Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 04.07.2023
Aprovado em: 01.08.2023

Revista de Direito, Governança e Novas Tecnologias

MERCOSUL X UNIÃO EUROPEIA: NECESSÁRIA ADEQUAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

MERCOSUL X EUROPEAN UNION: ADEQUACY OF THE NATIONAL DATA PROTECTION AUTHORITY

Bruno Alexander Mauricio*

Kennedy Josué Greca de Mattos**

*Resumo***:** A proteção de dados nos últimos anos está ganhando cada vez mais relevância em todo o mundo. A União Europeia detém a legislação considerada modelo para qualquer país ou bloco que está em processo de adaptação desta nova preocupação mundial. Nesse sentido, analisando a estrutura de proteção de dados da União Europeia e suas autoridades de proteção de dados, estabeleceu-se neste artigo um comparativo com a legislação de proteção de dados dos países signatários do Mercosul e as respectivas autoridades de proteção de dados. Metodologia: Utiliza-se o método dedutivo na presente pesquisa, por intermédio de uma abordagem qualitativa para produzir informações aprofundadas; quanto ao procedimento, é uma pesquisa bibliográfica, mediante a revisão de obras e artigos científicos, bem como documental, devido à revisão de textos legislativos. Resultados: Ao final, em virtude do o Acordo de Livre Comércio entre a União Europeia e o Mercosul, estudou-se sobre a LGPD, legislação brasileira de proteção de dados e a Autoridade Nacional de Proteção de Dados, de modo a identificar algumas ações necessárias para a real compatibilidade do Brasil à estrutura europeia para atender aos requisitos do acordo mencionado Contribuições: Considera-se que se faz necessária a adequação da ANPD Brasileira e demais Autoridades vinculadas aos Estados integrantes do Mercosul, para o fim de atender aos requisitos da GDPR.

*Palavras-Chave***:** Proteção de Dados; GDPR; LGPD; Mercosul; União Europeia.

Abstract: Data protection in recent years is gaining more and more relevance around the world. The European Union holds legislation considered a model for any country or bloc that is in the process of adapting to this new global concern. In this sense, analyzing the data protection structure of the European Union and its data protection authorities, this article establishes a

* Mestrando em Direito Empresarial e Cidadania pelo Centro Universitário Curitiba - Unicuritiba. Pós-Graduado em Direito Processual Civil, Cidadania e Meios Consensuais de Solução de Conflitos pelo Centro Universitário UnidomBosco. Pós-Graduado em Direito do Trabalho e Processo do Trabalho pelo Centro Universitário UnidomBosco. O autor cursou o Contract Law: From Trust to Promise to Contract pela Harvard Law School (EUA). Professor no Núcleo de Ensino à Distância - NEAD do Centro Universitário Unidombosco. E-mail: brunoamauricio@gmail.com ORCID: https://orcid.org/0000-0001-7689-6753 / LATTES: http://lattes.cnpq.br/2617404431469890.

** Graduado em Direito pela Pontifícia Universidade Católica do Paraná. É Juiz de Direito do Estado do Paraná. Mestre e doutorando em Direitos Fundamentais e Democracia pela UNIBRASIL - PR. E-mail: kgm@tjpr.jus.br. LATTES: http://lattes.cnpq.br/6189159194669956

comparison with the data protection legislation of the Mercosur signatory countries and the respective data protection authorities. Methodology: The deductive method is used in this research, through a qualitative approach to produce in-depth information; as for the procedure, it is a bibliographical research, through the review of works and scientific articles, as well as documentary, due to the review of legislative texts. Results: In the end, due to the Free Trade Agreement between the European Union and Mercosur, LGPD, Brazilian data protection legislation and the National Data Protection Authority were studied, in order to identify some necessary actions for the real compatibility of Brazil with the European structure to meet the requirements of the aforementioned agreement Contributions: It is considered that the adequacy of the Brazilian ANPD and other Authorities linked to the member States of Mercosur, in order to meet the requirements of the GDPR.

*Keywords**:** Data Protection; GDPR; LGPD; Mercosul; European Union.*

Introdução.

Nos últimos anos, a forma como a informação é coletada e processada tem levado à necessidade de revisitar o contexto da privacidade e, por conseguinte, de novas estratégias para regular a matéria, sobretudo a proteção de dados pessoais. Neste contexto, além da própria privacidade, a proteção de dados pessoais e outros direitos da personalidade ganharam ainda mais relevância, pois a utilização das ferramentas existentes, – talvez - não sejam o suficiente para solucionar as situações mais básicas. A proteção de dados pessoais tornou-se um direito fundamental de autonomia. Nas palavras de Ulrich Beck, "o direito de proteger a privacidade, combinado com o dever de proteção de dados é o supremo direito humano internacional"[1].

As discussões sobre a proteção da privacidade e proteção de dados existem há muito tempo, como Boyd v. Estados Unidos, caso em que a Suprema Corte dos Estados Unidos julgou inconstitucional a divulgação de documentos fiscais nos termos da Quarta Emenda[2]. Hoje, sob outro viés, as novas tecnologias de inteligência artificial[3] e *big data* dão outro tom para a necessidade de proteger a privacidade, desafiando limitações anteriores.

[1] BECK, Ulrich, A metamorfose do mundo: novos conceitos para uma nova realidade. (Trad.) Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018. p. 187.

[2] 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.

[3] Nesse sentido, Klaus Schwab cita a inteligência artificial como uma nova forma de produção que revolucionou as relações de trabalho, vinculando tarefas de reconhecimento de padrões e processamento de informações complexas (2016, p. 50).

Nesse sentido, este desenvolvimento tecnológico cada vez mais rápido, bem como o fenômeno identificável da integração económica e social da UE e do MERCOSUL, trazem novos desafios em termos de proteção de dados, incluindo o intercâmbio de informação entre entidades públicas. Portanto, fica claro que a proteção de dados pessoais hoje está diretamente relacionada ao comércio e à troca de bens e serviços, razão pela qual a legislação deve promover segurança e previsibilidade[4].[5]

Por isso, as informações pessoais estão se tornando cada vez mais públicas em escala global, o que exige uma posição afirmativa das autoridades competentes, exteriorizada por regras: na UE, a Diretiva 95/46/CE, do Parlamento Europeu ("RGPD") e; no MERCOSUL, com as normas individuais de cada membro interno, com foco no padrão de Proteção de Dados Pessoais da *Red Iberoamericana de Protección de Datos* e, no Brasil, Lei nº 13.709/2018, a Lei Geral de Proteção de Dados.

Na América Latina, alguns países promulgaram legislações de proteção de dados com especial atenção à proteção dos direitos dos titulares dos dados e ao armazenamento e transferência de informações, porém, nem todos preveem a criação de órgãos nacionais de proteção, o que torna a proteção de dados difícil no contexto da vigilância.[6]

Portanto, este estudo questiona como a legislação da UE e alguns países da América Latina regula a proteção de dados pessoais, especialmente no que diz respeito à independência e autonomia das autoridades de proteção de dados. Isso porque as estratégias regulatórias constituem uma verdadeira defesa contra os indivíduos que terão controle significativo sobre seus dados, limitam interesses financeiros e preservam a dignidade humana, antes reduzida aos limites tradicionais da privacidade, a dicotomia de "coletar" e "expor"".

Para abordar as questões acima mencionadas, o objetivo geral deste artigo é destacar o contexto internacional no campo da proteção de dados pessoais, especialmente na União Europeia e na América Latina. Com base nesse cenário delineado, os objetivos específicos são

[4] No original: 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 (tradução livre).

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

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

(i) identificar as principais características da legislação de proteção de dados, em especial o Regulamento Europeu de Proteção de Dados (GDPR) e as leis locais de proteção de dados na América Latina; (ii) verificar nesses locais as estrutura do órgão de proteção; (iii) analisar se com a Autoridade Nacional de Proteção de Dados (ANPD) do Brasil, a partir da introdução do acordo de livre comércio firmado entre a UE e o MERCOSUL, colocará obstáculos ao comércio futuro.

Nesse sentido, a pesquisa começa com uma abordagem hipotética dedutiva, com explicações comparativas e históricas de processos e sistemas. A natureza da pesquisa é teórica, o objetivo é exploratório e interpretativo, e a pesquisa é bibliográfica quanto ao objeto de pesquisa.

Dito isso, a pesquisa dá continuidade à analise da recente legislação de proteção de dados no Brasil, América Latina e União Europeia, começando pelo GDPR e pelas autoridades de proteção de dados do Bloco Europeu, partindo da premissa de que a proteção de dados pessoais é atualmente uma lista de direitos fundamentais dos cidadãos devido ao princípio da dignidade humana.

1. A *General Data Protection Regulation* (GDPR) e Autoridades de Proteção de Dados.

A *General Data Protection Regulation* (GDPR) ou, Regulamento Europeu de Proteção de Dados deu forma às primeiras ideias no continente Europeu sobre proteção dos dados pessoais. Ou seja, desde a campanha do estado alemão de Hesse, até o atual regulamento 2016/679, a UE vem estabelecendo o padrão a ser seguido nesta questão.

Portanto, dada a parceria comercial entre EU e MERCOSUL, a efetiva proteção de dados torna-se um elemento de observação relevante nas negociações do novo acordo econômico firmado. Aqui, deve-se mencionar que as novas tecnologias aceleraram muito o processo de comércio, então, mais do que nunca os países devem ter uma postura ativa na regulação e proteção de dados nacionais (e internacionais).

A razão é que, apesar da natureza transnacional da Internet e de uma economia global crescente, os direitos sobre os dados e as regulamentações de proteção de dados ainda são muito

fragmentados (SCHWAB, 2016, p. 50), apesar do impacto potencialmente positivo da tecnologia no crescimento econômico.[7]

Como tal, é relevante o trabalho das Autoridades Nacionais de Proteção de Dados (ou Autoridades de Proteção de Dados, "DPAs"), entidades destinadas a garantir o direito de todos à privacidade e proteção dos seus dados.

A partir disso, pode-se inferir que, a partir de agora, a "força de expansão" da proteção de dados pessoais formou uma tendência clara, ou seja, a privacidade não é apenas uma característica inata dos chamados "novos direitos".[8]

Dito isso, antes de entrar na realidade brasileira e reflexo do acordo de livre comércio firmado entre a UE e o MERCOSUL, é necessário analisar (i) as características gerais das normas europeias de proteção de dados e (ii) como as autoridades protegem os dados nacionais.

1.1. Características gerais da GDPR.

O Regulamento Geral de Proteção de Dados (GDPR) foi ratificado em 15 de abril de 2016 e foi implementado pelo Parlamento Europeu em 25 de maio de 2018. Possui 99 artigos e um longo preâmbulo de "Instruções", que estabelece todos os princípios básicos aplicáveis à proteção de dados.

Os novos regulamentos surgiram para intensificar o tratamento de dados pessoais de todos os indivíduos dentro da União Europeia e do Espaço Económico Europeu (EEE), bem como a transferência de exportação de dados pessoais para fora da União Europeia e do Espaço Econômico Europeu. Como tal, o GDPR oferece aos cidadãos novas maneiras de controlar seus dados e harmoniza com os regulamentos já existentes, no entanto revogando a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/EC).

O GDPR reforça o entendimento de que, na UE, o direito à proteção de dados é uma estrutura jurídica, modelada a partir da experiência alemã. Assim, o direito à proteção de dados

[7] 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. p. 26.

[8] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 15.

está atualmente elevado no direito comunitário à categoria de direitos fundamentais, ao lado do direito à privacidade[9], sempre levando em consideração a aplicação em casos específicos.

Este fato se deve principalmente à natureza legislativa do Regulamento, que, ao contrário da Diretiva, é um ato legislativo vinculativo que se aplica a todos os elementos em todos os países da UE[10], formando uma padronização que, uma vez aprovada, é imposta indiscriminadamente a todos, desde que sejam membros da UE. Para Schütze[11], o regulamento deve ser de aplicabilidade geral, vinculante em seu conjunto e diretamente aplicável a todos os integrantes do bloco, conforme art. Artigo 288.º do TFUE.

Por exemplo, esta Diretiva, assim como a Diretiva 95/46, que trata da proteção de dados da UE, é um ato legislativo que estabelece objetivos gerais que todos os países da UE devem alcançar. No entanto, cada país deve desenvolver sua própria legislação para conseguir isso. É assim que Lima Filho define 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.[12]

Neste contexto, na UE, existe um sistema de governo multifacetado e, como resultado, a legislação está a ser cada vez mais desenvolvida para ter um caráter regulatório e não redistributivo.[13] Em outras palavras, os parâmetros estabelecidos pelo GDPR não permitem a

[9] ZANON, João Carlos. Direito à proteção dos dados pessoais. São Paulo: Revista dos Tribunais, 2013. p. 81-82.

[10] 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. p. 14.

[11] SCHÜTZE, Robert. European constitutional law. 2. ed. Cambridge: University Printing Hause, 2017. p. 89-90.

[12] 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. p. 103-104.

[13] 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. p. 87-90.

relativização de seus termos, justamente para facilitar um ambiente seguro para as negociações comerciais.

Vale ressaltar que quando os europeus criaram o sistema de proteção de dados (isto é, o GDPR), criaram uma regra que mais tarde foi descrita como aplicação extraterritorial da lei, ou seja, como disse Maldonado, em qualquer lugar do mundo das empresas fornecedoras de bens para os países da UE, deve cumprir as regulamentações europeias – essas regras se aplicam ao "tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como por meios não automatizados, de acordo com o art. Artigo 2º do GDPR.[14]

Por isso, hoje, os processos de negócio que tratam de dados pessoais, ou seja, aqueles que tratam de tais informações, precisam ser desenhados desde o início, com medidas padrão respeitando os princípios de proteção de dados, *privacy by default* e *privacy by design*. Ou seja, os dados devem ser armazenados usando um pseudo-anonimato ou anonimato total, que por padrão possui as configurações de privacidade mais altas.

O estatuto também proíbe qualquer processamento de dados fora do escopo legal nele estabelecido, a menos que o controlador de dados tenha obtido o consentimento expresso do proprietário dos dados. Entende-se que a qualquer momento, o proprietário ainda tem o direito de revogar a licença.

Ou seja, de acordo com o artigo 3.º, n.º 1, o regulamento se aplica ao tratamento de informações pessoais por um responsável pelo tratamento ou operador localizado no território europeu, ainda que o tratamento seja realizado fora do território europeu.

Nesse sentido, vale destacar o caso Weltimmo, em que o Tribunal de Justiça Europeu esclareceu que o conceito de instituição se estende a todas as atividades reais e efetivas – ainda que as menores, realizadas por meio de instituições estabilizadoras. Ali se estabeleceu um conceito flexível e informal, especialmente para empresas especializadas na prestação de serviços pela Internet:

> 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

[14] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 226.

> especialmente para as empresas que se dedicam a oferecer serviços exclusivamente na Internet.[15]

Além disso, de acordo com os termos do Regulamento, a localização do tratamento de dados pessoais é irrelevante se a agência responsável estiver localizada na União Europeia. Dada a evolução da Internet, os novos regulamentos extremamente relevantes.

Por exemplo, atinge empresas e entidades responsáveis pelo tratamento de dados utilizando computação em nuvem, ou seja, fazem uso de arranjos que disponibilizam recursos computacionais de forma flexível e independente de localização, permitindo alocação rápida e ininterrupta de recursos sob demanda.[16]

Não obstante, apesar dos elementos extraterritoriais do GDPR e do possível impacto ou eventual conflito de leis de regulamentos europeus no ordenamento jurídico brasileiro, resta observar o possível impacto relacionado à transferência internacional de dados pessoais, (Artigos 44 a 50 do GDPR).

Do ponto de vista analítico, a transferência transfronteiriça de dados pessoais envolve pelo menos três operações de tratamento: (i) a operação de fornecimento de informações pessoais ao agente ou operador responsável (transmissor) – ou seja, a coleta de dados ou (ii) o cedente transfere essas informações para um destinatário localizado ou residente em um país estrangeiro; (iii) o processamento do destinatário de dados pessoais em sua instituição localizada em um terceiro país (ou seja, armazenamento em um banco de dados).[17]

Essencialmente, a regra está enraizada em um modelo geográfico que regula o fluxo de dados através das fronteiras, pois é "projetado para evitar riscos decorrentes dos países ou locais para os quais os dados são transferidos".[18] A Comissão Europeia é responsável pelo nível de proteção em países terceiros, que é analisado e uma decisão de adequação que é emitida com base nos critérios estabelecidos no art. Artigo 45.º, n.º 2, do Regulamento, pelo que, se tal

[15] EUROPEAN COURT OF JUSTICE. Acórdão de 1º de outubro de 2015, Weltimmo, C-230/14, ECLI:EU:C:2015:639.

[16] MILLARD, Christopher. Cloud Computing Law. Oxford: Oxford University Press, 2013. p. 78.

[17] 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. p. 214.

[18] 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. p. 20.

decisão for tomada – sujeita a revisão de quatro anos – a transferência internacional de dados não carece de autorização prévia e específica.

Por esses motivos, após as alterações promovidas pela Lei nº 13.853/2019, para atender ao disposto no GDPR e na própria Lei Geral de Proteção de Dados, a relevância da forma de analisar a legislação brasileira criou a Autoridade Nacional de Proteção de Dados e questionou a forma como foi implementado se afetará a validade do acordo de livre comércio entre o MERCOSUL e a UE. Antes que isso aconteça, no entanto, alguns esclarecimentos sobre o funcionamento das autoridades europeias de proteção de dados são necessários sob os auspícios do GDPR.

1.2. A autoridade de proteção de dados na estrutura da GDPR.

A Autoridade de Controle – ou Autoridade de Supervisão – é uma entidade autônoma do sistema político nacional de cada Estado membro do Grupo Europeu que regula e implementa o artigo 20.º do Regulamento Geral de Proteção de Dados. Destaca-se que este órgão foi criado pela Diretiva 46/95/CE e regulamentado por alguns países (considerando que até 2016 a legislação de proteção de dados era facultativa nos países deste bloco.

De acordo com o artigo 51 do GDPR, os estados membros da UE podem designar uma ou mais autoridades públicas independentes ou autoridades de proteção de dados (DPAs) para monitorar e aplicar o GDPR. As regras sublinham o papel das autoridades na proteção dos direitos e liberdades fundamentais das pessoas no que diz respeito ao tratamento de dados, para além da livre circulação desses dados na UE. Também destaca a necessidade de cooperação entre as DPAs para melhor aplicar o GDPR em todos os estados membros.[19]

Dito isso, Philip Schütz entende que, para melhor caracterizar a autoridade controladora, ela deve ser vista sob a ótica de uma autoridade reguladora independente (IRA), assim definida:

> The IRA can be defined as "a public-law body with its own powers and responsibilities, which is organizationally separate from departments and is neither

[19] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 227.

> directly elected nor governed by elected officials. As the name implies, independence from government intervention plays a role in the design of the IRA. key role.[20]

Ou seja, em essência, esse tipo de "agência" (não há termo melhor em assuntos administrativos) deve ser completamente independente dos poderes públicos – executivo, legislativo e judiciário – para cumprir fielmente suas obrigações legais, uma vez que a sua função principal é fiscalizar o tratamento dos seus dados.

Na mesma linha de raciocínio, a DPA deve seguir os mesmos rigores da IRA, Conforme Define o Mesmo Author[21]. Das definições dadas, pode-se concluir que a característica central que uma autoridade controladora deve apresentar é a independência no exercício de suas funções. Nesse sentido, Gilardi[22] desenvolveu um índice para compreender a independência formal do IRA, composto por quatro indicadores, a saber: autoridade fiscalizadora.

No que diz respeito ao campo comercial, que também é objeto deste trabalho, para fins de vigência do Acordo de Livre Comércio firmado entre os representantes da UE e do MERCOSUL, cabe destacar que o Encarregado de Proteção de Dados ("DPO") não se limita ao órgão nacional de serviço público, pois o RGPD também estipula que as empresas que processam dados, especialmente em grande escala, podem nomear um DPO, conforme art. Artigos 3725 e 3826 GDPR.

Então, o que se tentou demonstrar até agora é que a independência é um elemento central do bom funcionamento dos controles de proteção de dados, que por sua vez é um pilar fundamental da estrutura organizacional criada para impedir a existência de perfis reais de varejo que existiam anteriormente. O futuro das relações comerciais, especialmente aquelas com grandes fluxos de dados pessoais, passa pelo fiel cumprimento da legislação nesta área para promover um ambiente de troca seguro, comprometido com o que hoje é considerado um direito fundamental – a proteção dos dados e a privacidade.

---

[20] 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. p. 5-6.

[21] Idem. p. 2.

[22] GILARDI, Fabrizio. Policy credibility and delegation to independent regulatory agencies: a comparative empirical analysis. Journal of European Public Policy, 9, n. 6, 2002. p. 880.

2. A proteção de dados na América Latina.

Além do Brasil, vários países possuem legislação de proteção de dados na América Latina, como Chile, Argentina, Uruguai e Colômbia. Em todos os casos, a proteção dos direitos dos titulares dos dados e o armazenamento e transferência de dados e de especial interesse, mas nem todos os regulamentos se referem especificamente à aplicação territorial, pelo que o âmbito da lei é aberto, em comparação com o RGPD para os seguintes propósitos. Esta é a parte que será exposta.

A Lei Chilena de Proteção de Dados, Ley nº 19.62829, de 18 de agosto de 1999, *Ministerio Secretaría General de la Presidencia* (“*Ley sobre Protección de la Vida Privada*” ou “LPVP”) foi o primeiro regulamento sobre proteção de dados. A América Latina, como outros países, estabeleceu parâmetros para o tratamento de dados pessoais e garante ao titular o direito de acesso às informações detidas por qualquer pessoa jurídica ou física, para corrigi-las ou excluí-las caso o armazenamento não atenda aos requisitos da lei ou a finalização do tratamento.

Nos demais países citados estabelecem parâmetros semelhantes de proteção de dados, alterando alguns aspectos principiológicos da proteção de dados. Na Argentina, por exemplo, a Ley nº 25.326 proíbe qualquer tipo de transferência de dados internacionais para países que não possuam uma legislação “adequada”, sem que haja autorização específica e expressa do titular. No Uruguai, a Ley nº 18.331, o grande destaque é a possibilidade de aplicação da penalidade de “clausura da base de dados”.

No Brasil, foi promulgada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula as operações de tratamento de dados pessoais, seja por meio digital ou não, seja na Internet ou fora dela, e abrange questões como os direitos dos titulares dos dados, as obrigações dos agentes de tratamento e controladores de dados, parâmetros de segurança da informação, transferências internacionais de dados , etc., e até mesmo instruções de fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD). Portanto, o Brasil está incluído no grupo de países da América Latina com Lei Geral de Proteção de Dados.

Além disso, em nível latino-americano, destaca-se o "Padrão Nacional Ibero-Americano de Proteção de Dados", aprovado pela Rede Ibero-Americana de Proteção de Dados (RIPD ou Rede) para atingir objetivos específicos.

Todas as entidades que a compõem e um acordo adotado na 25ª Conferência Ibero-Americana de Chefes de Estado e de Governo, realizada na Colômbia de 28 a 29 de outubro de 2016, exigindo que a rede desenvolva e proteja os dados pessoais Proposta de cooperação efetiva com privacidade, alterando as normas estabelecidas no documento "RIPD 2020".

2.1. Breve exposição sobre as características gerais das autoridades nacionais de proteção de dados na América Latina.

Atualmente vivemos em uma sociedade onde os dados são cada vez mais importantes, exigindo regras claras e transparência sobre como os dados são tratados e manipulados, coletados e armazenados, compartilhados e descartados. Nesse contexto, as leis de proteção de dados e, em última instância, as autoridades nacionais de proteção de dados trazem a confiança e a previsibilidade necessárias para a transformação digital sustentável.[23]

Não há, na América Latina, ao contrário do que foi destacado na estrutura da UE, um padrão estrutural ou de atuação das Autoridades Nacionais de Proteção de Dados. No Uruguai, a Autoridade possui a maior autonomia técnica, uma vez que pode realizar todas as ações necessárias para o cumprimento dos objetivos da lei.

Na Argentina, a estrutura de proteção de dados garante que a autoridade não sofra riscos de "ingerências hierárquicas e menores possibilidades para investigar e sancionar as infrações do poder público".[24]

A Lei de Proteção de Dados Pessoais da Colômbia prevê que as atividades inerentes ao órgão de controle serão controladas pela então administração pública federal. A grande crítica à estrutura da Colômbia, é que se permite que o Presidente nomeie para os cargos da Autoridade de Proteção de Dados, o que pode significar interferência política.[25]

[23] GUTIERREZ, apud. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 400.

[24] 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. p. 36.

[25] Idem. p. 22.

No Brasil, a estrutura inicial da Autoridade Nacional de Proteção de Dados não foi vista no cenário internacional com bons olhos, pois foi criada como órgão da administração pública federal direta, integrante da Presidência da República. No entanto, foi publicada em 14 de junho de 2022 a Medida Provisória nº 1.124/2022, que altera a LGPD para transformar a natureza jurídica da Autoridade Nacional de Proteção de Dados para uma autarquia especial, com patrimônio próprio e plena autonomia (inclusive administrativa e orçamentária) para o desempenho de suas funções e competências.

Diante desta situação, e tendo apresentado as principais características do GDPR e a principal legislação de proteção de dados na América Latina, inclusive sobre as autoridades controladoras, uma análise do acordo de livre comércio firmado entre a UE e o MERCOSUL e sua efetividade. estrutura da ANPD, estabelecer relações comerciais com o Brasil.

3. O acordo de livre comercio entre a União Europeia e o Mercosul.

Em 28 de junho de 2019, foi ratificado o acordo de associação do Mercosul com a UE 58, que visa promover o livre comércio baseado em regras e mutuamente benéfico. O novo quadro comercial – parte de um vasto acordo conjunto entre as duas regiões – apoiará parcerias políticas e econômicas estratégicas e fornecerá apoio ao crescimento sustentável, respeito ao meio ambiente, proteção ao consumidor e setores econômicos sensíveis para ambas as partes.

O acordo é significativo em todo o mundo; o MERCOSUL e a UE juntos representam 25% do PIB da economia mundial, o equivalente a 19 trilhões de euros, e um mercado consumidor de 773 milhões de pessoas. A UE é atualmente o segundo maior parceiro comercial do MERCOSUL, depois da China. Além disso, o MERCOSUL é o oitavo maior parceiro extrarregional da UE.

Segundo a Comissão Europeia, em 2018, o comércio bilateral de bens atingiu 88 mil milhões de euros e o comércio de serviços atingiu 34 mil milhões de euros, num total de 122 mil milhões de euros.[26]

[26] DOMINGUES, Juliana Oliveira; MONTENEGRO, Adriane Takahara. Acordo de Associação entre o Mercosul e a União Europeia. Jota, 1º ago. 2019.

Após as isenções do acordo, 92% das importações do MERCOSUL e 95% das linhas tarifárias entrarão na UE com isenção de impostos. Rotas com desoneração tarifária parcial (cotas, preços de importação e preferências fixas), as cotações europeias respondem por 99% dos volumes de comércio. Por sua vez, o MERCOSUL liberalizará 91% das importações originárias da UE e 91% das linhas tarifárias seguindo as isenções previstas no acordo.[27] Diante disso, espera-se que as exportações para a UE aumentem em quase US$ 100 bilhões até 2035, pois as tarifas e as importações não serão mais cobradas.[28]

Assim, o avanço político e econômico dos blocos em questão representados por este acordo é evidente, porém, devido ao princípio da extraterritorialidade, as partes relevantes da Convenção são normas exigidas para proteção de dados, conforme descrito em outro lugar. Com isso em mente, o Acordo de Livre Comércio aborda questões de proteção de dados em cinco áreas do material fornecido pelo Itamaraty, a saber: (i) comércio de mercadorias, (ii) facilitação aduaneira e comercial, (iii) comércio de serviços e (iv) Protocolo aduaneiro sobre Assistência Administrativa Mútua em Assuntos e (v) Medidas Bilaterais de Segurança. Portanto, alguns pontos relacionados a eles serão agora apontados.

Com relação à documentação e requisitos de dados, foi determinado que, no que diz respeito ao uso de informações técnicas, as partes devem emitir declarações aduaneiras e, sempre que possível, demonstrar o cumprimento de outros requisitos de dados para remessas de importação e exportação submetidas eletronicamente para formatar e facilitar seus respectivos comerciantes

Troca eletrônica de dados entre autoridades reguladoras e outras agências relacionadas ao comércio. Além disso, no caso dos serviços postais, o acordo especifica "requisitos essenciais", ou seja, razões gerais não econômicas para impor condições à prestação de serviços postais, que podem incluir confidencialidade, comunicações, transporte de mercadorias perigosas, como segurança cibernética, proteção e planejamento regional.

O Protocolo de Assistência Administrativa Mútua em Matéria Aduaneira define, de forma muito relevante, "dados pessoais" como toda a informação relativa a qualquer pessoa singular ou, quando a lei das partes assim o preveja, a uma pessoa coletiva (ver artigo 1.º, "f ");

[27] Disponível em: https://www.gov.br/mre/images/2019/2019_07_03_-_Resumo_Acordo_Mercosul_UE.pdf acessado em 29/07/2022.

[28] DOMINGUES, Juliana Oliveira; MONTENEGRO, Adriane Takahara. Acordo de Associação entre o Mercosul e a União Europeia. Jota, 1º ago. 2019.

portanto, apenas os dados pessoais podem ser trocados se o destinatário se comprometer a proteger esses dados da maneira que a outra parte considerar adequada.

Se as informações fornecidas exigirem um certo nível de proteção, elas devem ser especificadas pela autoridade que as fornece. A parte que utiliza os dados pessoais deve comunicar por escrito a finalidade da utilização da informação e os resultados obtidos a pedido do fornecedor. Não bastando, o item 6 afirma que em hipótese alguma os dados pessoais devem estar relacionados à origem racial, opiniões políticas, crenças, saúde e orientação sexual.

Quanto às medidas de segurança bilaterais, o período de coleta de dados para investigações de lesões geralmente deve ser de pelo menos 30 a 6 meses e terminar assim que o pedido for apresentado.

Da mesma forma, quando as informações relativas à produção, capacidade de produção, emprego, salários, vendas domésticas e valor forem fornecidas sob condições confidenciais, a autoridade investigadora deve garantir que resumos materiais não confidenciais divulguem pelo menos dados agregados ou, no caso de divulgação, Dados agregados que colocam em risco a confidencialidade dos dados da empresa, indexados a cada 12 meses de investigação para garantir direitos de defesa adequados às partes interessadas.

De acordo com o artigo 13, em relação à implementação do Protocolo, a cláusula foi encerrada, afirmando que o Protocolo deve ser aplicado "tendo em conta as respectivas leis e regulamentos, especialmente a proteção de dados pessoais".

No entanto, considerando todas as questões que foram levantadas, a questão mais importante é: Dada a forma como a Autoridade Nacional de Proteção de Dados brasileira foi criada, ela atende ao nível de equivalência exigido pela UE?

De antemão, vale lembrar que, como aponta Mendes, a LGPD é inspirada no conceito de modelo europeu de proteção de dados amparado pela Convenção de Proteção de Dados 2016/679 da Comissão Europeia.

> 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.[29]

[29] 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. p. 187.

Assim, será mesmo que a atual estrutura da Autoridade Nacional de Proteção de Dados Brasileira comporta adequação aos requisitos do acordo realizado entre os blocos? Na estrutura inicial, quando se vinculava ao Governo Federal, podia-se afirmar que não. Mesmo assim, com a recente alteração, haveria toda a autonomia como autarquia especial?

A pergunta foi formulada pelo seguinte motivo: Na maioria dos quadros regulamentares de proteção de dados, a autoridade de proteção de dados é, na maioria dos casos, um dos seus principais pilares, ou seja, como parte integrante das técnicas legislativas utilizadas para abordar questões de proteção de dados.

Portanto, de acordo com os termos do GDPR, para a validade de um acordo de livre comércio, e contrariamente ao disposto na LGPD, uma autoridade funcional de proteção de dados deve ser "uma entidade ou agência pública, dotada de substancial independência do governo, caracterizada por sua organização, financeira e autonomia contábil e contábil, falta de controle e submissão ao poder executivo".[30]

Considerações finais.

Tomadas em conjunto, as hipóteses levantadas são respondidas, uma vez que a legislação da UE e da América Latina regula a proteção de dados pessoais por mais tempo e mais profundamente que o Brasil. Isso significa que, embora o Brasil tenha um importante histórico regulatório de proteção e privacidade de dados, como a Lei de Cidadania na Internet e a Lei de Acesso à Informação, a LGPD é uma lei geral e, como tal, precisa ser regulamentada em várias frentes.

Portanto, é inegável que a LGPD representa um marco na garantia do Brasil à privacidade e proteção dos dados dos cidadãos. Além de proteger as informações pessoais de quem usa a internet e a divulgação diária de seus dados devido às práticas do dia a dia, principalmente durante a pandemia de Covid-1973, a nova legislação ajudará e já está ajudando a melhorar a competitividade dos empresas estrangeiras - também pela assinatura de

[30] CARINGELLA, Roberto Garofolo Francesco. Le autoritá indipendenti. Napoli: Simoni, 2000. p. 10.

convenções como o Tratado de Livre Comércio entre Mercosul e União Européia - obrigando-as a operar em condições adequadas ou comparáveis às empregadas nos mercados mais exigentes do mundo.

Portanto, outras conclusões só podem ser tiradas se as regras e diretrizes não relacionadas à proteção de dados forem discutidas e elaboradas com a participação dos diversos setores da sociedade afetados, especialmente as autoridades de supervisão direta.

Ou seja, em tempos de transformação tecnológica como este, público, privado e sociedade civil devem trabalhar juntos para aderir e aplicar fielmente a LGPD para fortalecer as relações comerciais atuais e futuras, em um ambiente quase seguro. Portanto, é necessária uma mudança real na cultura corporativa e organizacional.

Mesmo assim, considernado os fatores expostos neste artigo, apenas se poderá afirmar que o Mercosul e, especialmente o Brasil, estará completamente adequado com as diretrizes do RGPD, quando, de fato, houver plena autonomia da ANPD.

A transformação da ANPD em autarquia representa um avanço para o sistema de proteção de dados do Brasil, pois a agência ganha autonomia para alocar recursos e priorizar agendas. Com isso, há mais flexibilidade na regulamentação de diversos temas abordados pela LGPD, que ainda carecem de maiores esclarecimentos da sociedade civil. Com isso, espera-se que as autoridades tomem ações mais rápidas e abrangentes para investigar e reprimir as infrações à LGPD, com possíveis sanções administrativas, uma vez que a ANPD finalmente regular as sanções para questões de dosimetria.

Além disso, a separação direta do Presidente da República permite fortalecer a autonomia técnica e decisória da ANPD, aumentando a segurança jurídica da aplicação da LGPD. Ter uma autoridade verdadeiramente autônoma alinha o Brasil às melhores práticas internacionais de proteção de dados pessoais, aumentando assim sua credibilidade no assunto.

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.

BECK, Ulrich, **A metamorfose do mundo: novos conceitos para uma nova realidade**. (Trad.) Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018.

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.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. 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.

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.

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.

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.

EUROPEAN COURT OF JUSTICE. **Acórdão de 9 de março de 2010**, European Commission v. Federal Republic of Germany, C-518/07.

EUROPEAN COURT OF JUSTICE. **Acórdão de 1º de outubro de 2015**, Weltimmo, C-230/14, ECLI:EU:C:2015:639.

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.

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.

GABEL, Detlev; HICKMAN, Tim. **New EU Guidelines on Data Protection Officers**. White & Case, [s.l], 16 jan. 2017.

GILARDI, Fabrizio. **Policy credibility and delegation to independent regulatory agencies: a comparative empirical analysis**. Journal of European Public Policy, 9, n. 6, 2002.

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.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. Policy Paper – **Transferência Internacional de Dados no PL 5.276/2016**. Belo Horizonte: IRIS, 2017.

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.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **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.

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

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.

UNIÃO EUROPEIA. **Court of Justice of European Union. Grand Chamber.** Case C-518/07, European Comission v. Federal Republico f Germany. Luxemburgo, 9 mar. 2010.

UNIÃO EUROPEIA. **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.

URUGUAY. **Ley nº 18.331, de 11 de agosto de 2008**. Centro de Información Oficial, Montevideo.

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