidade, alterando os *standards* estabelecidos no documento "RIPD 2020".

52 "*Art. 26. Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial*."

Os Padrões Ibero-Americanos conformam um conjunto de diretrizes orientadoras, que contribuem para a emissão de iniciativas regulatórias de proteção de dados pessoais na região ibero-americana para aqueles países que ainda não contam com esses ordenamentos, ou, no caso, para servir de referência na modernização e atualização das legislações existentes. Destaca-se que diversos instrumentos internacionais serviram de referência para os Padrões, tais como o Convênio nº 108 do Conselho da Europa, o Marco de Privacidade do Fórum de Cooperação Econômica Ásia-Pacífico e o Regulamento do Parlamento Europeu e do Conselho.

Entre os objetivos dos Padrões Ibero-Americanos encontram-se (*i*) o estabelecimento de um conjunto de princípios e direitos comuns para proteção de dados pessoais, que os Estados ibero-americanos podem adotar e desenvolver em sua legislação nacional, com a finalidade de contar com regras homogêneas na região; (*ii*) garantir o efetivo exercício e tutela do direito à proteção de dados pessoais de qualquer pessoa física, mediante determinação de regras comuns; (*iii*) facilitar o fluxo de dados pessoas entre os Estados ibero-americanos e fora de suas fronteiras, para coadjuvar o crescimento econômico e social da região; e (*iv*) encorajar a cooperação internacional entre as entidades de controle dos Estados com outras autoridades de controle não pertencentes à região.

Ressalte-se que os Padrões de Proteção de Dados para os Estados ibero-americanos admitem aplicação mesmo naqueles Estados que não contam com uma legislação na matéria, porque considera-se que o acelerado uso de tecnologias da informação pode afetar a preservação e o tratamento da informação a nível comunitário, havendo comunicação massiva de dados pessoais de maneira imediata e quase ilimitada.

Com efeito, os Padrões se aplicam, (*i*) em âmbito subjetivo, para todas as pessoas *físicas ou jurídicas* de índole privada, autoridades e órgãos públicos, que tratem dados pessoais no exercício de suas atividades e funções, e, (*ii*) em âmbito objetivo, ao tratamento de dados pessoais que estejam em suportes físicos, automatizados total ou parcialmente, ou em ambos suportes, independentemente da forma ou da modalidade de sua criação, tipo de suporte, processamento, armazenamento e organização.

Quanto à transferência internacional de dados pessoais, os Padrões elencam regras gerais para a circulação dos dados, estabelecendo que as

legislações nacionais aplicáveis na matéria poderão limitar as transferências internacionais de categorias de dados pessoais por razões de segurança, segurança pública, proteção à saúde pública, proteção dos direitos e das liberdades de terceiros, bem como questões de interesse público.

Ainda, os Padrões referem, em seu Capítulo IX, o direito de indenização, de acordo com o qual a legislação nacional dos Estados ibero-americanos aplicável reconhecerá o direito do titular de ser indenizado quando tiver sofrido danos e prejuízos, como consequência de uma violação de seu direito à proteção de dados pessoais. O direito interno dos Estados indicará, nesse sentido, a autoridade competente para receber esse tipo de ações apresentadas pelo titular afetado, bem como prazos, requerimentos e termos através dos quais será indenizado, em caso de corresponder.

Com isso, percebe-se que a proteção de dados já está na pauta da política da América do Sul há tempo muito maior do que no Brasil, o que demonstra ainda mais a urgência para a implementação da Lei Geral de Proteção de Dados e a efetividade dos dispositivos nela previstos, inclusive para favorecer as futuras relações comerciais proporcionadas pelo Acordo de Livre Comércio.

2.2 Autoridade nacional de proteção de dados na América Latina

Atualmente, vivemos em uma sociedade na qual os dados assumem importância crescente, necessitando de regras claras e transparência sobre a maneira com a qual os dados são tratados e manipulados, coletados e armazenados, compartilhados e descartados. Neste contexto, as leis de proteção de dados e, em última análise, as autoridades nacionais de proteção de dados trazem a confiança e a previsibilidade necessárias para uma transformação digital sustentável (Gutierrez *in*: Maldonado; Blum, 2019, p. 400).

A lei uruguaia criou a *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento* (Agesic), dotado da mais ampla autonomia técnica, podendo realizar todas as ações necessárias para o cumprimento dos objetivos da lei. Inclusive, recentemente, o Uruguai lançou a política *Datos 360º – Una Visión Integral para la Gestión de los datos en el Estado*, que é uma iniciativa criada pela Agesic para promover um enfoque holístico e interdisciplinar da gestão de dados pela Administração Pública. O seu objetivo é incorporar no trata-

mento de dados do Estado distintas perspectivas, como a proteção de dados pessoais, o acesso à informação pública e a segurança da informação[53].

A autoridade de proteção de dados argentina, por sua vez, passou por uma severa modificação em seu modelo ao longo dos anos. A sua criação foi determinada em 2000, a partir da aprovação da Lei nº 25.326/2000, e regulamentada pelo Decreto nº 1558/2001, que a batizou de *Dirección Nacional de Protección de Datos Personales*, um órgão da Administração direta, subordinada a uma secretaria do Ministério da Justiça. Quer dizer, a autoridade foi criada como órgão sem personalidade jurídica própria, sob o argumento de não aumentar despesas públicas (Simão; Oms; Torres, 2019, p. 36).

Anos depois, em 2017, a estrutura da autoridade de proteção de dados argentina foi modificada, para que a atividade da autoridade não sofresse riscos de "ingerências hierárquicas e menores possibilidades para investigar e sancionar as infrações do poder público" (Simão; Oms; Torres, 2019, p. 36). A *Dirección* foi integrada à *Agencia de Acceso a la Información Publica*, criada em 2016, passando a fazer parte da Administração indireta do Estado argentino (Simão; Oms; Torres, 2019, p. 12).

De outra sorte, a Lei de Proteção de Dados Pessoais da Colômbia estabeleceu que as atividades inerentes à autoridade de controle ficariam a cargo da Superintendência de Indústria e Comércio (SIC), um órgão, à época, desconcentrado[54], da Administração Pública federal (Simão; Oms; Torres, 2019, p. 22). A SIC já existia anteriormente à promulgação da lei, porque já era responsável pela regulação da propriedade industrial, proteção do consumidor, proteção da concorrência e regulamentação da metrologia legal no país, motivo pelo qual o modelo da SIC lembra o da *Federal Trade Commission* (FTC) dos Estados Unidos[55] (Simão; Oms; Torres, 2019, p. 22). De toda forma, com a promulgação da Lei de Proteção de Dados na

53 Disponível em: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/datos-360deg-vision-integral-del-uso-datos-estado-0>.

54 Concentração administrativa – conforme a tradição do Direito espanhol – ocorre quando as funções são exercidas pelo Poder Executivo, com o qual os órgãos concentrados mantêm uma relação de hierarquia. A desconcentração, por outro lado, é uma ferramenta que atribui através de lei alguma competência permanente a órgão inferior da mesma entidade, mantendo, assim, a hierarquia ao Poder Executivo. Já a centralização é definida como o agrupamento de várias matérias em um centro comum, de forma que os órgãos centralizados dependem e são subordinados do poder central. Na contramão, a descentralização é a transferência de funções estatais a entes com personalidade jurídica própria e autoadministração, reduzindo a hierarquia frente o Poder Executivo (Dromi, 2000, p. 496-497)

55 A FTC é uma agência do governo dos Estados Unidos, criada em 1914 pelo Federal Trade Commission Act, e sua principal missão é a promoção da proteção ao consumidor e a eliminação e prevenção de práticas

Colômbia, em 2012, a Superintendência criou uma pasta específica nomeada "*Delegatura de proteção de dados pessoais*" e, "em 2015, a SIC passou a ser enquadrada como parte da administração descentralizada, deixando de ser órgão meramente desconcentrado para ganhar personalidade jurídica própria" (Simão; OMS; Torres, 2019, p. 22).

Nesse sentido, na Colômbia, apesar da autoridade ter personalidade jurídica própria – sendo, pois, da Administração indireta –, o fato de os membros serem indiretamente nomeados pelo Presidente (tal como no Uruguai) foi apontado como fator que prejudica a neutralidade dos cargos da autoridade. Por conta desse desenho, corre-se o risco de as posições deixarem de ser técnicas, para serem utilizadas com finalidades políticas.

No Brasil, a Medida Provisória nº 869/2018 ("MP"), a qual culminou na Lei nº 13.853/2019, estabeleceu os parâmetros para a criação da Autoridade Nacional de Proteção de Dados ("ANPD"), os quais foram formalizados com o Decreto nº 10.474/2020[56], que aprovou a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da ANPD. Contudo, atualmente, a ANPD se encontra vinculada à Presidência da República e possui natureza transitória[57], o que coloca em xeque a independência e a imparcialidade necessárias para o bom desempenho de suas funções de fiscalização tanto das atividades públicas quanto privadas. Portanto, a forma com a qual a ANPD foi estruturada parece não ser um bom desenho institucional para o órgão; a falta de autonomia administrativa, rije-se, foi alvo de crítica tanto na Argentina quanto no Uruguai.

Tendo em vista esses exemplos, fica evidente que, no caso brasileiro, a vinculação da autoridade à Administração direta e a livre nomeação dos membros pelo Presidente da República, sem participação da oposição, influenciam sua eficácia e dificultam a concretização da independência enquanto órgão fiscalizador, em que pese na letra fria da lei estar disposta a autonomia do órgão. Como visto, todos as autoridades possuem amplos poderes de investigação conferidos pela legislação, motivo pelo qual causa

comerciais anticompetitivas. Desde a década de 1970, a FTC tem sido a principal agência federal responsável pelo *enforcement* do direito à privacidade, quando começou a aplicar o Fair Credit Reporting Act.

56 Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>. Acesso em: 10 maio 2021.

57 "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República."

estranheza a vinculação da ANPD, "que não possui poderes expressos para requisitar acesso a bases de dados e sistemas de arquivamento, tampouco para fazer busca e apreensão" (Simão; Oms; Torres, 2019, p. 37):

> Além disso, a MP 869/2018 não previu a possibilidade de a ANPD realizar, como forma de fiscalização, auditorias sobre o tratamento de dados pessoais de forma ampla, em descompasso com o Projeto de Lei foi aprovado no Congresso Nacional. Dessa forma, tal possibilidade ficou restringida a casos de verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (Simão; Oms; Torres, 2019, p. 37-38)

Diante desse cenário e já tendo sido apresentadas as principais características do RGPD e das principais legislações de proteção de dados na América Latina, inclusive no que toca às autoridades de controle, parte-se à análise do Acordo de Livre Comércio assinado entre a União Europeia e o Mercosul e sua efetividade para as relações comerciais a serem travadas com o Brasil e ante a atual estrutura da ANPD.

3 O ACORDO DE LIVRE COMÉRCIO ENTRE A UNIÃO EUROPEIA E O MERCOSUL E O CASO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS BRASILEIRA

Em 28 de junho de 2019, foi aprovado o Acordo de Associação entre Mercosul e União Europeia[58], que visará promover o livre comércio baseado em regras e benefícios recíprocos. O novo quadro comercial – parte de um acordo de associação vasto entre as duas regiões – consolidará uma parceria política e econômica estratégica e criará oportunidades significativas para o crescimento sustentável de ambas as partes, respeitando o ambiente e preservando os interesses dos consumidores e setores econômicos sensíveis.

O Acordo é significativo a nível mundial; somados, Mercosul e União Europeia representam um PIB de 25% da economia mundial, equivalente a 19 trilhões de euros, e um mercado de consumo de 773 milhões de pessoas. A UE é atualmente o 2º maior parceiro comercial do Mercosul, perdendo só para China, e o Mercosul é o 8º principal parceiro extrarregional da UE. Segundo dados da Comissão Europeia, em 2018, o comércio birregional de produtos alcançou 88 bilhões de euros, e o de serviços, 34 bilhões de euros, totalizando a cifra de 122 bilhões de euros (Domingues; Montenegro, 2019).

58 Disponível em: <http://www.itamaraty.gov.br/images/2019/2019_07_03_-_Resumo_Acordo_Mercosul_UE.pdf>.

Após a desgravação prevista no acordo, 92% das importações do Mercosul e 95% das linhas tarifárias entrarão livres de tarifas na UE. Incluídas as linhas com desgravação parcial (quota, preço de entrada e preferência fixa), a oferta europeia se eleva a 99% do volume de comércio. O Mercosul, por sua vez, liberalizará 91% das importações originárias da UE e 91% das linhas tarifárias após a desgravação prevista no acordo[59]. Com isso, a expectativa do incremento das exportações para a UE gira em torno de quase US$ 100 bilhões até 2035, tendo em vista as tarifas e a importação, que deixarão de ser cobradas (Domingues; Montenegro, 2019).

Especificamente para o contexto econômico brasileiro, o Acordo é extremamente relevante, porque removerá tarifas aduaneiras, o que é justificado pelo intenso comércio do país com a União Europeia. Apenas em 2018, o país registrou um comércio de US$ 76 bilhões, com superávit de US$ 7 bilhões, dos quais US$ 42 bilhões são de exportações para a UE, representando 18% do total de exportações brasileiras, segundo dados do Comex Vis do Ministério da Economia, Indústria, Comércio Exterior e Serviços do Brasil[60]. Com relação aos aspectos tarifários, então, serão removidas as tarifas aduaneiras de 92% dos bens exportados pelo Mercosul para a UE e de 91% dos produtos exportados da UE para o Mercosul. Atualmente, apenas 24% das exportações brasileiras entram no mercado europeu livre de entraves tributários.

Após a revisão técnica e jurídica do acordo, bem como sua tradução nas línguas oficiais do Mercosul e da UE, o Acordo estará apto a ser oficialmente assinado pelas partes, com o que ele será enviado para aprovação do Conselho da Europeu no Parlamento Europeu. Sucessivamente, no Mercosul, cada Estado-membro deve concluir seus respectivos processos internos para ratificação de tratado internacional. Concluídos esses procedimentos, o Acordo entra em vigência no plano internacional.

Então, é evidente o avanço político e econômico que o Acordo representa para os blocos envolvidos; contudo, parte relevante da Convenção são os padrões exigidos para proteção de dados, em decorrência do princípio da extraterritorialidade, conforme apresentado alhures. Tendo isso em vista, o Acordo de Livre Comércio abordou a matéria de proteção de dados

59 Disponível em: <http://www.itamaraty.gov.br/images/2019/2019_07_03_-_Resumo_Acordo_Mercosul_UE.pdf>.

60 Disponível em: <http://www.mdic.gov.br/comercio-exterior/estatisticas-de-comercio-exterior/comex-vis/frame-bloco?bloco=uniao_europeia>.

em cinco aspectos do material disponibilizado pelo Itamaraty, quais sejam: (*i*) comércio de mercadorias, (*ii*) facilitação aduaneira e comércio, (*iii*) comércio de serviços e estabelecimentos, (*iv*) protocolo de assistência administrativa mútua em matéria aduaneira e (*v*) medidas de segurança bilaterais. Assim, passar-se-á a indicar alguns pontos a eles relacionados.

Quanto ao comércio de mercadorias, o Acordo fala que qualquer parte que introduza procedimentos de licenciamento ou mudanças nesses procedimentos deverá disponibilizar tais informações em *site* oficial do Governo, as quais deverão estar sempre acessíveis e, quando possível, 21 dias antes da data efetiva da exigência[61].

Quanto à facilitação aduaneira e de comércio, a cooperação internacional deve incluir a troca de informações sobre legislação aduaneira e outras relacionadas com o comércio, envolvendo, principalmente, intercâmbios sobre o uso da tecnologia da informação, requisitos de dados e documentação e sistemas de janela única, incluindo o trabalho para a sua futura interoperabilidade[62]. Ainda, estabeleceu-se que o Mercosul trabalhará no sentido de aplicar requisitos de dados para a liberação de mercadorias[63].

Quanto aos requisitos de documentos e dados, estabeleceu-se que, no que toca ao uso de informações tecnológicas, as partes deverão emitir uma declaração aduaneira e, sempre que possível, demonstrar o preenchimento de outros requisitos de dados importação e exportação de mercadorias a serem submetidas em formato eletrônico e promover o intercâmbio eletrônico de dados entre seus respectivos comerciantes, administrações e outras agências relacionadas com o comércio[64]. Ainda, para fins de serviços postais, o Acordo prevê "requisitos essenciais", os quais são razões gerais não econômicas para a imposição de condições relativas à oferta de serviços postais, que podem incluir a confidencialidade, a correspondência, a segurança da rede no que se refere ao transporte de mercadorias perigosas, a proteção ambiental e o planejamento regional[65].

O protocolo de assistência administrativa mútua em matéria aduaneira, de forma muito relevante, define que "dados pessoais" são toda a infor-

61 Art. 6º, sobre procedimentos para licenciamento de importação e exportação.
62 Art. 2º, sobre cooperação alfandegária.
63 Art. 17, sobre requisitos de documentações e dados.
64 Art. 18, sobre requisitos de documentações e dados.
65 Art. 19, Subseção 3, sobre serviços postais.

mação relacionada com qualquer pessoa singular ou, quando a legislação das partes o preveja, pessoa coletiva (*vide* art. 1º, "f"); assim, tem-se que os dados pessoais só podem ser trocados quando a parte que os recebe se comprometa a proteger esses dados de maneira considerada adequada pela outra parte[66]. Quando um específico grau de proteção for necessário para as informações fornecidas, isso deve ser especificado pela autoridade fornecedora. A parte que utilizar os dados pessoais deverá comunicar por escrito, no pedido da parte que os forneceu, o objetivo para o qual essa informação foi utilizada e os resultados obtidos. Não suficiente, o item 6 preceitua que em nenhuma circunstância os dados pessoais podem ser relacionados a origem racial, opiniões políticas, convicções, saúde e orientação sexual.

Quanto às medidas de segurança bilaterais, o período de recolhimento de dados para as investigações sobre lesões deve normalmente ser de pelo menos trinta até seis meses, prazo que se encerrará tão próximo da data de apresentação do pedido[67]. Da mesma forma, se as informações relativas à produção, à capacidade de produção, emprego, aos salários, ao volume e ao valor das vendas no mercado interno forem apresentadas em condições de confidencialidade, as autoridades investigadoras assegurarão que resumos não confidenciais significativos divulguem pelo menos dados agregados ou, nos casos em que a divulgação de dados agregados colocaria em risco a confidencialidade dos dados da empresa, são apresentados índices para cada período de 12 meses sob investigação, de forma a assegurar o direito de defesa adequado das partes interessadas[68].

O art. 13, sobre a implementação do Protocolo, encerra as disposições, referindo que o protocolo deverá ser aplicado "levando em consideração suas respectivas leis e regulamentos, em particular para a proteção de dados pessoais". Assim, em síntese, o Acordo pretende: (*i*) eliminar as barreiras comerciais e facilitar às empresas da UE vender bens e serviços ao Mercosul e investir; (*ii*) ajudar a UE e o Mercosul a moldar as regras do comércio global em conformidade com os mais elevados padrões da UE; (*iii*) enviar um sinal ao mundo em favor do comércio baseado em regras e que dois dos seus maiores blocos econômicos rejeitam o protecionismo;

66 Art. 12, sobre troca de informações e confidencialidade, item 5.

67 Seção 4, sobre investigação e procedimentos de transparência, art. 9º, item 3: "*The period of data collection for injury investigations normally should be at least thirty-six months ending as close to the date of the lodging of the application as is practicable*".

68 Art. 11, Item 2, Seção 4. A este respeito, os pedidos de confidencialidade devem ser considerados em situações em que determinadas estruturas do mercado e/ou da indústria nacional o justifiquem.

(*iv*) integrar ainda mais as cadeias de valor entre as nossas duas regiões, ajudando, assim, as indústrias de ambos os lados a permanecerem competitivas no mercado global; e (*v*) projetar nossos valores por meio de obrigações detalhadas sobre comércio e desenvolvimento sustentável, incluindo mudanças climáticas e trabalho (European Comission, 2019). Trata-se, portanto, de um Acordo que orientará ambas as partes a seguir uma Agenda baseada em valores comuns, em atenção ao Considerando 5 do RGPD, o qual dispõe que a integração econômica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais.

Nada obstante, o questionamento que se impõe, ante tudo que foi posto, é: Considerando a forma com a qual a autoridade nacional de proteção de dados no Brasil foi criada, ela atende ao nível de equivalência demandado pela União Europeia, para fins de eficácia do Acordo de Livre Comércio?

De antemão, vale lembrar que a LGPD se inspira no conceito que ficou conhecido como o modelo europeu de proteção de dados, amparado na Convenção do Conselho da Europa nº 108, de 1981, na Diretiva nº 46/95/CE e no Regulamento Geral de Proteção de Dados (Regulamento nº 2016/679), conforme apontam Mendes e Doneda (2018, p. 1):

> Isso pode ser percebido na exigência de uma base legal para o tratamento de dados, nos princípios gerais, nas regras especiais para os dados sensíveis, bem como no fato de ter como um de seus pilares a criação de uma autoridade para a aplicação da Lei. São influências europeias também a edição de regras distintas de responsabilidade para o operador e controlador e a novidade da portabilidade dos dados, claramente inspirada no Regulamento Europeu. (Mendes; Doneda, 2018, p. 1; European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 187)

Dito isso e conforme já adiantado, a forma com a qual a autoridade nacional de proteção de dados brasileira foi criada gera dúvidas quanto à forma com a qual levará a cabo, de forma imparcial e independente, a legislação de proteção de dados. Isso porque (*i*) ela é órgão da Administração Pública federal, integrante da Presidência da República, nos termos do *caput* do art. 55-A[69] da LGPD, e (*ii*) sua natureza é transitória, *vide* § 1º[70] do

69 "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública federal, integrante da Presidência da República."

70 "[...] § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República."

artigo. Em outras palavras, mesmo que o art. 55-B assegure autonomia técnica e decisória à ANPD, há dúvidas que ela possa cumprir com os estândares de equivalência demandados pela União Europeia, para fins de efetividade do Acordo de Livre Comércio.

Em síntese, o aspecto central debatido é que, hoje, na maioria dos marcos regulatórios de proteção de dados, as autoridades de proteção de dados constam, na maior parte das vezes, como um de seus sustentáculos principais, ou seja, como elemento integrante da técnica legislativa utilizada para abordar o tema de proteção de dados[71]. Assim, uma autoridade de proteção de dados funcional, em conformidade com os termos do RGPD, para fins de efetividade do Acordo de Livre Comércio, ao contrário do que prevê a LGPD, deveria ser "ente ou órgão público dotado de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder Executivo" (Caringella, 2000, p. 10). A ANDP, nos termos do art. 55-A da LGPD, parece não atender tais requisitos.

Isso porque, sendo a ANPD órgão integrante da Presidência da República, ela deixa de possuir atributo fundamental a sua funcionalidade, a independência, ou seja, a ausência de ingerência governamental sobre seus atos (Doneda, 2019, p. 314). As atividades fiscalizatória, sancionatória e decisional da Autoridade não devem se subordinar hierarquicamente a outros órgãos. Aliás, ao contrário do que consta na literalidade do art. 55-A, a independência da Autoridade implica em um necessário afastamento hierárquico da Administração Pública direta. Verifica-se, portanto, uma clara afetação desse aspecto tão relevante na legislação de proteção de dados brasileira, o que implica em dúvidas quanto à consistência que se espera do País para fins de continuidade do Acordo de Livre Comércio.

Destarte, muito embora o pano de fundo ora sob análise seja a conformidade da LGPD para fins de aplicação e efetivação do Acordo entre a União Europeia e o Mercosul, em verdade, não se trata da emulação de algum modelo estrangeiro, mas sim a devida consideração das características fundamentais da Autoridade de Proteção de Dados – as quais parecem não terem sido refletidas pela Lei nº 13.853/2019. Aqui, refere-se à necessária ação de uma autoridade para a proteção de dados pessoais, como a realiza-

71 Inclusive, a Carta de Direitos Fundamentais da União Europeia de 2000 trouxe a significativa previsão de que a constituição de uma autoridade de fiscalização é um ponto integral e orgânico do próprio direito fundamental à proteção de dados pessoais (Doneda, 2019, p. 308-309).

ção de uma garantia constitucional[72], precisamente porque o Estado apresenta demasiado interesse na coleta e no processamento de dados pessoais para que sua atividade possa harmonizar-se com a proteção desses mesmos dados.

CONSIDERAÇÕES FINAIS

Diante de todo o exposto, responde-se à hipótese formulada, no sentido de que as legislações na UE e na América Latina vêm regulamentando a proteção de dados pessoais há mais tempo e com mais profundidade do que no Brasil. Isso quer dizer que, ainda que o Brasil conte com um significativo contexto regulatório no que toca à tutela da proteção de dados e da privacidade, a exemplo do Marco Civil da Internet e a Lei de Acesso à Informação, entre outros, a LGPD é uma lei geral e, como tal, precisa ser regulamentada em muitos de seus aspectos.

Além disso, quanto à segunda parte da hipótese apresentada ao início, parece que a forma com a qual a ANPD foi criada, de forma vinculada à Presidência da República e com natureza transitória, afeta significativamente a independência e a autonomia da autoridade, que, rije-se, deve ser capaz de fiscalizar o tratamento de dados realizado tanto por pessoas jurídicas de direito público quanto de direito privado – além, é claro, das pessoas físicas.

Assim, é inegável que a LGPD representou um marco para a garantia da privacidade e da proteção dos dados dos cidadãos no Brasil. Além de proteger as informações pessoais daqueles que fazem uso da Internet e, cotidianamente, divulgam seus dados por conta de práticas rotineiras, especialmente durante a pandemia do Covid-19[73], a nova legislação contribuirá

72 Doneda prossegue, referindo que, "além disso, o recurso a uma tutela baseada na responsabilidade civil não é, por si só, capaz de proporcionar uma tutela eficiente para o direito fundamental que representa a proteção de dados pessoais – como não o é a tutela exercida somente pelo interessado ou a autorregulamentação pelo mercado" (2019, p. 320-321).

73 "Se, por um lado, a implementação em larga escala do *home office* – ou teletrabalho, como a legislação brasileira convencionou chamar – revela-se uma importante medida de combate ao coronavírus, por outro impõe às empresas um recente desafio: como compatibilizar mecanismos de monitoramento remoto e controle de produtividade com a proteção dos dados pessoais de colaboradores? Qual a medida apta a equilibrar a esfera privada do lar do indivíduo com suas responsabilidades enquanto funcionário e, consequentemente, com os interesses do empregador?" (SABOYA, Maria Beatriz. Ferramentas de trabalho remoto em tempos de Covid-19: Como achar o equilíbrio entre controle de produtividade no *home office* e proteção de dados pessoais? *Migalhas*, [s.l.], 5 maio 2020. Disponível em: <https://www.migalhas.com.br/depeso/326029/ferramentas-de-trabalho-remoto-em-tempos-de-covid-19--como-achar-o-equilibrio-entre-controle-de-produtividade-no-home-office-e-protecao-de-dados-pessoais>. Acesso em: 10 maio 2021)

– e já vem contribuindo – para o fomento à competitividade das empresas nacionais no exterior – também por conta da assinatura de convenções como o Acordo de Livre Comércio entre Mercosul e União Europeia –, ao obrigá-las a operar em condições adequadas ou equivalente às praticadas nos mercados mais exigentes do mundo.

Portanto, não se extrai outra conclusão, se não a de que as normas e orientações atinentes à proteção de dados só são realmente eficazes quando discutidas e elaboradas com a participação de diversos segmentos sociais afetados, em especial os setores diretamente regulados. Em outras palavras, em um momento de tamanha transformação tecnológica, é imperativo do momento que haja uma conjugação de esforços entre Poder Público, privado e sociedade civil, para fielmente cumprir e aplicar a LGPD, de forma a potencializar as presentes e futuras relações comerciais, em um ambiente virtualmente seguro. É necessário, portanto, uma verdadeira mudança de cultura corporativa e organizacional.

REFERÊNCIAS

ARGENTINA. Ley nº 25.326 de 30 de octubre de 2000, que dispone sobre la protección de los datos personales. Senado y Camara de Diputados de la Nación Argentina, Buenos Aires. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília/DF, Seção 1, ano 139, n. 8, p. 1-74, 15 ago. 2018.

_____. 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. *Diário Oficial da União*, Brasília/DF, Seção 1, ano 139, n. 8, p. 1-74, 20 dez. 2019.

CARINGELLA, Roberto Garofolo Francesco. *Le autoritá indipendenti*. Napoli: Simoni, 2000.

CHILE. Ley nº 19.628 de 6 de agosto de 1999, que dispone sobre protección de la vida privada. Ministerio Secretaría General de la Presidencia, Santiago. Disponível em: <https://www.leychile.cl/Navegar?idNorma=141599>.

COLOMBIA. Decreto nº 1.377, de 27 de junio de 2013, que reglamenta parcialmente la Ley nº 1.581, de 2012. Ministério de Comercio, Industria y Turismo, Bogotá. Disponível em: <https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf>.

DÖHMANN, Indra Spiecker Gennant. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *Revista do Instituto de Direito Público*, Brasília, v. 17, n. 93, p. 9-32, maio/jun. 2020.

DOMINGUES, Juliana Oliveira; MONTENEGRO, Adriane Takahara. Acordo de Associação entre o Mercosul e a União Europeia. *Jota*, 1º ago. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/acordo-de-associacao-entre-o-mercosul-e-a-uniao-europeia-01082019>.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DROMI, Roberto. *Derecho administrativo*. 10. ed. Buenos Aires: Editora, 2000.

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS. Red Iberoamericana de Protección de Datos, 20 jun. 2017.

EUROPEAN COMISSION [Principal]. Bruxelas, [2019]. Disponível em: <https://ec.europa.eu/trade/policy/in-focus/eu-mercosur-association-agreement/agreement-explained/>. Acesso em: 4 dez. 2019.

EUROPEAN COURT OF JUSTICE. Acórdão de 9 de março de 2010, *European Commission v. Federal Republic of Germany*, C-518/07. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62007CA0518&from=PT>. Acesso em: 1º jun. 2021.

EUROPEAN COURT OF JUSTICE. Acórdão de 1º de outubro de 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=168944&text=&doclang=EN&pageIndex=0&cid=9376711>. Acesso em: 1º jun. 2021.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. European Court of Human Rights, Handbook on European Data Protection Law, p. 187 e ss., 2014. Disponível em: <www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf>.

FINCATO, Denise Pires; SILVA, Cecília Alberton Coutinho. Empregabilidade como um direito: necessária partilha de esforços. *Revista Magister de Direito do Trabalho*, v. 1, jul./ago. 2020.

FOSCH-VILLARONGA, Eduard; MILLARD, Christopher. Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems. *Robotics and Autonomous Systems*, v. 119, p. 77-91, sep. 2019. Disponível em: <https://doi.org/10.1016/j.robot.2019.06.003>. Acesso em: 30 maio 2021.

GABEL, Detlev; HICKMAN, Tim. New EU Guidelines on Data Protection Officers. *White & Case*, [s.l], 16 jan. 2017. Disponível em: <https://www.whitecase.com/publications/alert/new-eu-guidelines-data-protection-officers>. Acesso em: 23 fev. 2020.

GILARDI, Fabrizio. Policy credibility and delegation to independent regulatory agencies: a comparative empirical analysis. *Journal of European Public Policy*, 9, n. 6, 2002. Disponível em: <https://doi.org/10.1080/1350176022000046409>. Acesso em: 30 maio 2021.

GIMÉNEZ, Alfonso Ortega. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*. Madrid: Agencia Española de Protección de Datos, 2015.

IAPP. Study: RGPD's global research to require at least 75,000 DPOs worldwide. *The Privacy Advisor*, [s.l.], 9 nov. 2016. Disponível em: <https://iapp.org/news/a/study-RGPDs-global-reach-to-require-at-least-75000-dpos-worldwide/#>. Acesso em: 23 fev. 2020.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. Policy Paper – Transferência Internacional de Dados no PL 5.276/2016. Belo Horizonte: IRIS, 2017. Disponível em: <http://irisbh.com.br/wp-content/uploads/2017/05/Policy-Papper-Portugues.pdf>. Acesso em: 20 maio 2018.

KUNER, Christopher. Regulation of transborder data flows under data protection and privacy law: past, present and future. *OECD Digital Economy Papers*, n. 187, OECD Publishing, 2011.

LIMA FILHO, Francisco das C. A ordem jurídica comunitária europeia: princípios e fontes. *Revista Jurídica Unigran*, Dourados, Minas Gerais, p. 103-104, jan./jun. 2006.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *Comentários ao RGPD*. 2. ed. São Paulo: Thomson Reuters Brasil.

_____; _____. *Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

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

MILLARD, Christopher. *Cloud Computing Law*. Oxford: Oxford University Press, 2013.

MONCAU, Luiz Fernando; MACIEL, Marília Ferreira; VENTURINI, Jamila; LUCA, Belli; LOUZADA, Luiza; FODITSCH, Nathalia; MIZUKAMI, Pedro Nicoletti. Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, 2015. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/17472>. Acesso em: 30 jul. 2019.

RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

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

SABOYA, Maria Beatriz. Ferramentas de trabalho remoto em tempos de Covid-19: Como achar o equilíbrio entre controle de produtividade no *home office* e proteção de dados pessoais? *Migalhas*, [s.l.], 5 maio 2020. Disponível em: <https://www.migalhas.com.br/depeso/326029/ferramentas-de-trabalho-remoto-em-tempos-de-covid-19--como-achar-o-equilibrio-entre-controle-de-produtividade-no-home-office-e-protecao-de-dados-pessoais&$>. Acesso em: 10 maio 2021.

SCHÜTZ, Philip. *Comparing Formal Independence of Data Protection Authorities in selected EU Member States*. Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference 2012.

SCHÜTZE, Robert. *European constitutional law*. 2. ed. Cambridge: University Printing Hause, 2017.

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

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. *Proteção de dados na América Latina*: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. São Paulo: Instituto Brasileiro de Defesa do Consumidor, 2019.

THATCHER, Mark. Regulation after delegation: independent regulatory agencies in Europe. *Journal of European Public Policy*, 9, n. 6, 2002.

UNCTAD. *Data protection regulations and international data flows*: implications for trade and development. United Nations Publication: New York and Geneva, 2016.

UNIÃO EUROPEIA. Court of Justice of European Union. Grand Chamber. Case C-288/12, *European Comission v. Hungary*. Luxemburgo, 8 abr. 2014. Disponível em: <http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-288/12>. Acesso em: 20 dez. 2019.

_____. Court of Justice of European Union. Grand Chamber. Case C-518/07, *European Comission v. Federal Republico f Germany*. Luxemburgo, 9 mar. 2010. Disponível em: <http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-288/12>. Acesso em: 16 nov. 2019.

_____. Court of Justice of European Union. Third Chamber. Case C-230/14, *Weltimmo s. r. o. v. Nemzeti Adat-védelmi és Információszabadság Hatóság*. Luxemburgo, 1º out. 2015. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN>. Acesso em: 10 maio 2018.

URUGUAY. Ley nº 18.331, de 11 de agosto de 2008. Centro de Información Oficial, Montevideo. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008/29>.

ZANON, João Carlos. *Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013.

Sobre as autoras:

Regina Linden Ruaro | *E-mail:* ruaro@pucrs.br

Decana Associada da Escola de Direito da PUCRS. Doutora em Direito pela Universidad Complutense de Madrid (1993 com titulo revalidado pela UFRGS em 1994) e Pós-Doutorado pelo Universidad San Pablo – CEU de Madri (2006-2008), Estágio Pós-Doutoral na Universidade San Pablo – Ceu de Madri (2016). Compõe o Grupo Internacional de Pesquisa "Protección de datos, transparencia, seguridad y mercado". Atualmente, é Professora titular da Pontifícia Universidade Católica do Rio Grande do Sul e Membro da Comissão Coordenadora do Programa de Pós-Graduação em Direito do Estado da Faculdade de Direito. Procuradora Federal/AGU aposentada. Professora convidada do Master Protecciòn de Datos, Transparencia y Acceso a la Información da Universidad San Pablo de Madrid-CEU de Madri/Espanha. Membro Honorário do Instituto Internacional de Estudos de Direito do Estado (IEDE). Lidera o Grupo de Pesquisa cadastrado no CNPq: Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação. Pesquisadora do Grupo Nedef/PUCRS.

Cecília Alberton Coutinho Silva | *E-mail:* coutinhocecilia1@gmail.com

Mestranda em Direito na linha de pesquisa de "Direito, Ciência, Tecnologia & Inovação" na Pontifícia Universidade Católica do Rio Grande do Sul (2021/2022). Bacharel em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (2016/2021). Membro do Grupo de Pesquisa cadastrado no CNPq "Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação", vinculado à PUCRS. Membro do Grupo de Pesquisa cadastrado no CNPq "Governança Corporativa, *Compliance* e Proteção de Dados", vinculado à Universidade Mackenzie. Assistente Jurídica da Área de Propriedade Intelectual e Tecnologia da Informação do Veirano Advogados, com foco em Proteção de Dados.

Data de submissão: 14 de abril de 2020.

Data do aceite: 22 de junho de 2021.