UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO

MÁRTIN MARKS SZINVELSKI

O DIREITO À PROTEÇÃO DE DADOS NA SOCIEDADE EM REDE: A PERSPECTIVA COMPARADA ENTRE A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E A UNIDADE REGULADORA E CONTROLADORA DOS DADOS PESSOAIS (URCDP) DO URUGUAI

São Leopoldo
2021

MÁRTIN MARKS SZINVELSKI

O DIREITO À PROTEÇÃO DE DADOS NA SOCIEDADE EM REDE: A PERSPECTIVA COMPARADA ENTRE A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E A UNIDADE REGULADORA E CONTROLADORA DOS DADOS PESSOAIS (URCDP) DO URUGUAI

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

Área de concentração: Direito Público

Orientadora: Profa. Dra Têmis Limberger

São Leopoldo

2021

S998d Szinvelski, Mártin Marks

O direito à proteção de dados na sociedade em rede: a perspectiva comparada entre a Autoridade Nacional de Proteção de Dados (ANPD) e a Unidade Reguladora e Controladora dos Dados Pessoais (URCDP) do Uruguai. / Mártin Marks Szinvelski -- 2021.

161 f. ; 30cm.

Dissertação (Mestrado em Direito) -- Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, 2021.

Orientadora: Profa. Dra. Têmis Limberger.

1. Direito digital. 2. Autoridade Nacional de Proteção de Dados. 3. Unidade Reguladora e Controladora de Dados Pessoais (URCDP). 4. Agências Reguladoras. 5. Sociedade da informação. I. Título. II. Limberger, Têmis.

CDU 34:004.738.5

Catalogação na Publicação: Bibliotecário Eliete Mari Doncato Brasil - CRB 10/1184

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
NÍVEL MESTRADO

A dissertação intitulada: **"O DIREITO À PROTEÇÃO DE DADOS NA SOCIEDADE EM REDE: A PERSPECTIVA COMPARADA ENTRE A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E A UNIDADE REGULADORA E CONTROLADORA DOS DADOS PESSOAIS (URCDP) DO URUGUAI"** elaborada pelo mestrando **Mártin Marks Szinvelski,** foi julgada adequada e aprovada por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO.

São Leopoldo, 30 de março de 2021.

Prof. Dr. **Anderson Vichinkeski Teixeira**
Coordenador do Programa de Pós-Graduação em Direito.

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dra. Têmis Limberger *Participação por Webconferência*

Membro: Dra. Laura Nahabetiàn Brunet *Participação por Webconferência*

Membro: Dr. Fabiano Menke *Participação por Webconferência*

Membro: Dr. Wilson Engelmann *Participação por Webconferência*

AGRADECIMENTO À COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL EM NÍVEL SUPERIOR (CAPES)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Com muita gratidão, registro o apoio financeiro concedido pela Coordenação de Aperfeiçoamento de Pessoal em Nível Superior (CAPES), por meio do Programa de Excelência Acadêmica (PROEX), cujo investimento em aprimoramento acadêmico – colhido do esforço social dos contribuintes brasileiros – destina-se ao retorno teórico e prático da investigação científica, dos quais participam a emancipação do ser pela liberdade de pensamento e a apresentação dos resultados de propostas de avanços nacionais em ciência, tecnologia e inovação, que não excluem o Direito e as ciências da administração do Estado. Os resultados do investimento puderam ser verificados ao longo do curso de Mestrado em Direito, realizado no biênio 2019-2020, no Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos, com produção científica, premiações e, acima de tudo, o exercício da reflexão propositiva, identificada pela necessidade de avançar, para além da crítica, à contribuição; para além da desconstrução, à reconstrução de modelos aptos a serem adequados à realidade brasileira. Em contraste com eventuais produções antagônicas, sobre temas conectados à pesquisa desenvolvida, ao menos, consigno que me esforcei, nos limites de minhas finitudes intelectuais.

AGRADECIMENTOS

A conclusão do Mestrado em Direito, no Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos, realizado no biênio 2019-2020, é de extrema satisfação pessoal, individual e familiar. Haveria, nesse sentido, uma lista de pessoas que poderiam ser elencadas e letras dedicadas à exaltação de suas contribuições. Contudo, aqueles que me conhecem, reconhecem a minha gratidão, essa que não pode ser expressa em palavras, pois assim como o universo, é infinita a mente humana, de modo que estaria, sempre, a faltar palavras à manifestação de meus agradecimentos, especialmente, aos meus pais (Ildo Mario e Valkíria).

Cabe, portanto, a tarefa de distribuir minhas as *menções* às pessoas que muito me orgulham, a começar pela profunda satisfação em ter a Professora Têmis Limberger como professora orientadora. Compreensiva, dedicada, respeitosa e comprometida com a valorização do Direito Administrativo, campo que jamais poderia ser negligenciado, especialmente em tempos de hiperinformação, do incremento e aceleração de novas relações sociojurídicas, cada vez mais mediadas por mecanismos informatizados, baseados em tecnologias que desafiam o nível de intervenção ética e técnica que os profissionais que atuam, primordialmente, com o Direito devem desempenhar.

De valor notar a honra de ter sido *aluno-seguidor* de duas personalidades jurídicas do Rio Grande do Sul, cujo reconhecimento e repercussão acadêmica são internacionais. Cito as figuras dos professores Leonel Severo Rocha, responsável pela sedutora difusão do conhecimento associado à Teoria do Direito e dos Sistemas Sociais e pela incrível conservação da jovialidade de outrora; e Lenio Luiz Streck, o *mestre* de muitos, eterna inspiração para outros, polêmico como os gigantes, mas, em convergência, o grande propagador de uma hermenêutica filosófica *para* o Direito, ao tom de sugerir que as correntes da linguagem nunca se afastarão da *applicattio*.

Ao Professor Wilson Engelmann, pesquisador e professor dedicado ao estudo das novas tecnologias e da profunda necessidade de se (re)pensar as estruturas de regulação à forma do tempo contemporâneo, congregando as novidades da ciência nanotecnológica e a interdisciplinaridade. Considero, de igual forma, como relevantes à conclusão da investigação, as sugestões da Professora Laura Brunet, da Universidade da República, do Uruguai, as quais se mostraram valorosas.

Agradeço aos excelentes professores que compõem o Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos. Não poderia deixar de realizar um

destaque ao Professor Anderson Vichinkeski Teixeira, pela cordialidade que nos faz reconhecer um jurista equilibrado; ao Professor Darci Guimarães Ribeiro, advogado combativo e brilhante professor. A cara Professora Jânia Maria Lopes Saldanha, de grande cultura e de postura favorável à implementação ética dos direitos humanos, pautada pela *visão cosmopolita envolvente e vinculante* dos setores públicos e privados.

Deixo meus cumprimentos, aos colegas do Grupo de Pesquisa CNPq *Estado e Novas Tecnologias* e *Cibertransparência*, do Mestrado e do Doutorado e para os muitos conhecidos que fiz nessa trajetória. Gostaria de destacar, por fim, o empenho e a prestatividade dos funcionários da Universidade do Vale do Rio dos Sinos, em especial, aos da Secretaria do Programa de Pós-Graduação em Direito.

Em derradeiro agradecimento, saliento o esforço empreendido pelo Ministério de Ciência e Tecnologia na pessoa do Ministro Marcos Cesar Pontes pela reorientação rumo ao progresso científico-tecnológico e ao desenvolvimento nacional.

“[...] paz é amizade: e não há boa sólida amizade, que não se faça de afeto e respeito; e não é possível respeito mútuo, quando não existe o respeito próprio, que nasce da consciência da própria força. [...]. O Uruguai é lindo e admirável, nos limites do seu pequeno território e na curta idade de sua vida de nação autônoma. O trabalho e a justiça, a força e a graça, o pensamento e a beleza, o heroísmo e o ideal animam esse torrão bendito. Montevidéu, que resume e retrata todo o país, é ao mesmo tempo um ninho e um baluarte, um sorriso e uma energia. Aquela metrópole clara e alegre, inteligente e perfumada, cheia de frescos jardins e deliciosas vivendas, e famosa pela incomparável formosura de suas flores e de suas mulheres, é aquele mesmo reduto da liberdade e da bravura, refúgio dos oprimidos, que, durante mais de nove anos, resistiu ao cerco de uma tirania”.

BILAC, Olavo. *A defesa nacional (discursos)*. Rio de Janeiro: Liga da Defesa Nacional, 1917. p. 121-122.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) apresenta-se como relevante campo de estudo na sociedade em rede. Com a entrada em vigência da legislação, desafios de adequação surgiram e dependem da atuação da Autoridade Nacional de Proteção de Dados (ANPD), especialmente na promoção e regulamentação de mecanismos de proteção que assumam caráter de compatibilidade com o Regulamento Geral de Proteção de Dados (RGPD), adotado em sede europeia. Nesse sentido, mostra-se relevante analisar como ocorreu o processo de estruturação da proteção de dados no Uruguai, que é reconhecido internacionalmente como "adequado" e apto a receber transferências de dados pessoais por meios informatizados. Esse caminho dependeu da atuação da Unidade Reguladora e Controladora de Dados Pessoais (URCDP), órgão regulador de mesma função que a ANPD. Partindo do método comparado, busca-se estabelecer aproximações e dissonâncias entre as autoridades, de forma a compreender os fatores que determinam a atuação do órgão regulador uruguaio ajustado às necessidades de adequação europeia, mas aptas a serem incorporadas com maior aceitabilidade pelo Brasil. Como resultados da pesquisa, verifica-se a existência de aproximações como o mandato dos dirigentes, poderes normativos e de supervisão próprios de uma agência reguladora desvinculada de subordinações e ingerências, embora, no momento, tanto a ANPD quanto URCDP, não possuam personalidade jurídica própria. Foram analisadas as resoluções que permitiram a especificação da adequação uruguaia ao RGPD e dos mecanismos que impedem a identificação dos titulares dos dados adotados pela URCDP, de modo que essa atuação promove a adequação no plano concreto, efetivando a normatividade das regulamentações e dos *stardards* internacionais e regionais. A análise da perspectiva de adoção de selos de qualidade, importante instrumento de conformidade com as melhores técnicas de proteção de dados revelou que esses desempenham função real de proteção aos titulares dos dados. Por fim, em vista do contraste e do sucesso da experiência uruguaia, promove-se a ideia de que a existência da autoridade é passo fundamental para a consolidação da proteção de dados no Brasil e que existem mecanismos previstos na legislação que não impedem a promoção e o desempenho das atividades da ANPD de maneira técnica e imparcial.

Palavras-chave: Autoridade Nacional de Proteção de Dados. Unidade Reguladora e Controladora de Dados Pessoais (URCDP). Agências Reguladoras. Sociedade da Informação.

ABSTRACT

The General Data Protection Law (LGPD) is presented as a relevant field of study in network society. With the legislation entering into force, adequacy challenges have arisen and depend on the work of the National Data Protection Authority (ANPD), especially in the promotion and regulation of protection mechanisms that assume a character of compatibility with the General Data Protection Regulation (GDPR), adopted in Europe. In this sense, it is relevant to analyze how the data-protection structuring process took place in Uruguay, which is internationally recognized as "adequate" and able to receive transfers of personal data by computerized means. This path depended on the performance of the Personal Data Regulatory and Controlling Unit (URCDP), a regulatory body with the same function as the ANPD. Starting from the comparative method, we seek to establish approximations and dissonances between the authorities to understand the factors that determine the performance of the Uruguayan regulatory body adjusted to the needs of European adequacy, but able to be incorporated with greater acceptability by Brazil. As a result of the research, it is possible to verify the existence of approximations such as the mandate of the leaders, as well as normative and supervisory powers that are proper to a regulatory agency unrelated to subordinations and interference, although, at the moment, both the ANPD and URCDP lack their own legal personality. The resolutions that allowed the specification of the Uruguayan adequacy to the GDPR and the mechanisms that prevent the identification of the data holders adopted by the URCDP were analyzed, so that this action promotes the adequacy in the concrete plan, making the regulation effective in international and regional standards. The analysis of the perspective of adopting quality seals, an important instrument of compliance with the best data protection techniques and suggested as a mechanism to be strengthened by the ANPD and URCDP, revealed that they perform the function of a real protection mechanism for data subjects. Finally, in view of the contrast and success of the Uruguayan experience, we promote the idea that the existence of authority is fundamental for the consolidation of data protection in Brazil and that there are foreseen mechanisms in the legislation that do not prevent the promotion and performance of ANPD activities in a technical and impartial manner.

Keywords: National Data Protection Authority. Regulatory and Controlling Unit of Personal Data (URCDP). Regulatory agencies. Information Society.

SUMÁRIO

1 INTRODUÇÃO

O advento da Lei Geral de Proteção de Dados (LGPD) traz um novo campo de pesquisa nas áreas afetas à privacidade e à proteção de dados. Mas não só isso: coloca em cena as possibilidades de uma regulação estatal voltada à prevenção de vazamentos de dados e à violação de direitos. A tendência é identificada no Regulamento de Proteção de Dados da União Europeia (RGPD), em vigor desde 2018, modelo adotado como norte para formulação da lei brasileira em debate, especialmente como fonte de inspiração após a reformulação da Diretiva Europeia de Proteção de Dados editada em 1995. Com vistas a aproveitar a escassa doutrina disponível em torno das autoridades administrativas responsáveis pela fiscalização da proteção de dados no Brasil, e diante da função destacada desempenhada por elas no exterior, procura-se abordar a temática da proteção de dados e dos instrumentos próprios do Direito Administrativo, aptos a fomentar a prevenção de danos aos direitos fundamentais da pessoa.

Nessa linha de ideias, o estudo das autoridades europeias encontra farto campo de pesquisa na doutrina internacional, mas poucos estudos nacionais. Esse espaço será ocupado rapidamente, pela simples transportação dos estudos europeus à doutrina brasileira. Com efeito, há diferenças importantes na comparação com o modelo de agências reguladoras, em razão dos diferentes níveis de independência adotados. Nesse sentido, pouco se sabe como, no Uruguai, a Unidade Reguladora e de Controle de Dados Pessoais (URCDP) atua e está organizada, qual o modelo de regulação adotado e a forma como desempenha as atividades. A compreensão do modelo uruguaio assume relevância, em razão do reconhecimento pela Comissão Europeia de que o país possui níveis adequados de proteção de dados pessoais.

O objetivo do presente trabalho é estabelecer linhas comparativas entre a estruturação da URCDP e o quadro normativo de estruturação da Autoridade Nacional de Proteção de Dados (ANPD), no âmbito das transformações vividas pela sociedade contemporânea e da Administração Pública brasileira. A escolha da autoridade uruguaia, nesse sentido, mostra-se adequada porquanto ela permite compreender o motivo pelo qual uma autoridade de proteção de dados latino-americana é reconhecida como órgão que garante a proteção de direitos fundamentais (direito à proteção de dados pessoais), ao mesmo tempo em que possui uma estrutura vinculada à Presidência da República daquele país (como é a ANPD brasileira) e características do Direito Administrativo semelhantes ao Brasil. Nesse sentido, um ponto relevante que será analisado na dissertação será: a vinculação da Autoridade de Dados ao

Poder Executivo e a possibilidade da atuação técnica e imparcial de um órgão (entidade) que será de fundamental importância à medida que as relações em sociedade se digitalizam.

Nesse sentido, a pergunta a qual se busca responder é a seguinte: em que medida a Unidade Reguladora e de Controle de Dados Pessoais (URCDP) apresenta traços que podem ser utilizados para a consolidação da Autoridade Nacional de Proteção de Dados (ANPD) brasileira, tendo em vista que o Uruguai é reconhecido pela Comissão Europeia como país que adota níveis adequados de proteção de dados? Em razão do que foi dito, apresentamos como *hipóteses* as seguintes propostas: em caso positivo, é possível identificar traços contributivos da URCDP que permitam a estruturação da ANPD técnica e capaz de promover níveis internacionais de proteção de dados[1]. Em caso negativo, entende-se que a ausência de independência das autoridades traz efeitos sociojurídicos que podem prejudicar a proteção de dados pessoais dos cidadãos, em termos da inexistência de um nível mínimo de proteção intencionalmente validado, especialmente tendo em vista a força do Regulamento Europeu de Proteção de Dados.

A presente investigação se utiliza dos instrumentos disponíveis no Direito Comparado, partindo-se da compreensão de que a tutela de direito relativo à proteção de dados, para que seja efetiva, necessita de um órgão capaz de fiscalizar, regular e estabelecer parâmetros que permitam a tutela de direitos fundamentais no âmbito anterior à violação de direitos, dado o caráter irreversível de danos no âmbito tecnológico. Justifica-se o método porque o Regulamento Europeu de Proteção de Dados (com efeitos inspiradores na construção da LGPD) trouxe consequências que extrapolam o âmbito do direito privado e permeia uma sociedade em rede e interconectada. A possibilidade de rastreamento e identificação da pessoa por meio de esquemas informáticos ou cibernéticos de vigilância reassumiu relevância pela reconfiguração das perspectivas de análise trazidas pela violação de informações pessoais na internet combinada com o prestígio jurídico da autonomização do direito à proteção de dados ocorrida na última década e regulamentada recentemente. Em torno da discussão acerca da associação dos dados à personalidade ou ao patrimônio pessoal, segue-se um campo de trabalho vinculado à necessidade de tratamento adequado dos dados mencionados e da

[1] Nesse sentido, por meio de estudo comparativo, cogitamos que esta independência – que será "medida" com o estudo da *Unidade Reguladora e de controle de Dados Pessoais (URCDP)* – permite um ambiente de cooperação internacional entre órgãos independentes (autoridades de proteção de dados) e um ambiente regulatório nacional que permita a participação privada no desempenho de funções regulatórias. Supõe-se que a referida independência ocorrerá por meio do estabelecimento de garantias funcionais (substanciais e formais) que garantam atuação técnica, especializada e imune a influências políticas, de modo que a atuação ocorra associada à garantia da transparência do exercício das funções estatais.

possibilidade de violação objetiva dos mecanismos de proteção, por organizações privadas ou públicas.

O primeiro capítulo é direcionado a oferecer uma descrição da sociedade contemporânea, que passa a depender da progressiva conversão de momentos da vida humana em dados, por meio da vigilância, cujos efeitos atingem a regulação em proteção de dados. O segundo apresenta os quadros comparativos entre os órgãos reguladores, a ANPD, a AGESIC e URCDP. Por sua vez, o último capítulo visa compreender os mecanismos de atuação da URCDP que permitem ao Uruguai atender os *standards* de proteção de dados, como é o caso da adoção de políticas educacionais, guias e de resoluções visando a desidentificação do titular dos dados e a possibilidade de utilização de selos de qualidade em matéria de proteção de dados, como forma de estabelecer confiança nos níveis de proteção.

A progressiva demanda por manutenção de reputações faz com que organizações públicas e privadas busquem formas de estabelecer vínculos de confiança com *cidadão*. À medida que as relações sociais passam a ser digitalizadas, a demanda estende-se ao setor informático e tecnológico, especialmente ante às possíveis violações de direitos. A introdução de elementos como a responsabilidade à cultura jurídica oferece maior flexibilidade na busca por soluções para casos concretos e específicos, além de permitir a adaptação rápida às futuras mudanças tecnológicas. Todavia, a escolha implica maior incerteza jurídica para os responsáveis habituados à extensa regulação característica do modelo legal continental, seguido no Brasil. Apresenta-se, portanto, um problema de adaptação ou de transição para ordens jurídicas que tendem a convergir. O alto grau de tecnicidade das questões regulatórias e o papel crucial dos especialistas na sociedade contemporânea contribui para o fenômeno em que *standards* e os padrões comportamentais das organizações são utilizados como fonte do direito e desempenham um papel decisivo na proteção de direitos subjetivos, representando, de igual forma, um desafio às teorias regulatórias. Esse processo deve concatenar a ANPD, que deve orientar e viabilizar as possibilidades de cooperação internacional em matéria de proteção de dados.

A presente investigação possui inserção no âmbito da Linha de Pesquisa "Hermenêutica, Constituição e Concretização de Direitos", do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (UNISINOS), no sentido de buscar reconhecer a capacidade do Estado Democrático de Direito e da nova regulação brasileira em matéria de proteção de dados, no qual se insere a ANPD. De igual forma, enquadra-se nas

pesquisas coordenadas pela Professora Têmis Limberger, coordenadora do Grupo Estudos *Cibertransparência*.

2 SOCIEDADE EM REDE E O DIREITO À PROTEÇÃO DE DADOS: VISÃO DO BRASIL/URUGUAI

O período de emergência da sociedade da informação viabilizou acesso aberto e em massa a sistemas de comunicação, que, por sua vez, sustentaram transformações no plano da expansão de tecnologias, da educação, das ideias inovadoras, do combate à corrupção por meio da transparência governamental e no campo das liberdades e dos direitos[2]. Esse caminho de solidariedade e liberdade em rede foi modificado pelos episódios terroristas do início do século XXI, propulsionadores de medidas restritivas à liberdade em rede em nome da soberania e da segurança nacional. O efeito prático dessa revolução pode ser identificado no papel das informações e do conhecimento na sociedade contemporânea, como fonte de poder e de riqueza das nações ou das empresas transnacionais sediadas naqueles centros de irradiação[3].

A necessidade de pensar o Direito sob uma ótica mais aproximada da velocidade das novas tecnologias apresenta-se como ponto primeiro da abordagem prevista. No ambiente de permanente interconexão como é a internet, a proteção de direitos fundamentais ganha um espaço já definido: o ciberespaço. O conceito, embora não seja novo, assim como a noção de cibercultura introduzido por Pierre Levy[4], é necessário, especialmente no ambiente em que se tornam opacas as linhas que separavam o público do privado, o íntimo do externo e o publicável do não-publicável. Nesse novo tempo, a expressão *alguém de fora sabe alguma coisa sobre mim* torna-se mais verdadeira do que antes, nos idos tempos do boato e da fofoca das aldeias. A prova disso está nas *time-line* das diferentes (e inúmeras) redes sociais.

Assiste-se ao fim de um passado definitivo e de um futuro previsível. O encurtamento do espaço/tempo é percebido como consequência do avanço tecnológico, especialmente pelo uso da internet, que aproxima o distante, torna célere o que, antes, dependia do lapso de

---

[2] Segundo o documento oficial publicado no início do século, a "[...] sociedade da informação não é um modismo. Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico. É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infraestrutura de informações disponível. É também acentuada sua dimensão político-econômica, decorrente da contribuição da infraestrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante dimensão social, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação". BRASIL. *Sociedade da informação no Brasil*: livro verde – organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000.p.5.

[3] CASTELLS, Manuel. *Comunicación y poder*. Ciudad de México: Siglo XXI, 2012. p.53.

[4] LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999.

tempo. A instantaneidade é marca da Era Digital[5]. Nesse contexto, Pérez Luño ressalta que a internet passou a ser o "lar global", em razão das facilidades de acesso que passou a permitir[6]. No entanto, as novas tecnologias trazem consigo o desafio de proteção aos dados do cidadão, em especial pelo conteúdo econômico que possuem e, por esse motivo, pela utilidade à formação de um diagnóstico preciso da personalidade, das características pessoais e das preferências do titular dos dados[7]. Nesse passo, verifica-se que a intimidade deslocou-se de um âmbito fechado do ser para o lado diametralmente oposto, à exterioridade, no que se denominou a *socialização da intimidade*[8]. A questão "quem ocupa o papel de regulador?" trazida por Piñar-Mañas[9], referindo-se ao cenário de relacionamento entre tecnologia da informação e Direito, revela-se central no processo de aceleração da história ou de aprofundamento do ciclo de mudanças cujo símbolo é a internet[10].

Manuel Castells, sociólogo espanhol de enorme prestígio internacional, alerta que a caracterização ou descrição do tempo contemporâneo passa, ou passou (tendo em vista que a primeira obra foi editada na década de noventa), pela emergência da *Era da Informação*, entendida como período histórico em que ocorre a difusão e a globalização de uma nova estrutura social provocada pela revolução tecnológica multidimensional. O paradigma das mudanças sociais que reestruturaram o modo de produção capitalista dos anos oitenta, das administrações estatais, das organizações empresariais nacionais e transnacionais e, especialmente, do modo pelo qual ocorre a interação social pela tecnologia (mediação tecnológica). Como primeiro a usar o conceito de "sociedade em rede" para descrever as transformações no plano global, o autor procurou descrever a passagem do paradigma industrialista para o informacional o qual representaria um novo "paradigma sociotécnico"[11],

---

[5] CASTELLS, Manuel. *A Galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 8.

[6] PÉREZ LUÑO, A.. Internet y los derechos humanos. *Anuario de Derechos Humanos*. Nueva Época, Norteamérica, n. 12, p.292, dic. 2011. Disponible en: <https://revistas.ucm.es/index.php/ANDH/article/view/38107/36859>. Acesso em: 23 out. 2020.

[7] LIMBERGER, Têmis. *O direito à intimidade na era da informática*: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado Editora, 2007. p.51.

[8] LIMBERGER, Têmis. *Cibertransparência*: informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado Editora, 2016. p.60.

[9] PIÑAR MAÑAS, José Luis. Administración electrónica y protección de datos personales. *Revista Jurídica da Universidade de Santiago de Compostela*, Santiago de Compostela, n.1, p.149, 2011.

[10] Sobre o tema, afirma Pérez Luño, "(…) el momento presente, para designar el marco de nuestra convivencia se alude reiteradamente a expresiones tales como la "sociedad de la información", la "sociedad informatizada" o la "era de Internet". Para las nuevas generaciones (indignadas o no), "ya está todo en la Red". Y lo que no no merece la pena conocerse." PÉREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. *Revista Brasileira de Políticas Pública,* Brasília, DF, v.4, n.2, p.10, 2014.

[11] Pode-se dizer, nesse sentido, que o centro da análise de M. Castells possa ser sintetizada nas relações de poder e das múltiplas manifestações por ele provadas nos cidadãos, nas cidades e nos governos, já que apenas o que ou

em que a *internet* é a base material pela qual a sociedade passa a se desenvolver e que desempenhará função que, similarmente, a fábrica desempenhava no período industrial[12].

A teoria, que procura estabelecer uma abordagem interdisciplinar entre economia e sociedade, permite sustentar que os temas relacionados à "sociedade em rede", à "sociedade da informação" ou à "sociedade do conhecimento"[13], termos que tendem a indicar mesmo fenômeno, demonstram a presença ou a amplitude da informatização da sociedade[14] e do grau de entrelaçamento comunicacional que a sociedade atingiu no final do século XX e nas primeiras décadas do século XXI[15]. Nesse contexto, a informação (e os dados envolvidos) surge como matéria-prima de uma nova economia[16], sendo que as tecnologias desenvolvidas atuam no tratamento dos dados e das informações geradas por uma sociedade que intrinsecamente é produtora de informação[17]. Estima-se que, a cada segundo, cada pessoa produza cerca de um novo dado[18], o qual pode ser tratado por sistemas informatizados ou baseados em algoritmos, que pressupõe uma rede de terminais (infraestrutura física e virtual) capaz de coletar, guardar e tratar informações. Portanto, a rede é um mecanismo de flexibilização da comunicação e o canal por meio do qual a informação pode circular com velocidade e qualidade, o que acelera novos processos comunicativos.

Pode-se sustentar que há uma aparente contraposição entre os modos de produção industrial e da sociedade da informação. O que se observa no capitalismo informacional é a integração entre conhecimento e produção ou disponibilização de serviços por meio da rede. Para além do período da automação das tarefas, a sociedade contemporânea experimenta, por

---

quem o detém [o poder] alberga capacidade de modificar as instituições da sociedade com base em normas, valores e interesses espontaneamente produzidos e observar a realização concreta, ou não, daqueles valores ou princípios que serviram de base para a transformação social.

[12] SAARENPÄÄ, Ahti. Derechos Digitales. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.292.

[13] Para um outro olhar, sobre a perspectiva apontada, conferir: OLIVETTI, Miguel. Tensiones discursivas sobre la sociedad de la información, el caso de AGESIC Uruguay. *Políticas de Comunicación e Integración Económica Intercontinental*, p. 37-44, 2018.

[14] NORA, Simon; MINC, Alain. *A informatização da sociedade*. Rio de Janeiro: FGV, 1980.

[15] CASTELLS, Manuel. Internet e sociedade em rede. MORAES, D. (Org.). *Por uma outra comunicação*. Rio de Janeiro: Record, 2003. p.285-287.

[16] Convém notar que essa perspectiva já era percebida anteriormente no Brasil, como demonstra o seguinte segmento do Livro Verde, "[...] impacto positivo que a 'nova economia' pode gerar para o País depende ainda da participação do maior número possível de pessoas, organizações e regiões como usuárias ativas das redes avançadas de informação". BRASIL. *Sociedade da informação no Brasil*: livro verde – organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000.p.6.

[17] CASTELLS, M. *A era da informação: economia, sociedade e cultura:* sociedade em rede. 1 vol. São Paulo: Paz e Terra, 2011. p.53-54.

[18] MARR, Bernanrd. 20 fatos sobre a internet que você (provavelmente) não sabe. 1 out. 2015. https://forbes.com.br/fotos/2015/10/20-fatos-sobre-a-internet-que-voce-provavelmente-nao-sabe/#foto11. Acesso em 20 set. 2020.

meio da utilização tecnológica, uma utilização progressiva da rede. Por sinal, a arquitetura em rede constitui o modo principal a partir do qual a sociedade se organiza desde o plano individual até o macrossocial[19]. Na antecessora sociedade de massas ou pós-industrial, havia a ideia de que eram as organizações, comunidades, coletividades ou grupos sociais – isto é, o que se denominava de massas – que determinavam a funcionalidade social. A perspectiva de Van Dijk revela que essa estrutura transformou-se e aglutinou-se em torno da noção de rede[20].

A ideia de "meios de vida tecnológicos" ou pós-humanidade aparenta seguir um forte caminho de ascensão[21]. No início do século em curso, o pensamento sociofilosófico relativo à pluralidade de culturas ou ao multiculturalismo se associou à emergente cultura a distância, mediada por equipamentos informatizados, responsável por criar um ambiente não-linear de comunicações na sociedade, associadas à *(i)* compressão da informação, *(ii)* aceleração da produção da informação, *(iii)* profusão e difusão de informações e pela *(iv)* descontinuidade dos sistemas de comunicação em rede[22].

Anteriormente à era da informação, o conhecimento – ainda que superficial – estruturava-se por meio de metanarrativas ou conjunto de discursos seguindo uma certa visão, e permitia que algo fizesse sentido em termos de compreensão[23]. Em contraste, novo período sugere a ideia de que pequenos fragmentos de informação (dados) já são suficientes a desencadear processos socioculturais ou socioeconômicos[24]. A diminuição do tamanho dos conteúdos associada à incapacidade de estabelecer ligações entre diferentes informações (não necessariamente à sobrecarga informativa) pode desencadear um novo colorido à sociedade: o pequeno dado/informação também é relevante e capaz de produzir resultados importantes no campo social[25].

A incerteza provocada por essa abertura que permeia a informação e as diferentes interações sociais é característica marcante que não pode ser desprezada. Assume, por consequência, ares de paradoxo (contradição) ou aporias (becos sem saída): quanto mais incerteza, maior a busca por segurança e confiança, em pessoas e em sistemas. Em sua face

---

[19] MONSÁLEZ, Carlos Reusser. O que és la sociedade en red? In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.1231-1235.

[20] VAN DIJK, Jan. *The network society*. SAGE: Publications Limited, 2006. p.35.

[21] PÉREZ-LUNO, Antonio Enrique. Inteligencia artificial y posthumanismo. In: BRAVO, Alvaro S. (editor). *Derecho, Inteligencia Artificial y Nuevos Entornos Digitales*. Sevilla, 2020. p.9-12.

[22] LASH, Scott. *Critique of information*. Londres: Sage Publications, 2002. p.15.

[23] BRUSEKE, Franz Josef. Risco e contingência. *Revista Brasileira de Ciências Sociais*, São Paulo, v. 22, n. 63, p. 69-70, Feb., 2007 .

[24] MORENO, José. The economic value of information in the network society. *Observatorio*, Lisboa, v. 9, n. 2, p. 11-15, jun., 2015.

[25] TLACUILO FUENTES, Itzayana. Legal Recognition of the Digital Trade in Personal Data. Mexican Law Review, [S.l.], p. 91-97, dec. 2019.

contemporânea, vincula-se à aceleração do tempo, das informações e da resposta social (e jurídica) esperada, que não está sujeita aos trâmites legais vagarosos e está a exigir velocidade das ferramentas normativas[26].

De uma maneira geral, a humanidade evoluiu passo a passo, descobrindo novas tecnologias, novas ferramentas e novas utilidades químicas ou físicas aplicáveis ao uso humano, sem contar a capacidade de descobrir os meandros da natureza. Contudo, o tempo medido em períodos milenares, progressivamente passou a ser medido em séculos, logo em seguida, em décadas e, no atual estágio contemporâneo, em menos de uma década. A notícia publicada no jornal em um site passa a ser desatualizada, a partir do momento em que uma nova informação surge e a substitui, assim como novas descobertas científicas ou novas regulações, a ponto de nos tornarmos "hiper-históricos"[27]. Está-se diante, portanto, do *tempo da efemeridade*, um tempo que não pode ser refletido ou racionalizado com o cotejo à metanarrativa vigorante, porquanto simplesmente não existe a disponibilidade de tempo para realizar a tarefa em questão.

O que se pode notar, na sociedade contemporânea, é o fato de quem detém os dados e as informações colhidas das redes obtém uma vantagem especial nos planos do poder, da competição empresarial e da atuação governamental[28]. As plataformas de comércio eletrônico utilizam e tratam os dados dos consumidores[29] como nome, endereço, dados de cartão de crédito, sendo que muitas delas utilizam os *cooki*es (históricos das atividades do usuário na rede) para o oferecimento de produtos personalizados, o que demandará a autorização específica dos consumidores, em razão da impossibilidade jurídica da coleta e utilização sem consentimento do usuário, o que pode atingir os serviços de logística e atendimento ao cliente[30].

Nesse contexto, a grande quantidade de aplicativos, recursos tecnológicos e serviços gratuitos projetados para o entretenimento ou facilitação da vida colocam os cidadãos nessa rota, ou, no mínimo, no âmbito de uma *espécie de jogo* em que todos são chamados a participar como forma de pertencer à sociedade, cujo impulsionador é o setor privado, por

---

[26] FENWICK, Mark; KAAL, Wulf; VERMEULEN, Erik P.M. Regulation Tomorrow: What Happens When Technology Is Faster than the Law?, *American University Business Law Review*, v. 6, n. 3, p.572-573, 2017.
[27] FLORIDI, Luciano. The Rise of the MASs. In: FLORIDI, Luciano (Ed). *Protection of Information and the Right to Privacy – A New Equilibrium?*. Springer, 2014. p.96-97.
[28] BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, v. 273, p. 123-163, 2016.
[29] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*, vol. 1009, p. 173-222, nov, 2019.
[30] CATE, Fred, MAYER-SCHÖNBERGER, Victor. Notice and Consent in a World of Big Data. *International Data Privacy Law*, v.3, n.2, p.70-71, 2013.

meio de uma massiva coleta e tratamento de um novo ativo financeiro, o qual aglutina diferentes dimensões da personalidade do indivíduo (os dados pessoais) e os torna fonte de riqueza que faz imaginar ser possível um novo capitalismo. Nesse sentido, do ponto de vista do comércio em rede, a Associação Brasileira de Comércio Eletrônico (ABComm) projetou, para o ano de 2020, que o setor de *e-commerce* movimentaria o volume de R$ 106 bilhões de reais[31].A expressão monetária do poderio das empresas de tecnologia (e demais setores que coletam dados) associa-se ao valor econômico que cada usuário possui, o que, segundo levantamento da OCDE, aproxima-se de centenas de dólares, a variar conforme a atividade do consumidor em rede[32]. É nesse contexto que podemos inserir a questão do monitoramento de dados como ponto inicial da discussão, tendo em vista que o rastreio da navegação em rede pode ter utilidade comercial.

2.1 O capitalismo informacional e a necessidade de prevenção ao abuso da vigilância

O ponto que se deseja destacar reside na noção de que o capitalismo informacional é uma estrutura modificada do capitalismo industrial, mas, ainda sim, vincula-se com a noção de geração de riquezas por meio da disponibilização de produtos e serviços[33]. É informacional porque condensa a noção de conhecimento e informação como elementos impulsionadores e de dependência do avanço de sua própria estrutura, por meio do processamento da informação por mecanismos digitais e pela difusão do conhecimento[34]. É global no sentido de vincular

---

[31] ABCOMM. *Comércio eletrônico deve crescer 18% em 2020 e movimentar R$ 106 bilhões*. Disponível em: <https://abcomm.org/noticias/comercio-eletronico-deve-crescer-18-em-2020-e-movimentar-r-106-bilhoes/> Acesso em 2 dez. 2020.

[32] OCDE. Exploring the economics of personal data: a survey of methodologies for measuring monetary value. *OECD Digital Economy Papers*, n. 220, OECD Publishing, Paris. Disponível em: <http://dx.doi.org/10.1787/5k486qtxldmq-en>. Acesso 25 nov.2020. Nesse sentido, o Supervisor Europeu de Proteção de Dados, órgão independente superior na União Europeia, publicou um relatório, informando que o reconhecimento de um valor econômico aos dados pessoais não se afigurava como compatível com a ótica econômica e constitucional europeia, em razão da impossibilidade de se equiparar dados pessoais ao dinheiro, como contraprestação obrigacional. UNIÃO EUROPEIA. Supervisor Europeu de Proteção de Dados. *Ditamen sobre el cumplimento efectivo de la legislación en la economía de la sociedad digital*. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018XX0704(01)&from=ES>. Acesso 30 de mar. 2020.

[33] Para o autor, "o informacionalismo está ligado à expansão e ao rejuvenescimento do capitalismo, como o industrialismo estava ligado a sua constituição como modo de produção". CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura:* sociedade em rede. 1 vol. São Paulo: Paz e Terra, 2011. p.55.

[34] Para Piñar Manãs, "[…] en realidad la mayor parte de las innovaciones tecnológicas que están produciéndose en la actualidad tienen directa (las más de las veces) o indirecta relación con el tratamiento de datos de carácter personal. Ya hace años se habló de las RFID, las cookies o más recientemente del cloud computing. Hablamos ahora también de big data, Internet de las cosas, wearables, bitcoin, block chain, robótica, drones, inteligencia artificial, gene drive technology, data driven innovation, ciudades inteligentes… Cualquiera de estos conceptos es imposible sin el uso de datos". PIÑAR MAÑAS, José Luis. Sociedad, innovación y privacidad. Información Comercial Española, ICE: *Revista de economía*, Madrid, n. 897, p.70, jul./ago, 2017.

diversos pólos produtivos e funcionar em rede, o que representa uma dinâmica informacional flexível e dinâmica coordenada horizontalmente pelos atores[35].

A diferença presente do capitalismo industrial em relação ao capitalismo informacional está na alteração da estrutura do retorno financeiro com base no ciclo investimento-produção-venda que resulta na massificação do consumo de mercadorias para a estrutura do *valor de mercado* das companhias ou da valorização das ações em torno dos novos negócios[36]. As companhias que administram redes sociais (Facebook e Twitter), empresas inovadoras de software (Google, Microsoft, Oracle) e de massificação de conteúdo e serviços (Uber, Airbnb, Waze, Spotify e Netflix) possuem projeção global não pelo lucro atual, que é elevado, mas também pela expectativa futura de valorização[37]. Para Castells, o capitalismo informacional associa-se à noção de que a tecnologia gera valor e a expectativa futura de valorização das tecnologias inflaciona positivamente a rentabilidade dos negócios tecnológicos. Portanto, de uma economia pautada pela produção e comercialização, agrega-se a fator projeção e remuneração pelo mercado de capitais.

O horizonte de Castells permite sustentar que no sentido de um capitalismo *inclusivo*, por meio da inclusão de setores minoritários das comunidades globais menos favorecidas e, por outro lado, de setores majoritários da economia global (como os centros de maior produtividade industrial e potencial de consumo), de tal forma a incluir equitativamente conforme o potencial, nuances e diferenciais para a produção de riquezas, valores e progresso cultural-tecnológico. Isso porque, na sociedade em rede ocorre a hiperconexão de uma sociedade global[38]. O símbolo são as redes sociais, plataformas independentes e interconectadas que viabilizam o contato humano por meio da digitalização. Do ponto de vista econômico, a sociedade em rede viabiliza a incorporação global dos mercados, como

---

[35] CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura:* sociedade em rede. 1 vol. São Paulo: Paz e Terra, 2011. p.57.

[36] Para Rodotà, "[...] deve projetar-se também sobre os novos 'Senhores da Informação' que, por meio das gigantescas coletas de dados, governam as nossas vidas. Em face de tudo isso, a palavra "privacy" evoca não apenas uma necessidade de intimidade, mas sintetiza as liberdades que nos pertencem no mundo novo onde vivemos. O próprio modo de ser desses sujeitos – chamados Amazon ou Apple, Google ou Microsoft, Facebook ou Yahoo! – mostra-nos uma presença de oportunidade para a liberdade e a democracia e de um poder soberano exercido sem controle sobre a vida de todos". RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet?. *Civilistica.com*, Rio de Janeiro, nº 2, jul./dez.2015. Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/. Acesso em: 20 out. 2020.

[37] SCHIAVI, Pablo. El derecho al olvido en tiempos de "google": primeras aproximaciones a su regulación en Uruguay. Revista de Direito Administrativo e Infraestrutura, v. 2, n. 7, p. 179-196, 2018. Essas grandes companhias são consequência da "vitória americana" na revolução informacional, status difícil de ser perdido, mesmo em tempos de avanço do poderio tecnológico chinês. CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura:* sociedade em rede. 1 vol. São Paulo: Paz e Terra, 2011. p.99 e ss.

[38] CASTELLS, Manuel. *Comunicación y poder*. Ciudad de México: Siglo XXI, 2012.

podemos notar pelo fato de que a denominada "economia dos dados", baseada na utilização e emprego de tecnologias no tratamento de informações pessoais movimentou, apenas em 2016, 2% do Produto Interno Bruto (PIB) da União Europeia, tendo como projeção para 2020, resultado de operações baseadas em dados, cerca de 739 bilhões de euros[39]. Por essa lógica, empresas transnacionais possuem valor de mercado estimado em bilhões de dólares, muito maior que o PIB de países na América Latina.

A questão da sustentabilidade do capitalismo, pautado pelo consumo e gerador de desigualdades, apresentado criticamente por diferentes autores[40], é trabalhada pelo sociólogo catedrático com uma perspectiva positiva e diversa de uma orientação para o fracasso econômico global[41]. Agrega-se, contudo, a esse capitalismo informacional, a ideia de *vigilância*[42]. Nesse particular, insere-se o discurso/narrativa que induz a aparência de uma existência humana livre, repleta de direitos, entretenimento e progresso humano por meio da hiperconexão via internet, apesar da vigilância e do controle incansavelmente e invisivelmente realizados pelas organizações estatais e empresariais que realizam os procedimentos de monitoramento[43]. Para Zuboff, as operações são realizadas de forma indetectável, mascaradas pela retórica que nos desconcerta[44]. Essa descrição é muito aproximada à visão de Byung-Chul Han, no livro *La Sociedad de la Transparencia*[45], quando afirma que a sociedade contemporânea também é a sociedade do cansaço, que, formada por

---

[39] VAQUERO, Juan Pablo. El valor económico de un derecho fundamental: la monetización de los datos personales. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montev ideo: La Ley, 2019. p.1028.

[40] BUFFON, Marciano. ¿La economía del conocimiento reduce la desigualdad de renta y riqueza? In: BRAVO, Alvaro S. (editor). *Derecho, Inteligencia Artificial y Nuevos Entornos Digitales*. Sevilla, 2020. p.483.

[41] Conforme se verá, o novo capitalismo informacional é virtual. As novas tecnologias não destroem os empregos, são produtoras de novos empregos e novas alternativas profissionais. Não que não exista um desemprego estrutural, mas não existe uma causa direta entre o avanço das tecnologias com o incremento do desemprego. A posição em sentido contrário apresenta-se orientada por fatores de ordem ideológica. O que pode ser sustentado é reposicionamento do mercado de trabalho e uma reorientação em torno de novas perspectivas profissionais, porque sem novas tecnologias ou o emprego de tecnologia em diferentes setores da economia (não apenas a digital) se perdem empregos, por conta da produtividade e da qualidade do serviço ou dos produtos produzidos ou prestados. Em outras palavras, o mercado dedicará atenção a produtos melhores e atrativos economicamente, o que apenas é viabilizado pelo emprego de tecnologias disruptivas ou remodeladoras.

[42] SCHIAVI, Pablo. La protección de los datos personales en las redes sociales. *Revista de Direito Administrativo e Constitucional*, v. 13, n. 52, p. 145-178, 2013.

[43] Conforme Sérgio Amadeu, "[...] plataformas como o Google e o Facebook adquiriram um poder descomunal, pois são capazes de organizar, modelar e modular os fluxos de informação e controlam o que é amplamente visto, lido e ouvido. Podem influenciar e sugestionar os comportamentos de forma pouco ou nada visível". SILVEIRA, Sérgio Amadeu. Democracia e os códigos invisíveis: como algoritmos estão modulando comportamentos e escolhas políticas [e-book]. Rio de Janeiro: Editora Sesc, 2018. p.40.

[44] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, v. 30, n. 1, 2015, p. 85.

[45] HAN, Byung-Chul. *Sociedad de la Transparencia. Barcelona:* Herder, 2013. p.92.

pessoas assoberbadas de informações, não consegue discernir o rumo pelo qual estamos nos dirigindo.

No capitalismo industrial, os proprietários dos meios de produção são os empresários, que suportam financeiramente a estrutura necessária para a produção de bens e serviços, de modo a contratar profissionais para esse fim ou automatizar a produção. O objetivo final é colocar esses produtos ou serviços no mercado. O meio no qual todo o sistema de capitalismo de vigilância repousa, no entanto, é a infraestrutura digital ou plataformas da internet: o monitoramento de vidas humanas, conforme alerta Shoshana Zuboff[46]. Sustenta a pesquisadora que os mecanismos da economia digital da vigilância possuem como objeto as nossas experiências pessoais e privadas, de modo a utilizá-las como fonte de orientação para a personalização de produtos digitais extremamente rentáveis, que são oferecidos aos usuários na rede. No início do século, estes dados baseados no rastro digital ("fumo digital") eram considerados adicionais. Percebeu-se, ao longo da última década, que o "caminho na rede" continha dados reveladores do comportamento do usuário que poderiam ser aproveitados pelos desenvolvedores de tecnologia nas plataformas.

Em termos mais claros, a proteção de dados contemporânea não está mais ligada à proteção simples e genérica do cadastro no banco de dados, mas a um arranjo completo de proteção que transita entre a coleta até o uso e tratamento das informações, em razão da vigilância utilizada por empresas de tecnologia. A exposição nas redes de comunicação, que reflete essa liberdade, é, paradoxalmente, a fonte de monitoramento e controle de organizações (sejam estatais ou empresariais). De forma geral, as informações relativas ao indivíduo, desde o seu nascimento até a morte, tendem a ser tratadas por algum meio digital, o que acaba por tornar o ser humano parte de um ciclo infinito de armazenamento e utilização de informações. Ainda que o consentimento do consumidor seja o meio de autorização para que empresas nacionais e transnacionais realizem o tratamento de dados e informações de cunho pessoal, o que deles se faz não é conhecido em completude – isto é, não se conhece o que é feito para além do melhoramento do serviço prestado. Afinal, quem pode utilizar nossa informação pessoal e para quê? A estrutura regulatória de dados brasileira passará a exigir a conformidade das "políticas de privacidade" das plataformas digitais[47].

---

[46] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, v. 30, n. 1, p. 82, 2015.

[47] BIONI, Bruno Ricardo; LIMA, Cíntia Rosa Pereira de. *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*. 2016.

Todavia, outro fator mostra-se relevante: o *big data,* que se refere a conjuntos de dados tão variados e coletados em grande quantidade que as tradicionais técnicas de análises mostram-se incapazes de tratá-las. O termo *big data* foi utilizado inicialmente no início do século XXI por astrônomos e geneticistas, a partir do momento em que a memória dos computadores não era mais capaz de armazenar a enorme quantidade de informação disponível, obrigando, assim, a se pensar em novas formas e instrumentos a análise dos gigantes bancos de dados. Pode-se dizer que, apesar de ser objeto de ampla difusão, há na expressão certa ambiguidade, vagueza e imprecisão[48] já que comporta diversas interpretações e significados. Mayer-Schonberger, da Universidade de Oxford, defende que a expressão "[...] *big data* refere-se a coisas que se pode fazer em grande escala, que não podem ser feitas em escala menor"[49]. Nessa linha de pensamento, o grande número de sensores e câmeras e a multiplicidade de formas de acesso à rede torna *o dado pessoal um grão de areia no deserto das informações em rede*, a ser tratada e compreendida por sistemas de alta potencialidade de comparações e de identificação de semelhança ou traços de valor significativo. Veja-se que o Instituto de Tecnologia & Sociedade[50] do Rio, ao apresentar uma tentativa de definição ao fenômeno, o enuncia como:

> conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos nos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.

Por outra via, Ira Rubinstein[51], torna factível que o *big data* deve ser apenas *caracterizado* como modelo, pautado por características. A disponibilidade de dados em grande escala, coletados não somente *on-line (via computadores e redes sociais)*, mas através do uso de dispositivos móveis com recursos de rastreamento de localização e milhares de aplicativos que compartilham dados, *primeiro*; a alta velocidade de processamento e armazenamento, *segundo*; a crescente utilização de novas ferramentas ou estruturas

---

[48] GOMES, Rodrigo Dias de Pinho. *Big data: desafios à tutela da pessoa humana na sociedade da informação*. Rio de Janeiro: Lumen Juris, 2017. p. 18.

[49] Tradução literal de: "big data refers to things one can do at a large scale that cannot be done at a smaller one" MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013. p.6.

[50] ITS Rio. *Big Data no projeto Sul Global*: Relatório sobre estudos de caso. Disponível em:<https://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 03 jul. 2019.

[51] RUBINSTEIN, Ira S. Big Data: The end of privacy or a new beginning?, *International Data Privacy Law*, v.2, n.3, p.78, 2013.

computacionais na verificação e tratamento de informações, *terceiro*. Entretanto, a perspectiva adotada não exclui os malefícios da utilização da tecnologia.

Richards e King[52] estabelecem a transparência, a identidade e o poder como elementos paradoxais do fenômeno analisado. A promessa de utilização dos dados de forma transparente acaba entrando em choque como o fato das pessoas não saberem onde estarão os pontos coletores de informações pessoais ou os sensores: se em sites serão contabilizados os cliques do mouse e, até mesmo, em que medida será avaliada a interação em redes sociais. A possibilidade de minimização da pessoa surge como segundo paradoxo. O *big data* pode ter como consequência a utilização do dado pessoal em ferramentas que incutam comportamentos não espontâneos nas pessoas[53]. Trata-se da possibilidade de influenciar ou até restringir a edificação da identidade pessoal. Esse paradoxo conecta-se como o paradoxo do poder relativo ao controle das informações de pessoa. O *big data* é, perceptivelmente, mais invasivo, em vista da capacidade de conseguir coletar, armazenar e tratar de maneira mais detalhista e minuciosa as informações pessoais[54].

Nesse ponto que reside, portanto, a aproximação gradativa com a pessoa, de modo a abrir espaço, de igual forma, para o seguinte questionamento: *qual o impacto do big data na regulação da proteção de dados*?[55] Essa perspectiva informa uma nova dimensão do tratamento de dados cadastrais e pessoais (nome, números de identificação, endereços físicos e eletrônicos, como históricos médicos, acadêmicos, de navegação na internet ou de uso de informações), mas alia-se à perspectiva do necessário controle e correção ao uso não autorizado de informações – o que ocorre por meio do cruzamento com múltiplos bancos de dados de diferentes informações, espionagem, controle populacional, manipulação com base na disponibilização direcionada de informações com base na personalidade identificada a partir da coleta de dados.

A maior parte dos dados coletados é analisada para criar modelos que se compõem de padrões de comportamento humano, que servirão para identificar como as pessoas com

---

[52] RICAHARDS, Neil M.; KING, Jonathan H. Three Paradoxes of Big Data. Disponível em: <https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/>. Acesso em: 20 jun. 2020.

[53] FAINI, Fernanda. Big data, algoritmi e diritto. *DPCE Online*, [S.l.], v. 40, n. 3, sep., p.1881, 2019. Available at: <http://www.dpceonline.it/index.php/dpceonline/article/view/785>. Acesso em: 15 abril 2021.

[54] Não há paralelo com as enquetes, censo demográficos, pesquisa de consumo.

[55] A LGPD estabelece como fundamentos de aplicabilidade da lei o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

determinadas características se comportam habitualmente ao longo do tempo e prever qual será o comportamento futuro. O problema, segundo Zuboff, é que o capitalismo da vigilância não se manifesta apenas quando estamos *online* ou está limitado à publicidade *online*: uma série de equipamentos eletrônicos (com ou sem inteligência artificial) é desenhada para coletar dados pessoais, de forma que a desabilitação da coleta de informações acabe por afetar o desempenho do produto. Em outras palavras, desenha-se um produto que funciona com base em dados, não deixando margem à opção do consumidor acerca da utilização deles, se quiser continuar utilizando o produto. Para a pesquisadora, o consumidor é forçado a viver de forma analógica ou viver num mundo digital em que a autodeterminação e a nossa privacidade são destruídas em vista do desejo do mercado (a menos que haja resistência)[56]. Por isso, torna-se necessária a reflexão em torno da necessidade de proteção progressiva de dados pessoais[57].

Atualmente, a exposição de dados pessoais ao público – como fotos e manifestações de pensamento, por exemplo – tornou-se um elemento relevante na formação da identidade da pessoa, de tal forma que as linhas que divisavam o público do privado passaram a ser tênues ou inexistentes e cuja consequência está relacionada à redução da autonomia do desenvolvimento de nossa própria personalidade[58]. Dito de outro modo, ao mesmo tempo em que há liberdade de exposição nas redes de comunicação, paradoxalmente, e em razão do constante monitoramento, a liberdade acaba por ser constrangida, conforme registra Pérez Luño:

> En las sociedades avanzadas con tecnología punta ya no se puede juzgar como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad[59].

Nesse sentido, a privacidade e a vida íntima das pessoas – isto é, e a proteção de seus dados pessoais – ganham destaque a partir do momento em que se torna factível a possibilidade concreta de violações por diversos interesses, sejam eles econômicos, de expressão de poder estatal ou, até mesmo, terroristas. Trata-se do reflexo de uma sociedade

---

[56] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, v. 30, n. 1, p. 84,2015.

[57] SCHIAVI, Pablo. Primeras reflexiones sobre la nueva ley de telemedicina en Uruguay. *Revista de Direito Administrativo e Infraestrutura*, v. 5, n. 16, 2021.

[58] LIMBERGER, Têmis. *Cibertransparência:* informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado Editora, 2016. p.63.

[59] PÉREZ LUÑO, A.. Internet y los derechos humanos. *Anuario de Derechos Humanos*. Nueva Época, Norteamérica, n. 12, p.293, dic. 2011. Disponible en: <https://revistas.ucm.es/index.php/ANDH/article/view/38107/36859>. Acesso em: 23 out. 2020.

pós-industrial repleta de informações em rede, cujo desafio tecnológico é continuar inovando e evoluindo sem vulnerar direitos da pessoa, direita ou reflexivamente. Eis o desafio do Direito do século XXI: harmonizar o desenvolvimento tecnológico com as novas (ou eficientes) formas de controle/regulação, que passará pelo desempenho satisfatória da ANPD.

Por outro lado, a rastreamento à pessoa não se limita aos registros em rede. As aplicações de monitoramento por câmera, do uso de sistemas de pagamento via *smartphones* e, especialmente, das publicações multimídias em redes sociais, facilitam a coleta e registro dos passos dos cidadãos por organizações públicas e privadas. O filósofo sul-coreano Byung-Chul Han[60] sustenta que, a partir da constante utilização de celulares e equipamentos baseados em coleta e utilização de dados, pessoas passaram a ser "terminal" de fluxos de dados, subministradores de informações e objeto do tratamento de informações por sistemas baseados em algoritmos, o que permite que os detentores da informação possuam o potencial de "influenciar, controlar e dominar" o agir humano.

Dessa forma, resta evidenciado que as regulações contemporâneas não se restringem aos aspectos econômicos, meramente contratuais ou tratadísticos, como se poderia sugerir há pouco tempo, direcionando-se para o campo da tutela de direitos fundamentais, na composição de um denso *tecido jurídico* desenvolvido, especialmente na última década, com o avanço tecnológico e com a noção de avançar "além do estado". O questionamento, no que interessa à análise proposta, refere-se a saber se a globalização apresenta-se como interconexão mundial de propósitos ou se assume a feição de expansão do mundo ocidental e das características corporativas do mundo financeiro e da dominância das corporações transnacionais. Logicamente, não se está a fazer uma crítica à relevante função da economia no desenvolvimento das nações, mas ressalta-se a importância de que não se deve viver uma *ilusão planetária* enquanto vivemos uma *dominação planetária*. A ideia que reside na antessala dessa lógica de coleta e tratamento de informações é "click" ou o contato com as telas sensíveis ao toque. Em 2015, o estudo denominado *Ocean* conduzido por pesquisadores do Centro de Psicometria da Universidade de Cambridge apontou que a personalidade pode ser medida por meio da exposição a conteúdos, de forma que, com base no número de "curtidas", se possa saber como a pessoa se comportaria[61], inclusive com inferências em termos de qualidade de vida. Essa pesquisa foi utilizada no desenvolvimento de um sistema

[60] HAN, Byung-Chul. *Sociedad de la Transparencia. Barcelona:* Herder, 2013.
[61] YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computers judge personalities better than humans. *Proceedings of the National Academy of Sciences*, n. 112, v. 4., p. 1036-1040, jan, 2015

que analisou a personalidade de pessoas, de modo a promover conteúdos para determinados públicos, no que ficou conhecido como escândalo *Cambridge Analytica*.

O escândalo revelado pelo jornal britânico *The Guardian*[62] reascendeu o debate sobre a necessidade da uniformização da proteção de dados em torno de instrumentos regulatórios sólidos e que confiram padrões mínimos de segurança e de confiabilidade na utilização de dados pelos controladores, nos limites do consentimento do usuário. Pensar que o incidente passou ao largo da realidade brasileira é um equívoco: o episódio de vazamento de dados atingiu cerca de 500 mil cidadãos brasileiros, participantes da rede social. O desnudamento dos efeitos do relacionamento entre tecnologia e cidadãos põe forma ao poder simbólico do processo de aceleração dos rumos da história. Embora os contornos apresentem-se, ainda, indefinidos, revela a conclusão de que se está diante do fenômeno da reinvenção da privacidade, ressignificada pelo devir tecnológico e o corolário da (re)construção contínua da identidade da pessoa. O tempo pauta-se em milissegundos – não mais em horas e minutos – e a dependência crescente dos modelos da sociedade do consumo e da cultura cosmopolita assenhoram-se do sujeito[63].

A noção de consentimento cristalizada na doutrina nacional e internacional possui como norte a ideia de manifestação livre, informada e inequívoca de concordância do titular com o tratamento de seus dados pessoais. No entanto, não há como anuir de forma livre, informada e inequívoca no contexto em que sensores, câmeras e demais dispositivos estão coletando dados pessoais de modo automático, uma vez que a compra dos produtos já poderá implicar o consentimento tácito da coleta de dados para o *grande banco de dados*. Possivelmente, se trabalhará, no futuro não tão distante, com a inversão da lógica civilista preponderante atualmente: ao invés de consentir, o titular deverá *deixar de consentir* ou eliminar dispositivos da vida cotidiana, porque não terá certeza do nível de captação de informações pessoais. Vale dizer, é possível que se instaure a paranoia da vigilância, numa sociedade em que todos são vigiados e todos são vigias. Por isso, a transparência *(i)* de quais dados serão coletados, *(ii)* dos métodos na coleta de dados orientados de acordo com a

---

[62] CADWALLARD, Carole; GRAHAM-HARRISON, Emma. Revealed**:** 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. [S.L.]. 27 de mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 25 dez. 2020.

[63] RODOTÀ, Stefano. *El derecho a tener derechos.* Madrid: Trotta, 2014, p.293-294. LIMBERGER, Têmis. *Cibertransparência informação pública em rede*: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

finalidade anuída, *(iii)* dos programas de segurança e de correção de falhas da tecnologia adotados pela organização.

Dessa forma, resta evidenciado que o conhecimento da personalidade das pessoas também pode ser usado para manipulá-las e influenciá-las. As pessoas podem desconfiar ou rejeitar as tecnologias digitais depois de perceberem que o governo, provedor de internet, navegador da web, rede social on-line ou mecanismo de pesquisa podem inferir suas características pessoais com mais precisão do que seus familiares mais próximos. É importante que se adotem mecanismos que garantam a transparência e a regular adoção de mecanismos de segurança em matéria de proteção de dados. O fundamento de uma autoridade de proteção de dados está na estruturação de mecanismos de controle, de formas de regulação e de transparência que orientem as organizações estatais e privadas a realizar o tratamento de dados pessoais, conforme se verá a seguir.

2.2. O direito à proteção de dados pessoais: por uma noção/definição de dado pessoal

Para Rallo Lombarte, os "[...] novos direitos digitais são, em grande medida, o corolário de uma evolução em que o direito à proteção de dados tem servido como uma verdadeira ponta de lança diante da realidade digital"[64]. Todavia, essa perspectiva representa um longo caminho percorrido, especialmente considerando que definir o direito à privacidade não é uma tarefa fácil, por se entender que se trata de um conceito amplo[65], inserido no direito à vida privada que é incapaz de ser confundido com a privacidade ou simplificado em definições exaustivas. Do ponto de vista histórico, o Convênio Europeu de Direitos Humanos (CEDH), de 1950, estabelecia o respeito à vida privada e familiar[66]. O fato é que a transformação desse conceito é consolidada a partir da década de setenta. A edição de legislações específicas e de decisões judiciais de diversos países, bem como a partir da aprovação de acordos internacionais e transnacionais em diferentes níveis. Os instrumentos compartilham o conceito segundo o qual os dados pessoais constituem uma projeção da

[64] LOMBARTE, Artemi Rallo. Del derecho a la protección de datos a la garantía de nuevos derechos digitales. LOMBARTE, Artemi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.23-52.
[65] PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018.
[66] CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos (CEDH*). Disponível em: < https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso 4 nov. 2020.

personalidade do indivíduo[67]. O surgimento dos diplomas normativos deveu-se ao advento do processamento eletrônico de bancos de dados em organizações públicas e privadas.

As Diretrizes de Privacidade da OCDE, datadas de 1980, foram os primeiros princípios de privacidade acordados internacionalmente[68]. A atualização realizada em 2013 manteve essas diretrizes como uma referência essencial, mas com ajustes relevantes ante ao incremento das aplicações e segue sendo adotada pela OCDE em nível de atuação interna. Na primeira versão, da década de oitenta, adotou-se seis princípios: *(i*) o da limitação da coleta, a ser exercido por meio legais e com o conhecimento ou consentimento do titular dos dados/informações; *(ii)* qualidade dos dados, traduzindo a ideia de adequação e relevância entre o dado, a coleta e os fins de tratamento; *(iii)* o cumprimento da finalidade da coleta, de modo que o dado não seja utilizado para fins não conhecidos ou consentidos; *(iv)* a limitação do uso, no sentido de limitar o tratamento e vedar o compartilhamento não informado; *(v)* medidas de segurança, como forma de reduzir ameaças ou riscos, como a perda dos dados ou acesso não autorizado; *(vi)* a transparência, acerca do uso dos dados, práticas e políticas com respeito a dados pessoais; *(vii)* participação do usuário, no sentido de afirmar a garantia do titular requerer que eles sejam apagados, retificados, completados ou alterados e *(viii)* o princípio da responsabilidade (accountability), no sentido da prestação de contas pelo cumprimento das medidas relativas à aplicação dos princípios mencionados.

Nesse sentido, o ponto 17 das Diretrizes estabelecia que o membro da OCDE devesse abster-se de restringir os fluxos transfronteiriços de dados pessoais se o país de destino observasse substancialmente as diretrizes citadas e se existissem medidas técnicas de contenção de riscos e ameaças suficientes, demonstrando a aplicação eficaz das Diretrizes. O Convênio 108 do Conselho da Europa, de 1985, tornou-se o primeiro documento jurídico vinculante no tocante ao tratamento de dados automatizados de caráter pessoal de qualquer pessoa e foi relevante na harmonização da Diretiva para a Cooperação e Desenvolvimento Econômico, na década de 1980 com a proteção de dados pessoais[69]. As regulamentações

---

[67] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555-587, nov-dez, 2018.

[68] OCDE. Diretrizes de Privacidade da OCDE. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> Acesso em 27 set. 2020.

[69] CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y proceso de reforma sobre protección de datos en la unión europea. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016. p. 36.

comunitárias não impediam, entretanto, que, desde a década de 1970, os países pertencentes à União Europeia adotassem sistemas de regulação próprios (nacionais).

A crítica produzida em torno da regulação nacional encontra espaço a partir das diferentes normas e esferas de proteção adotadas nos países que tiveram por consequência prejudicar o comércio interior na comunidade europeia e a livre circulação de dados. Nesse sentido, os países convergiram no sentido de conferir um equilibro e uniformidade à proteção dos dados pessoais, de modo a compatibilizar a livre circulação de dados e o nível adequado de proteção de dados pessoais, o que resultou na adoção da Diretiva 95/46. Para Piñar Mañas, a referida Diretiva Comunitária revolucionou o modo pelo qual ocorria a proteção de dados na Europa, servindo como referência mundial[70].

As novas tecnologias e a globalização informática, que permite o fluxo de dados de forma transnacional, fizeram com que ajustes legislativos fossem estudados pela Comissão Europeia. Com efeito, o fator preponderante à reformulação da regulamentação refere-se à positivação do direito à proteção de dados com direito fundamental no artigo 8.º da Carta de Direitos de Nice (ratificado pelo Tratado de Lisboa)[71], conferindo-lhe autonomia em relação ao direito à intimidade[72]. Observe-se que, a partir do Tratado de Lisboa, a Carta de Nice passou a ser juridicamente vinculante, exercendo, inclusive, função constitucional no âmbito

---

[70] PIÑAR MAÑAS, José Luis. Introducción. Hacia un nuevo modelo europeo de protección de datos. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016.

[71] UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf> Acesso em 14 out. 2020.

[72] O direito à privacidade surgiu nos Estados Unidos, em 1890, como expressão do direito de ser deixado em paz (*the right to be let alone*)[72]. A doutrina americana em relação à *privacy* teve como precursores Samuel Warren e Louis D. Brandeis[72].Com efeito, as teorizações norte-americana não realizam a diferenciação entre privacidade e intimidade, pois concebe o direito à privacidade como direito geral reconhecível por meio da sistematização dos princípios da *false light*, *defamation*, *public disclosure of facts* e *intrusion upon seclusion*. De fato, a *privacy* foi formulada como uma parcela integrante da direito de propriedade; vale dizer, está vinculada ao relacionamento do particular com sua vida privada e com o poder dele escolher se pretende externar publicamente fatos ocorridos naquele âmbito. Nos Estados Unidos, o caso *Griswold vs. Connecticut*, julgado pela Suprema Corte norte-americana (1965), é paradigmático porquanto reconheceu a privacidade como implicitamente reconhecida na Constituição Americana. A doutrina alemã trata da privacidade no âmbito da *privatsphäre*, por meio da noção lógica de que existe uma fronteira entre a autonomia pessoal e a vida social. São notáveis as contribuições do Tribunal Constitucional Alemão em matéria de proteção de dados pessoais, especialmente a partir do caso do Censo de 1983, por meio do qual se "criou", ou melhor, se "definiu" o conceito de autodeterminação informativa. No plano legislativo, a primeira legislação de proteção de dados entrou em vigor 1970, no Estado-membro de Hesse (Alemanha), o que foi seguido, em 1977, pela primeira legislação federal europeia sobre o tema. Na França, a privacidade é tratada como a *protection a la vie privè*, em que se busca compatibilizar a informação com as liberdades fundamentais e os direitos humanos. Como antecedente histórico no direito francês, temos o caso *Affaire Rachelix c. O'Connell*, no século XIX, em que uma atriz que foi fotografada no seu leito de morte, a seu pedido. Ver: RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito* – UFPR, Curitiba, n.53, p.51-58, 2011. RODRIGUES JUNIOR, Otávio Luiz. *A mudança na jurisprudência alemã sobre vida privada*. Disponível em: <https://www.conjur.com.br/2012-jul-18/direito-comparado-mudanca-jurisprudencia-alema-vida-privada>. Acesso 4 jul. 2020.

comunitário, além de incorporar o Tratado de Funcionamento da União Europeia (TFUE), que codificou a forma de tutela da proteção de dados no artigo 16 do diploma legal, disciplinando que caberia ao Parlamento Europeu e ao Conselho da Europa estabelecer as normas de proteção de dados pessoais aplicáveis aos órgãos da União Europeia e aos países membros.

Nesse sentido, dois traços podem ser identificados na estruturação dos novos diplomas reguladores, especialmente em matéria de proteção de dados e da privacidade: *(i)* a valorização dos princípios como instrumentos de vinculação e estruturação dos sistemas protetivos e *(ii)* a construção de organizações baseadas na prevenção do dano e a orientação de um sistema de normas para fortalecer a responsabilidade (princípio da responsabilidade proativa) dos agentes. Muda-se, portanto, a lógica de um sistema de regulação baseado na reatividade e na sanção, para se apostar na responsabilidade preventiva dos envolvidos na cadeia de proteção dos direitos da pessoa (no caso de estudo, os dados pessoais)[73].

Vale pontuar que a equivalência entre informação e dado é afastada por expressiva parcela dos estudiosos da teoria da informação e suas diversas interfaces. No Brasil, se sustenta que o termo "dado" possui um caráter mais primitivo e fragmentado. Por sua vez, a informação é agregação de sentido ao dado apresentado, reduzindo a incerteza. A doutrina não raro trata esses dois termos indistintamente, conforme salienta Doneda[74].

Tanto em sede europeia quanto na emergente regulação de dados brasileira, entende-se como dado pessoal qualquer informação relativa à determinada pessoa identificada ou identificável[75]. Para Danilo Doneda e Diego Machado[76], a "[...] delimitação do conceito de dado pessoal é hoje imprescindível na interpretação do alcance normativo de leis de proteção

---

[73] PIÑAR MAÑAS, José Luis. Administración electrónica y protección de datos personales. *Revista Jurídica da Universidade de Santiago de Compostela*. p.149, 2011. Conferir, também, REIGADA, Antonio Troncoso. Del principio de seguridad de los datos al derecho a la seguridad digital. *Economía industrial*, Madrid, [s.v.], n. 410, p.127-151, 2018.

[74] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. ed. São Paulo: Thompson Reuters, 2019. p.105.

[75] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da Europa,* de 27 de abril de 2016. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 14 out. 2020.

[76] Essas informações diferenciadoras são relevantes à constatação e podem ser entendidas como proteção de dados básica ou profunda. Será básica quando se protege a pessoa no âmbito de uma relação específica, típica e legítima em que o responsável conhece o titular dos dados. Será uma proteção de dados profunda quando toma as providências para que não se reidentifique o titular da informação, por qualquer meio. Assim o é também para definir o objeto do tratamento de dados pessoais, em razão do fato de que, uma vez desidentificado (anonimizado) cessará o alcance da legislação protetiva. Em outros termos, o dado pessoal será dado comum, não relacionável e, portanto, passível do tratamento que o responsável ou controlador bem aprouver.

de dados"[77], os quais podem ser conceitos restrito e amplo. Do ponto de vista restrito, para os autores, "[...] dado pessoal entende-se a representação de fatos sobre pessoa identificada, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade"[78]. Do ponto de vista restrito, haverá dado pessoal quando os dados potencialmente conduzem à individuação da pessoa. Em outras palavras, a ideia de privacidade, muito debatida, passa a estar associada à ideia de proteção de dados pessoais.

Para a LGPD, dado pessoal é definido como qualquer informação relativa à pessoa identificada ou identificável[79]. A primeira observação que pode ser traçada está na relevância histórica relativa à mutação da valorização da privacidade, fato ou característica que não era significativa da vida tribal ou de aldeia. O valor humano "privacidade" tornou-se mais significativo durante o pós-revolução industrial e a consolidação do modelo capitalista de produção e consolidada no modo informacional, considerando-se os efeitos importantes à privacidade, à proteção de dados e às diferentes formas de utilização da tecnologia e de acesso a novos conteúdos, uma forte tendência da sociedade da informação.

O Parecer n.4/2007, do Grupo de Trabalho de Proteção de Dados do Artigo 29[80], endereçado à Comissão Europeia, define o dado pessoal como aquele que permite diferenciar uma pessoa da outra[81]. Trata-se, em verdade, do reflexo do que Mayer-Schonberger e Cukier[82] descrevem como *datificação social*, uma perspectiva que supera a digitalização da sociedade rumo à *especificação por meio de dados*, capazes de ser analisados e tratados por sistemas algorítmicos. Vale dizer, não basta o suporte ser digital, é necessário que este objeto multimídia seja convertido em um formato passível de ser reconhecido e processado pelos computadores: o *dado*. A perspectiva, todavia, não exclui os dados tratados de forma física.

---

[77] MACHADO, Diego; DANILO, Doneda. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Caderno Especial - A Regulação da Criptografia no Direito Brasileiro*, vol. 1, p. 102, 2018.

[78] MACHADO, Diego; DANILO, Doneda. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Caderno Especial - A Regulação da Criptografia no Direito Brasileiro*, vol. 1, p. 102, 2018.

[79] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

[80] UNIÃO EUROPEIA. Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Parecer 4/2007 sobre o conceito de dados pessoais.* Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>. Acesso em: 2 jul. 2020.

[81] Conferir, também, DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Victor Rozatti (Org.). Direito Digital: direito privado e internet. São Paulo: Foco, 2019. p.36-37.

[82] MAYER-SCHONBERGER, V.; CUKIER, K. *Big data: a revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt: New York, 2013.

Nesse sentido, em matéria de proteção de dados, o RGPD tende a assumir protagonismo. Como inovações, a novel normatização europeia incorporou o princípio da *responsabilidade proativa*, como forma de alterar o panorama de proteção de dados para a lógica da prevenção. Registre-se que a Diretiva 95/46 recorreu a um modelo regulativo que prevê um responsável reativo e passivo, cuja atuação era afeta ao cumprimento das normas de segurança dos dados e à resposta aos cidadãos em termos de acesso aos dados, retificação e cancelamento. O novo regulamento propõe uma conduta mais proativa e positiva do responsável pelo tratamento de dados, de modo que ele adote medidas técnicas e organizativas de acordo com a natureza dos dados protegidos, o contexto tecnológico e o risco de violação a direitos e liberdades fundamentais. Além disso, prevê-se um modelo fluido de organização, em que as técnicas de proteção de dados devam ser atualizadas quando houver necessidade ou mutação tecnológica. Trata-se de um modelo que torna o responsável não somente um cumpridor de normas, mas também um agente pautado pela previdência e diligência, que anteveja o descumprimento de normas por meio de expedientes típicos da tradição do direito anglo-saxão, como o *accountability* e o *compliance*[83].

O RGPD, além de aprimorar o regramento relativo aos códigos de conduta (*compliance*), também o inovou ao trazer os princípios da proteção de dados desde a concepção e por defeito, cuja aplicação é obrigatória e, seu descumprimento, sancionável. Outra obrigação incorporada ao texto do regulamento refere à obrigatoriedade da elaboração de um relatório de impacto sobre a proteção de dados (*data protection impact assesment*), quando o responsável indicar como provável que determinado tratamento coloque em risco a proteção de dados da pessoa física.

Saliente-se, também, RGPD consolidou princípios aplicáveis à proteção de dados. Por exemplo, o princípio da *legitimação*, pelo qual os regulamentos atribuem aos responsáveis o dever de adotar medidas protetivas aos dados pessoais do titular. Nesse sentido, o consentimento do usuário passa a ser o principal fator que confere legitimidade ao tratamento. Além disso, outro princípio relevante em matéria de proteção de dados é o da *licitude*, pelo qual o responsável pelo tratamento de dados deve comportar-se conforme as regras do Estado de Direito, de modo que não viole arbitrariamente o que deveria proteger[84].

---

[83] REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016.

[84] PIÑAR MAÑAS, José Luis. El objeto del reglamento. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.56-58.

O conceito de privacidade desde a concepção da tecnologia (desde o design) está baseado numa postura pró-ativa e não reativa da vulneração do direito à privacidade. Com relação à proteção de dados, a privacidade desde o design estaria relacionada com a diminuição dos riscos e, nesse caso, poderia ser uma manifestação do princípio da precaução, levando-se em conta a natureza, o âmbito, o contexto e os fins do tratamento. Um segundo sentido do princípio da privacidade desde o design seria a adoção de processos, procedimentos e políticas, que seriam medidas protetoras da privacidade, voltadas para avaliação dos riscos e da segurança e as avaliações de impacto na proteção de dados pessoais. A proteção de dados desde a concepção da tecnologia está prevista no parágrafo 1.º do artigo 25 do Regulamento[85]. Dessa forma, o conceito de privacidade desde a concepção da tecnologia culmina o conceito de proteção da privacidade por defeito na tecnologia. A privacidade por defeito garante que mesmo que o usuário não tome as cautelas para proteger seus dados, o sistema da própria arquitetura de software, baseada na privacidade, garantiria a confidencialidade de toda a informação de caráter pessoal. O parágrafo 2.º do artigo 25 do regulamento afirma que o responsável aplicará medidas técnicas e de organização para que, em caso de defeito, os dados não sejam acessíveis[86].

2.3 O perfil jurídico uruguaio em matéria de proteção de dados

A emergência de processos econômicos e culturais viabilizados pela convergência tecnológica elevou utilização, função e necessidade de proteção aos dados pessoais (e informações em rede)[87]. Esse processo tem como catalisador a reforma dos marcos regulatórios da privacidade impulsionada pela entrada em vigor do RGPD na União Europeia. Na América Latina, os países progridem ao adotar e desenvolver regulações de tutela da privacidade e de dados pessoais, como é o caso do Brasil, com a adoção da LGPD, cujo desafio começa a centrar-se no desempenho das funções associadas às autoridades de proteção de dados. Por outra via, Chile, Uruguai e Argentina passaram a atualizar a legislação

[85] CALÉS, Rosario Duaso. Los principios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.295-320.

[86] CALÉS, Rosario Duaso. Los principios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.295-320.

[87] LOHNER, Wolfrang. Tecnología de la información. Su impacto social y efectos legislativos. Algunas consideraciones. *Informática y Direito*: Revista iberoamericana de derecho informático, s.l., n.5, p.1427, 1994.

e a tomar medidas para adaptá-la às alterações do modelo europeu e às novas imposições próprias da economia digital. Há, nesse sentido, uma amplitude de atividades de compatibilização e diferentes estágios de avanço, conforme o ritmo de cada país. Leis de aplicação horizontal nesses países ajudarão a proteger a privacidade dos usuários e a gerar segurança jurídica para o uso de dados, independentemente do setor e da tecnologia. Os governos da região estão avançando em projetos de reforma regulatória para liberar o potencial dos dados[88], com o cidadão digital no centro. O uso aplicado de dados está tendo um efeito transformador em todos os setores da economia e podem ajudar a enfrentar vários desafios sociais. Ao mesmo tempo, a massificação de tecnologias inovadoras e disruptivas, como 5G, inteligência artificial ou a internet das coisas, aumentou a necessidade de confiança e estabilidade nos serviços digitais[89]. Há um intenso esforço na produção de marcos e regulamentações que permitem o desenvolvimento de políticas públicas baseadas em evidências[90], o aproveitamento de todo o potencial tecnológico nos diversos setores da economia e a geração de confiança nos serviços, mas desde que respeitando a proteção de dados.

Está se formando uma incipiente agenda comercial que considera os fluxos internacionais de dados como um acelerador da economia digital regional. Os dados são a força vital de uma sociedade digital e são essenciais para a economia global. O comércio de hoje depende muito da capacidade das organizações movimentar dados, incluindo dados pessoais de cidadãos, no interior dos países e entre países, sem restrições. A capacidade de fazer isso oferece crescimento de longo prazo e desenvolvimento inclusivo[91], não apenas para essas organizações, mas também para os cidadãos e os países em geral. Nos últimos dois anos, a assinatura ou anúncio de acordos comerciais internacionais por países da região

---

[88] PUCCIELI, Oscar. El derecho de la protección de datos personales en perspectiva latino-americana. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.373-429. Conferir, também, RUIZ, Cláudio. Privacy and security, the Latin American way. In: MAGRANI, Eduardo. *Digital rights: Latin America and the Caribbean*. Rio de Janeiro : Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017.p.24-26.

[89] SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016. p.136-141.

[90] Sobre a relevância do tema, consultar: HANS, Rosling. *Factfullnes*s: o hábito libertador de só ter opiniões baseados em fatos. 4ed. São Paulo: Record, 2020.

[91] CASAMAYOU, Adriana. *Las nuevas tecnologías:¿son para todos?*. 2016. Disponível em: < http://repositorio.mides.gub.uy:8080/xmlui/bitstream/handle/123456789/623/640_Casamayou%2C%20Las%20nuevas%20tecnolog%C3%ADas%2C%20son%20para%20todos.pdf?sequence=1&isAllowed=y.>. Acesso em 21 nov. 2020.

somam-se à crescente busca de adequação ao RGPD e à reformulada Convenção 108[92], além da criação das Normas de Proteção de Dados para Estados Ibero-americanos (*standards*).

O Uruguai – país cujo território e população apresentam características distintas das do Brasil – é, antes de tudo, um modelo qualitativo, por apresentar níveis adequados de amadurecimento democrático[93], acumular índices de transparência relevantes e deter uma economia estável. Não apenas isso: trata-se de um país que vem se programando para a transformação digital, a qual depende da adoção de mecanismos organizacionais e governamentais compatíveis com a *nova era*, orientados pela atuação da Agência de Governo Eletrônico e da Sociedade da Informação e do Conhecimento – AGESIC e da Unidade Reguladora e de Controle de Dados Pessoais – URCDP[94].

Empresas de *software* uruguaias despontam na América latina[95]. O Banco Interamericano de Desenvolvimento (BID)[96] e a Organização dos Estados Americanos (OEA) publicaram o *Relatório de Segurança Cibernética: Riscos, Progresso e o caminho a seguir na América Latina e no Caribe*. Em particular, o relatório informa que o Uruguai está liderando a região em quatro das cinco áreas do modelo de maturidade da cibersegurança, que incluem

---

[92] Para Mantelero, a "[...] longa história da Convenção 108+ e do RGPD demonstra a complexidade e a dificuldade de criar convergência sobre essa questão, especialmente em um contexto em que o interesse econômico e político na soberania digital desempenha um papel proeminente. Isso não exclui a possibilidade de que o padrão internacional estabelecido pela Convenção 108 possa um dia tornar-se o padrão global ou ser transposto para um instrumento internacional vinculativo adotado em nível global. Em ambos os casos, no entanto – uma Convenção 108 adotada globalmente ou um tratado global baseado em seus princípios – parece improvável que um padrão regulatório baseado em princípios e disposições que difira significativamente do modelo de Estrasburgo possa fornecer uma referência global de sucesso." MANTELERO, Alessandro. The future of data protection: gold standard vs. global standard. *Computer Law & Security Review*, p.3, nov., 2020. https://doi.org/10.1016/j.clsr.2020.105500. Acesso em 29 jan. 2021.

[93] Para Laura Brunet, a "[...] proteção efetiva da privacidade é posicionada como o elemento básico para que uma sociedade possa continuar a chamar-se democrática. Esse direito fundamental não pode ser enquadrado no esquema de 'ficar só', mas se especifica na atribuição a cada um do poder de 'governar' a informação que lhe diz respeito. A privacidade é transformada, assim, em elemento capital da liberdade do cidadão na sociedade da informação e conhecimento". NAHABETIÁN BRUNET, Laura. Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*, n. 39, p. 204, 2015.

[94] Importante citar o texto anterior a LPDP que demonstrava o cenário antes da edição da legislação uruguaia e expunha a necessidade de proteção de dados naquele momento. NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, n. 3, p. 1-30, 2007.

[95] Segundo o *site* especializado em ranqueamento de companhias *Clutch*, sete empresas uruguaias estão listadas entre as *15 Top Latin America App Development Companies* embora o Brasil tenha a primeira colocada e três entre as 15.URUGUAI XXI. Oito Empresas Uruguaias Entre As Melhores Da Latam No Desenvolvimento De Aplicações Móveis. 8 de julho de 2020. Disponível em: <https://www.uruguayxxi.gub.uy/pt/noticias/artigo/ocho-empresas-uruguayas-entre-las-mejores-de-latam-en-desarrollo-de-apps-moviles/>. Acesso em 10 dez.2020. Consultar, também, CLUTCH. Top Latin America App Development Companies. Disponível em: < https://clutch.co/app-developers/latin-america/leaders-matrix>. Acesso em 10 dez.2020.

[96] Banco Iberoamericano de Desenvovimento (BID). *Nota Técnica. AGESIC, um modelo exitoso*. Disponível em: <https://www.alejandrobarros.com/wp-content/uploads/2016/04/Nota_Tecnica_-_Agesic.pdf> . Acesso em 28 nov.2020.

política e estratégia de segurança cibernética, cultura e sociedade cibernética, educação, treinamento e habilidades em segurança cibernética, estruturas legais e regulamentares e padrões, organizações e tecnologias.

A liderança uruguaia torna-se relevante já que, no âmbito de uma sociedade em rede, os consumidores utilizam dados pessoais para acessar e utilizar sites, mídias sociais e tecnologias disponíveis por meio de aplicativos ou aplicações. A viabilização desse contato com a rede ocorre pelos fluxos de dados transfronteiriços. O caminho bilateral de disponibilização de dados e acesso a informações e conteúdo, permite que empresas de tecnologia os utilizem para obter lucro, embora não exista uma compensação pecuniária aos consumidores em razão da análise e da utilização dos dados por diferentes corporações. Por trás da utilização gratuita de serviços e aplicativos, há a monetização e a rentabilização dos serviços prestados, por meio da personalização do conteúdo ofertado. Nesse sentido, surge a necessidade de proteger os dados pessoais, preocupação que vem de algum tempo em sede europeia. O *e-commerce* e a constante digitalização da vida por diferentes canais digitais demanda a presença de instrumentos que guarneçam um mínimo de proteção técnica, jurídica e de conformidade – em termos de legitimidade – para operações relativas ao tratamento de dados pessoais de pessoas singulares pelas empresas controladoras de banco de dados[97]. A adoção de uma regulamentação que discipline a coleta, o tratamento e os direitos do titular surge como imposição tácita do mundo interconectado por meio da internet[98]. A transformação digital não é apenas *e-commerce*, embora esse espaço tenha uma ascendência importante, em razão de que 70% dos brasileiros estão conectados à internet, enquanto que mexicanos, com 67%, chineses, com 57% e indianos, com 41% apresentem um percentual inferior, o que deve ser contextualizado à luz da população e dos níveis de acesso aos dispositivos. No Brasil, o percentual do PIB que reflete o setor das novas tecnologias é 2,6%, enquanto a Índia apresenta indicador de 5,1%, a China, 4,8% e México, o percentual de 3%. Assim como no Brasil, no Uruguai, a proteção do consumidor e de dados pessoais possui tratamento diferenciado e separado[99]. A proteção do consumidor é prevista na Lei 17.250, de

---

[97] SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. *Perspectivas em Ciência da Informação*, n. 4, v. 24, p. 132-144, 2019.

[98] Sobre a inovação do Regulamento Europeu e o cotejo com a Lei Brasileira ver: LIMBERGER, Têmis. Informação em rede: uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Victor Rozatti (Org.). Direito Digital: direito privado e internet. São Paulo: Foco, 2019. p.253-266.

[99] AVELLARDUARTE. Internet no Brasil 2020 (estatísticas). Disponível em: https://www.avellareduarte.com.br/internet-no-brasil-2020estatisticas/ . Acesso em 14 jan. 2021.

2000[100] e regulamentado pelo Decreto 244/000. A URCDP cuida da matéria de proteção de dados pessoais, enquanto que a Área de Defesa do Consumidor, da Direção Geral de Comércio do Ministério de Economia e Finanças, atua na defesa do consumidor.

Em 2014, um estudo realizado pela AGESIC sugeriu que o comércio eletrônico está a caminho de se consolidar como uma nova forma de comercialização para as empresas, alcançando volumes de vendas que podem ser gerenciados remotamente, dando maior abertura ao comércio mundial das empresas uruguaias. Naquele ano, os uruguaios realizaram cerca de 380 mil transações eletrônicas por mês. Ao mesmo tempo, foi indicado para o mesmo ano que 15% dos uruguaios que utilizava a internet todos os dias havia feito pagamentos ou transferências pela internet, cerca de 270 mil usuários[101].

No Uruguai, o direito à proteção de dados pessoais incorpora-se à previsão constitucional do artigo 72, em razão da conexão entre a privacidade à pessoa humana[102]. Para compreender o panorama normativo da proteção aos dados no Uruguai, deve-se recorrer, especialmente, à LPDP[103] objetivação da tutela normativa, por meio da especificação e pormenorização de conceitos e distribuição de responsabilidades, inclusive com as alterações previstas pela Lei de Responsabilidade Fiscal uruguaia. A regulamentação da legislação ocorre pelo Decreto n. 414/009, de 31 de agosto de 2009[104], e, recentemente, pelo Decreto n. 64/2020, de 21 de fevereiro de 2020[105].

---

[100] URUGUAI. Lei 17.250, de 2000. Defensa del Consumidor. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp3295160.htm>.Acesso 14 nov.2020.

[101] URUGUAI. Comercio Electrónico en el Uruguay, da Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), 2014. Disponível em: < https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/1er-estudio-de-comercio-electronico-en-uruguay.>. Acesso em 15 nov. 2020. Conferir também URUGUAI. Resultados EUTIC2019: internet al alcance de todos en Uruguay, da Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. p.45-46. Disponível em: <https://www.ine.gub.uy/documents/10181/35704/Principales+resultados+de+la+Encuesta+de+Usos+de+Tecnolog%C3%ADas+de+la+Informaci%C3%B3n+y+la+Comunicaci%C3%B3n+2019/2488b09e-9cd5-453b-b6fc-7d66b2ba89ff>. Acesso em: 15 nov.2020.

[102] Segundo Ana Brian Nougrères, anteriormente à edição da LPDP, o "[...] direito à proteção dos dados pessoais nasce como uma garantia do indivíduo no exercício dos seus direitos fundamentais, uma garantia de que ele é um elemento chave no controle da comunicação ou utilização dos seus dados pessoais". NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, n. 3, p. 4, 2007.

[103] URUGUAI. Ley n. 18331, de 11 de agosto de 2008. Lei de Protección de Datos Personales. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 1 set. 2020.

[104] URUGUAI. Decreto n. 414/009, de 31 de agosto de 2009. Reglamentacion de la ley 18.331, relativo a la proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>.Acesso em 1 set. 2020.

[105] URUGUAI. Decreto 64/020, Reglamentacion de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 1 set. 2020.

Nessa linha, a primeira parte da legislação uruguaia cuida do reconhecimento da proteção de dados como direito pessoal[106] e das definições de princípios orientativos e de direitos e responsabilidades de controladores. Nesse sentido, a atuação das organizações responsáveis pelas bases de dados devem observar os seguintes princípios, que servem com critérios interpretativos: *(i)* legalidade, *(ii)* veracidade, *(iii)* finalidade, *(iv*) consentimento prévio informado, *(v*) segurança de dados, *(vi*) confidencialidade ou caráter reservado e *(vii)* responsabilidade[107].

Por sua vez, o Decreto 414/009[108] estabelece que o escopo de proteção de dados pessoais tem como objeto a proteção de que indivíduos que possam ser identificados, direta ou indiretamente, por meio de qualquer informação numérica, alfabética, gráfica, fotográfica, acústica ou outro meio ou suporte de identificação. Nessa linha de ideias, o regime jurídico para a proteção de dados pessoais[109] aplica-se à coleta, registro e aos tipos de tratamento, automatizado ou não, sob qualquer suporte e modo de uso, nas organizações públicas e privadas, excluindo-se *(i)* os dados utilizados para finalidades exclusivamente pessoais ou domésticas, como informações de sigilo de correspondência ou agendas pessoais; *(ii)* os dados utilizados para a defesa e segurança nacional e aqueles associados à repressão criminal; e, de forma aberta, *(iii)* às exceções criadas por legislação especial. No ponto de vista da amplitude de aplicação territorial, o Decreto 414/009 estabelece que a aplicabilidade da normativa ocorre sobre o tratamentos de dados *(i)* realizado em território uruguaio, sendo este o local onde o operador exerce a atividade, qualquer que seja a sua forma jurídica e ao *(ii)* responsável pela base de dados ou tratamento que não está estabelecido em solo uruguaio, mas que faz uso de dados coletados no país.

Fato relevante da normativa uruguaia é a previsão contida no artigo 6.º da LPDP que estabelece a obrigatoriedade da inscrição das bases de dados, de forma a dar cumprimento ao

---

[106] Para Laura Brunet, o "[...] fundamento da proteção de dados fornece proteção à dignidade humana, constituindo um fundamento substancial da liberdade individual. Envolverá uma concretização, de forma indiscutível, dos direitos clássicos da personalidade, quais são a honra, privacidade e autoimagem". NAHABETIÁN BRUNET, Laura. Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*, n. 39, p. 203, 2015. Sobre o direito ao esquecimento, conectado à proteção dos dados, consultar: SCHIAVI, Pablo. El derecho al ovido ya la protección de datos personales en Uruguay. *Revista de Direito Administrativo e Infraestrutura*, v. 1, n. 2, p. 309-331, 2017.

[107] Em uma perspectiva anterior à legislação, consultar também: BRAUSE-BERRETA, Alberto. La situación en Uruguay sobre protección de datos personales. PIÑAR-MAÑAS, José Luis. *Protección de datos de carácter personal en Iberoamérica*, Valencia: Tirant Lo Blanch, 2005. p. 337-342.

[108] URUGUAI. Decreto n. 414/009, de 31 de agosto de 2009. Reglamentacion de la ley 18.331, relativo a la proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>.Acesso em 1 set. 2020.

[109] URUGUAI. Ley n. 18331, de 11 de agosto de 2008. Lei de Protección de Datos Personales. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 1 set. 2020.

princípio da legalidade do tratamento de dados pessoais. A inscrição do banco de dados deve ser realizada na URCDP. O Decreto 414/009 prevê a forma de inscrição desses bancos de dados, no artigo 15 e 16[110]. Os bancos de dados devem ser registrados na Unidade de Regulamentação e Controle de Dados Pessoais ("URCDP"). É importante observar que não apenas bancos de dados pessoais escritos devem ser registrados, mas também bancos de dados de áudio, vídeo[111] e de videovigilância[112].

Nesse sentido, a regulamentação das formas de controle está prevista no artigo 1.º do Decreto nº 664/008[113], de 22 de dezembro de 2008, que prevê que devem se registrar *(i)* pessoas físicas que criam, modificam ou excluem bases de dados pessoais, exceto para uso exclusivamente pessoal ou doméstico e *(ii)* pessoas jurídicas públicas, estaduais ou não, e privadas, que criam, modificam ou excluem bancos de dados pessoais, *(iii)* os códigos de conduta utilizados para a prática profissional que estabelecem regras para o tratamento de dados pessoais e *(iv)* autorizações para transferências internacionais de dados pessoal. Nesse sentido, pode-se notar um importante controle, por parte da URCDP, sobre os bancos de dados, por meio da formação de um banco de dados dos bancos de dados cadastrados. Essa perspectiva permite a inspeção posterior por parte da autoridade de controle.

Além disso, os responsáveis por todas as bases de dados ou tratamentos devem cadastrá-los no Cadastro da URCDP de acordo com o art. 4.º, do Decreto nº 664/008, fornecendo as seguintes informações: *(i)* identificação da base de dados e do seu responsável, *(ii)* procedimentos para obtenção e processamento de dados; *(iii)* medidas de segurança e descrição técnica da base de dados, *(iv)* proteção de dados pessoais e exercício de direitos, *(v)* destino dos dados e pessoas físicas ou jurídicas a quem podem ser transmitidos, *(vi)* tempo de conservação de dados, *(vii)* forma e condições em que as pessoas podem acessar os dados referidos a eles e os procedimentos a serem realizados para a retificação ou atualização de

---

[110] URUGUAI. Decreto n. 414/009, de 31 de agosto de 2009. Reglamentacion de la ley 18.331, relativo a la proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>.Acesso em 1 set. 2020.

[111] MOSCA, Javier Berdaguer. La imagen como dato personal. *Doctrina y jurisprudencia de derecho civil*, n. 6, p. 31-40, 2018.

[112] GIUZIO, Graciela. Video-vigilancia: La jurisprudencia de la unidad reguladora y de control de datos personales (AGESIC). *Derecho Laboral*. Revista de doctrina, jurisprudencia e informaciones sociales, v. 56, n. 250, p. 355-368, 2013.

[113] URUGUAI. Decreto nº 664/008, de 22 de dezembro de 2008. Creacion del registro de bases de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/664-2008>. Acesso em 1 set. 2020.

dados, *(viii)* dados submetidos a tratamento na referida base de dados e *(ix)* endereço cadastrado para fins de comunicações e notificações que correspondem[114].

[114] URUGUAI. Decreto nº 664/008, de 22 de dezembro de 2008. Creacion del registro de bases de datos personales. Disponível em: https://www.impo.com.uy/bases/decretos/664-2008. Acesso em 1 set. 2020.

3 A COMPARAÇÃO ENTRE ÓRGÃOS REGULADORES: URCDP E A ESTRUTURAÇÃO DA ANPD NO BRASIL

Pensar a *proteção de dados* na sociedade contemporânea demanda a reflexão conjunta com as múltiplas zonas de interação, nos planos interno e externo. A perspectiva relacional entre a tecnologia e o humano, que pode ser desenvolvida com base em diferentes e possíveis *inícios*, é revista com a aceleração da disponibilidade de informações e tecnologias ao dispor humano. Nesse sentido, o objeto de uma pesquisa comparativa deve encontrar cortes de análise vertical e horizontal, de forma que a exploração dos resultados não se resuma à mera comparação legislativa. Promover o aprimoramento institucional encontra-se entre os desideratos dessa abordagem[115]. Nesse sentido, busca-se estabelecer quadros comparativos com a experiência uruguaia, por meio da atuação da AGESIC e URCDP, cuja atuação possui como plano de fundo a sociedade da informação e amplitude dos processos de digitalização.

Com base nessa premissa, poderemos delimitar, com melhor qualidade de precisão, o papel de uma autoridade de proteção de dados no ambiente de uma sociedade digital, tendo em vista que o RGPD, em vigor na União Europeia, e a LGPD, no Brasil, demonstram uma caminhada humanitária em direção à ampliação do universo protetivo dos dados pessoais, porém que pode se revelar insuficiente sem a apreensão do contexto de uma sociedade remodelada, com novas dinâmicas, e que, portanto, demanda novas formas de enfrentamento do problema de violação direita ou invisível de direitos. Uma delas reside em levar a constituição, estruturação, planejamento da ANPD, compatível com a realidade e ascensão das transformações da sociedade em rede.

O modelo de autoridades independentes[116], que tomou dimensões relevantes na década de 1980 e 1990 como alternativas de regulação econômica e sinal à credibilidade institucional

---

[115] Godoy e Ribeiro sustentam que o "[...] processo de internacionalização jurídica pelo qual o mundo passa amplia a necessidade e os rumos dos estudos de direito comparado. Em um primeiro momento, sugere que estudemos os efeitos da internacionalização em relação ao direito interno. Percepções de qualidade podem sugerir que se indiquem direitos melhores ou piores. Os direitos são apenas diferentes. O estudioso do direito comparado deve estar preparado para a armadilha que se lhe põe a todo o momento. O exercício da comparação não se fundamenta, necessariamente, em orientação que exija montagem de tabela qualitativa. Em princípio, direitos não são melhores nem piores, mais ou menos avançados, mais ou menos iluminados. Os direitos são diversos. O direito comparado não é, necessariamente, e de modo ingênuo, instrumento que garanta melhor relacionamento entre os diversos povos". GODOY, Arnaldo Sampaio de Moraes; RIBEIRO, Gustavo Fereira. O direito comparado: esforço de resgate historiográfico e de problemas metodológicos. *Revista de Direito Internacional*, Brasília, v. 17, n. 1, p. 38, 2020.

[116] [116] LIMBERGER, Têmis. *O direito à intimidade na era da informática*: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p.148. Conferir também a monografia de CARDONA, Maria Celeste. *Contributo para o conceito e a natureza das entidades administrativas independentes: autoridades reguladoras*. Coimbra: Almedina, 2017.

ante as crises estatais, passou a ser sugerido como maneira de conferir confiança e credibilidade ao modelo de proteção de dados brasileiro iniciado, pautado pela definição de regras e princípios, o estabelecimento de um órgão regulador e o conjunto de tarefas cominadas a serem exercidas ativamente pelo setor público e privado. Insere-se no quadro de superação do modelo estatal preponderantemente intervencionista para o modelo regulador[117]. Observe-se que expoentes da doutrina da proteção de dados no Brasil tomaram posição no sentido de defender a independência de um órgão que ainda estava em formação, embora se defendesse há mais de anos a noção de independência total, seguindo, em boa medida, o modelo europeu[118]. O problema nuclear de toda a discussão reside em saber se há, na tradição brasileira, uma agência ou autoridade que resguarde todos os atributos que permitam identificar a independência normatizada em sede europeia[119], especialmente o ponto distintivo fundamental: a ausência de subordinação hierárquica[120]. Em outras palavras, cabe conferir se existe, no Brasil, paralelo organizacional e institucional de uma autoridade administrativa ao modelo europeu, tema que, inclusive, não é inerte de polêmicas naquele âmbito comunitário[121]. Opta-se por realizar uma análise integrada entre os conceitos fundamentais e estruturais das agências regulatórias ou autoridades administrativas e as tarefas desempenhadas pela ANPD.

O tema das autoridades regulatórias emerge com as crises das décadas de 1970 e 1980, pautadas, não exclusivamente, na ausência de condições materiais e financeiras de suportar o custo da prestação direta pelo Estado de serviços à população. A década de oitenta provou-se ser um período decisivo na transformação do modelo estatal anterior, de cunho mais social e intervencionista[122]. Nessa linha, a criação de um ambiente que viabilizasse a menor

---

[117] LA SPINA, Antonio. *Lo Stato Regolatore*. Bolonha: Il Mulino, 2000.

[118] VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 717-739.

[119] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. 2015.Universidade de São Paulo, Ribeirão Preto, 2015.

[120] ARAGÃO, Alexandre Santos de. Supervisão ministerial das agências reguladoras: limites, possibilidades e o parecer AGU nº AC - 51. *Revista de Direito Administrativo*, v. 245, p. 237-262, 2007. Conferir, também, GUERRA, Sérgio. Agências reguladoras e supervisão ministerial. In: Alexandre Santos de Aragão. (Org.). Poder Normativo das Agências Reguladoras. Rio de Janeiro: Ed. Forense, 2006.

[121] FRANCHINI, Claudio. Autonomia e independenza nell'amministrazione europea. *Diritto amministrativo*, Milano, n.1, p. 91, 2008.

[122] Em uma linha crítica, salienta Cunha que é "[...] importante enfatizar que o modelo de agências reguladoras é tido, dentro da lógica anglo-saxã de Estado regulador, como uma peça-chave, pois supostamente viabiliza a desejada separação entre as decisões políticas e técnicas. Todavia, o modelo de agências independentes não deve ser visto como solução única, tampouco como inexorável, sob o ponto de vista da regulação das atividades econômicas. Sua adoção, no Brasil, decorreu de opção dos reformistas da época, alimentada pelo forte

intervenção do Estado, com intensificação de sua atividade regulatória, elevou o ramo público-administrativista ao papel de viabilizar as mudanças preconizadas em nível político. Nesse sentido, o avançar das privatizações, do advento das parcerias público-privadas e das concessões de serviços públicos revelou uma face do Estado como ator organizador das atividades desempenhadas.

Se por um lado, é possível verificar o pragmatismo da adoção de agências reguladoras ou autoridades administrativas, o que vem sendo modificado desde o final do século passado[123]; por outro, não é possível desconsiderar a emergência da consolidação do tratamento uniforme da matéria de proteção de dados e dos instrumentos estatais por meio dos quais a proteção se viabiliza, entre eles, a previsão de um órgão regulador dotado de garantias formais e subjetivas de independência. Falta, no entanto, conforme já denunciava Amato, que as "[...] autoridades independentes, ou melhor, as instituições indiscriminadamente chamadas assim, são hoje vítimas do inexorável fascínio que sempre exercem, mesmo sobre os mais prudentes, as simplificações unificadas"[124]. Nessa linha de ideias, é necessário distinguir, restringir e racionalizar o que se entende por autoridade independente, porquanto o simples fato de se denominar ou defender a adoção de um órgão administrativo como independente ou com autonomia técnica e decisória, não garante a independência preceituada[125]. Pelo contrário, a existência e verificação concreta de um modelo de regulação consolidado, reconhecido internacionalmente e que resulte no incremento da confiança externa às atividades de regulação e fiscalização apresenta-se como ponto de análise o qual prescinde de adjetivos e qualificações atribuídas de antemão. Somente a verificação concreta permite concluir a veracidade da autonomia, mesmo porque, seguindo uma linha comparatista tecida por Ancel,"[...] não se deve contentar, passiva e rapidamente, com um texto de lei estrangeira que,

---

paralelismo criado com experiências de países avançados, notadamente Estados Unidos e Reino Unido". CUNHA, Bruno Queiroz. Antagonismo, modernismo e inércia: a política regulatória brasileira em três atos. Cadernos EBAPE.BR, v.14, [s.n.], p.477, jul., 2016.

[123] Para Giandomenico Majone, o "[...] novo modelo, que começou a surgir no fim dos anos 70, inclui a privatização, a liberalização, a reforma dos esquemas de bem-estar e também a desregulação. [...] A verdade é que, neste período, métodos tradicionais de regulação e de controle estavam ruindo sob a pressão de potentes forças tecnológicas, econômicas e ideológicas, e foram desmantelados ou radicalmente transformados". MAJONE, Giandomenico. Do Estado positivo ao Estado regulador: causas e conseqüências de mudanças no modo de governança. *Revista do Serviço Público*, v. 50, n. 1, p. 9, 1999.

[124] AMATO, Guilio. Autorità semi-indipendenti e autorità di garanzia. *Rivista trimestrale di diritto pubblico*, n.3, p.645,1997.

[125] Na mesma linha de argumentação de Guilio Amato, Aragão salienta que existem "[...] grandes disparidades entre elas em função dos distintos graus de 'autonomia reforçada' que lhes é assegurada, o que inclusive leva a um sem-número de divergências doutrinárias quanto à inclusão desta ou daquela entidade na categoria". Em outra linha de visão, analisando se as autoridades são independentes, na prática, em solo europeu, verificar: GROENLEER, Martijn. *The autonomy of European Union agencies*: A comparative study of institutional development. Eburon Uitgeverij BV, 2009.

aparentemente, dê a indicação desejada, mas que não foi nem verificado, nem confrontado com o seu contexto"[126].

A contextualização assume fundamental relevância tendo em consideração que o surgimento dos órgãos reguladores surgiu no contexto de profundo liberalismo econômico nos Estados Unidos[127], sendo, após, incorporado na experiência inglesa – por meio dos *quangos* – na doutrina administrativa europeia, especialmente na França[128], não se olvidando da experiência portuguesa[129]. O problema fundamental que reside na incorporação ou espelhamento está na não observância que, por exemplo, na Inglaterra, as instituições em comento foram adaptadas à tradição do *commom law*[130], cujas construções jurídicas têm como fundamental marca o aspecto consuetudinário. Nessa linha de ideias, observar que *quangos* desempenhavam atividades com maior preponderância de caráter executivas do que regulatórias e que o setor de atuação tinha nas funções ministeriais um suporte governamental diferenciado[131].

No Brasil, há a inconveniência terminológica decorrente da utilização do termo agências, uma espécie de aglutinação ou incorporação da nomenclatura norte-americana de *agencies*, provocadora, inclusive, de certa aversão doutrinária à utilização do termo, mas que demarca a intensa influência da adoção de um modelo similar ao americano[132]. Para Floriano

---

[126] ANCEL, Marc. *Utilidade e Métodos do Direito Comparado*. Tradução de Sérgio José Porto. Porto Alegre: Sérgio Antonio Fabris, 1980. p.112.

[127] Esse modelo não foi estanque a problemas de controle, legitimidade e coordenação, conforme se percebe pelo artigo: SHAPIRO, Martin. The problems of independent agencies in the United States and the European Union. *Journal of European Public Policy*, v. 4, n. 2, p. 276-277, 1997.

[128] No direito francês, as autoridades administrativas independentes não possuem personalidade jurídica, contudo podem perseguir seus interesses em juízo, já que possuem autonomia peculiar ao quadro de descentralização. BADIN, Luiz Armando. As autoridades administrativas independentes na França: finalidades institucionais e meios de atuação. In: DI PIETRO, Maria Sylvia Zanella. (Org.). Direito regulatório: temas polêmicos. Belo Horizonte: Ed. Fórum, 2003, p. 491-508. Consultar também, POMED SÁNCHEZ, Luis. Fundamento y naturaleza jurídica de las administraciones independientes. *Revista de Administración Pública*, Madrid, v.132, p.133-138, 1993.

[129] CARDONA, Maria Celeste. *Contributo para o conceito e a natureza das entidades administrativas independentes: autoridades reguladoras*. Coimbra: Almedina, 2017.

[130] LOMBARTE, Artemi Rallo. Las administraciones independientes: una aproximación constitucional. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás (Org.). *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009. p.11.

[131] POMED SÁNCHEZ, Luis. Fundamento y naturaleza jurídica de las administraciones independientes. *Revista de Administración Pública*, Madrid, v.132, p.122-123, 1993.

[132] Nos Estados Unidos, o termo é utilizado para designar o gênero dos órgãos públicos, no âmbito regulatório, com a *independent regulatory agencies* ou *commissions* e as *executive agencies*, responsáveis pela execução da legislação (law enforcement), mas não as atividades de regulação. Naquele país, existem inúmeras agências estaduais e federais, cada qual com características próprias e formas de controle que demandam explanações. Mesmo órgãos similares como o *Federal Bureau of Investigation* (FBI) e a Polícia Federal, no Brasil, possuem pontos de não convergência estrutural e de pessoal. A *Federal Trade Commission*, outra agência americana, possui o perfil de proteção ao consumidor e controle da concorrência, mas guarda profundas diferenças com o

Marques Neto, o termo que guarda maior espaço de credibilidade é o de *autoridade*, por incorporar a feição pública, regulatória e de autonomia técnica e decisória[133]. Esse é um ponto positivo da adoção, por parte da técnica legislativa brasileira, da nomenclatura de "Autoridade Nacional de Proteção de Dados" (ANPD), especialmente, por elidir de críticas o fato de que o texto constitucional brasileiro trata as entidades reguladoras como órgãos reguladores[134] e não de outra forma. Tradicionalmente, as autoridades nacionais assumem a função de tornarem-se as *guardiãs* do sistema nacional de proteção de dados e adotar medidas que equilibrem o respeito do direito fundamental à vida privada e à livre circulação de dados, resultante da inovação, do desenvolvimento econômico e tecnológico. Conforme destaca Piñar Mañas, no horizonte crítico da necessidade de independência das autoridades, "[...] se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho"[135]. Aliás, conforme lecionam Schertel Mendes e Doneda "[...] sem uma autoridade central, independente e com credibilidade técnica, dificilmente será possível a aplicação consistente e harmônica da Lei em setores tão diversos como *aqueles que compõe seu âmbito de aplicação"*[136].

"paralelo" Conselho Administrativo de Defesa Econômica (CADE), inclusive em termos da natureza da regulação americana em contraste com a brasileira. Essa perspectiva ilustra a polêmica transposição linguística, propensa a gerar confusões e refração doutrinária. Nesse sentido, Aragão afirma que, a "[...] demora na adoção do modelo das agências reguladoras independentes pelos demais países se deve menos a um suposto atraso na evolução do Direito Administrativo e mais às circunstâncias político-econômicas neles verificadas. Mais especificamente, os EUA sempre tiveram uma perspectiva liberal e não-estatizante bastante forte, ao passo que a América Latina e a Europa Continental se viram ao longo de todo o século passado envolvidas em uma série de demandas e convulsões sociais que levaram o Estado a adotar uma política estatizante". ARAGÃO, Alexandre Santos de. As agências reguladoras independentes: algumas desmistificações à luz do direito comparado. *Revista de Informação Legislativa*, n.155, p.296, jul-set., 2002.

[133] Floriano Marques Neto prefere o termo de autoridades reguladoras independentes, salientando que essa escolha ocorre para referir a entes administrativos reguladores de nova geração, justo porque essa "[...] designação (constante na doutrina europeia, portuguesa em particular) tem o mérito de nela embutir os três aspectos centrais para caracterização das agências: serem elas i) órgãos públicos, dotados de autoridade; ii) voltados ao exercício da função de regulação e iii) caracterizados pela independência. Se bem entendidos, estes três aspectos estarão expostos aos pressupostos das agências no direito brasileiro." MARQUES NETO, Floriano Peixoto de Azevedo. *Agências Reguladoras Independentes*: Fundamentos e seu Regime Jurídico. 1. ed. Belo Horizonte: Editora Fórum, 2005. p.55.

[134] Nesse sentido, no que tange à intervenção estatal, a Constituição sempre trata os órgãos responsáveis como órgãos reguladores, como se depreende da consulta dos artigos 21, XI e do artigo 177, §2.º, III. BRASIL. *Constituição da República Federativa do Brasil*. Disponível em:< http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 14 nov.2020.

[135] PIÑAR MAÑAS, José Luis Administración electrónica y protección de datos personales, *Revista Jurídica da Universidade de Santiago de Compostela*, Santiago de Compostela, n.1, p.167, 2011.

[136] SCHERTEL MENDES, Laura; DONEDA, Danilo. Reflexões gerais sobre a nova lei de proteção de dados. *Revista do Direito do Consumidor*, v.120, p.478, nov./dez. 2018.

3.1 Funções de uma autoridade administrativa

A amplitude de atuação de um órgão regulador precisa ser analisada, em vista da definição do que deve executar uma autoridade de dados e quais são as funções que desempenha. Nesse sentido, a experiência indica como atribuição de agências reguladoras a tarefa de regular o setor econômico, de acordo com os limites previstos no texto constitucional e conforme a vontade legislativo-democrática estabelecida nas leis especiais. Saliente-se que, conforme destaca Aragão, no Brasil, não há, nas leis que instituíram as agências reguladoras, a previsão expressa de serem elas "autoridades independentes" ou outorgarem às entidades o papel de ser a "última instância administrativa"[137]. A feição destacada de regular um segmento da ordem econômica, como fazem as autoridades de concorrência ou monetárias, apresenta-se como característica diferenciada da instituição da ANPD, no Brasil, já que ela desempenhará funções de regulação, normatização e fiscalização das tarefas cominadas em lei para a proteção de dados pessoais. Enquanto a experiência das agências regulatórias foca atenções preponderantemente no aspecto econômico, o órgão administrativo regulador cuida das múltiplas facetas da proteção de um direito fundamental, o que o diferencia sensivelmente de outras instituições[138].

Partindo-se de uma perspectiva genérica, o exercício da regulação depende da atribuição às agências reguladoras de uma amplitude de poderes ou funções para que as finalidades institucionais sejam atingidas[139]. O que se realiza é a delegação de atribuições aos órgãos mais especializados, à semelhança do que ocorreu internacionalmente, com a transferência de responsabilidades e a auditoria posterior, por meio da prestação de contas e controle das atividades reguladas.

Nesse sentido, podem ser enumerados os seguintes elementos como pertencentes à gama de poderes exercidos: *(i)* poder normativo, associado à edição de comandos ao setor ou segmento[140], de forma a complementar as previsões que se utilizam de conceitos abertos; *(ii)* o

---

[137] Nesse sentido, já se advogou pela maior fluidez e independência de autoridades, de modo a desviá-las de amarras, conforme se lê com Michelle Everson. EVERSON, Michelle. Independent agencies: hierarchy beaters?. *European Law Journal*, v. 1, n. 2, p. 180-204, 1995. Na doutrina brasileira, consultar: ARAGÃO, Alexandre Santos de. Supervisão ministerial das agências reguladoras: limites, possibilidades e o parecer AGU nº AC - 51. *Revista de Direito Administrativo*, v. 245, p. 247, 2007.

[138] ALMAGRO, Ricarlos. Agências reguladoras independentes e legitimidade democrática. *De jure*: revista jurídica do Ministério Público do Estado de Minas Gerais, n. 9, p. 67–84, jul./dez., 2007.

[139] MARQUES NETO, Floriano Peixoto de Azevedo. *Agências Reguladoras Independentes*: Fundamentos e seu Regime Jurídico. 1. ed. Belo Horizonte: Editora Fórum, 2005. p.60.

[140] Os referidos órgãos têm, nas palavras de Sérgio Guerra, o "[...] poder-dever de exercer uma função normativa secundária, desde que observadas as normas hierarquicamente superiores. Isto é, a norma não pode ser primária,

poder de fiscalizar a atuação dos particulares e dos órgãos públicos que desempenhem atividades previstas; *(iii)* o poder de outorgar ou credenciar particulares, em consonâncias com as autorizações previstas na legislação; *(iv) o* poder sancionatório, no âmbito do que se denomina de direito administrativo sancionador[141], consistente em estabelecer parâmetros e aplicar punições administrativas àquelas organizações que venham a descumprir as instruções legais e infralegais; *(v)* poder de instrução ou de recomendação administrativa, consistente em elaborar relatórios, estudos e documentos de orientações e informativos aos setor regulador, inclusive sugerindo medidas técnicas a serem adotadas pelos poderes constituídos da repúblicas[142]; e, por fim, *(vi)* poderes de julgamento ou de conciliação[143], de forma a compor, sem a provocação do Poder Judiciário, conflitos que advindo do desempenho de atividades pelos sujeitos da regulação[144].

Embora as funções administrativas como a concessão de autorizações não seja questionada, disso não decorre a inexistência de polêmicas quanto aos poderes de normatização. As funções de natureza normativa trazem à consideração a superação da noção clássica de separação dos poderes que privilegia o princípio da legalidade e da preponderância da vontade parlamentar. Aos órgãos reguladores restaria a função de atuar na construção

---

haja vista que, entre nós, a função normativa primária é precípua do Poder Legislativo". GUERRA, Sérgio. *Introdução ao Direito das Agências Reguladoras*. Rio de Janeiro: Freitas Bastos, 2004. p.42-43. Nesse sentido, "[...] por sua sede constitucional, temos uma reserva inquestionavelmente legítima de poder normativo delegificado em favor de órgãos ou entidades estranhas ao Poder Legislativo. E mais, como essas esferas normativas autônomas fundamentam-se diretamente no Poder Constituinte, estão protegidas contra as ingerências que a elas venham a ser impostas, ressalvada, naturalmente, a incidência de normas da própria Constituição, mormente as concernentes à Administração Pública, e a possibilidade de balizamento e coordenação de caráter político – não técnico – pelo Poder Legislativo". ARAGÃO, Alexandre Santos de. O poder normativo das agências reguladoras independentes e o Estado Democrático de Direito. *Revista de Informação Legislativa*, n. 148, p.291-292, out./dez., 2000.

[141] OSÓRIO, Fábio Medina. *Direito Administrativo Sancionador*. 7.ed. São Paulo: Revista dos Tribunais, 2020.

[142] Cabe o registro ofertado por Franchini, no sentido de que a "[...] atribuição de determinadas competências, de autonomia de gestão e organizativa, orgânica, financeira e contábil, por um lado, e a prestação de certas garantias aos proprietários de empresas, por outro, são instrumentais para o efeito de reconhecimento concreto de uma posição de imparcialidade e neutralidade, pois contribuem para o desenho do arcabouço jurídico adequado ao melhor exercício da função". FRANCHINI, Claudio. Mito e realtà delle autorità indipendenti. *Impresa e Stato*, , n. 35, p. 34, 1996.

[143] GUERRA, Sérgio; SALINAS, Natasha Schmitt Caccia. Resolução eletrônica de conflitos em agências reguladoras. *Rev. direito GV*, 2020, vol.16, no.1.

[144] Sérgio Guerra, conectado ao tema do que denominou dizer funções quase-legislativas ou quase-judiciais, destaca que se pode concluir "[...] com aqueles doutrinadores que sustentam a legalidade e a legitimidade do exercício da função judicante pelas agências reguladoras, que somente as entidades tecnicamente preparadas e dotadas de todas as informações e mecanismos para regular um subsistema econômico ou social, têm condições de visualizar todo o cenário que envolve uma decisão isolada diante do caso concreto. Esse aspecto prospectivo da decisão que põe fim a um conflito entre agentes regulados, tem reais condições de sopesar, ponderar e estabelecer um efetivo equilíbrio entre os diversos interesses em presença". GUERRA, Sérgio. *Introdução ao Direito das Agências Reguladoras*. Rio de Janeiro: Freitas Bastos, 2004. p.44. Nesse sentido, também, BARBOSA, Joaquim. Agências reguladoras: a metamorfose do estado e da democracia (uma reflexão de direito constitucional e comparado). *Doutrinas Essenciais de Direito Administrativo*, vol. 6, p. 943-984, 2012.

normativa, sem inovar e apenas respeitando os limites previstos em lei. Contudo, a capacidade técnica e a disponibilidade tecnológica das agências e organizações regulatórias estatais permitem a formulação de um amplo conjunto de regras especializadas que distam da previsão legal anterior, porém não violam frontalmente o texto constitucional[145].

3.2 Regulação e independência: o desafio para a construção da ANPD

A aceleração provocada pelos processos econômicos – notadamente, com o avanço e progresso de políticas de abertura econômica e de competitividade, vinculadas ou não ao deslocamento industrial de países desenvolvidos para países em desenvolvimento – teve como consequência o fenômeno da regulação e da instrumentalização em forma de estruturação em agências. A regulação surge como meio de garantir a continuidade política e a segurança institucional, como freio à politização excessiva de assuntos técnicos, mas equalizando os interesses de diferentes atores, especialmente em momentos de crise[146]. Além da noção de atribuir aos órgãos regulatórios à continuidade diretiva de determinados assuntos relevantes econômica e socialmente[147], os órgãos reguladores têm como função conferir aparência de neutralidade e objetividade, destacando-se da administração central ou desconcentrando as atividades desempenhadas. O núcleo desse processo reside na imunização da administração de fatores burocráticos e da pressão de interesses[148].

A viabilização conecta-se à necessária existência e concentração de ativos intelectuais – ou do conhecimento especializado – por parte do órgão, que deverá estabelecer novas regras, *standards* ou produzirá informações técnicas para o correto desempenho das atividades reguladas, reduzindo a assimetria informativa ou viabilizando a cooperação entre organizações privadas e públicas[149]. Instituir garantias de manutenção para que os quadros

---

[145] MOREIRA, Egon Bockmann; CAGGIANO, Heloisa Conrado. O poder normativo das agências reguladoras na jurisprudência do STF - Mutação constitucional do princípio da legalidade? *Revista de Direito Público da Economia - RDPE*, Belo Horizonte, ano 11, n. 43, jul./set. 2013.

[146] GUERRA, Sérgio; SALINAS, Natacha; GOMES, Lucas As agências reguladoras em resposta à crise da COVID-19. *Revista de Administração Pública (Impresso)*, v. 54, p. 874-897, 2020.

[147] Para Marques Neto, "[...] regulação pelas agências, portanto, consagra a estabilidade e a permanência na consecução das políticas públicas. Refreia, porém, a absorção destas pela política governamental de mais curto prazo, aquela que não predique objetivos gerais de governo, mas apenas os objetivos imediatos do governo. A regulação, portanto, i) favorece o planejamento; ii) incrementa a estabilidade e a institucionalidade (não a imutabilidade) das políticas; e iii) dá consistência à mudança". MARQUES NETO, Floriano Peixoto de Azevedo. *Agências Reguladoras Independentes*: Fundamentos e seu Regime Jurídico. 1. ed. Belo Horizonte: Editora Fórum, 2005. p.94.

[148] FRANCHINI, Claudio. Mito e realtà delle autorità indipendenti. *Impresa e Stato*, n. 35, p. 29, 1996.

[149] Nessa linha de ideias, Marques Neto sustenta que "[...] capacidade técnica do regulador é também um requisito para a própria legitimação da regulação. Quanto mais a agência (e seus agentes) dominar os códigos,

técnicos permaneçam atualizados e informados, dispondo de mecanismos de permitam a realização de pesquisas e estudos técnicos, torna-se relevante, ao ponto de tornar a edição de resoluções e instruções normativas mais precisas e em conformidade com a evolução tecnológica e, inclusive, a correta auditoria e análise da documentação apresentada por organizações sujeitas à supervisão do órgão.

Têmis Limberger[150] sustenta que as autoridades independentes possuem duas marcas essenciais: a independência e a neutralidade. A primeira vincula-se ao aspecto estrutural, conforme visto. Por sua vez, a neutralidade – a outra característica –vincular-se-ia à condução da autoridade de forma desvinculada da política[151]. Nessa linha, na medida em que existem espaços isentos de controle e influência governamental, caberia ao poder político, no máximo, a nomeação dos dirigentes. Nesse sentido, seguindo a doutrina de Rallo Lombarte[152], houve quem considerasse os perfis e as características do fenômeno como descumpridor dos dispositivos constitucionais básicos. Nesse sentido, abortar o tema da administração independente, dos poderes neutros, poderes independentes, poderes autônomos não seria constitucionalmente viável porquanto a autonomia negaria o círculo democrático, as regras básicas de legitimação democrática do poder.

Em torno da temática, sustentou-se, de forma contrária, que o problema da existência de autoridades independentes residiria na ideia de que, uma vez nomeados os diretores e estruturada, ninguém poderia destituir os poderes e decisões – e que, portanto, não responderiam a ninguém, em razão da independência se materializar em não responder a ninguém[153]. Todavia, vale destacar a posição de Lombarte no sentido de que a construção de uma autoridade independente passa pela noção de que esta pessoa jurídica não está acima da Constituição ou das leis. Pelo contrário, a independência é exercida conforme os limites que

---

necessidades e possibilidades do setor regulado, mais será eficiente a regulação." MARQUES NETO, Floriano Peixoto de Azevedo. Agências Reguladoras Independentes: Fundamentos e seu Regime Jurídico. 1. ed. Belo Horizonte: Editora Fórum, 2005. p.62.

[150] LIMBERGER, Têmis. *O direito à intimidade na era da informática*: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p.147.

[151] LIMBERGER, Têmis. *O direito à intimidade na era da informática*: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p.147.

[152] LOMBARTE, Artemi Rallo. Las administraciones independientes: una aproximación constitucional. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás (Org.). *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009.p.13.

[153] LOMBARTE, Artemi Rallo. Las administraciones independientes: una aproximación constitucional. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás (Org.). *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009.p.13.

os princípios constitucionais estabelecem, especialmente, conforme já se cosolidou em solo europeu[154].

Esse estatuto da independência se reflete na existência de garantias estatutárias e independência orgânica e funcional[155]. Quanto à independência orgânica, ela se faz presente na composição colegiada dos órgãos; as garantias estatutárias cuidam da existência de um mandato de duração fixa e a garantia da inamovibilidade dos seus membros, já a independência funcional assegura a gestão material e financeira e pela competência normativa para a elaboração do seu próprio regulamento interno.

A discussão acerca da independência dos órgãos responsáveis pela regulação e fiscalização não passou longe de debates, inclusive tendo o modelo considerado em "xeque" pelo jurista português Vital Moreira[156], por considerar que persistia a supervisão ministerial, mesmo que os poderes e as limitações do exercício dos controles superiores não tenham sido definidos, razão que inviabilizaria formalmente poderes independentes às agências reguladoras[157]. Não há, na Constituição Federal dispositivo que defina os limites dessa supervisão. A descentralização, por meio da criação de um órgão no âmbito da Administração Indireta, repercute na inexistência de relação hierárquica, restando, contudo, o que se denomina de tutela administrativa. Por outro lado, a desconcentração administrativa, no âmbito dos órgãos da administração direta levaria à noção de relação de subordinação. Todavia, é necessário olhar os detalhes da construção de uma autoridade. É importante notar,

---

[154] LIMBERGER, Têmis. *O direito à intimidade na era da informática*: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.p.150.

[155]Segundo Garcia Costa, deve-se empregar técnicas para que se implementem as garantias: do ponto de vista orgânico com "[...] a) criação por lei; b) o reconhecimento da personalidade jurídica própria; c) a atribuição de poder regulamentar para aprovar os seus estatutos ou regulamentos internos" e do ponto de vista funcional, o fato de que "[...] no desempenho de tais funções, em nenhum caso solicitarão ou receberão ordens ou instruções do Governo, de qualquer outro órgão público ou entidade privada; b) o segundo deles, a atribuição exclusiva às autoridades autónomas da função para que foram criadas, de forma a que exerçam com exclusividade e com exclusão de todas as competências de um determinado domínio da regulação social". Existe também a questão vinculada á autonomia de pessoal. GARCÍA COSTA, Francisco Manuel. La independencia de las autoridades administrativas garantes del derecho de acceso a la información pública. Disponível em: <http://laadministracionaldia.inap.es/noticia.asp?id=1510342>. Acesso em 15 de dez. 2020.

[156] MOREIRA, Vital. Agências reguladoras independentes em xeque no Brasil. In: MARQUES, Maria Manuel Leitão; MOREIRA, Vital. *A mão visível*: mercado e regulação. Coimbra: A1medina, 2003, p. 228-229. Cf., também, GUERRA, Sérgio; SALINAS, Natacha. O Congresso Nacional e a frágil autonomia das agências reguladoras. *Conjuntura Econômica (Rio De Janeiro)*, v. 74, p. 26-28, 2020.

[157] Por outro lado, conforme Aragão,"[...] a Constituição de 1988 não permite que a ingerência do Chefe do Poder Executivo sobre as Agências chegue ao ponto de excluir, na prática, a sua autonomia, como, inclusive, já foi verificado pela doutrina brasileira com relação às antigas autarquias, fenômeno este que chegou a ser denominado de 'desautarquização das autarquias', não mais compatível com o Estado Democrático de Direito e com a constitucionalização da diferença entre a Administração Direta e Administração Indireta". ARAGÃO, Alexandre Santos de. Supervisão ministerial das agências reguladoras: limites, possibilidades e o parecer AGU nº AC - 51. *Revista de Direito Administrativo*, v. 245, p. 255, 2007.

inclusive, que a Lei 13.848[158], de 2019, a denominada Lei das Agências Reguladoras, estabeleceu no artigo 3.º, inexistir relação de tutela e subordinação hierárquica, uma importante inovação no cenário jurídico[159].

É possível afirmar que o surgimento das agências reguladoras originou-se com a necessidade de correção de *falhas de mercado*, seja ela vinculada à ocorrência de monopólios, mas também à falta de ordenação setorial. A busca pela homogeneidade entre os diversos agentes do mercado almejava evitar o risco de desestruturação ou desmoralização da atuação de determinado país no âmbito da área regulada. Portanto, a descentralização administrativa permite, por outro lado, a centralização das expectativas regulatórias e a condução da confiança para o grau de atuação do órgão regulador[160].

Cabe salientar que os processos de criação e de execução regulatória não exigem a existência de uma estrutura prévia em forma de autoridade administrativa ou de agência reguladora, inclusive com o revestimento de personalidade jurídica. Na tradição brasileira, o extinto Instituto do Açúcar e do Álcool exercia regulação de forma diferente de uma agência e vinculava-se à estrutura da Presidência da República, posteriormente existindo pelos planos de desestatização iniciados na década de noventa. Por outra via – e seguindo a mesma premissa, importa notar que antes da criação da Agência Nacional de Aviação Civil (ANAC), as atividades de regulação eram desenvolvidas por meio de um departamento especializado. Significa dizer que a atividade de regulação não demanda a criação de uma agência reguladora ou que se atribua personalidade jurídica diferenciada. Contudo, é desejável que se adote um modelo diferenciado, conforme a evolução da criação de agências permite concluir que a contemporaneidade impõe, ante ao intenso fluxo de informações e da necessidade de atuar de forma precisa, clara e responsável, o que demanda uma blindagem institucional[161].

Nessa linha, o órgão regulador deve possuir um nível de independência desses interesses, de forma a cercar-se de imunizantes à captura institucional por parte do Poder

---

[158] BRASIL. Lei nº 13.848, de 25 de junho de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13848.htm>. Acesso em: 29 nov. 2020.

[159] Pode-se considerar uma evolução, tendo em vista que até os últimos recentes anos, "[...] nota-se que poucas modificações foram promovidas no arranjo institucional do modelo de Estado regulador consolidado especialmente em virtude da ampla reforma do Estado dos anos 1990. O aspecto positivo é que isso assegurou estabilidade e gradualismo no Brasil. Do lado negativo, atestou a incapacidade política de promover aprimoramentos e de testar novos conceitos na prática – ou mesmo o desinteresse quanto a isso". CUNHA, Bruno Queiroz. Antagonismo, modernismo e inércia: a política regulatória brasileira em três atos. Cadernos EBAPE.BR, v.14, [s.n.], p.483, jul., 2016.

[160] MOREIRA, Egon Bockmann. Agências reguladoras independentes, poder econômico e sanções administrativas.*Revista de Direito do Estado*, v. 2, p. 163-192, 2006.

[161] VILLELA SOUTO, Marcos Juruena. As agências reguladoras e os princípios constituicionais. *Revista de Direito Constitucional e Internacional*, v. 58, p. 220-234, jan-mar, 2007.

Público ou dos setores regulados. A captura[162] do regulador setorial por parte de atores tende a levar à diminuição do exercício eficiente da função regulatória e, de forma colateral, das funções próprias da função sancionadora. O equilíbrio dos interesses em tensão mostra-se relevante na medida em que a não calibragem dos poderes compromete não apenas o funcionamento normal das rotinas em diferentes organizações, como também possui amplitude capaz de afetar os direitos dos cidadãos.

Portanto, a "independência" torna-se, como corolário, o caracterizador de uma atuação de agência reguladora equilibrada. Há que se pensar, portanto, que esta só é adquirida por meio da outorga legal de personalidade jurídica própria, representada na personalização de sua função no cenário da administração. Todavia, não se deve confundir a independência com a autonomia gerencial, compreendendo essa as esferas patrimoniais, de execução financeira e administrativa. A razão é que as entidades da administração pública possuem a prerrogativa em destaque. Nessa linha, é a independência funcional o caráter essencial para o repúdio da captura ou intervenção político-partidária no exercício das atividades relativas à decisão técnica e desvinculada de interesses diversos do equilíbrio setorial[163].

A atividade de regulação estatal, desempenhada pelas autoridades administrativas, destina-se ao acompanhamento de setores específicos. A emergência de uma preocupação maior com a proteção de dados demonstra essa linha de identificação de setores a serem regulados e de formas de atuação menos genéricas e mais especializadas. Em outras palavras, deve existir uma *(i)* relevância da área a ser regulada e que *(ii)* se identifique um risco em caso de não atuação pública. A lógica ínsita à intervenção na natureza técnica da atuação estatal desvincula-se de um dirigismo político ou amadorismo técnico. Dessa forma, conjuga-se o interesse de intervenção corretiva do órgão regulador com o resguardo à segurança jurídica, de forma a estabilizar os setores nacionais e demonstrar seriedade institucional aos observadores internacionais. Afasta-se, com a criação desses órgãos, o despreparo e a surpresa

---

[162] OLIVEIRA, Anderson; Haase, Lucas. Ordem econômica nacional: análise sobre as agências reguladoras brasileiras e a teoria da captura do interesse coletivo pelo interesse individual. *Revista de Direito do Consumidor*, v. 128, p. 101-116, mar-abr, 2020.

[163] Em letras críticas, Jordão e Ribeiro, salientam que, dentre as muitas formas de destruir a atuação de uma agência, pode-se utilizar a seguintes "[...] estratégias que podem ser (e já vêm sendo) implementadas por eles para produzir o enfraquecimento das agências. Aqui também são três as estratégias principais: (i) limitar o leque de ações ou instrumentos à disposição das agências; (ii) amedrontar os seus funcionários; e (iii) interferir nas suas escolhas e decisões concretas. As duas primeiras servem para atrapalhar o funcionamento e a eficiência das agências reguladoras. A terceira, para minar a sua legitimidade". JORDÃO, Eduardo; RIBEIRO, Maurício Portugal. Como desestruturar uma agência reguladora em passos simples. *Revista Estudos Institucionais*, v. 3, n. 1, p. 193, ago. 2017.

da decisão eivada de pretensões políticas-intervencionistas, cujos efeitos podem frustrar atores do mercado e da sociedade civil.

A consecução da independência dos órgãos reguladores está pautada na diluição do poder, o que ocorre por meio da separação entre o político, essencialmente vinculado à formulação de políticas públicas, e a execução das políticas adotadas em lei, por meio da atuação direcionada das autoridades administrativas[164]. A agência reguladora ou entidade administrativa desempenha funções de operacionalizar o que foi determinado pela política, concretizando-as[165]. Cabe, todavia, a especialização técnica das políticas previstas em lei, por meio da atuação normativa, com a anuência dos conselhos diretivos e consultivos que integram a organização do órgão.

Nessa linha, a implementação de políticas setoriais cabe ao Conselho Diretor, cujos membros são indicados por possuir conhecimento especializado. A escolha do Presidente da República passa pelo processo de confirmação política no Senado Federal. A nomeação torna definitiva a escolha e permite aderir à independência técnica do membro, não podendo ele ser demitido *ad nutum.* Trata-se, portanto de uma garantia substancial de independência, o qual permite concluir pela diferença relevante dos denominados cargos em comissão. Ainda que o membro do conselho tenha sido indicado por motivações próprias relacionadas ao interesse do governante, e não aprovado em concurso público para cargo efetivo, há o controle parlamentar da indicação, de forma a confirmar a capacidade técnica do indicado. Posteriormente, a garantia se operacionaliza pelo cumprimento do mandato e da inviolabilidade do juízo técnico adotado nas decisões.

A direção colegiada deve ser composta de maneira que os mandatos não sejam coincidentes com as trocas de mandato do Chefe do Poder Executivo, evitando, assim, que um mesmo Presidente da República detenha o poder de substituir todos os membros da conformação diretiva da autoridade administrativa, interferindo politicamente na modificação dos membros nomeados anteriormente. Evidencia-se, portanto, que a composição dos membros dos conselhos diretivos dos órgãos reguladores em análise não é formada por cargos comissionados ou que exercem função de confiança do Presidente da República. Dessa forma, o agrado ou descontentamento com o exercício da atuação não implicaria a remoção por

---

[164] MOREIRA NETO, Diogo de Figueiredo. A Independência das Agências reguladoras. *Boletim de Direito administrativo*, p. 416-418, jun., 2000.

[165] A forma de concretização ocorre por meio da execução do contrato de gestão. Cf. ARAGÃO, Alexandre Santos de. Agências reguladoras e agências executivas. *Revista de Direito Administrativo*, v. 228, p. 105-122, 2002.

decisão unilateral, devendo ser comprovada a falta grave, após a instauração de processo administrativo.

A nomeação técnica para mandato fixo apresenta-se como modelo a ser seguido, mesmo que a indicação pelo conhecimento não seja seguida, mas vem sendo reformulada e ajustada periodicamente, especialmente com o advento da Lei 13.848, de 2019, que pode ser entendida como Lei Quadro das Agências Reguladoras[166]. Especificou-se, nesse diploma legal, por meio da alteração legislativa de outras leis, prazo do mandato, requisitos para indicação e o regime de incompatibilidades. Ocorreu, nesse sentido, a uniformização do tratamento das onze agências reguladoras existentes no momento. O estabelecimento de uma ouvidoria, por meio da Lei Quadro, permite, na mesma linha da sabatina no Senado Federal, uma maior participação da sociedade civil, permitindo-se assim a *(i)* verificação da qualidade e da tempestividade dos serviços prestados pela agência e *(ii*) o acompanhamento da apuração de denúncias e reclamações dos interessados contra a atuação da agência[167].

Dessa forma, nota-se, pelo menos no plano normativo, a superação da preponderância do Poder Executivo no controle puro das atividades desempenhadas pelas agências, no sentido da verificação prévia das capacidades dos nomeados e da ultrapassagem do argumentado *déficit democrático* em termos de indicação dos nomes. Por meio da triagem, submete-se o escolhido aos representantes da federação, diminuindo o debatido fortalecimento do governo central em relação aos controles político-representativo e esvaziando a "fragilização da nossa já frágil democracia" brasileira. Existe, pelo contrário, a possibilidade de controle prévio e concomitante à atuação das autoridades administrativas. Como pode ser visto, trata-se de uma adaptação às exigências democráticas, de forma que a tecnocracia – ou a ditadura dos especialistas, integrada por uma elite técnica, apolítica e irresponsável com a condução dos interesses nacionais do setor – sofre prévio controle e evidente restrição, ao menos, no plano teórico.

---

[166] Sobre o tema, veja que uma lei geral que unifica o enquadramento já era pauta no início do século. MARQUES NETO, Floriano Peixoto de Azevedo. As Agências Reguladoras Independentes e seu Enquadramento Legal: A Importância de Uma Lei Quadro. *Revista de Direito de Informática e Telecomunicações*, v. 1, p. 41-58, 2006.

[167] ARAGÃO, Alexandre Santos de. A participação e a composição de conflitos nas agências reguladoras independentes: o caso brasileiro. Revista da Faculdade de Direito da UERJ, v. 13/14, p. 103-119, 2006.

2.3 A visão comparativa entre a AGESIC, a URCPD e a ANPD

As autoridades reguladoras passaram a representar a preocupação do Poder Público em dotar maior competição, criando espaços regulatórios onde antes havia apenas a atuação livre do mercado ou múltiplos critérios de tomada de decisão. O surgimento de uma autoridade reguladora está associado à viabilização de uma atuação equilibrada entre o interesse privado e os interesses permitidos pelo Direito. A experiência brasileira, em termos de atuação das agências, consorciou-se à garantia da concorrência. Por outro lado, o caso da ANPD vincula-se à tutela do direito à proteção de dados, que se mostra de feição mista, ligada à ideia de assegurar a livre concorrência e à licitude do tratamento de informações pessoais.

A importância de analisar o órgão regulador uruguaio responsável pela proteção de dados reside na semelhança hipotética do modelo inicialmente adotado no Brasil. Há traços institucionais similares, ao mesmo tempo em que existem diferenças consideráveis[168]. A nota distintiva que leva ao interesse comparatista reside no reconhecimento, por parte da Comissão Europeia, de que o modelo uruguaio é compatível com o nível adequado de proteção de dados[169], característica que não deve ser menosprezada ou colocada em segundo plano, como sendo modelo inferior[170]. O caminho percorrido pelo país-irmão levou-os ao reconhecimento do mercado europeu, esse que possui potencial econômico ainda a ser explorado pela indústria e pelos serviços tecnológicos que o Brasil oferece. Descuidar ou apenas refletir internamente o modelo europeu pode não garantir o imediato reconhecimento, mesmo porque, inclusive na Europa, todos os países estão passando pela revisão dos mecanismos

---

[168] Bárbara Simão, Juliana Oms e Livia Torres sustentam que "[...] caso comparada com o modelo previsto pela Medida Provisória nº 869/2018, a autoridade uruguaia resguarda mais autonomia por ser um órgão 'desconcentrado'". SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. *Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai*. Disponível em: <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso 2 jul 2020. p.37.

[169] INSTITUTO TECNOLOGIA E SOCIEDADE. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Disponível em: < https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acesso em 1 dez. 2020.

[170] Com efeito, há uma centralização, conforme salienta Guidi, que sustenta que a "[...] configuração permite à Autoridade de Proteção de Dados que realize um controle prévio do tratamento previsto, através da análise de informações como os procedimentos de coleta e tratamento de dados, medidas de segurança e descrição técnica da base de dados, destino dos dados em caso de comunicação, entre outras. A Autoridade pode também, seja através de denúncias, inspeções ou solicitação de informações, fiscalizar o cumprimento da lei, podendo aplicar as sanções administrativas permitidas, quais sejam, advertência, multa ou suspensão de bases de dados". GUIDI, Guilherme Berti de Campos. *Modelos regulatórios para proteção de dados pessoais*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. p.18. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 20 out. 2020.

administrativos e devem passar pela revalidação de compatibilidade com as disposições do RGPD[171].

O Uruguai é divido em departamentos, uma relevante diferença com o Brasil, em que há, no âmbito da federação, a divisão em estados-membros com competências e atribuições previamente delimitadas no texto constitucional[172]. Notadamente, trata-se de decisão que leva em consideração o tamanho territorial e populacional daquele país. Do ponto de vista das relações entre tecnologia e relações estatais, a AGESIC é o órgão que lidera, como unidade executora, a estratégia de implementação da *agenda de governança eletrônica e da política de cidadania digital*, com autonomia técnica, ainda que dependente da Presidência da República Oriental do Uruguai. A legislação de criação da agência (a Lei n. 17.930, de 2005[173]) estabeleceu também quatro níveis de conselho *(i)* Conselho de Administração Honorário, *(ii)* o Conselho para a Sociedade da Informação, *(iii)* o Conselho Consultivo Empresarial e *(iv)* o Conselho Consultivo de Informática Pública[174]. Embora a análise se distancie do momento temporal da criação, pertencendo o processo como memória institucional, pode-se verificar a presença de universidades públicas e privadas, entidades do setor empresarial e a presença de diretores-presidentes de outras agências incumbidas de temas conectados à agenda de digitalização, o que sugere uma presença estatal compromissária com as atividades de utilização de mecanismos digitais.

A primeira e a segunda Agenda de Digitalização (de 2006 a 2010) estiveram voltadas *(i)* à criação da institucionalidade, *(ii)* criação dos marcos normativos – incluindo a Lei de

---

[171] Para López, a "[…] garantia do direito fundamental à proteção dos dados pessoais exigiu a existência de autoridades independentes, já previstas na Diretiva 95/46 / CE e elevadas à categoria constitucional europeia". LÓPEZ, Manuel Valín. Las autoridades autonómicas de protección de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valencia: Tirant lo Blanch, 2019. p.523. Nesse sentido, Nafarrete expõe que além dos"[…] o Regulamento inclui outros adicionais relacionados com a disponibilidade como recursos, controle de pessoal e controle financeiro que possam condicionar direta ou pelo menos indiretamente as possibilidades de exercício seus poderes e poderes de forma independente". NAVARRETE, Jesús Rubí. La agencia española de protección de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.500.

[172] O governo administrativo e executivo de cada departamento é exercido por um Intendente eleito. A Junta Departamental é o órgão com funções legislativas e de controle das contas públicas. Dentro de cada departamento, há divisões territoriais do terceiro nível, chamados Municípios, responsáveis pela administração local, que estão a cargo de um Conselho Municipal, presidido por um Alcalde.

[173] URUGUAI. Lei 17.930, de 23 de dezembro de 2005. Presupuesto Nacional. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp3511048.htm>. Acesso em: 14 dez. 2020.

[174] O dispositivo de criação (art.72) previu que haverá "[...] um Conselho de Administração Honorário, encarregado de desenhar as linhas gerais, avaliar desempenho e resultados obtidos. Será composto por cinco membros, um dos quais será o Diretor Executivo da Agência para o Desenvolvimento do Governo da Gestão Eletrônica e Sociedade da Informação e do Conhecimento, um representante da Presidência da República e três membros indicados pelo Presidente da República". URUGUAI. Lei 17.930, de 23 de dezembro de 2005. Presupuesto Nacional. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp3511048.htm>. Acesso em: 14 dez. 2020.

Dados, *(iii)* da infraestrutura e *(iv)* da formação de pessoal para atuação especializada no desempenho das atividades previstas em lei e em decretos presidenciais. Em contrapartida, a Terceira Agenda de Digitalização teve como objetivo *(i)* universalizar as iniciativas em matéria digital e *(ii)* criar linhas de atuações estratégicas, como forma de expandir a utilização de sistemas baseados em tecnologia da informação. Nos últimos anos, buscou-se viabilizar a utilização da tecnologia para criação de modelos de gestão e empregá-la em favor do desenvolvimento sustentável e da redução das desigualdades.

A URCDP é a autoridade de controle dos dados pessoais do Uruguai, criado pelo artigo 31 da LPDP. Trata-se de um órgão descentralizado com autonomia técnica, cuja competência é zelar pelo cumprimento da legislação de proteção de dados pessoais e pelo respeito aos seus princípios. O Conselho Executivo é composto por três membros: *(i)* o Diretor Executivo AGESIC e *(ii)* dois membros nomeados pelo Poder Executivo entre pessoas que, devido à sua formação pessoal, profissional e de conhecimento na matéria, garantam o exercício independente dos cargos de acordo com os critérios da eficiência, objetividade e imparcialidade. O mandato dos membros indicados possui duração de quatro anos de mandato, podendo ser reconduzido.

Conforme a LPDP[175], as funções diretivas cessarão apenas após o término de seu mandato e a nomeação de seus sucessores, ou para o caso de destituição ordenada pelo Poder Executivo nos casos de inépcia, omissão ou crime, de acordo com as garantias do devido processo. Saliente-se que, durante a gestão, os membros do conselho executivo não receberão ordens ou instruções no plano técnico, o que se constitui de uma importante garantia funcional.

No âmbito da estrutura da URCDP, o artigo 32 da LPDP prevê a existência do Conselho Consultivo, que é formado por membros que possuem mandato de quatro anos, compondo-se *(i)* pessoa com histórico reconhecido de promoção e defesa direitos humanos, designados pelo Poder Legislativo, que não pode ser membro do Congresso em exercício, *(ii)* um representante do Judiciário, *(iii)* um representante do Ministério Público e (iv) representante da área acadêmica e *(v)* um representante do setor privado, a ser eleito no formulário estabelecido por regulamento.

A LPDP estabelece que entre as competências do órgão regulador estão as atribuições de *(i)* assessorar o Poder Executivo e recomendar políticas de tratamento, segurança e

[175] URUGUAI. Ley n. 18331, de 11 de agosto de 2008. Lei de Protección de Datos Personales. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 1 set. 2020.

manipulação de dados pessoais, *(ii)* realizar relatórios sobre o alcance e os mecanismos de defesa previstos em lei, *(iii)* cadastro das bases de dados e códigos de conduta, *(iv)* autorizar a transferência de dados pessoais para países sem níveis adequados de proteção na matéria, *(v)* inspecionar entidades públicas e privadas em relação ao tratamento de dados pessoais, *(vi)* punir as infrações de acordo com o quadro jurídico existente em matéria de proteção de dados pessoais. A ação administrativa da URCDP se desenvolve de acordo com os princípios de imparcialidade, presteza, eficácia, verdade material, informalismo, devido processo, comércio, boa fé, motivação de decisões e simplicidade, que servirão de critério interpretativo para resolver os problemas que possam surgir no processamento de controvérsias associadas à proteção de dados.

O Decreto 414/2009[176] é o documento normativo que estabelece a pormenorização das funções do órgão de regulação dos dados pessoais uruguaio, articulando um conjunto de direitos e obrigações relacionados ao tratamento, automatizado ou manual. O documento normativo em questão, em seu artigo 21, estabelece a direção técnica e administrativa da URCDP será exercida por um Conselho Executivo de três membros, oferecendo conformidade com o que estabelece o artigo 31 da LPDP. O artigo 23, por sua vez, dita importantes tarefas a serem desempenhadas pelo Conselho Executivo, entre as mais importantes as de *(i)* difundir o conhecimento dos direitos que este regime garante e promover seus conhecimentos, *(ii)* o de estabelecer acordos com organizações internacionais, antes autorização do Poder Executivo, *(iii)* garantir a regularidade e eficiência das atividades desenvolvidas pelo órgão, *(iv)* assessorar o Poder Executivo na formulação de regulamentos e projetos de lei que se referem total ou parcialmente à proteção de dados pessoais, *(v)* editar as regras e regulamentos que devem ser cumpridos no desenvolvimento das atividades previstas na legislação que regulamenta; incluindo medidas de segurança no tratamento e conservação de dados pessoais, que devem ser observados pelos responsáveis, controladores e usuários de bancos de dados públicos e privados, *(vi)* solicitar relatórios e aplicar sanções administrativas aos atores submetidos ao controle e *(vii)* emitir autorizações e certificados previstos na LPDP.

No Brasil, a LGPD trouxe novos direitos e estabeleceu requisitos de conformidade para organizações públicas e privadas. Em torno das transformações impulsionadas pela digitalização da sociedade, torna-se necessária a exposição da composição da ANPD prevista

[176] URUGUAI. Decreto 64/020, Reglamentacion de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 1 set. 2020.

em lei e de suas principais funções[177]. A Lei nº 13.853, de 2019, estabeleceu o órgão como integrante da Presidência da República, sendo assegurada autonomia técnica e decisória, conforme disposições dos artigos 55-A e 55-B. Embora subestimada, a presença dessa previsão é relevante em termos de garantia de que as decisões serão tomadas de forma técnica e com estabilidade, embora que, no primeiro momento, exista a integração à Presidência. Com efeito, a natureza jurídica – integrante da Presidência – foi estabelecida em lei como transitória, cabendo um ajuste futuro e a consequente transformação em órgão submetido ao regime autárquico especial.

A ANPD é composta de *(i)* um Conselho Diretor, órgão máximo de direção, *(ii)* do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade[178], *(iii)* dos órgãos auxiliares como corregedoria, ouvidoria e de órgão de assessoramento jurídico próprio e *(iv)* unidades administrativas e unidades especializadas. O Conselho Diretor é composto por cinco membros que são escolhidos pelo Presidente da República e passam pelo processo de sabatina no Senado Federal.

Nesse sentido, a LGPD estabelece critérios como possuir reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos, que terão mandato de quatro anos. Existe, na LGPD, previsão de mandatos desencontrados, de forma que eventual mudança do Chefe do Executivo Federal não implique na alteração completa do quadro, de forma que essa é uma garantia contrária à ingerência política desencadeada pela alternância de poder. Os membros do Conselho Diretor não são demissíveis *ad nutum*, de forma que somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar iniciado pelo Ministro de Estado Chefe da Casa Civil da Presidência da República[179].

A premissa da qual partimos é relevante na discussão do modelo de autoridade de proteção de dados previsto na legislação brasileira, apesar do não estabelecimento legislativo como órgão totalmente independente. Nessa linha de ideias, a definição da autoridade

---

[177] LIMA, Cíntia Rosa Pereira de. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados*: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

[178] LUCCA, Newton; LIMA, Cíntia Rosa P. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: Cíntia Rosa Pereira de Lima. (Org.). *Comentários à Lei Geral de Proteção de Dados*. 1ed.São Paulo: Almedina, 2020, v. 1, p. 373-397.

[179] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

independente guarda relação com a existência de um ente especializado[180]. De fato, não há no Brasil, nem no Uruguai, uma previsão constitucional da existência de órgãos plenamente isolados de controle parlamentar. ANPD e a URCDP são órgãos integrantes de outra estrutura: no caso do Brasil, da Presidência da República; no caso uruguaio, da AGESIC. Com efeito, tanto no Brasil, quanto no Uruguai se asseguram independência técnica e decisória aos membros dos respectivos conselhos diretivos, o que garante certa estatura de distanciamento entre o poder central e os membros do Conselho, o que sugere o surgimento de uma descentralização material mais reforçada[181]. Nesse sentido, não se observa a personalidade jurídica própria, que, conforme referido na seção anterior, é desejável, mas não impositiva ao exercício das funções de regulação[182].

O artigo 11 do Decreto 10.474, de 2020[183] fornece o regime de incompatibilidades, que são mecanismos de contenção de interesses estranhos aos determinados pela LGPD. O membro do Conselho não poderá *(i)* receber honorários ou percentagens, *(ii)* exercer profissão liberal, exceto as constitucionalmente permitidas, *(iii)* participar, na forma de controlador, diretor, administrador, gerente, preposto ou mandatário, de sociedade civil, comercial ou empresas, *(iv)* emitir parecer sobre matéria de sua especialização, ainda que em tese, ou atuar como consultor de empresa, *(v)* manifestar, por qualquer meio de comunicação, opinião sobre processo pendente de julgamento ou juízo depreciativo sobre despachos, votos ou sentenças de órgãos judiciais, ressalvada a crítica nos autos, em obras técnicas ou no exercício do magistério e *(vi)* exercer atividade político-partidária. Trata-se, nesse sentido, de uma limitação negativa do membro da ANPD, que garante a independência técnica e decisória da atuação dos membros por meio da atribuição de limitações.

Existe, no decreto, a denominada "quarentena", que, em verdade, limita o membro que recentemente deixa o Conselho Diretor, pelo período de cento e oitenta dias, contado da data em que é publicada a exoneração, de representar interesse que não o particular perante ANPD.

---

[180] Em sede europeia, pode-se verificar as conclusões estabelecidas por MANETTI, Michelle. Autorità indipendenti: tre significati per una costituzionalizzazione. *Politica del diritto, Rivista trimestrale di cultura giuridica fondata e diretta da Stefano Rodotà*, Milano, n.4,. p. 657, 1997. PETRLIC, Ronald. The General Data Protection Regulation: From a Data Protection Authority's (Technical) Perspective. *IEEE Security & Privacy*, vol. 17, no. 6, p. 31-36, nov-dec., 2019.

[181] FONSECA CARVALHO, João Pedro Antunes Lima da. A natureza jurídica da autoridade nacional de proteção de dados à luz da teoria do estado regulador: há espaço para a adoção do conceito material de descentralização administrativa no brasil? *Revista De Direito, Estado e Telecomunicações*, vol. 12, n. 2, 127-130, 2020.

[182] REIGADA, Antonio. Las agencias de protección de datos como administración independiente. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás. *Las Administraciones independientes*, 2009. p27-29.

[183] BRASIL. Decreto 10.474, de 26 de agosto de 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226> . Acesso em 1 set. 2020.

De igual forma, o membro do Conselho Diretor não pode utilizar informações privilegiadas obtidas em decorrência do exercício do cargo e possuir interesse relevante na regulação pela ANPD de atividades vinculadas ao tratamento de dados pessoais. O Decreto em análise, portanto, dificulta a utilização do cargo, em tese, para o acolhimento de interesses pessoais dos membros do Conselho Diretor que estão no exercício da função ou de quem recentemente deixa de exercê-la[184].

Note-se que, recentemente, a Lei das Agências Reguladoras estabeleceu, no art. 3.º, que a agência reguladora, em razão da natureza especial, é caracterizada pela ausência de tutela ou de subordinação hierárquica, pela autonomia funcional, decisória, administrativa e financeira e pela investidura a termo de seus dirigentes e estabilidade durante os mandatos. Em regra, cuida-se do estabelecimento de uma legitimação técnica da ação dos poderes públicos em temáticas sensíveis[185] e que demandem certa especialização[186]. No âmbito de uma escala de independência, o contraste entre os órgãos administrativos e os independentes residiria no fato de que os primeiros exerceriam suas competências na forma de independência contida e, os últimos, ocupariam a posição de pessoas jurídicas com personalidade própria, as quais passariam a exercer suas funções como centros autônomos de decisão e atuação.

A questão central reside na busca de critérios de incorporação de medidas de independência[187] e da análise de quais critérios são factíveis de serem considerados. A LPDP e

---

[184] BRASIL. Decreto 10.474, de 26 de agosto de 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226> . Acesso em 1 set. 2020.

[185] Conforme Sérgio Guerra, "[...] foco era criar um ambiente que privilegiasse certeza e estabilidade, de modo a atrair investimentos, sobretudo estrangeiros, e gerar salvaguardas institucionais que significassem um compromisso com a manutenção de regras e contratos de longo prazo. A competência preponderantemente técnica foi destacada nas mãos de entidades descentralizadas, demonstrando-se que a regulação de sistemas complexos e sensíveis deixava de ser assunto de Governo para ser assunto de Estado". GUERRA, Sérgio. *Agências Reguladoras***:** da organização administrativa piramidal à governança em rede. 1. ed. Belo Horizonte: Fórum, 2012. p. 106.

[186] FERNÁNDEZ ROJAS, Gabriel. Las administraciones independientes de regulación y supervisión en españa. Vniversitas, [S. l.], v. 54, n. 109, p. 419-460, 2005. Disponível em: https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/14710. Acesso em: 19 dez. 2020.

[187] Para Cerqueira, além da prudência, esse "[...] critério poderia ser o *conservadorismo*. Para além das interpretações errôneas dessa noção, a perspectiva conservadora não recusa a inovação, o progresso. Questiona, porém, suas vantagens e desvantagens admitindo como ponto de partida que a herança do passado possui uma consistência própria. É, portanto, um método fundado na razão e não uma matriz ideológica, dotada de conteúdo próprio, abstrato, intransigente e imutável." CERQUEIRA, Gustavo. Comparação jurídica e ideias de modernização do direito no início do Século XXI. *Revista de Direito Internacional*, Brasília, v. 17, n. 1, p. 20, 2020.

os decretos que regulamentam a legislação foram criados inspirados na Diretiva 95/46[188], a qual não precisou o que compreendia a "total independência" prevista.

O RGPD, por sua vez, indicou garantias substanciais e formais de independência das autoridades, de modo que está servindo de parâmetro das adequações posteriores na legislação uruguaia e dos decretos. Inácio Laita, caracterizando a independência de uma autoridade de proteção de dados sugere que determinado órgão de proteção de dados é funcionalmente independente quando a tomada de decisões ocorre sem interferência dos poderes legislativo, executivo e judiciário, submetendo ao seu controle tanto o setor público quanto o privado. Por outra via, também é independente do ponto de vista organizacional, quando se analisa a nomeação dos diretores da autoridade. Fundamentalmente, é juridicamente independente, quando possui competência para a elaboração e aprovação de suas próprias instruções e seus atos esgotam os procedimentos administrativos[189].

Vista sob o último plano, o da independência jurídica, o LGPD, no artigo 55-J, inciso XX, prevê que cabe a ANPD "[...] deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos", sendo que a edição de regulamentos e das normas aplicáveis deve ser precedida de consulta e audiência públicas, bem como de análises de impacto regulatório. De fato, embora críticas tenham sido tecidas em torno do grau de influência Presidencial do atual modelo, nesse ponto fica cristalizado que a legislação especial de proteção de dados confere à autoridade administrativa o papel de intérprete maior da legislação. Aliada ao artigo 55-K, vislumbra-se a associação com a prevalência da competência sancionatória da ANPD, inclusive responsável pela articulação com outras autoridades em temas conectados à proteção de dados, de modo que assumirá a função de órgão central de interpretação da legislação e do estabelecimento de normas e diretrizes para a sua implementação.

Do ponto de vista financeiro, as receitas da ANPD são oriundas *(i*) das dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos, *(ii)* as doações, os legados, as subvenções e outros recursos que lhe forem destinados, *(iii)* os valores apurados na venda ou

---

[188] UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>. Acesso em 25 nov. 2020.

[189] LAITA, Inacio. Independencia y régimen jurídico de la agencia española de protección de datos. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás. *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009. p.225.

aluguel de bens móveis e imóveis de sua propriedade, *(iv)* os valores apurados em aplicações no mercado financeiro das receitas, *(v)* os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais e *(vi)* o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. Em parecer técnico-legislativo, já havia sido feita a referência da importância da autoridade de proteção de dados não depender de multas para o custeio, de forma que essa previsão inviabilizasse o custeio de toda a atuação da autoridade, por ser inexpressiva[190]. Houve, nesse sentido, certa atenção do legislador ao estabelecer as fontes de renda citadas. Quanto ao orçamento, do ponto de vista comparativo, a URCDP não conta com um orçamento próprio, de forma que integra o orçamento da AGESIC.

Dessa vista, a personalidade jurídica de autoridade, embora importante, não é o fator isolado a ser considerado[191]. Em outras palavras, é o circuito completo que deve determinar se a atuação de um órgão regulador se mostra independente. A análise comparativa em questão assume relevância, em razão de que as transferências de dados pessoais com países não integrantes da União Europeia, apenas serão permitidas se existir adequação ao nível de proteção previsto no RGPD. Dentre as inovações do RGPD, no aspecto das autoridades nacionais, está o incremento das denominadas faculdades de *enforcement*, no sentido de ampliar as capacidades investigatórias das autoridades, inclusive a cooperação internacional com outras autoridades[192], o que é compatível com a tendência de reforço dos mecanismos de

---

[190] Da perspectiva financeira, conclui-se que quanto "[...] ao custeio das agências reguladoras, importante ressalvar que o seu custeio não pode vir da aplicação das multas. Estas quando aplicadas, assegurados o contraditório e a ampla defesa, não devem ser destinadas à manutenção do órgão para evitar qualquer interesse financeiro por parte da agência quanto à aplicação desta sanção. O ideal seria a lei já estabelecer que estes valores deveriam ser destinados às políticas públicas sobre proteção de dados pessoais e às pesquisas científicas nessa área. Assim, a lei deveria criar uma agência reguladora em nível federal, estabelecendo uma tarifa a ser paga pelas empresas, que tratam dados pessoais conforme uma porcentagem do capital de cada empresa". CAMARA DOS DEPUTADOS. Parecer Técnico encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp>. Acesso em 10 out. 2020.

[191] Para uma visão crítica consultar, VASCONCELOS, Beto; PAULA, Felipe de. Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRASÃO, Ana; OLIVA, Milena. (Org.). *Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. 1ed.: Revista dos Tribunais, 2019, p. 717-740.

[192] Lombarte salienta que "[…] o REPD reforça o regime de sanções através da sua generalização para o território da União Europeia e através de um sistema de sanções eficazes, proporcionais, dissuasivas e potencialmente milionárias. O montante das multas será fixado tendo em conta a natureza, gravidade e duração da infração, a intencionalidade ou negligência na infração, o grau de responsabilidade da pessoa singular ou coletiva, a reincidência, as medidas técnicas e organizacionais e processuais aplicado pelos responsáveis, o grau de cooperação com a autoridade de controle para reparar a infração". LOMBARTE, Antonio. De la libertad

supervisão e de interconexão das organizações estatais. Essas disposições foram recepcionadas e incorporadas por ambas legislações. Em outros termos, o estatuto que assegura ao órgão em causa a possibilidade de agir com a liberdade, ao abrigo de qualquer instrução ou pressão política ou financeira[193]. Não significa, todavia, que a autoridade está imune a controles democráticos: ela se submete aos controles de natureza democrático e institucional (controle social, legislativo, judicial e de contas)[194].

As competências foram, em boa parte, reproduzidas na LGPD, no artigo 55-J, com restrição na competência da edição de normas regulamentares, a qual a ANPD deverá respeitar a mínima intervenção, observados os princípios de Direito Econômico previsto na Constituição da República (art. 170), sendo previamente precedidos de consulta e audiência públicas, assim como estudos de impacto regulatório. No entanto, apesar da redação legal apresentada pela Lei n.º 13.853/2019, é possível identificar o fomento de uma cultura da "responsabilidade" e da "autorregulação". É nesse contexto que, no artigo 55-J, os incisos VI e VII estabelecem como função da ANPD, respectivamente, "[...] promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança" e "[...] promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade"[195]. Dessa forma, o entendimento básico de como podem controlar seus dados pessoais deve ser promovido no âmbito das esferas de atuação da autoridade administrativa.

---

informática» a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, n.100, p.660, sep.-dez, 2017.

[193] FERNÁNDEZ ROJAS, Gabriel. Las administraciones independientes de regulación y supervisión en españa. Vniversitas, [S. l.], v. 54, n. 109, p. 419-460, 2005. Disponível em: https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/14710. Acesso em: 19 dez. 2020.

[194] PACHECO, Regina Silvia. Regulação no Brasil: desenho das agências e formas de controle. *Rev. Adm. Pública*, Ago, v.40, n.4, p.523-543, 2006.

[195] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

4 ADEQUAÇÃO E A POSSIBILIDADE DE APRENDIZADO COM A URCDP

A proteção de dados pessoais deve se subordinar aos princípios filosóficos do Direito. Há uma natureza dialética entre direitos humanos, a proteção de dados e novas tecnologias, especialmente com o fortalecimento das ligações entre ética dos dados, *big data* e as novas aplicações cotidianas viabilizadas pela internet das coisas. Se, por um lado, ocorre a crescente facilidade de acesso de serviços disponibilizados aos usuários de tecnologia; por outro, tornam-se vistosos novos desafios, ameaças para a proteção de dados pessoais[196]. Nesse contexto das relações sociotecnológicas, torna-se relevante compreender a interligação entre a ética e as novas tecnologias[197], especialmente de compreender os modelos normativos comunitários e de parceiros institucionais, como forma de aprender e ajustar à realidade cultural nacional. As facilidades da sociedade da informação permitem a comunicação, interligação e integração de conceitos, perspectivas de proteção de dados e de valorização das capacidades tecnológicas e de pessoal próprias de cada região ou país. As parcerias interinstitucionais, ainda que por meio de estudos regulatórios comparados ou de pesquisas amostrais, podem contribuir para o incremento da proteção de dados em nível nacional. A rentabilização progressiva dos dados pessoais[198] tornou-se um fenômeno global, o que leva a necessária atuação de atores para alcançar ferramentas eficazes, como códigos de conduta e princípios regulamentados por organizações internacionais (*soft law*)[199], bem como é imperativo ter em consideração as regras do Regulamento Geral Europeu sobre a Proteção de Dados[200] e repensar as estruturas em termos de conformidade normativa[201].

---

[196] Para Pérez-Luno, um dos novos desafíos da humanidade, na atual conjuntura, está na emergência do pós-humanismo, que "[...] por meio da instrumentalização da IA, implica um anti-humanismo, colocando-se frente ao que tem sido uma das principais conquistas históricas da tradição humanista: os direitos humanos". PÉREZ-LUNO, Antonio Enrique. Inteligencia artificial y posthumanismo. In: BRAVO, Alvaro S. (editor). *Derecho, Inteligencia Artificial y Nuevos Entornos Digitales*. Sevilla, 2020. p.18.

[197] MAGRANI, Eduardo. *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. 2. ed., Porto Alegre: Arquipélago Editorial, 2019.

[198] MORENO, José. The economic value of information in the network society. *Observatorio*, Lisboa, v. 9, n. 2, p. 1-28, jun., 2015.

[199] TORNARÍA, Felipe Rotondo. Protección de datos personales, autorregulación y transferencias internacionales de datos. *La justicia uruguaya: revista jurìdica*, n. 147, p. 63-69, 2013.

[200] Cf. LOMBARTE, Antonio. De la libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, n.100, p.639-669, sep.-dez, 2017. No Brasil, verificar LIMBERGER, Têmis. Informação em rede: uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Victor Rozatti (Org.). Direito Digital: direito privado e internet. São Paulo: Foco, 2019. p.253-266.

[201] MANTELERO, Alessandro. The future of data protection: gold standard vs. global standard. *Computer Law & Security Review*, p.4-5, nov., 2020. https://doi.org/10.1016/j.clsr.2020.105500. Acesso em 29 jan. 2021.

Saliente-se que a globalização comunicacional provoca a disputa pelas soluções tecnológicas e de mercado, além de colocar em contato o problema global do tráfego internacional de dados, um dos pontos mais relevantes da estruturação de respostas jurídicas relacionadas com a proteção de dados pessoais. Nessa linha, pensar eticamente a proteção de dados, seja por meio da adoção de *comitês de ética*, seja pela adoção de mecanismos técnicos de anonimização ou da adoção de selos de proteção de dados para a proteção especializada dos dados dos cidadãos nacionais e de estrangeiros que utilizem serviços baseados em solo nacional. Embora a construção de caminhos e de novos rumos passe por uma atuação basal – ou de programação – das mãos e dos conhecimentos de especialistas, existe um espaço para a participação dos cidadãos e de outros atores na construção de um modelo de proteção de dados que funcione[202]. Inclusive, no Uruguai, no âmbito das competências desenvolvidas pela URCPD, pode-se destacar o Programa *Tus Datos Valen*[203], o Plano Ceibal[204] e a disponibilização de diferentes materiais didáticos disponibilizados à consulta e que podem servir de base à construção de uma cultura de proteção de dados, desde a infância[205]. Revela-se a construção de ética para os dados desde os primeiros passos de crescimento do cidadão.

Não é suficiente apenas a incorporação de modelos prontos, especialmente se determinados modelos tendem a não funcionar sem o prévio ajuste cultural ou uma preparação institucional. Levar em consideração a dimensão ética para análise e desenvolvimento de iniciativas à proteção de dados pessoais tornou-se um imperativo próprio da preservação das liberdades e da vitória do modelo republicano de governo e de tratamento entre os próprios cidadãos. A proteção dos dados pessoais não deve ser apenas uma locução adagial ou mantra cuja mera menção e tratamento são suficientes para atingir o objetivo. Conforme mencionado, torna-se cada vez mais necessário trabalhar o cumprimento e a real eficácia dos objetivos prosseguidos com o estabelecimento dos planos e políticas de dados

---

[202] MAQUEO RAMÍREZ, María Solange; MORENO GONZÁLEZ, Jimena; RECIO GAYO, Miguel. Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho*, v. 30, n. 1, p. 77-96, 2017.

[203] URUGUAI. URCDP. *Tus Datos Valen*. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/librillo%2Binstrucciones%2Bbaja%2B%281%29.pdf>. Acesso em 24 nov. 2020.

[204] Banco Iberoamericano de Desenvovimento (BID). *Nota Técnica. AGESIC, um modelo exitoso*. Disponível em: <https://www.alejandrobarros.com/wp-content/uploads/2016/04/Nota_Tecnica_-_Agesic.pdf> . p.26. Acesso em 28 nov.2020.

[205] URUGUAI. URCDP. *La protección de los datos personales*. Disponível em: <https://uruguayeduca.anep.edu.uy/recursos-educativos?combine=datos+personales&field_nivel_target_id=All&field_asignatura_o_especialidad_target_id=All&field_destinatarios_target_id=All&field_etiquetas_target_id=All&field_formato_target_id=All&field_palabrasclave_target_id= >.Acesso em 24 nov. 2020.

definidos pela ANPD e pelo CNPD, assim como a abertura de espaço às doutrinas e aos conhecimentos produzidos em sede acadêmica.

Ainda que a proteção de dados pessoais esteja vinculada ao direito à privacidade, duas dimensões devem ser observadas para a consecução da proteção efetiva: *(i)* a versão ética, pautada pelo resguardo da vida privada das pessoas e *(ii*) a feição jurídica, consistente na regulamentação da forma de tratamento, da observação dos princípios ao acesso, da gestão da informação e do controle de segurança dos dados. O estreitamento da relação ocorre com o vínculo conforme ocorre a especificação do direito à de *não-lesão* (ou da proteção especial aos dados) e a responsabilidade pela lesão ou violação posterior, seja pelas infrações de ordem ética, seja por violações técnicas com repercussões jurídicas. O que determina ou não a adequação de dados[206] leva em conta aspectos técnicos e comportamentais, o que insere a política ética dos dados como relevante função a ser desempenha pelas autoridades de controle[207].

O fato é que o RGPD[208] leva em consideração que as regras e padrões sejam orientados para o *futuro*, de modo que seja considerado, como prioridade, o respeito ao humano em face do grau de poder de invasão – ou intrusivo – de novas tecnologias[209]. Apesar dos documentos normativos, prevendo regras de atuação tenha uma importância coercitiva, existe a contingência relativa à impossibilidade de abordar múltiplos cenários emergentes no mercado digital. Considerar que as organizações devem atuar de forma mais responsáveis, pautando-se pela abordagem ética para lidar com os dados pessoais que coletam. Ao desenvolver códigos e políticas que salvaguardam a dignidade humana, as organizações podem se autopoliciar, garantir sua conformidade com as leis de proteção de dados e demonstrar respeito pelas pessoas cujos dados pessoais que eles usam - só porque uma organização pode juntar as peças da vida de um cliente de sua trilha de dados não significa que sempre deveria.

A condução das inovações na área tecnológica deve estar pautada em um ambiente digital consciente, que pode oferecer tecnologia que processa dados ao mesmo tempo

---

[206] COMISSÃO EUROPEIA. Adequacy of the protection of personal data in non-EU countries. How the EU determines if a non-EU has an adequate level of protection. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 21 out. 2020.
[207] BUTTARELLI, Giovanni. *The transfer of personal data to third countries and international organisations by EU institutions and bodies*. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/16-04-19_mit_ethics1_en_0.pdf> Acesso em: 1 dez. 2020.
[208] UNIÃO EUROPEIA. Article 29 Data Protection Working Party: Guidelines on Data Protection Officers. Disponível em: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44100> Aceso em 21 dez. 2020.
[209] MAGRANI, Eduardo. *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. 2. ed., Porto Alegre: Arquipélago Editorial, 2019.

respeitando os direitos do indivíduo. Luciano Floridi[210], por exemplo, apresenta-se como filósofo preocupado com o tema da conexão entre ética e proteção de dados na Europa, de modo que eles são completamente aplicáveis à realidade brasileira e uruguaia. Nota-se que a existência de inúmeros desafios éticos vem sendo provocados pelo avanço da ciência dos dados, de modo que se tornou relevante viabilizar a construção da macroética dos dados e das aberturas de horizonte que ela provocaria, especialmente por meio da viabilização de soluções que tendam a maximizar o valor de ciência de dados para as sociedades. De fato, não há como duvidar da capacidade "revolucionária" ou de impacto dos dados em nossa vida, pública ou privada e do avanço do tratamento automatizado da informação. A consequência desse processo demanda equilíbrio (jogo limpo), responsabilidade e o respeito aos direitos apresentam-se como pontos de equalização na atualidade, de modo que a focalização da ciência de dados e dos inúmeros procedimentos de mineração de informações ao controle do ser humano, mesmo porque compreender a humanidade como um conjunto de dados rebaixa a dignidade.

Nesse contexto, a confiança apresenta-se como elemento relevante, especialmente pelo fato de que a ignorância às questões éticas pelas organizações pode levar a impactos negativos e ao descrédito junto à sociedade. Ao revés, o reforço pesado e enfático à proteção dos direitos individuais, em contextos errados, "[...] pode levar a regulamentos rígidos demais e isso, por sua vez, pode prejudicar as chances de aproveitar o valor da ciência de dados"[211]. Significa dizer que pautar-se por princípios éticos, até mesmo nos menores projetos em ciência dos dados, pode conduzir à preferência social e evitar que oportunidades sejam perdidas. O balanço ou ajuste entre a necessidade de proteger adequadamente e precisamente os diferentes direitos conexos aos setores que trabalham com tratamento de dados repercutirá no máximo aproveitamento da ciência dos dados.

Conforme Floridi, toda análise ética possui um nível de abstração. Se para as primeiras investigações científicas em torno das questões éticas em matéria de tecnologia estavam centradas no ser humano, conexas às responsabilidades de designers e usuários no desenvolvimento das tecnologias; logo após, nos anos oitenta, o objeto passou a ser a ética das aplicações de computador, vinculada ao impacto que os computadores podem ter na modelagem da dinâmica social. A atual ética centrada na informação leva em conta uma

---

[210] FLORIDI, Luciano. Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage, *Philos. Technol.* n.31, p.163–167, 2018.
[211] FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? *Philosophical Transactions of the Royal Society*, v. 374, n. 2083, p.2, 2016.

abordagem macroética capaz de lidar com todo o ciclo de criação, compartilhamento, armazenamento, proteção, uso e possível destruição futura da informação. A "ética dos dados", nesse passo, estuda e avalia problemas morais relacionados ao uso de dados por sistemas de processamento (incluindo geração, registro, curadoria, processamento, disseminação, compartilhamento e uso), algoritmos (incluindo inteligência artificial, agentes artificiais, aprendizado de máquina e robôs) e práticas correspondentes às inovações, a fim de formular e apoiar moralmente boas soluções, como a construção de condutas corretas ou valores corretos.

As análises com foco em dados associadas à privacidade abordarão questões relativas ao consentimento e responsabilidades profissionais; assim como a auditoria ética de algoritmos revelará as responsabilidades de seus projetistas, desenvolvedores, usuários e adotantes. Por outro lado, a denominada *soft ethics* defendida pelo autor apresenta uma dupla vantagem para a sociedade: é uma oportunidade estratégica e uma capacidade maior de lidar com riscos[212]. Nesse sentido, "[...] a aceitação pública e a adoção de tecnologias digitais, incluindo inteligência artificial, ocorrerão apenas se os benefícios forem vistos como significativos e os riscos como potenciais, mas evitáveis, minimizáveis ou pelo menos algo contra o qual alguém possa ser protegido"[213].

Os riscos são inerentes ao desenvolvimento das sociedades. Na atualidade, os riscos relacionam-se com incertezas e a impossibilidade de prever o futuro quando tratamos de aplicações de tecnologias. O risco associa-se ao comprometimento e à possibilidade de dano futuro à coletividade, isto é, o risco e o dano passam a ser coletivizados[214]. A perspectiva em análise considera o efeito relevante no plano da proteção de dados pessoais. Em outras palavras, a complexidade do risco aumenta com o incremento tecnológico, o que depende da *adaptação aos riscos*. A expressiva vulnerabilidade da natureza face à intervenção humana, especialmente porque nenhuma conduta humana afasta o risco, pois ele é inerente à decisão e deve ser "percebido socialmente"[215], entre os quais o da reidentificação posterior da pessoa.

---

[212] FLORIDI, Luciano. Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage, *Philos. Technol.* n.31, p.166–167, 2018.

[213] FLORIDI, Luciano. Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage, *Philos. Technol.* n.31, p. 167, 2018.

[214] ENGELMANN, Wilson; SZINVELSKI, Mártin M.. Risco cibernético no tratamento de dados pessoais e autodeterminação informativa: reflexões à luz da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). In: Dóris Ghilardi; Liz Beatriz Sass. (Org.). *Temas Atuais de Direito Privado e Sociedade da Informação*: o direito na era digital. 1ed.Florianópolis: Habitus, 2020, p. 95-114.

[215] VARA, Ana María. A un año de la muerte de Ulrich Beck: De la sociedad del riesgo a la metamorfosis del mundo. Rev. Iberoam. Cienc. Tecnol. Soc., Ciudad Autónoma de Buenos Aires, v. 11, n. 32, p. 215-237, mayo, 2016.

4.1 O nível adequado de proteção de dados e fluxos internacionais

No interior de um país, é a legislação específica que determina as regras, procedimentos e o papel de atuação de organizações que realizam a guarda e o tratamento de dados pessoais. Aplica-se, nesse sentido, o princípio da territorialidade. O crescente progresso de integração econômica global, baseada na internet, conduz, contudo, ao fluxo transfronteiriço de dados, a extraterritorialidade, fenômeno em consolidação desde o início do presente século[216]. Atento a esse processo e em busca da ampliação de seu potencial econômico e tecnológico, o Brasil demarcou o interesse em ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e de celebrar um acordo com a União Europeia, por meio da atuação e parceria do bloco comunitário (MERCOSUL), o qual o Uruguai é membro nato. Dessa forma, há um interesse comum dos países integrantes de associarem-se, de forma mais sólida, aos processos que permitiram maior capacidade de prospecção de renda e, por via de consequência, de desenvolvimento e emprego[217]. Estabelecer parâmetros e compatibilizar a proteção dos dados com normas internacionais ou comunitárias passa a ser um excelente ponto de partida: não de submissão cultural, mas de oportunidade de crescimento, mesmo conhecendo a intenção de países estabelecidos e estabilizados economicamente de proteger os respectivos mercados nacionais[218]. Do ponto de vista internacional, pode-ser verificar a criação de diretrizes a serem implementadas pelos blocos econômicos de países, como os guias da OCDE e da APEC[219].

Nas últimas décadas, foram estabelecidas metas de digitalização da administração pública, proporcionando à interoperabilidade entre sistemas de informação e, principalmente, da oferta de serviços públicos baseados na *internet*. O Governo Digital apresenta-se como forma de aproximação do governo com os cidadãos. No Brasil, atualmente, 948 serviços

---

[216] Conforme dito anteriormente, trata-se de uma preocupação anterior, que fica raízes na década de oitenta e se estabelece a partir do início do século XXI. PALAZZI, Pablo. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. *Derecho de internet & telecomunicaciones*. Bogotá: Universidad de los Andes, 2003.

[217] Na visão europeia, há um plano estratégico a ser implementado. Cf. UNIÃO EUROPEIA. Autoridade Europeia para a Proteção de Dados. Relatório 2019. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_ex_sum_pt.pdf>. Acesso em 12 nov. 2020.

[218] Também, verificar o seguinte documento: GSMA. Flujos transfronterizos de datos. Materializando los beneficios y eliminando las barreras. Disponível em: < https://www.gsma.com/latinamerica/wp-content/uploads/2019/07/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_SPANISH-2.pdf.>. Acesso em 1 jan.2021.

[219] APEC. APEC cross-border privacy rules system: policies, rules and guidelines. Disponível em: <https://www.apec.org/groups/committee-on-trade-and-investment/~/media/files/groups/ecsg/cbpr/cbpr-policiesrulesguidelines.ashx>. Acesso em: 14 nov. 2020.

foram transformados em serviços digitais. O Brasil é o vigésimo colocado entre 193 nações, e o primeiro lugar no quesito de serviços digitais na América do Sul e segundo nas Américas, à frente de nações como Canadá, Chile e Uruguai e atrás somente dos Estados Unidos[220]. A organização classificou o Brasil na 16.º posição em seu Índice de Governo Digital. O Brasil ficou acima da média dos países da OCDE e superando nações como Alemanha, Estônia, Países Baixos, Áustria e Irlanda. Dos quatro mil serviços disponibilizados aos brasileiros, 2,6 mil estão digitalizados, cerca de mil nos últimos vinte e quatro meses[221]. Todo esse processo apresenta-se como contexto favorável ao fluxo de dados internacional.

As tecnologias da informação elevaram a capacidade de utilização de meios digitais para realizar o comércio, o que, consequentemente, elevou a necessidade de organizações de transferir dados, como são os dados pessoais dos consumidores. O lado positivo do progresso tecnológico nessa área está na inclusão não apenas de organizações, mas também de pessoas, que se utilizando dos caminhos viabilizados pela internet, contribuem para a livre circulação de bens e serviços, de forma quase instantânea. Com efeito, a expansão de tais ferramentas ignora áreas geográficas, favorece a eficiência do mercado e amplia as opções para o consumidor, tendo em vista reduzem o preço disponibilizado.

Por outro lado, a transnacionalidade do fluxo de informações levou a blocos econômicos e países (atuando isoladamente) a adotarem medidas de proteção à segurança da informação e à privacidade de dados. O RGPD tornou-se um parâmetro a ser considerado de proteção de direitos para a compatibilização e inserção econômica digital global. Contudo, tornou-se, também, um instrumento de proteção econômica, justo por utilizar mecanismos associados à rigidez normativa em torno do consentimento dos usuários e do cumprimento de princípios aplicáveis para habilitar transferências internacionais. A Comissão Europeia, nesse sentido, prevê que o incremento da circulação de dados entre os países do bloco elevará a economia digital europeia e poderá incrementar o 0,7% adicional até 2020[222]. O ponto máximo de regulação com ênfase na proteção de dados e de proteção de mercado está na

---

[220] BRASIL Brasil está entre os 20 países com melhor oferta de serviços digitais. Disponivel em:< https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2020/07/brasil-esta-entre-os-20-paises-com-melhor-oferta-de-servicos-digitais#:~:text=O%20Pa%C3%ADs%20subiu%20duas%20posi%C3%A7%C3%B5es,de%20Servi%C3%A7os%20Online%20(OSI).&text=O%20Brasil%20ficou%20em%20primeiro%20lugar%20neste%20quesito%20na%20Am%C3%A9rica,atr%C3%A1s%20somente%20dos%20Estados%20Unidos>. Acesso em 29 set. 2020.

[221] BRASIL. Portal gov.br já tem mil serviços públicos digitalizados para acesso do cidadão. Disponível: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2020/10/portal-gov-br-ja-tem-mil-servicos-publicos-digitalizados-para-acesso-do-cidadao>. Acesso em 29 set. 2020.

[222] GSMA. Flujos transfronterizos de datos. Materializando los beneficios y eliminando las barreras. Disponível em: <https://www.gsma.com/latinamerica/wp-content/uploads/2019/07/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_SPANISH-2.pdf.>. Acesso em 1 jan.2021.

autorização prévia das autoridades de proteção de dados ou do Conselho da Europa para o exercício do fluxo de dados internacionais[223].

Os mecanismos para controlar as transferências de dados pessoais para "países terceiros"[224] fora do bloco comunitário europeu são amplamente semelhantes aos estabelecidos na Diretiva de Proteção de Dados[225] (artigos 44 a 50). A Comissão tem o poder de determinar se as leis de determinados países, se territórios, se setores ou mesmo organizações internacionais oferecem um "nível adequado de proteção" para os dados transferidos[226]. Aqueles poucos países que foram aprovados como adequados pela Comissão continuarão a gozar desse estatuto, pelo menos durante quatro anos, quando seu status será revisado. Outros métodos para efetuar transferências continuam a ser reconhecidos, incluindo a aprovação de cláusulas contratuais padrão, regras corporativas vinculativas e códigos de conduta. O RGPD combina, portanto, a abordagem (i) aos países, por meio da validação isolada; *(ii)* por organização, por meio da análise dos contratos registrados nos órgãos, em relação às transferências internacionais[227]. Nesse sentido, pode-se notar a adoção de contratos corporativos e a adoção de selos de qualidade em proteção de dados.

Os padrões de avaliação da adequação, no entanto, mudaram desde a decisão do Tribunal de Justiça da União Europeia no *Caso Schrems*[228], que invalidou o Acordo de Porto Seguro, entre União Europeia e Estados Unidos. A decisão consagrou que o "nível adequado de proteção" deve ser entendido como aquele em que o país terceiro se compromete em assegurar, em razão de seu direito interno ou de seus compromissos internacionais, um nível

---

[223] Nesse sentido, tanto o RGPD quanto a normativa que regula o fluxo transfronteiriço com o bloco europeu adotaram medidas impeditivas limitando a transferência livre de dados ou metadados pessoais de seus cidadãos.

[224] USTARÁN, Eduardo GARCÍA, Paula. Transferencias internacionales de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.459-490.

[225] UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>. Acesso em 25 nov. 2020.

[226] PAVÓN PÉREZ, Juan Antonio. La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, n.19-20, p.235-252, 2002. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/831270.pdf>. Acesso em 13 nov.2020.

[227] BENNETT, Colin J. The European General Data Protection Regulation: An instrument for the globalization of privacy standards?. *Information Polity*, v. 23, n. 2, p. 239-246, 2018.

[228] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho (JO 2016, L 207, p. 1.) Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250>. Acesso em 23 nov. 2020. Nesse sentido, a doutrina analisou as transferências internacionais, especialmente após anulação da decisão, *Cf.* ARAÚJO, Alexandra Maria Rodrigues. As Transferências Transatlânticas de Dados Pessoais: O Nível de Proteção Adequado Depois de Schrems. *Revista Direitos Humanos e Democracia*, Editora Unijuí, ano 5, n. 9, jan./jun., p.201-236, 2017.

de proteção de direitos e liberdades fundamentais essencialmente equivalentes aos garantidos na União Europeia[229]. A diferença entre a forma de regulação americana e a adotada no continente europeu inviabilizou a comprovação da similitude de tratamento, especialmente pela característica mais centralizadora do modelo europeu, em face da fluidez ou ausência de regulação norte-americana.

Ainda que a decisão tenha sido tomada sob o contexto da Diretiva 95/46, o parecer do Grupo 29 salientou que não é o mero espelhamento com a legislação europeia que determina a confluência e adequação, mas a comprovação dos requisitos essenciais e fundamentais, o que passa por uma análise qualitativa de previsão normativa e da instrumentalização dos meios de proteção de dados[230].

No Uruguai[231], país que aderiu ao Convênio 108, o artigo 23 da LPDP estabelece que a transferência de dados[232] é proibida com países ou organizações internacionais que não fornecem "níveis adequados" de proteção de acordo com as normas de direito internacional ou regional na matéria. O Decreto 414/2009[233] estabelece nos artigo 34 e 35 o procedimento de autorização para transferências internacionais de dados, que ter a anuência da URCDP. Nesse sentido, há um roteiro a ser seguido, consistente em *(i)* identificar o banco de dados – especialmente porque, no Uruguai, é obrigatória a prévia inscrição de bancos de dados –, *(ii)* descrever como se dará a transferência, com a indicação da finalidade que a justifica e comprovando documentalmente e *(iii)* a obtenção da autorização. Para as transferências entre

---

[229] Nesse sentido, fixou-se que a transferência internacional depende da "[…] avaliação desse nível de proteção deve ter em consideração tanto as estipulações contratuais acordadas entre o exportador dos dados estabelecido na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro". Todavia a decisão foi cancelada, em razão de que a "[...] Comissão avaliou na Decisão Escudo de Proteção da Privacidade, não estão enquadradas de forma a satisfazer requisitos substancialmente equivalentes aos exigidos, no direito da União, pelo princípio da proporcionalidade, na medida em que os programas de vigilância baseados nessa regulamentação não se limitam ao estritamente necessário". TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. O Tribunal de Justiça declara inválida a Decisão de Execução 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf >.Acesso em 23 nov.2020.

[230] CORY, Nigel. *Cross-border data flows: where are the barriers, and what do they cost?*. Information Technology and Innovation Foundation, 2017. Disponível em: < https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>. Acesso em 11 nov.2020.

[231] BERTONI, Eduardo. Convention 108 and the GDPR: Trends and perspectives in Latin America. *Computer Law & Security Review*, p.3, nov., 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105516. Acesso em 29 jan.2021.

[232] URUGUAI. Ley n. 18331, de 11 de agosto de 2008. Lei de Protección de Datos Personales. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 1 set. 2020.

[233] URUGUAI. Decreto n. 414/009, de 31 de agosto de 2009. Reglamentacion de la ley 18.331, relativo a la proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>.Acesso em 1 set. 2020.

as organizações multinacionais, a autorização é fornecida, para o caso de transferência de dados entre a matriz e suas subsidiárias, quando existirem códigos de conduta previamente registrados do URCDP.

Nessa linha, estabelece algumas exceções como é o caso *(i)* cooperação judiciária internacional, de acordo com as respectivas previsões contidas em instrumento internacional, seja tratado ou convenção, tomando como parâmetro o caso apresentado, *(ii)* troca de dados médicos, quando exigido pelo tratamento da pessoa afetada por razões de saúde pública ou higiene, *(iii)* transferências bancárias ou de ações, em relação às respectivas transações e de acordo com a legislação daí resultante aplicável, *(iv)* acordos no âmbito de tratados internacionais em que o Uruguai é parte, *(v)* cooperação internacional entre agências de inteligência para o luta contra o crime organizado, o terrorismo e o tráfico de drogas. Para a lei uruguaia é necessário uma base legal ou contratual que fundamente a necessidade de transmissão dos dados, o que deve ser comprovado.

Como exceção, a UCRDP pode autorizar uma transferência ou série de transferências de dados a um terceiro país que não garante um nível adequado de proteção, apenas na hipótese de existirem garantias suficientes prestadas pelo controlador em relação à proteção da privacidade, direitos e liberdades fundamentais das pessoas envolvidas na transferência.

A evolução normativa contida no RGPD permitiu o movimento de dados no interior da comunidade europeia e para outros países[234] que têm sistemas de proteção de dados considerados "adequados", com é o caso do Uruguai que, conforme mencionado, passa pelo ajuste. Nessa linha de ideias, as organizações precisam demonstrar que há, no interior dos processos de tratamento e controle de dados, medidas de processamento responsável, o que deve ser justificado mediante a comprovação às autoridades de proteção de dados. A utilização de *standards*, códigos de condutas, certificações podem ser utilizados para esse fim[235]. A LGPD, por exemplo, faculta às organizações que desejam realizar transferência de dados desde que no país ou as organizações se utilizem de mecanismos adequados para protegê-los[236]. Conhecer, ao menos, o que é um nível adequado de proteção de dados,

---

[234] ANGARITA, Nelson Remolina. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law*: Revista Colombiana de Derecho Internacional, v. 8, n. 16, 2010.

[235] REILLY, Marcelo Bauzá. Los estándares de protección de datos personales para los Estados iberoamericanos. *La justicia uruguaya: revista jurìdica*, n. 156, p. 7, 2018.

[236] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

reconhecido pelos órgãos comunitários[237], tornou-se um ponto importante de satisfação aos parâmetros internacionais e de inclusão econômica a ser procedido pela Brasil e ser ajustado pelo país vizinho[238].

O *Cisco Data Privacy Benchmark Study Infographic*[239], publicado em 2019, estima o percentual de preparo dos países após o advento do RGPD. Partindo de uma visão global, 59% dos países estariam preparados, 29% estariam preparados em menos de um ano e 9% em período superior a um ano. Os restantes 3% representam países em que o documento normativo não se aplica. O Japão, por exemplo, que submeteu à Comissão Europeia um pedido de comprovação de compatibilidade, segundo o estudo infográfico, teria níveis de compatibilidade de 45%, enquanto o Brasil, com 53%, a Argentina, com 69%, México, com 70% precisariam realizar ajustes regulatórios para completar o estrato. Por outra via, chama a atenção o fato de que países como França, Alemanha, Estados Unidos, Canadá e Austrália apresentem níveis de compatibilidade próximos ao termo médio de 60%, muito próximos aos níveis do Brasil. A França, por exemplo, segundo o mapeamento da Cisco, apresentaria taxa de compatibilidade de 62% e a Alemanha de 58%, mesmo pertencendo ao bloco o comunitário. Os dados demonstram que a comprovação da compatibilidade e da eficácia do sistema precisa de um atestado de credibilidade, não bastando a mera narração de direitos e de princípios aplicáveis.

O nível adequado de proteção de dados[240] não encontra uma definição precisa no Regulamento 45/2001, que atualmente encontra-se em revisão pela Comissão Europeia, em

---

[237] Centre for information policy leadership: Cross-Border Data Transfer Mechanisms [Mecanismos de Transferencia Transfronteriza de Datos], agosto de 2015. Disponível em: < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf> Acesso em: 25 nov. 2020.

[238] Como contraponto a essa ideia, no sentido de inexistir uma forte uniformização, os autores estabelecem que "[...] a ausência de critérios internacionais uniformes em relação ao direito à proteção de dados pessoais não só dificulta a relação com a Europa em termos de fluxos de informação entre as autoridades e o setor privado, mas também acentua as diferenças conceituais entre os vários sistemas de direitos humanos, cuja característica fundamental deve residir precisamente em sua 'universalidade'. A falta de padrões comuns entre as regiões dificulta o cumprimento de certos objetivos importantes para o progresso econômico e social, o desenvolvimento do intercâmbio entre os países e o bem-estar dos indivíduos, como a eliminação de restrições à livre circulação de dados pessoais, distorcendo a concorrência econômica e impedir que as administrações cumpram as tarefas que lhes incumbem, bem como questões de segurança de dados". MAQUEO RAMÍREZ, María Solange; MORENO GONZÁLEZ, Jimena; RECIO GAYO, Miguel. Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho*, v. 30, n. 1, p. 93, 2017.

[239] *Cisco Data Privacy Benchmark Study Infographic*. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-infographic.pdf. Acesso: 23 nov.2020.

[240] Do ponto de vista do Chile, mas com a mesma perspectiva, consultar: CERDA SILVA, Alberto. El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de derecho* (Valparaíso), n. 36, p. 327-356, 2011.

razão da necessária compatibilidade com o RGPD[241]. Saliente-se, todavia, que a adequação é um *conceito funcional*, portanto, e que leva em consideração as regras de destino e os mecanismos para eficácia da proteção de dados. Nesse sentido, o respeito aos princípios e diretrizes como os formulados pelo Grupo de Trabalho de Proteção de Dados do Artigo 29[242], tornou-se ponto de destaque utilizado pela AEPD, ainda que possam ser revisados nos próximos anos para adequação à nova normativa. Registre-se, contudo, que há uma continuidade de proteção, de modo que não haverá retrocesso consistente em minimizar níveis de cautela, especialmente em países em que existe a comprovação anterior da adoção de boas práticas.

Após a edição da LPDP e dos decretos que a regulamentam, por meio de Carta Diplomática enviada em 2011, o Uruguai[243] manifestou interesse em aderir à Convenção para a Proteção de Pessoas Singulares no que diz respeito ao Tratamento Automático de Dados Pessoais, a denominada Convenção 108 e ao seu Protocolo Adicional[244]. As URCDP comprovou e ofereceu garantias sobre a forma de aplicação da legislação uruguaia, inclusive no que concerne à interpretação, salientando o respeito aos princípios da proporcionalidade e finalidade no tratamento dos dados pessoais e a sujeição ao controle da própria URCDP[245].

Em relação ao princípio da transparência, URCDP comunicou que a obrigação de prestar as informações necessárias às pessoas a quem os dados dizem respeito é aplicável em todas as situações. Relativamente ao direito de acesso, a autoridade de proteção de dados especificou que é suficiente que a pessoa em causa prove a sua identidade no momento em que apresentar o pedido. As autoridades uruguaias de proteção de dados especificaram ainda que as exceções relativas ao princípio das transferências internacionais, previstas no artigo 23

---

[241] UNIÃO EUROPEIA. Supervisor Europeu para Proteção de Dados. Disponível: <https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf> Acesso em: 23 nov. 2020.

[242] UNIÃO EUROPEIA. Article *29 Working Party. Working Document Transfers of personal data to third countries*: Applying Articles 25 and 26 of the EU data protection directive. Disponível em: < http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827 >.Acesso em 1. Out.2020.

[243] CONSELHO DA EUROPA. *Convention for the Protection of Individuals with regard to Automatic rocessing of Personal Data (ETS No. 108)* - Request by Uruguay to be invited to accede Item to be considered by the GR-J at its meeting on 30 June 2011. Disponível em: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cce94>.Acesso em 14 nov. 2020.

[244] UNIÃO EUROPEIA. *Convenção para a proteção de indivíduos com relação ao processamento automático de dados pessoais*. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em 8 nov. 2020.

[245] COMISSÃO EUROPEIA. Decisão de execução da Comissão de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 215 de 25.8.2000, p. 1. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484 Acesso em 14 nov.2020.

da LPDP não poderiam ser interpretados com maior amplitude do que a prevista no artigo 26. Diretiva 95/46/CE.

Seguindo basicamente as orientações da OCDE, inclusive em conformidade com o RGPD, o documento "Normas Ibero-americanas de Proteção de Dados Pessoais" apresenta-se como um marco para a proteção de dados pessoais na América Latina, por sistematizar pontos fundamentais tratados nas normas internacionais e que pode auxiliar os diferentes países latino-americanos na modernização de suas leis, considerando os princípios, direitos e disposições nelas estabelecidas. Há nesse sentido uma aspiração universal que permite sua aplicação por qualquer país que deseje realizar um processo de modernização de sua regulamentação, centrando-se na proteção dos dados pessoais como um direito fundamental das pessoas[246]. Servindo como documento de sistematização e harmonização compatível com os documentos comunitários, ele pode servir como ferramenta de estandardização.

Por outra via, a *Global Privacy Assembly* é o principal fórum mundial para autoridades de proteção de dados pessoais, permitindo que se forneça liderança internacional e a conexão entre mais 130 autoridades de proteção de dados do mundo. A URCDP faz parte das entidades que integram este fórum, participando ativamente nas atividades que desenvolve e na elaboração dos documentos de impacto informativo na área. Pertencer à comunidade constitui-se de um ponto facilitador da uniformização dos parâmetros de adequação.

Segundo a LGPD, cabe à ANPD regular quais países possuem o nível adequado para viabilizar transferências internacionais. Isso significa que caberá ao órgão definir quais países se enquadram e possuem grau semelhante à legislação brasileira em matéria de proteção de dados. Conforme visto, o Uruguai já avançou na aplicação dos princípios contidos no Acordo Original da Convenção 108 e no Regulamento Europeu[247], portanto, em substância, a emenda à Convenção Original (108+) não possui novidades. Conforme referiu-se, a decisão do Conselho da Europa no sentido de reconhecer o Uruguai no patamar de país adequado deve-se a intensidade de regulamentação temática. O ajuste foi realizado por meio do Decreto 64/020 que regulamentou a avaliação de impacto regulatório, a escolha do delegado de proteção de dados e os princípios da responsabilidade demonstrada[248].

---

[246] KAMARA, Irene. Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation'mandate'. *European journal of law and technology*, v. 8, n. 1, 2017.

[247] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da Europa,* de 27 de abril de 2016. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 14 out. 2020.

[248] O estado atual da proteção de dados pessoais conduziu ao reforço do princípio da responsabilidade, na sua evolução para um princípio da responsabilidade demonstrada, que impõe ao responsável a obrigação de demonstrar que as atividades de tratamento cumprem a legislação aplicável. Nesse sentido, foi incorporado um

Para a regulamentação uruguaia, da avaliação de impacto sobre a proteção de dados pessoais deverá ser feita, com maior importância, *(i)* no caso de tratamento de dados sensíveis ou de pessoas vulneráveis, *(ii)* no tratamento de grandes volumes de dados pessoais, *(iii)* envolver a avaliação dos aspectos pessoais dos titulares com vista à criação ou utilização de perfis pessoais, com a utilização de mecanismos de mineração baseados em inteligência artificial para inferir aspectos relacionados ao desempenho no trabalho, situação econômica, saúde, preferências ou interesses pessoais, fiabilidade, comportamento e financeiro solvência e localização e *(iv)* transferir dados pessoais a outros países ou organizações internacionais onde não haja um nível adequado de proteção de dados[249].

O conteúdo deverá conter *(i)* a descrição sistemática do tratamento a ser realizado e sua finalidade, *(ii*) uma avaliação do tratamento em relação ao cumprimento das normas de proteção de dados pessoais, *(iii)* a avaliação dos riscos para os direitos dos titulares dos dados e *(iv)* o detalhamento das medidas e mecanismos de segurança para demonstrar o cumprimento das normas de proteção de dados pessoais. Os tratamentos já iniciados devem apresentar o relatório de impacto no prazo de um ano, sendo que no caso de identificação do risco potencial e significativo para os direitos dos proprietários dos dados, o responsável deverá informar a URCDP de forma detalhada e apresentar as medidas necessárias que irão ser adotadas. Caberá, por fim, a URCDP apresentar outros critérios para a perfectibilização da avaliação do impacto a depender do tipo e volume de dados e seu tratamento.

A título comparativo, o artigo 55-J da LGPD, inciso XIII, estabeleceu que cabe à ANPD "[...] editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais". Nesse sentido, há apenas, nesse momento, a previsão legal da edição desse regulamento na legislação brasileira, sendo que a fixação dos requisitos ocorrerá após a edição do ato pelo poder da ANPD.

---

mínimo de medidas, entre as quais *(i)* a proteção dos dados desde o desenho e por defeito e *(ii)* as avaliações de impacto anteriores, nos casos em que haja maior risco para as pessoas.

[249] URUGUAI. Decreto 64/020, Reglamentacion de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 1 set. 2020.

O Decreto 64/2020[250] regulamentou, de igual forma, a incorporação da figura do delegado para a proteção de dados (conhecido no inglês como *Data Privacy Officer*), com o motivo de estabelecer as competências e garantir a independência técnica do profissional, figura que é relevante no âmbito das organizações públicas, organizações que tratam dados sensíveis ou que tratam grandes volumes de dados pessoais. Trata-se, de compatibilizar a legislação aplicável às novas previsões do RGPD. A função do DPD está vinculada ao assessoramento na formulação, desenho e aplicação de políticas de proteção de dados pessoais no âmbito das organizações, e viabilizar a adoção de medidas que considere pertinentes para a adaptação aos regulamentos e normas internacionais em matéria de proteção de dados pessoais, fiscalizando a execução desses processos. Deverá atuar como elo entre sua organização e a URCDP.

Outra medida de compatibilização é a regulamentação da responsabilidade proativa das organizações por meio da qual se afirma a lógica da prevenção, mediante a utilização de normas técnicas, modelos comportamentais de atuação, a internalização de padrões técnicos na condução dos processos. A ideia que subjaz está vinculada a incorporar na concepção das bases de dados (privacidade pelo desenho), nas operações de tratamento, nas aplicações e nos sistemas informáticos, medidas destinadas a cumprir a regulamentação em matéria de proteção de dados pessoais. Para atingir esse objetivo, o responsável pelo tratamento, segundo o Decreto 64/2020, deve adotar medidas técnicas *(i)* de dissociação, pseudonimização e minimização de dados, *(ii)* mecanismos para assegurar o exercício dos direitos dos titulares de dados pessoais, *(iii)* fornecer os termos de consentimentos ou outros fundamentos que legitimam o tratamento, *(iv)* estabelecer o tempo de conservação dos dados, considerando seus tipos e seu tratamento, *(v)* prever e adotar de planos de contingência e modelos de análise que incluam medidas de segurança da informação, além de outras exigências requeridas pela URCDP. Por outro lado, se durante o tratamento de dados ocorrer defeito da tecnologia, apenas os dados pessoais necessários para atingir a finalidade da operação deverá ser empregada, no que entende por privacidade por defeito, isto é, a programação de minimização do dano causado, na hipótese de falha da tecnologia. A LGPD, no artigo 46, estabeleceu a necessidade de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição,

[250] URUGUAI. Decreto 64/020, Reglamentacion de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 1 set. 2020.

perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, sendo que "[...] as medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução"[251].

Assim como no Uruguai, cuja regulação pormenorizada cabe à URCDP, é dever da ANPD dispor sobre padrões técnicos mínimos natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis. A URCPD lançou um *Guia de Boas Práticas em Proteção de Dados*[252], em relação ao preenchimento de formulário na internet. A ANPD, de igual forma, possui um *Guia de Boas Práticas para Implementação na Administração Pública Federal*[253], de forma a disponibilizar aos interessados um formulário para o preenchimento de avaliação do relatório de impacto e dos principais conceitos envolvidos nesse processo.

4.2 A técnica de anonimização de dados pessoais vista por meio da atuação da URCDP – o papel instrutivo a ser desempenhado pela ANPD

Para a proteção de dados pessoais tornar-se efetiva, há que ser considerado o relevante o emprego de técnicas especializadas que garantam a concreção em formas de mecanismos que atestem a confiabilidade da proteção de dados[254], já que a efetividade do direito em análise depende do correto emprego de medidas tendentes a atingir essa finalidade[255]. Essa é uma decorrência do poder de colaboração público-privada – no sentido do estabelecimento de diretrizes e padrões de unificação – por meio da realização de um estudo pela ANPD, assim como o executado pela URCDP, e o emprego ou adoção por organizações do setor privado, na maior parte[256].

---

[251] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 out. 2020.

[252] URUGUAI. URCDP. *Buenas prácticas en protección de datos personales para el uso de formularios por entidades públicas*. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/buenas-practicas-proteccion-datos-personales-para-uso-formularios>. Acesso: 24 out. 2020.

[253] BRASIL. Guia de Boas Práticas para Implementação na Administração Pública Federal. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf>. Acesso em: 16 out. 2020.

[254] SANTOS, Marina; CERQUEIRA, Norma; MENEGHETTI, Rayssa. Anonimização de dados como garantia ao direito à privacidade na internet das coisas (Internet of Things-IoT). *Revista Brasileira de Direito e Gestão Pública,* v. 8, n. 5, p. 1219-1229, 2020.

[255] VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto N. G. de. Dados anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. In: TEPEDINO, Gustavo; FACHIN, Luiz E. (Org.). *Pensamento crítico do direito civil brasileiro*. Curitiba: Juruá, 2011.

[256] Para Navarrete, de uma visão europeia convergente, sugere que "[...] a maior relevância desta função tão importante da Agência traduziu e será traduzida na prática na emissão dos chamados relatórios obrigatórios

No Uruguai, foi aprovada a lista de critérios pela autoridade uruguaia, pela Resolução nº 68/017, de 26 de abril de 2017, normativa que aprovou o documento que estabelece os *Critérios para Dissociação de Dados Pessoais*[257], com base na antiga Diretiva Europeia, mas que ainda permanecem válidos. O que subjaz à perspectiva é a possibilidade de minimizar a reidentificação do proprietário dos dados[258], ainda que a dinâmica das tecnologias da informação permita o surgimento de novos mecanismos de identificação[259]. A minimização do risco de reidentificação repercute na esfera da redução progressiva do dano e da quantificação final da responsabilidade pública ou privada pelos prejuízos causados.

No Brasil, a LGPD estabelece no §3.º do artigo 48 que o controlador dos dados, deve comprovar "[...] que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los", o que pode servir de atenuação da sanção administrativa para o caso de violação de dados, conforme prevê o §1.º, do artigo 52[260]. O Decreto 10.474, de 2020, no artigo 4.º, inciso III, alínea "a", estabelece que cabe ao Conselho Diretor dispor sobre "[...] os padrões e as técnicas utilizados em processos de anonimização e verificar a sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade". Trata-se, portanto, de competência prevista que deve ser desempenhada de forma que corresponda a modelos já empregados e que apresentam resultados satisfatórios.

---

sobre projetos de disposições de natureza em geral. A importância desses relatórios é capital em um duplo sentido: uma parte, porque permitem avaliar a adequação das regras às bases legais, princípios e direitos de proteção de dados no assunto regulamento. Por outra, porque contribuem de forma essencial para garantir o sistema do ordenamento jurídico como um todo e, com ele, a segurança jurídica." NAVARRETE, Jesús Rubí. La agencia española de protección de datos. LOMBARTE, Artmi (Diretor). Tratado de Protección de Datos. Valencia: Tirant lo Blanch, 2019. p.511.

[257] URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado "Criterios de disociación", que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017>.Acesso em 10 dez. 2020.

[258] SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1814-1894, dec. 2011.

[259] Nesse sentido, Ohm entende que a simples remoção da informação pessoal não significa a proteção integral da privacidade. OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, n. 57, p. 1701-1777, 2010.

[260] Conforme a LGPD, as "[...] sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: [...] VIII - adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados".

O Grupo 29[261], por meio do Parecer Técnico Parecer 05/2014, estabeleceu que a anonimização é a técnica que possui o objetivo de viabilizar que os dados desagregados da pessoa titular sirvam para que organizações empresariais e públicas possam utilizá-los, sem gerar conflitos aos respectivos titulares, como importante instrumento de proteção de dados.

A dissociação apresenta-se como gênero dos processos de tratamento de dados em que não se possa estabelecer, futuramente, por meio de simples reversão, vínculos com uma pessoa específica ou determinável. A pseudonimização[262] não se confunde, portanto, com a dissociação, porquanto permite a identificação posterior e é entendida como forma de tratamento em que se perde "[...] a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro"[263]. Na mesma linha, para Doneda e Machado, esse processo se desenvolve de forma que inexista conexão com o titular dos dados, "[...] sem que se recorra a informações suplementares, desde que estas sejam mantidas separadamente, empregadas medidas organizativas e de segurança"[264]. A anonimização, por sua vez, consiste, quase que no completo apagamento da identificação, porque os mecanismos empregados na limpeza do rastro tecnológico ou cadastro torna complexa a reversão do procedimento para a identificação do titular[265].

---

[261] Grupo de Trabalho de Proteção de Dados do Artigo 29, no Parecer 05/2014 sobre a anonimização de dados no contexto do direito da União Europeia, foram destacadas quatro características fundamentais das técnicas de anonimização: (i) a anonimização pode ser um resultado do tratamento de dados pessoais com a finalidade de impedir de forma irreversível a identificação do titular dos dados; (ii) várias são as técnicas de anonimização que podem ser utilizadas, visto que não há prescrição na legislação europeia de técnica específica; (iii) os elementos contextuais são muito importantes, ou seja, na avaliação deve ser tomado o conjunto "dos meios 'suscetíveis de serem razoavelmente' utilizados para identificação pelo responsável pelo tratamento e por terceiros", de acordo com o estado da técnica; e (iv) à anonimização é inerente a existência de um fator de risco. UNIÃO EUROPEIA. Grupo de Trabalho de Proteção de Dados do Artigo 29. Dictamen Nº 05/2014, de 10 de abril de 2014, adoptado por el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE. Disponível: <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831045040634.pdf.> Acesso em: 12 set. 2020.

[262] Para Bioni, "[...] a legislação de proteção de dados pessoais brasileira não sistematizou adequadamente a figura da pseudoanonimização, muito menos desenhou normativamente incentivos expressos para a sua adoção por parte dos agentes de tratamento de dados. Enquanto o regulamento europeu previu até mesmo o relaxamento de algumas obrigações legais, a lei geral brasileira de proteção de dados pessoais apenas citou pseudoanonimização de forma assistemática". BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*, São Paulo, n, 53, p. 194, jan-mar, 2020.

[263] LGPD, §4.º, do artigo 12. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.html> Acesso: 24 jun. 2020.

[264] MACHADO, Diego; DANILO, Doneda. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Caderno Especial - A Regulação da Criptografia no Direito Brasileiro*, vol. 1, p. 123, 2018.

[265] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*, São Paulo, n, 53, p. 193-194, jan-mar, 2020.

Em documento publicado pela URCDP e pela AGESIC[266] são estabelecidas diretrizes de atuação, com a explanação dos processos de anonimização a serem empregados pelos controladores, que podem ser analisados em três etapas: *(i)* pré-anonimização, *(ii)* anonimização e *(iii)* controle. Na fase de pré-anonimização, os controladores devem elaborar o *projeto de anonimização*, por meio do qual se identificam variáveis e vulnerabilidades e quais serão as técnicas apropriadas de anonimização, a depender do tamanho e conteúdo dos dados a serem desidentificados, considerando, inclusive, o risco de reidentificação. A segunda etapa consiste na anonimização propriamente dita, na qual ocorre o processo técnico de afastamento ou dissociação entre o titular do dado e o dado pessoal em tratamento. A terceira etapa consiste no controle periódico pelos técnicos em virtude do surgimento de novas tecnologias de reidentificação – baseados em algoritmos e mecanismos cruzados de identificação – e o acompanhamento e emprego de novos métodos para prevenir e evitar possíveis riscos de reidentificação.

A etapa da pré-anonimização (ou de projeto) pode ser analisada pelo *prisma funcional*, haja vista que nesse momento, devem ser definidos os dados a serem tratados, consoante o perfil do dado, das capacidades das empresas, dos técnicos e da equipe jurídica de orientação. Por outro lado, nessa etapa é realizado plano de contingência para o caso de detecção do risco de reidentificação e da pronta resposta técnica. A etapa de anonimização deve seguir os padrões normativos enunciados principalmente pelo órgão regulador ou pelo bloco comunitário que demande uma proteção maior como mecanismo de proteção de cidadãos, como é o caso da União Europeia. Os padrões previstos em mecanismo de normalização oferecem um rol enunciativo de padrões a serem seguidos, como *(i)* a necessidade de que vínculos possam ser estabelecidos entre os dados e seu proprietário sem esforço técnico e tecnológico, *(ii)* a irreversibilidade do tratamento de anonimização, no sentido de que o produto do processamento dos dados não possa ser refeito de forma a identificar o titular dos dados, *(iii)* a utilização de mecanismos técnicos de anonimização sejam equivales ao apagamento permanente do dado e *(iv)* considere o risco da não utilização correta das técnicas ou do surgimento de mecanismos de identificação posterior, alheias ao conhecimento contemporâneo. Sobre o tema dos riscos, é importante ter em conta a não confusão entre

[266] URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado “Criterios de disociación”, que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: < https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017 >.Acesso em 10 dez. 2020.

pseudonimização com anonimização, por meio do qual a existência de uma informação adicional permita associar ao titular dos dados anonimizados[267].

A considerar as técnicas utilizadas para a anonimização não é tarefa que escapa do tema do direito à proteção de dados pessoais e da tarefa consultiva exercida pela ANPD, como forma de diminuir o risco de identificação posterior. A randomização ou aleatorização apresenta-se como forma técnica de proteção dos dados, de modo que a premissa empregada é que a técnica oferece um conjunto de procedimentos que modificam a veracidade dos dados, tornando-os ambíguos o suficiente ao ponto da quebra da possibilidade de identificação. A facilidade reservada ao processo está na capacidade de proteger contra ataques ou riscos de inferência, em razão da introdução de informações não fidedignas, como é o caso da inserção do ruído. Há uma parcela verdadeira e outra falsa, característica que dificulta a identificação[268].

Contudo, esse processo demanda cautela e por si não é suficiente, especialmente com a inserção de ruído inconsistente, com informações fora da escala ou da lógica empregada ao conjunto de dados, o que permite, pela simples filtragem das informações, a recuperação dos dados ou informações. Conforme alerta a URCPD, pensar que a adição de ruído é uma medida suficiente e que inviabiliza a completa identificação da pessoa é um erro, uma vez que esse procedimento é complementar e possui a finalidade de embaralhar mecanismos de análise e prospecção de informações contidas em um conjunto de dados, de forma que eventuais informações colhidas não possuam o mesmo índice de credibilidade, inclusive com as possibilidades de falsos positivos de reidentificação.

A permutação é a técnica de anonimização em que ocorre a mistura dos valores ou atributos em determinado banco de dados, por meio da adição de ruído informacional. A distinção em relação à randomização reside no fato de que os valores são substituídos, deslocando-se de um registro para outro, embaralhando o banco de dados[269]. Por outra via, se a modificação dos valores for realizada de forma for mínima, a simples troca no interior de

---

[267] PEIXOTO, Erick Lucena Santos; EHRHARDT JÚNIOR, Marcos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. EHRHARDT JÚNIOR, Marcos, LOBO, Fabíola Albuquerque (Org.). *Privacidade e sua compreensão no direito brasileiro*. Belo Horizonte: Fórum, 2019. p.49-51.

[268] URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado “Criterios de disociación”, que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017>.Acesso em 10 dez. 2020.

[269] MACHADO, Javam; NETO, Eduardo; BENTO FILHO, Manuel. Técnicas de Privacidade de Dados de Localização. SBBD 2019, p. 8.

um pequeno contexto, a expectativa de proteção de dados – e da privacidade – pode restar frustrada.

A *privacidade diferencial* apresenta-se como mecanismo diferenciado, em que o controlador dos dados possui os dados originais (em cópia), embora trate ou acesse dados anônimos. Essa técnica permite o compartilhamento de dados anônimos de terceiros, mas demanda uma supervisão constante, especialmente quanto ao grau de ruído que deve ser associado ao dado para impedir a reidentificação. Segundo o manual formulado pela URCDP, entre as "[...] vantagens da privacidade diferencial é o fato de conjuntos de dados são fornecidos a terceiros autorizados em resposta a um consulta específica e não simplesmente como consequência da publicação de um único conjunto de dados"[270]. Todavia, deve ser considerada a hipótese de que há o apagamento das informações, quando, em realidade, o controlador, por possuir uma cópia, detém também a capacidade de reidentificar o titular dos dados.

Por outra perspectiva, a técnica de *generalização das informações* permite que a proteção de dados pessoais. A perspectiva técnica em questão generaliza ou dilui os atributos das partes interessadas, modificando a escala, apesar de nem sempre a eliminar o estabelecimento de vínculos com o titular. A técnica do *k-anonimato*[271], por exemplo, tem como objetivo prevenir que o titular dos dados seja identificado quando o conjunto de dados é agrupado com outras informações de outros titulares (portanto, a proveniência da letra *k)*, suprimindo determinada informação do titular. Dessa forma, permite-se que determinado proprietário de dados seja incluído no interior de um estrato ou de uma faixa de dados. O

---

[270] URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado "Criterios de disociación", que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017>.Acesso em 10 dez. 2020.

[271] AFFONSO, Elaine Parra; SANT'ANA, Ricardo César Gonçalves. Preservação da privacidade no acesso a dados por meio do modelo k-anonimato. *Ponto de Acesso*, v. 11, n. 1, p. 27-28, 2017. A Comissão da Proteção de Dados Pessoais de Singapura, publicou um Guia para Técnicas Básicas de Anonimização de Dados, o que foi traduzido pelo Governo Governo da Região Administrativa Especial de Macau. Nessa fonte, há a explanação de como utilizar o método. Para emprego, de forma resumida, "[...] é necessário decidir um valor para k (o que essencialmente é igual a ou maior que o inverso do tamanho da classe de equivalência), o que promove que o k mais baixo seja atingido entre todas as classes. Geralmente, quanto mais alto o valor de k, mais difícil é para os sujeitos dos dados serem identificados; porém, a utilidade pode se tornar mais baixa à medida que o k aumenta e mais registros necessitam de ser suprimidos. Após outras técnicas de anonimização serem aplicadas, deve-se verificar que cada registro tem pelo menos k-1 outros registros com os mesmos atributos abordados pelo k-anonimato. Os registros em classes de equivalência com menos de k registros devem ser considerados para supressão; em alternativa, pode-se realizar mais anonimização." Guia para Técnicas Básicas de Anonimização de Dados do Gabinete para a Protecção de Dados Pessoais (GPDP) do Governo Governo da Região Administrativa Especial de Macau. Disponível em: <https://www.gpdp.gov.mo/uploadfile/2019/0417/20190417033911965.pdf>.Acesso em 16 dez. 2020.

problema do método é a inferência que colhida de uma informação privilegiada proveniente de fora do banco de dados, a qual permitiria a identificação posterior. Como extensão da técnica, para tornar a informação incerta e anônima, diminuindo o risco da proteção, utilizam-se mecanismos como a *diversidade l* e *proximidade t* que possuem como proposta reduzir a margem de certeza da generalização[272].

Por fim, a etapa do controle destina-se à auditagem dos processos utilizados, como forma preventiva da reparação de danos ao proprietário dos dados por violações ou da possibilidade de tomada de providências para o fim da adequação da proteção de dados, por meio da atuação do responsável.

4.3 Os Selos de Qualidade em Proteção de Dados: um campo a ser explorado pela ANPD e URCPD em parceria com o setor privado

O modelo global de proteção de dados que se estrutura encaminha para o balanço entre a liberdade na circulação de dados (desenvolvimento tecnológico e econômico) e a proteção da esfera privada dos cidadãos, o qual demanda *standards*[273] (em português, *estândares*) ou padrões de proteção de dados. Seguir os caminhos para a normalização da cultura da proteção de dados apresenta-se como ponto de fundamental apoio para o reconhecimento de um nível adequado de proteção de dados. Definir qual é o nível adequado de proteção não é uma tarefa fácil de ser realizada e racionalizada, de forma que não depende, conforme referido, da mera locução de direitos ou repetição de preceitos legais ou internacionais. O cumprimento dos requisitos previstos na legislação é certificável, e não a lei, em si[274].

---

[272] URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado “Criterios de disociación”, que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017>.Acesso em 10 dez. 2020.

[273] Conforme estabelece Lohner, “[…] desarrollo y aplicación de modelos (standards) es uno de los medios por los que la importancia de las condiciones sociales para la aplicación de la tecnología de información es mejor demostrada. La «modelización» (standardization) de interludios y protocolos es una necesaria precondición para una competitividad justa pues los productos de la tecnología de información son comparables mientras que esta estandarización sea pública y general. Los gobiernos e instituciones gubernamentales se encuentran con el dilema de una necesidad de detern1inar sus actitudes sobre el tema de la standardization y los grados de regulación. En este contexto, los elementos tecnológicos y económicamente innovadores, asumen junto con los aspectos jurídicos un papel importante. La standardization fortalece y facilita la cooperación entre, por ejemplo, compañías; pero los gobiernos deben limitar (como ya han hecho algunos) aquella cooperación extrema que pueda derivar en la creación de monopolios”. LOHNER, Wolfrang. Tecnología de la información. Su impacto social y efectos legislativos. Algunas consideraciones. *Informática y Direito*: Revista iberoamericana de derecho informático, s.l., n.5, p.1429, 1994.

[274] LACHAUD, Eric. What GDPR tells about certification. *Computer Law & Security Review*, p.1, nov., 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105457. Acesso em 29 jan.2021.

A uniformização demanda uma atuação em conjunto de autoridades e especialistas, de forma que o principal ponto de contato e de viabilização de parcerias e de inovações tecnológicas é a ANPD, órgão que permitirá ao Brasil estabelecer sua visão e políticas em matéria de proteção de dados, seus programas e problemas a serem analisados em parceria. O artigo 55-J, inciso IX, da LGPD, estabelece a responsabilidade da ANPD em "[...] promover a cooperação com autoridades de proteção de dados de outros países, de natureza internacional ou transnacional"[275]. Segue-se que a adoção de modelos de atuação na vida prática de diferentes organizações, público e privadas, demandam uma atuação interligada com a ANPD.

Benoit Frydman estabelece que a polissemia da palavra *standard* sugira a compreensão do termo enquanto "[...] norma técnica, como a norma ISO, por exemplo, como o modelo (de comportamento ou de objeto), de padrão (de medida) ou de *benchmark* (nível de referência)"[276]. Transportando a perspectiva de normalização para a ótica especializada da proteção de dados, seguida no Brasil e no Uruguai, segue-se que a adoção do recente *Standards de Proteção de Dados*[277], elaborado pela *Rede Ibero-americana de Proteção de Dados*, apresenta-se como mecanismo que interliga os dois países, sendo, inclusive, o referido documento ponto importante para a consolidação do modelo de ambos os países, especialmente, pela regionalidade.

Anteriormente, a *Resolução de Madrid*[278], de 2009, apresentava o conjunto de princípios a serem adotados, os quais foram incorporados pela LGPD. Destaca-se, no âmbito específico das autoridades de controle, a incumbência de *(i)* compartilhar relatórios, técnicas de investigação, estratégias de comunicação, regulatórias e informações para o funcionamento eficiente e eficaz da atuação de outras autoridades, em particular após um pedido de cooperação de autoridade de proteção de dados na condução de uma investigação ou intervenção; *(ii)* conduzir investigações ou intervenções coordenadas, tanto em nível nacional

---

[275] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

[276] FRYDMAN, Benoit. *O fim do Estado de Direito*. Porto Alegre: Livraria do Advogado, 2016. p.19-20.

[277] REDE IBEROAMERICANA DE PROTEÇÃO DE DADOS. *Standards de Proteção de Dados*. Disponível em: <https://www.dataguidance.com/sites/default/files/02.24.20_ibero-am_standards.pdf>. Acesso em: 30 nov. 2020.

[278] INTERNACIONAL STANDARDS ON THE PROTECTION OF PERSONAL DATA AND PRIVACY. Resolução de Madrid. Disponível em: <http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf>. acesso em: 4 dez. 2020.

como internacional, em questões onde os interesses de dois ou mais autoridades são compartilhados; *(iii)* participar de associações, grupos de trabalho e fóruns conjuntos, bem como em seminários, workshops ou cursos que contribuam para a adoção de cargos conjuntos ou para o aprimoramento da capacidade técnica do pessoal ao serviço dessas autoridades de supervisão; e *(iv)* manter o nível adequado de confidencialidade em relação às informações trocadas em o curso da cooperação. Em outras palavras, já havia uma relação de interligação entre as autoridades como forma de cooperar para a atuação eficaz na proteção de dados pessoais.

Essa perspectiva ficou marcada na realização das Conferências Internacionais de Autoridades de Proteção de Dados e Privacidade (ICDPPC)[279]. Além da formação da institucionalidade, a perspectiva da colaboração interinstitucional mostra-se necessária, por permitir que se abordem temas da convergência e conectividade e da busca de fórmulas para reforçar os níveis globais de proteção de dados. Da mesma forma, a visão do ICDPPC é manter um ambiente no qual as autoridades de privacidade e proteção de dados em todo o mundo possam atuar efetivamente para cumprir seus mandatos, tanto individualmente quanto em conjunto, disseminando conhecimento e conexões de apoio. A proposta é interligar os países e *(i)* estabelecer um conjunto de princípios e direitos comuns para a proteção de dados pessoais que pudessem ser adotadas pelos Estados Ibero-americanos e desenvolver suas legislações nacionais a respeito, com o objetivo de ter normas homogêneas na região; *(ii)* garantir o efetivo exercício e tutela do direito à proteção de dados pessoais de qualquer pessoa nos Estados Ibero-americanos, mediante o estabelecimento de regras comuns que assegurem o devido tratamento dos seus dados pessoais; *(iii)* facilitar o fluxo de dados pessoais entre os Estados Ibero-americanos e além de suas fronteiras, a fim de contribuir para o crescimento econômico e social da região e *(iv)* fomentar a cooperação internacional entre autoridades de controle dos Estados Ibero-americanos, com outras autoridades de controle não regionais e com autoridades e organismos internacionais da área.

Essa perspectiva se reforçará com a necessidade de regulamentar a utilização de certificação por selos em relação ao grau de proteção de dados[280] do cidadão, especialmente

---

[279] A Conferência Internacional de Autoridades de Proteção de Dados e Privacidade é um fórum global anual sobre autoridades de supervisão independentes sobre privacidade, proteção de dados e liberdade de informação que adotam resoluções e recomendações de alto nível dirigidas aos governos e às organizações internacionais. Da mesma forma, a visão do ICDPPC é manter um ambiente no qual as autoridades de privacidade e proteção de dados em todo o mundo possam atuar efetivamente para cumprir seus mandatos, tanto individualmente quanto em conjunto, disseminando conhecimento e conexões de apoio.

[280] RIFON, Nora J.; LAROSE, Robert; CHOI, Sejung Marina. Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of consumer affairs*, v. 39, n. 2, p. 339-362, 2005.

como processos de refinamento da ciberseguridade[281]. Por um lado, é reconhecido que as novas tecnologias e a globalização informática permitem o fluxo de dados de forma transnacional. Por outro, a preferência por instrumentos de autorregulação regulada, como é o caso de mecanismos de certificação por selos, associa-se à ideia de formular medidas "visíveis" aos cidadãos de que os dados estão sendo tratados de forma condizente com determinado padrão-técnico[282].

Em termos comparativos, a aposta da Diretiva n. 95/46, do Conselho da Europa, não atingiu o sucesso nas aspirações globais de adoção de selos em matéria de proteção de dados[283], fato esse que procura ser corrigido pelo Regulamento Europeu, que dedica sessão e capítulo exclusivo à temática na regulamentação regional europeia. Em razão da potencialidade econômica do tratamento de dados na sociedade contemporânea, a normatização europeia tende a servir de parâmetro normativo para a introdução de mecanismo de certificação por selos no plano nacional[284].

Em termos conceituais, um selo de proteção de dados serve para certificar que um determinado produto, serviço ou processo na prestação de determinado serviço adere a padrões ou rotinas de proteção de dados ou da privacidade do cliente, com extensão de aplicabilidade no plano físico ou online[285]. O processo de certificação é, portanto, uma avaliação de conformidade, voluntária, em que uma organização – pública ou privada – se submete à auditoria externa realizada por órgão certificador credenciado por autoridade reconhecida[286]. Ao final do processo avaliativo, que, em verdade, apresenta-se como um

---

[281] Conferir, sobre o risco cibernético: ENGELMANN, Wilson; SZINVELSKI, Mártin M.. Risco cibernético no tratamento de dados pessoais e autodeterminação informativa: reflexões à luz da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). In: Dóris Ghilardi; Liz Beatriz Sass. (Org.). *Temas Atuais de Direito Privado e Sociedade da Informação*: o direito na era digital. 1ed.Florianópolis: Habitus, 2020, p. 95-114.

[282] FRYDMAN, Benoit. *O fim do Estado de Direito*. Porto Alegre: Livraria do Advogado, 2016. p.36.

[283] O motivo para o não atingimento dos objetivos traçados no artigo 27 da Diretiva mencionada tenha sido a não inclusão de requisitos de certificação ou selos em relação à proteção de dados, mesmo com o incentivo ao uso de códigos de conduta no nível nacional e europeu. A ausência de requisitos pode ser percebida, também, com a falta de critérios para considerar uma autoridade independente, o que foi solucionado pelo Regulamento Europeu em vigor. Consultar a seguinte referência: RODRIGUES, Rowena; BARNARD-WILLS, David; WRIGHT, David [et all...]. *EU privacy seals projec*t. Luxemburg: Publications Office of the European Union, 2013.

[284] A LGPD incorporou a noção da relevância da adoção de selos para a transferência internacional de dados pessoais, de forma que o controlador deverá oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados na legislação brasileira. Os selos, certificados e códigos de conduta regularmente emitidos são instrumentos de relevo, nesse sentido (art. 33, da LGPD). Caberá à Autoridade Nacional de Proteção de Dados fazer a verificação dos requisitos, as condições e as garantias mínimas para a transferência internacional (art. 34, da LGPD).

[285] RODRIGUES, Rowena; PAPAKONSTANTINOU, Vagelis (Org.). *Privacy and Data Protection Seals*. Springer, Information Technology and Law Series, v. 28, 2018.

[286] LACHAUD, Eric. The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument. *Computer Law & Security Review*, v. 34, n. 2, p. 244-256, April 2018. Disponível em: <https://doi.org/10.1016/j.clsr.2017.09.002>. 6 de abril de 2020.

ecossistema de avaliação, é expedido um certificado escrito em que o auditor atesta que a organização preenche os requisitos para a realização de determinada atividade ou insere um selo (marca/logo*)* que permite a identificação de que o serviço, produto ou processo coaduna-se com o padrão recomendado[287].

Trata-se de uma forma de regulação/vinculação que parte diretamente da esfera da privacidade[288] por meio de instrumentos de corregulação, dos quais se destaca o papel desempenhado pela *International Organization for Standardization* – ISO[289]. A introdução de elementos da cultura jurídica dos países de tradição anglo-saxã, como as noções de autorregulação, desregulamentação e responsabilidade, oferece maior flexibilidade ao procurar soluções para casos concretos e específicos, além de permitir a adaptação rápida às futuras mudanças tecnológicas. Todavia, a escolha implica maior incerteza jurídica para os responsáveis habituados à extensa regulação característica do modelo legal continental, seguido no Brasil.

Por isso, em termos acadêmico-descritivos, a exposição da sociedade contemporânea como objeto de uma "governança global" pautada pela transformação de contexto de uma ideia de governo estado-centrado à ideia de internacionalização, implica na pavimentação de um diálogo transnacional em que se exigiria uma composição ou harmonização de diferentes pontos de vista na perspectiva em que a sociedade não admite mais hierarquias, mas interações entre diferentes atores[290].

De igual forma, argumenta-se em termos dos espaços jurídico-políticos "antes" para o "depois" da globalização[291]. Ao se estabilizarem os processos globais no interior de uma perspectiva transnacional, a demanda por regulamentações setoriais passa a ser satisfeita pelos próprios sistemas. É nesse particular que deriva a aceitação da hipótese de Gunther Teubner ante a ascensão dos mercados financeiros, a popularização de mídias e de contratos *on-line* e a participação ativa de empresas multinacionais nas redes socioeconômicas em formação, que

---

[287] Nesse quadro, cabe lembrar, que o surgimento dos certificados e, particularmente, da relação de confiança que tende a ser estabelecida com o cidadão no campo da indústria, circunstância que pode ser incorporada ao tratamento de dados em uma sociedade em franca digitalização. O primeiro registro da introdução de certificados remonta o século XIX , com a *Bureau Veritas*, ao introduzir testes de conformidade de meios de transporte com os padrões técnicos.

[288] LACHAUD, Eric. What GDPR tells about certification. *Computer Law & Security Review*, p.2-3, nov., 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105457. Acesso em 29 jan.2021.

[289] YATES, JoAnne; MURPHY, Craig N. Coordinating International Standards: The Formation of the ISO. *MIT Sloan Research Paper No. 4638-07*. Disponível em: http://dx.doi.org/10.2139/ssrn.962455. Acesso em 5 abril 2020.

[290] FISHER-LESCANO, Andreas; TEUBNER, Gunther. Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law. *Michigan Journal of International Law*, v.25, p.1005, 2004.

[291] ZUMBANSEN, Peer. Transnational Legal Pluralism. *Transnational Legal Theory*, [s.l.], v. 1, n.2, 2010, p.141-189. Disponível em: < https://doi.org/10.1080/20414005.2010.11424506 >. Acesso em 5 abril 2020.

encaminham o direito global e nacional para a hibridização, entendida como a mixagem entre o *soft law* e o *hard law*[292].

Por outra via, o alto grau de tecnicidade das questões regulatórias e o papel crucial dos especialistas na sociedade contemporânea[293], especialmente na elaboração de normas aplicáveis, que se posicionam no espaço jurídico e ganham validade de forma distante das formalidades dos processos legislativos tradicionais, representam um desafio às teorias regulatórias, cuja consequência imediata é a expansão sobre áreas regulatórias transnacionais, que tornam viáveis o estabelecimento de conjunto de regras públicas e privadas produzidas e aplicadas por um conjunto diversificado de atores e especialistas[294]. A ideia de que a regulamentação global é necessária passa pela necessidade de resposta ao surgimento de um objetivo público comum, que não pode ser alcançado exclusivamente pelas ações isoladas de estados-nacionais ou autoridades reguladoras locais.

Por isso mesmo, os regimes regulatórios globais caracterizam-se por não se estruturarem em forma de ordem jurídica unitária e desenvolvem-se por meio da conjunção de estruturas administrativas, públicas ou privadas, como é o caso das organizações como a já citada ISO, a American Engineering Standard Commitee (AESC), British Standardization Institution (BSI), Agence Française de Normalisation (AFNOR), além das multinacionais certificadoras e do ramo de auditorias como a Bureau Veritas, a TÜV Süd, TÜV Rheinlande e a Intertek, grupos que movimentam uma indústria bilionária de auditoria e certificações. Nesses espaços regulatórios, é possível destacar a presença de mecanismos organizacionais privados de gestão, códigos de conduta setoriais e mecanismos de *compliance*, os quais tendem a ser absorvidos pelo setor público o qual passa a ser o grande fomentador da cultura da *dataveillance.* Nas palavras de Mireille Delmas-Marty essa cultura estimula o duplo jogo da "ilusão/confusão" que conduz à obsessão pela segurança; ao mesmo tempo, estimulam a adoção de regras e princípios que assumem natureza administrativa, relacionadas ao estabelecimento de direitos e deveres do cidadão e formas de procedimentalização de demandas[295].

A conclusão natural alcançada refere-se ao maior grau de sofisticação administrativa viabilizada pelos regimes regulatórios, em torno da interação entre público e privado. Qual o

---

[292] BRUNSSON, Nils; JACOBSSON, Bengt. *A World of Standards*. Oxford/New York: Oxford University Press, 2000.
[293] DELMAS-MARTY, Mireille. *Por um direito comum*. São Paulo: Martins Fontes, 2004.p.211.
[294] É nesse sentido que se torna viável a comparação com a constitucionalização da internet.
[295] SZINVELSKI, Mártin; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo na era digital. *Revista dos Tribunais*, v. 1020, p.143-162, out., 2020.

papel desses diferentes atores no processo de estandardização e verificação de padrões técnicos? A dinâmica que envolve o processo de certificação tem origem na acreditação de empresas de certificação pelas autoridades públicas responsáveis pela regulação. As empresas certificadoras, submetidas à regulamentação da ISO/IEC 17.021, passam a ser habilitadas a realizar inspeções em empresas privadas, interessadas na obtenção de selo de qualidade ou certificação. O resultado do processo de auditagem de processos no interior relaciona-se à confiabilidade direcionada ao usuário/cidadão que a gestão de processos internos encontra-se em conformidade com os padrões técnicos.

Em vista da contextualização, no campo da proteção de dados, a implementação dos selos apresenta-se como forma de estabelecer a internalização de comportamentos empresariais pautados na proteção de dados e de afirmação de uma *common law constitution* em matéria de proteção de dados, entendida como o processo reiterado de afirmação de direitos fundamentais por atores transnacionais[296]. Mesmo que se sugira um cosmopolistismo elaborado[297], a tarefa não é de simples resolução, em razão das impossibilidades universalistas de origem de vontade política. A implementação de selos de qualidade propõe-se a resolver dois tipos de problemas *(a)* a quantificação e redução do risco de violação de dados e *(b)* da geração de confiança organização/cidadão e incremento da reputação corporativa[298].

Os padrões previstos na norma técnica ISO/IEC 27001 e na ISO/IEC 29100 servem de parâmetro para as autoridades que realizam auditorias e certificações por selos. Nos Estados Unidos, o *Entertainment Software Rating Board (ESRB) Privacy Certified* e o *TRUST e Privacy Certification* podem ser elencados como programas de certificação por selo que atestam a conformidade das rotinas no interior das organizações com as regulações globais e permitem compartilhar, em razão da posição privilegiada da indústria tecnológica norte-americana, as melhores práticas em matéria de proteção de dados. No âmbito europeu, o *EuroPriSe* é selo que atesta aos usuários que seus dados pessoais são tratados de acordo com a regulação europeia de proteção de dados, de forma a garantir a transparência dos processos e base legal para o processamento de dados pessoais sensíveis e pessoais, em consonância

[296] Para Teubner "[...] essa fórmula descreve exatamente o processo mediante o qual direitos fundamentais são positivados nos regimes transnacionais públicos e privados em um processo decisório reiterado, o qual tem lugar entre as decisões dos tribunais arbitrais, dos tribunais nacionais, dos contratos entre atores privados, da normatização social e das ações de escandalização de movimentos de protesto e ONGs". TEUBNER, Gunther. *Fragmentos Constitucionais*: constitucionalismo social na globalização. São Paulo: Saraiva, 2016. p.236.
[297] SALDANHA, Jânia Maria Lopes. *Cosmopolitismo jurídico*: teorias e práticas de um direito emergente entre a globalização e mundialização. Porto Alegre: Livraria do Advogado, 2018.
[298] SZINVELSKI, Mártin; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo na era digital. *Revista dos Tribunais*, v. 1020, p.155, out., 2020.

com princípios diretores e deveres previstos no Regulamento Europeu. No Canadá, o *Privacy by Design Certification* e *CPA WebTrust* apresentam-se como os principais instrumentos certificadores por selos em matéria de proteção de dados. Observa-se, nesse sentido, que a certificação de conformidade, e a posterior emissão de selo, é relevante para as organizações no âmbito da geração de confiança[299].

No caso brasileiro, a LGPD estabelece como impositivos: *(a)* o reconhecimento por parte da autoridade nacional de proteção de dados do programa de certificação por selo e *(b)* a validade internacional do selo ou do destino da transmissão de informações[300]. Em termos pragmáticos, do ponto de vista no setor de tecnologia nacional, em nada adianta seguir roteiros de auditoria de empresas certificadoras nacionais sem que exista o reconhecimento internacional ou regional (como no caso da União Europeia) da validade daquele selo.

A questão a ser discutida refere-se ao campo de extensão ou de dependência de empresas de certificação ou de auditorias (no caso específico das multinacionais) nos procedimentos de geração de confiança. Por um lado, se é verdade que as empresas consolidadas no mercado internacional conseguem atrair profissionais com grande qualidade de auditagem para a verificação de processos específicos (nos ramos de engenharia, materiais de diferentes gêneros, procedimentos de gestão processual até os sistemas informatizados); por outro, a concentração de "micropoderes" a esses atores privados, os fortalece como limitadores de oportunidades econômicas e viabilizadores de projetos socioeconômicos já estruturados, como das grandes corporações de engenharia de produtos, mineração, tecnologia da informação e da indústria farmacêutica e química. A advertência feita conduz–nos à relevância de se pensar e observar os efeitos sistêmicos provocados pelo avanço tecnológico, da necessidade de velocidade na validação de procedimentos e dos efeitos socioeconômicos da globalização econômica que marca os atuais modelos de negócio em rede e de forma globalizada[301].

Avançando-se na discussão, chega-se à conclusão de que serão as empresas certificadoras dos grandes centros econômicos que irão certificar a qualidade das rotinas adotadas por empresas nacionais no tratamento de dados de cidadãos europeus, americanos e

---

[299] RODRIGUES, Rowena; PAPAKONSTANTINOU, Vagelis (Org.). *Privacy and Data Protection Seals*. Springer, Information Technology and Law Series, v. 28, 2018.

[300] BRASIL. *Lei n.º 13.709*. 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 10 abril 2020.

[301] SZINVELSKI, Mártin; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo na era digital. *Revista dos Tribunais*, v. 1020, p.156-157, out., 2020.

brasileiros, por exemplo. O Regulamento Europeu, conforme dito anteriormente, representa um importante marco de transformação da proteção de dados, em razão de ser um instrumento vinculante que obriga os estados-nacionais e atores privados a comportarem-se de forma a resguardar os dados pessoais de usuários de plataformas e de serviços governamentais. Assumindo essa característica, os países e as empresas baseadas na Comunidade Europeia, multinacionais ou não, devem adotar políticas privadas de gestão da informação. Justamente, por isso, que a perspectiva da adoção da certificação por selos de qualidade torna-se o instrumento de verificação das rotinas de cuidados dos dados pessoais empregados nas organizações.

Por outro lado, a opção de verificação da qualidade no tratamento de dados tende a ocorrer por uma relação natural de proximidade baseada no centro empresarial ou produtivo, vale dizer: empresas europeias ou multinacionais adotarão selos de qualidade baseados na União Europeia e auditados por empresas europeias/multinacionais, porque essas já possuem afinidade com a cultura e as experiências anteriores de regulação em proteção de dados, como são as regulamentações anteriores da Diretiva n. 95/46 e o Convênio Europeu 108. A relação centro/periferia é marcada, nesse sentido, pelo fluxo transfronteiriço de dados informáticos. Empresas de outras nações deverão, para estabelecer relações do tipo econômicas, adotar selos de qualidade do padrão europeu. Nesse sentido, relevante descobrir o grau de possibilidade de uma empresa de certificação ou de auditoria não europeia "certificar" ou conferir um selo de qualidade, conforme a regulação europeia, a empresas nacionais sem estar baseada em solo europeu.

A tendência identificada é que somente empresas europeias ou transnacionais de certificação possam atestar, com credibilidade internacional, que empresas de outros países realizem operações de fluxo de dados transnacionais com relação direta com os países pertencentes à União Europeia. A opção que restaria às organizações empresariais sediadas no Brasil, por exemplo, dependerá da atuação da Autoridade de Proteção de Dados (órgão de acreditação de empresas certificadoras), que poderá estabelecer convênios com outras autoridades nacionais de proteção de dados, especialmente as europeias ou multinacionais, que implique no mútuo reconhecimento de certificados e selos ou o estabelecimento de equivalências de níveis de proteção baseadas em selos de qualidade. A solução em questão se apresentaria como um mecanismo de interconexão entre órgãos públicos responsáveis pela regulação/fiscalização estatal da forma como os dados são tratados e ilustraria a nova forma de interação entre público e privado, em articulação conjunta em matéria em torno da

proteção de direitos, com as ressalvas relativas aos efeitos sistêmicos associados à concentração de mercado e de "micropoderes" limitativos do desenvolvimento econômico e tecnológico de empresas sediadas em países que buscam uma posição de dignidade no cenário global[302].

O alto grau de tecnicidade das questões regulatórias e o papel crucial dos especialistas na sociedade contemporânea contribui para o fenômeno dos *standards* e dos padrões comportamentais que desempenham um papel decisivo na proteção de direitos, representando, de igual forma, um desafio às teorias regulatórias. Os selos de proteção em matéria de proteção de dados representam uma pequena parcela no panorama regulatório que se forma. A autorregulação regulada oferece maior flexibilidade ao permitir que soluções para casos específicos sejam encontradas pelos próprios atores, além de permitir a adaptação rápida às futuras mudanças tecnológicas.

Os efeitos negativos vinculam-se à possibilidade de monopolização do mercado de auditorias e de concessão de selos, uma vez que o reconhecimento por parte da autoridade nacional de proteção de dados do programa de certificação por selo deverá levar em conta a validade internacional do selo ou do destino da transmissão de informações, o que tenderia privilegiar empresas multinacionais. No entanto, trata-se de um efeito natural de uma sociedade global, marcada pela transnacionalização ou internacionalização.

O debate que cerca a proteção de dados pessoais e a adoção de selos de qualidade em matéria de proteção revela uma noção de participação ou de ajuste entre o público e o privado. A *dataveillance,* ou vigilância cibernética, fomenta a busca por instrumentos que assegurem a ciberseguridade ou à proteção de informações conectadas à individualidade, não são apenas de instrumentos do *hard law* e do cumprimento ostensivo por parte de operadores que tratam informações pessoais. A adoção de rotinas de verificação de procedimentos adotados por atores públicos e privados, com é a certificação por selos, modifica o cenário de atuação empresarial e estatal, caso sejam adotadas. A internacionalização de direitos, como se verifica no caso da proteção de dados pessoais, revela a perspectiva da internacionalização dos instrumentos de proteção. Por esse motivo, sustenta-se que a atuação concatenada entre autoridades regulatórias em matéria de proteção de dados deve pautar-se pela uniformização de mecanismos que permitam ao consumidor/cidadão orientar sua atividade online com base na confiança de que as informações pessoais que disponibiliza estão sendo utilizadas

[302] SZINVELSKI, Mártin; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo na era digital. *Revista dos Tribunais*, v. 1020, p.157, out., 2020.

conforme padrões internacionalmente aceitos e que o fluxo de dados informáticos não está sendo utilizado com propósitos ilusórios ou de dominação. Por esse motivo, a adoção de padrões (*standards*) em termos de tutela do direito à proteção de dados reflete um ambiente técnico-jurídico que conecta tanto a atuação administrativa estatal como também a adoção de mecanismos privados de correção, a regulação especializada e a utilização consciente das ferramentas tecnológicas em benefício da humanidade, pautadas pela eticidade e a orientação humanizada da utilização das ferramentas (como selos em proteção de dados), com vistas à harmonização entre o progresso e a proteção de direitos.

5 CONSIDERAÇÕES FINAIS

O encerramento dessa dissertação passa pela *esperança* da resolução da pandemia global provocada pelo Sars-CoV-2 (*Covid-19*), que nos leva à citação do momento emergencial, não alheio ao processo desempenhado. Os efeitos foram variados, repercutindo em setores econômicos e sociopolíticos, não deixando de afetar temas conectados à proteção de dados e à estruturação da Autoridade de Proteção de Dados (ANPD) criada pela Lei Geral de Proteção de Dados. Tratou-se de um aprendizado humanitário, da seleção e identificação das virtudes humanas e de suas inúmeras falhas. O Direito Constitucional e Administrativo foram exigidos, dessa vez, pautados nas exceções ou emergências, de forma não vista até a consolidação de diferentes processos de redemocratização, aceleração econômica e incremento tecnológico que o mundo experimentou durante a segunda metade do século passado.

Sob a perspectiva regulatória, os cidadãos do mundo reconheceram, por meio de notícias e informações difundidas por meio tradicionais e alternativos que são marca da sociedade da informação, o papel fundamental desempenhado pelas agências reguladoras sanitárias no controle dos dados apresentados pelas fabricantes do setor biotecnológico e na aprovação das vacinas havidas como *ponto de virada* no combate à pandemia citada. Anotações críticas à suposta interferência política, ao excesso burocrático, à demora na homologação foram tecidas e advindas de diferentes setores; assim como, ao contrário, mostrou que a independência técnica é possível apesar dos excessos. Embora a conexão entre o ambiente epidemiológico e objetivo da pesquisa apresente-se como um universo distante, a situação emergencial sanitária deve ser observada como campo de aprendizado para o que está por vir em termos de estruturação e atuação da ANPD, em uma sociedade que se adaptou à necessidade de digitalizar-se para evitar a propagação do vírus e estabelecer mudanças em processos que não voltarão ao estágio anterior ao estado que nos encontramos. Essa conclusão é reforçada pela relevância dos dados, das revoluções periódicas e cada vez mais constantes da tecnologia da informação, da engenharia química ou física de ponta e das novas capacidades de sistemas baseados em algoritmos, os quais avivam robôs físicos ou virtuais. Mediar conflitos de um *momento digital* o qual se torna presente e futuramente projetado não alijará a atuação da Autoridade de Proteção de Dados, ainda mais em um país com enorme potencial humano, natural e econômico como o Brasil.

Sobre o tema da pandemia e da proteção de dados, verifica-se que o cerne da questão foi utilização dos dados pessoais colhidos por diferentes sistemas e aplicações. Contudo, é de se notar, inclusive, a aceitabilidade de exposição das pessoas às mídias sociais, compartilhando momentos, localizações, atividades privadas, conferindo permissões de utilização dos *cookies* e diferentes *scripts* em aplicações nos aparelhos para as *big techs* – os gigantes dos setores tecnológicos – e se revoltar contra a utilização de informações pelas entidades governamentais para a elaboração de uma estratégia pública de combate à pandemia. Sem adentrarmos às questões ideológicas, não se pode deixar de identificar um *duplo padrão* consistente em fornecer um conjunto de dados – com o consentimento informado ou não – às empresas transnacionais do setor privado e, ao mesmo tempo, crer em teorias conspiratórias de implantação do totalitarismo por meio do controle de dados por parte das organizações estatais, em um país cujo governo nunca foi tão fiscalizado e sujeito às críticas como o atual e os anteriores. Apesar do que vem ocorrendo, em termos institucionais, o Brasil não desmoronou, sugerindo – *contra communem sensum* – uma demonstração da fortaleza democrática do país, esta que é especial, brasileira e *sui generis*. Portanto, *confiança no Brasil*.

A pergunta a qual se buscou responder é a seguinte: em que medida a Unidade Reguladora e de Controle de Dados Pessoais (URCDP) apresenta traços que podem ser utilizados para a consolidação da Autoridade Nacional de Proteção de Dados (ANPD) brasileira, tendo em vista que o Uruguai é reconhecido pela Comissão Europeia como país que adota níveis adequados de proteção de dados? Apresentamos como *hipóteses* as seguintes propostas: em caso positivo, é possível identificar traços contributivos da URCDP que permitam a estruturação da ANPD técnica e capaz de promover níveis internacionais de proteção de dados. Cogitou-se, em caso negativo, que a ausência de independência das autoridades traz efeitos sociojurídicos que podem prejudicar a proteção de dados pessoais dos cidadãos, em termos de não existir um nível mínimo de proteção intencionalmente validado, especialmente tendo em vista a força do Regulamento Europeu de Proteção de Dados.

Como se viu, a reposta foi positiva, existindo pontos de apoio que podem auxiliar a estruturação da ANPD de forma a que se aproxime dos níveis internacionais, tarefa que, todavia, demandará tempo. A explicação da resposta encontra justificação na forma como o Uruguai estruturou institucionalmente a URCDP, integrante da AGESIC. Na face pregressa da escolha encontrou-se a linha de pensamento de que o conhecimento adquirido pelo *país-irmão*, durante mais de dez anos de existência do órgão regulador, marcado pela *forte*

institucionalidade pode ser utilizado, ao feitio cooperativo, como aprendizado para a rápida adequação às exigências mundiais atinentes autoridades de proteção de dados.

Nesse sentido, a linha traçada demanda explicações, haja vista que a tendência jurídico-doutrinária quase sempre foi buscar em comunidades e tradições com estágios organizacionais mais avançados – se isso é verdade – a solução para os problemas regulatórios vivenciados no Brasil, sem muito se importar com a realidade cultural brasileira e capacidade de adaptação eficiente ao modelo importado. Ao revés, esse quase sempre foi o quesito de sofisticação das abordagens e destacamento individual de pesquisadores. Observa-se, em uma visão cada vez mais aproximada da contemporânea, que o resultado da atuação administrativa deve ser social e constitucionalmente adequado. Em outras palavras, não se deve *importar soluções mágicas* se essas não ajustadas a colher o imediato fruto do resultado ou sem a existência de uma trajetória institucional assentada que leve à adequação posterior e à possível convergência de modelos, pautadas em interesses comuns de diferentes tradições jurídicas. Nelson Rodrigues, ao cunhar a expressão "complexo de vira-lata", em referência à derrota do Brasil para o Uruguai na Copa do Mundo de 1950, no Maracanã lotado, identificou algo que não se atém ao ambiente futebolístico sugerindo certa inferioridade ou baixa autoestima do brasileiro. A noção de pensamento de que aos modelos estrangeiros são mais sofisticados e suficientes aos produzidos no Brasil – que devem ser adquiridos e seguidos independentemente de ajustes contextuais – pode explicar, de forma não comprovada estatisticamente, a simples adesão doutrinária ao modelo das autoridades independentes europeias, sem perceber que os órgãos, autarquias e agências reguladoras brasileiras, ao longo dos anos republicanos, estiveram vinculados seja à estrutura seja à supervisão ministerial, ou diretamente ao Poder Executivo. A instituição desse modelo repercutiria em uma inovação no plano jurídico-administrativo do país, além de inexistir, no plano constitucional, autorização expressa ou tácita da adoção do modelo em questão. Portanto, entende-se que o *olhar como aprendizado* de modelos – e não como *simples cópia* – é mais coerente com a realidade própria do país.

O *olhar como aprendizado* para a URCDP e AGESIC esteve entre as diretrizes da proposta desenvolvida. A ANPD não possui personalidade própria e, de acordo com a LGPD, integra a Presidência da República. Assim a ANPD, não apresenta modelo dissociado das características de estruturação de outros setores. Ocorre, no Brasil e no Uruguai, a desconcentração administrativa, por meio da qual, no interior de uma mesma pessoa jurídica, se destaca um órgão para realizar as atividades administrativas. Mesmo que a legislação

específica disponha sobre a *natureza transitória* desse modelo, permitindo a transformação em autarquia especial, a contar de dois anos da posse dos Diretores e da entrada em vigor da estrutura regimental. Após a transformação em autarquia, integrará a administração indireta, seguindo a tradição das agências brasileiras que regulam setores diversos. Ainda assim, foram previstas competências e garantias à autoridade brasileira, que não se constituem em obstáculos ao desempenho da função de zelo e condução da política de proteção de dados no Brasil.

A constituição tardia da ANPD, sem dúvidas, prejudicou uma adequação célere ao regime proposto pelo RGPD, como forma de facilitar o acesso das empresas brasileiras a novos mercados. Inclusive, recentemente, houve a manifestação do interesse brasileiro em ingressar, como membro, na OCDE, como forma de obter uma vantagem competitiva no mercado europeu – o maior do mundo, o que sofreu críticas francesas, país que mais se prejudicaria com participação brasileira. Entre as exigências está o fomento ao governo digital, permitindo que os cidadãos acessem serviços públicos como maior comodidade. O ajuste às exigências de proteção de dados, por meio do reconhecimento da Comissão Europeia, e a compatibilidade com o nível adequado de proteção de dados se insere nesse rumo. O Uruguai, ainda que não integre a OCDE, aderiu à Convenção 108, após se submeter à Comissão o interesse em participar e conseguiu o reconhecimento europeu de compatibilidade com a antiga norma reguladora, a Diretiva 95/46. É nesse sentido que se torna oportuno observar as etapas traçadas tanto pela AGESIC como URCDP, na busca pela compatibilização.

A AGESIC apresenta-se como unidade executora, considerada *dependente* da Presidência da República, e é o órgão responsável por impulsionar a digitalização de serviços e propagação de conhecimentos da sociedade da informação aos uruguaios. Apesar disso, não é correto sustentar que se trata de um órgão de governo; ao revés, com mais de quinze anos de existência foi gerenciada por mais de uma coloração partidário-ideológica. Com exceção do Diretor-Executivo, indicado pelo Presidente, os membros diretivos possuem mandato, o qual pode ser renovado. Pode-se considerar, nessa linha de ideias, que existem mecanismos de *institucionalidade* e de proteção da continuidade da modernização administrativo rumo à administração digital. Nesse sentido, possui uma intensa produção normativa no sentido de promover o desenvolvimento digital.

A URCDP está inserida na estrutura da AGESIC, e também possui mecanismos de proteção à atuação por meio de mandatos e garantias de atuação técnica previstas na LPDP.

Existem mandatos fixos para os dois membros do conselho executivo, os quais possuem a prerrogativa de não se submeter a ingerências ou pressões exteriores. O estabelecimento de mandatos apresenta-se como uma garantia orgânica de atuação, similar, portanto, à inamovibilidade. Nesse sentido, há uma convergência legislativa, em razão de que a LGPD adota modelo semelhante, com a diferença apenas no número de diretores. O fato é que essa garantia é própria do modelo de agências, inclusive sendo adotado como um dos fatores de relevância na caracterização da independência de órgãos reguladores na experiência internacional. Sobre esse ponto, críticas foram produzidas à condução da ANPD, inclusive por meio de representações jornalísticas retratando, ou caricaturizando, um processo de militarização, a desconsiderar as especializações dos membros indicados e aprovados pelo Senado Federal, conforme o rito constitucional nos termos da alínea "f" do inciso III do art. 52, da Constituição. Com a publicação da Lei das Agências Reguladoras esse procedimento foi institucionalizado para todos os órgãos reguladores, garantido controle parlamentar das características e especialidades para o exercício do cargo dos membros ocupantes de cadeiras diretivas dos órgãos de regulação, que desempenham papeis similares aos que serão desempenhados pela ANPD.

Como se verificou, o exercício do poder de regulação não depende, de igual forma, do estabelecimento de personalidade jurídica própria ao órgão, ainda que esta seja recomendada. A análise da LGPD, bem como LPDP, indica que é possível o exercício da regulação e do exercício das funções administrativas de supervisão de forma adequada, mesmo que, do ponto de vista formal, exista integração à Presidência da República ou vinculação. A legislação, nesse sentido, alberga autonomia técnica e decisória ao órgão, de forma muito semelhante às regulamentações próprias das agências reguladoras brasileiras. Do ponto de vista normativo, inexistem amarras à atuação do ANPD. Do ponto de vista material, do desempenho de suas funções inerentes, os obstáculos ou facilidades de atuação ainda deverão ser provados. Nesse sentido, ausência da previsão normativa, resguardando total independência à ANPD deve ser vista com cautela, justo porque não pode servir de subterfúgio para o não cumprimento da legislação.

Nessa linha, nota-se que para a garantia da proteção de dados e do desenho das políticas públicas em relação à segurança da informação, não é suficiente, apenas, a repetição de princípios jurídicos ou mantras de respeito à constitucionalidade dos atos normativos. O conhecimento especializado, técnico e, por vezes, estranho à atuação profissional jurídica ou administrativa deve ser valorizada, como forma de garantir a eficácia dos meios empregados à

tutela preventiva e sancionadora de violações de direitos pessoais conectados à personalidade. Essa é uma perspectiva que foi adotada pelo Grupo de Trabalho do Artigo 29, no sentido que a mero paralelismo normativo não significa a adequação aos *standards* internacionais ou comunitários.

Ao contrário, a proposta de adequação do Uruguai, ainda sob a regulação da Diretiva 95/46 não foi verificada apenas pela leitura dos dispositivos legais presentes na LPDP. Primeiramente, o Uruguai manifestou interesse em adotar o Convênio 108. Após a aprovação pelo Conselho da Europa, o país-irmão necessitou comprovar a compatibilidade normativa, associada a garantias de que a interpretação dos conceitos previstos também estaria em conformidade com a perspectiva europeia e que, por isso, não poderia ampliá-la, para o caso de transferências internacionais. Nesse sentido, a URCDP fixou-se como órgão encarregado de garantir a contínua adequação das práticas no Uruguai com as práticas adotadas na Europa. Em outras palavras, o Uruguai passou a integrar ativamente o processo de compatibilização.

Nessa linha, a URCDP passou a integrar diferentes grupos de trabalho como é a *Global Privacy Assembly* que é o principal fórum mundial para autoridades de proteção de dados pessoais, permitindo que se forneça liderança internacional e a conexão entre mais 130 autoridades de proteção de dados do mundo. Não apenas ela, como também participa das Conferências Internacionais de Autoridades de Proteção de Dados e Privacidade (ICDPPC). Por fim, é membro ativo da Rede Ibero-americana de Proteção de Dados Pessoais, cujo papel foi fundamental na estruturação dos *Standards de Proteção de Dados*, que pretende uniformizar os princípios aplicáveis à proteção de dados em nível regional, já em consonância com a Resolução de Madrid estabeleceu os padrões internacionais. Trata-se, portanto, de uma vantagem uruguaia e de uma oportunidade de maior aproximação com a rede de colaboração que o Brasil deve observar.

O RGPD, conforme visto, provocou uma importante aceleração em termos de ajustes nacionais em busca da rápida conformidade. Nesse sentido, logo após a vigência da normativa europeia, o Uruguai adicionou à LPDP as novidades incorporadas, inclusive regulamentando os requisitos para que as organizações públicas e privadas se adequassem. Nesse sentido, delimitou as competências do delegado de proteção de dados, estabeleceu quem deveria realizar o estudo de impacto e a documentação a ser apresentada, bem como casos de comunicação de vazamento e do estabelecimento normativo das noções de privacidade desde o desenho da tecnologia e por defeito. A pronta adequação indica, ao menos, o interesse do país em manter-se “adequado” em termos de reconhecimento pelo bloco comunitário, mesmo

que não haja um conceito preciso sobre a adequação, tanto na doutrina quanto na jurisprudência europeia. Sugere que o caminho de adequação está na aproximação entre as tutelas normativas da origem quanto do destino.

Para que determinado país se mostre adequado, nesse sentido deve haver uma forte atuação do órgão de controle em termos de normatização ou de indicação de medidas a serem implementadas. Em outras palavras, não basta a reprodução de princípios e diretrizes. A necessidade de se objetivar as formas de proteção de dados mostra-se relevante, como a anonimização e a pseudoanonimização dos dados dos usuários. Todavia, não basta que a organização pública ou privada exponha que utiliza as técnicas nominadas. Nesse sentido, a URCDP possui um guia de atuação e de procedimentos que tendem auxiliar na correta adoção dos procedimentos, no exercício da função normativa, por meio da aprovação de resolução. Além de ocorrer a publicidade dos mecanismos de proteção efetiva dos usuários, o documento permite que o órgão controlador, futuramente, confira a adequação aos procedimentos adotados. É recomendável que a ANPD estabeleça os parâmetros para evitar a identificação posterior do titular dos dados que utiliza serviços digitais, aproximando o órgão regulador com a prática de proteção de dados em diferentes setores.

Outra ferramenta que pode ser ampliada na esfera de atuação prática da proteção de dados é a adoção de selos de qualidade específicos, seguindo uma tendência europeia. Após a validação, pela ANPD ou URCDP, da entidade que auditará os processos e profissionais envolvidos na proteção de dados, diferentes setores poderão ser beneficiados com a certificação de que suas atividades seguem parâmetros reconhecidos, seja pelos *standards* regionais, como internacionais. Trata-se de uma vantagem que permite a pronta adequação dos procedimentos em empresas que necessitam acrescer credibilidade aos seus processos.

A proteção de dados no Brasil, de forma efetiva, como ocorre no Uruguai, por exemplo, demanda a consolidação dos processos de estruturação da ANPD, a qual corresponde a primeira fase do Plano Desenvolvido pela AGESIC e a URCDP. O processo de adaptação considerada as dificuldades pregressas à construção do progresso tecnocientífico, estas que podem assumir feições políticas, no interior e no exterior das instituições. Tratar da proteção de dados pessoais apresenta-se como consequência do desenvolvimento e especificação do direito à vida privada (privacidade), de modo a permitir que o titular de dados desempenhe o controle de suas informações em uma sociedade marcadamente associada à utilização de diferentes dispositivos, como também da vigilância dos dados. O cidadão deve ter o direito de controlar seus dados, especialmente quando sujeito ao perigo de

violação ou quando haja risco tolerado, que não poderia sê-lo; ao mesmo, é dever das organizações prever e evitar que os seres humanos se tornem uma jazida de dados a ser explorada, sem a supervisão. Por isso, a atuação da ANPD deve ser conduzida com passos firmes à fixação de mecanismos e parâmetros técnicos que influenciem diretamente na proteção de dados pessoais dos cidadãos, de forma que a legislação e os *standards* saiam dos respectivos documentos e assumam caráter de influência permanente na transformação de um ambiente de vazio normativo à quase-plenitude de mecanismos de proteção.

REFERÊNCIAS

ABCOMM. *Comércio eletrônico deve crescer 18% em 2020 e movimentar R$ 106 bilhões*. Disponível em: <https://abcomm.org/noticias/comercio-eletronico-deve-crescer-18-em-2020-e-movimentar-r-106-bilhoes/> Acesso em 2 dez. 2020.

AFFONSO, Elaine Parra; SANT'ANA, Ricardo César Gonçalves. Preservação da privacidade no acesso a dados por meio do modelo k-anonimato. *Ponto de Acesso*, v. 11, n. 1, p. 20-41, 2017.

ALMAGRO, Ricarlos. Agências reguladoras independentes e legitimidade democrática. *De jure*: revista jurídica do Ministério Público do Estado de Minas Gerais, n. 9, p. 67–84, jul./dez., 2007.

AMATO, Guilio. Autorità semi-indipendenti e autorità di garanzia. *Rivista trimestrale di diritto pubblico*, v.47, n.3, p.645-664,1997.

ANCEL, Marc. *Utilidade e Métodos do Direito Comparado*. Tradução de Sérgio José Porto. Porto Alegre: Sérgio Antonio Fabris, 1980.

ANGARITA, Nelson Remolina. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law*: Revista Colombiana de Derecho Internacional, v. 8, n. 16, p. 490-523 2010.

APEC. APEC cross-border privacy rules system: policies, rules and guidelines. Disponível em: <https://www.apec.org/groups/committee-on-trade-and-investment/~/media/files/groups/ecsg/cbpr/cbpr-policiesrulesguidelines.ashx>. Acesso em: 14 nov. 2020.

ARAGÃO, Alexandre Santos de. Agências reguladoras e agências executivas. *Revista de Direito Administrativo*, v. 228, p. 105-122, 2002.

ARAGÃO, Alexandre Santos de. As agências reguladoras independentes: algumas desmistificações à luz do direito comparado. *Revista de Informação Legislativa*, n.155, p.293-317, jul-set., 2002.

ARAGÃO, Alexandre Santos de. O poder normativo das agências reguladoras independentes e o Estado Democrático de Direito. *Revista de Informação Legislativa*, n. 148, p.275-299, out./dez., 2000.

ARAGÃO, Alexandre Santos de. Supervisão ministerial das agências reguladoras: limites, possibilidades e o parecer AGU nº AC - 51. *Revista de Direito Administrativo*, v. 245, p. 237-262, 2007.

ARAÚJO, Alexandra Maria Rodrigues. As Transferências Transatlânticas de Dados Pessoais: O Nível de Proteção Adequado Depois de Schrems. *Revista Direitos Humanos e Democracia*, Editora Unijuí, n. 9, p.201-236, jan./jun 2017.

AVELLARDUARTE. Internet no Brasil 2020 (estatísticas). Disponível em: https://www.avellareduarte.com.br/internet-no-brasil-2020estatisticas/ . Acesso em 14 jan. 2021.

BADIN, Luiz Armando. As autoridades administrativas independentes na França: finalidades institucionais e meios de atuação. In: DI PIETRO, Maria Sylvia Zanella. (Org.). Direito regulatório: temas polêmicos. Belo Horizonte: Ed. Fórum, 2003, p. 491-508.

Banco Iberoamericano de Desenvovimento (BID). *Nota Técnica. AGESIC, um modelo exitoso*. Disponível em: <https://www.alejandrobarros.com/wp-content/uploads/2016/04/Nota_Tecnica_-_Agesic.pdf> . Acesso em 28 nov.2020.

BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, v. 273, p. 123-163, 2016.

BARBOSA, Joaquim. Agências reguladoras: a metamorfose do estado e da democracia (uma reflexão de direito constitucional e comparado). *Doutrinas Essenciais de Direito Administrativo*, vol. 6, 2012. p. 943-984.

BENNETT, Colin J. The European General Data Protection Regulation: An instrument for the globalization of privacy standards?. *Information Polity*, v. 23, n. 2, p. 239-246, 2018.

BERTONI, Eduardo. Convention 108 and the GDPR: Trends and perspectives in Latin America. *Computer Law & Security Review*, p.1-5, nov., 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105516. Acesso em 29 jan.2021.

BILAC, Olavo. *A defesa nacional (discursos)*. Rio de Janeiro: Liga da Defesa Nacional, 1917.

BIONI, Bruno Ricardo; LIMA, Cíntia Rosa Pereira de. *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*. 2016.Universidade de São Paulo, São Paulo, 2016.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*, São Paulo, n, 53, p. 191-201, jan-mar, 2020.

BRASIL. *Constituição da República Federativa do Brasil*. Disponível em:< http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 14 nov.2020.

BRASIL. Decreto 10.474, de 26 de agosto de 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226> . Acesso em 1 set. 2020.

BRASIL. Guia de Boas Práticas para Implementação na Administração Pública Federal. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf>. Acesso em: 16 out. 2020.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2020.

BRASIL. *Lei nº 13.848, de 25 de junho de 2019*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13848.htm>. Acesso em: 29 nov. 2020.

BRASIL. *Sociedade da informação no Brasil*: livro verde – organizado por Tadao Takahashi. Brasília: Ministério da Ciência e Tecnologia, 2000.

BRAUSE-BERRETA, Alberto. La situación en Uruguay sobre protección de datos personales. PIÑAR-MAÑAS, José Luis. *Protección de datos de carácter personal en Iberoamérica*, Valencia: Tirant Lo Blanch, 2005. p. 337-342.

BRUNSSON, Nils; JACOBSSON, Bengt. *A World of Standards*. Oxford/New York: Oxford University Press, 2000.

BRUSEKE, Franz Josef. Risco e contingência.*Revista Brasileira de Ciências Sociais*, São Paulo, v. 22, n. 63, p. 69-80, Feb., 2007 .

BUFFON, Marciano. ¿La economía del conocimiento reduce la desigualdad de renta y riqueza? In: BRAVO, Alvaro S. (editor). *Derecho, Inteligencia Artificial y Nuevos Entornos Digitales*. Sevilla, 2020.

BUTTARELLI, Giovanni. *The transfer of personal data to third countries and international organisations by EU institutions and bodies*. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/16-04-19_mit_ethics1_en_0.pdf> Acesso em: 1 dez. 2020.

CADWALLARD, Carole; GRAHAM-HARRISON, Emma. Revealed**:** 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. [S.L.]. 27 de mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 25 dez. 2020.

CALÉS, Rosario Duaso. Los principios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.295-320.

CAMARA DOS DEPUTADOS. Parecer Técnico encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp>. Acesso em 10 out. 2020.

CARDONA, Maria Celeste. *Contributo para o conceito e a natureza das entidades administrativas independentes: autoridades reguladoras*. Coimbra: Almedina, 2017.

CASAMAYOU, Adriana. *Las nuevas tecnologías:¿son para todos?*. 2016. Disponível em: < http://repositorio.mides.gub.uy:8080/xmlui/bitstream/handle/123456789/623/640_Casamayou%2C%20Las%20nuevas%20tecnolog%C3%ADas%2C%20son%20para%20todos.pdf?sequence=1&isAllowed=y.>. Acesso em 21 nov. 2020.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura:* sociedade em rede. 1 vol. São Paulo: Paz e Terra, 2011.

CASTELLS, Manuel. *A Galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. *Comunicación y poder*. Ciudad de México: Siglo XXI, 2012.

CATE, Fred, MAYER-SCHÖNBERGER, Victor. Notice and Consent in a World of Big Data. *International Data Privacy Law*, v.3, n.2, p.67-73, 2013.
CENTRE FOR INFORMATION POLICY LEADERSHIP: Cross-Border Data Transfer Mechanisms [Mecanismos de Transferencia Transfronteriza de Datos], agosto de 2015. Disponível em: < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf> Acesso em: 25 nov. 2020.

CERDA SILVA, Alberto. El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de derecho* (Valparaíso), n. 36, p. 327-356, 2011.

CERQUEIRA, Gustavo. Comparação jurídica e ideias de modernização do direito no início do Século XXI. *Revista de Direito Internacional*, Brasília, v. 17, n. 1, p. 7-23, 2020.

CISCO. Cisco data privacy benchmark study infographic. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-infographic.pdf. Acesso: 23 nov.2020.

CLUTCH. Top Latin America App Development Companies. Disponível em: < https://clutch.co/app-developers/latin-america/leaders-matrix>. Acesso em 10 dez.2020.

COMISSÃO Europeia. Adequacy of the protection of personal data in non-EU countries. How the EU determines if a non-EU has an adequate level of protection. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 21 out. 2020.

COMISSÃO EUROPEIA. Decisão de execução da Comissão de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 215 de 25.8.2000, p. 1. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32012D0484 Acesso em 14 nov.2020.

CONSELHO DA EUROPA. *Convênio Europeu de Direitos Humanos (CEDH*). Disponível em: < https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso 4 nov. 2020.

CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic rocessing of Personal Data (ETS No. 108) - Request by Uruguay to be invited to accede Item to be considered by the GR-J at its meeting on 30 June 2011. Disponível em:

<https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cce94>.Acesso em 14 nov. 2020.

CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y proceso de reforma sobre protección de datos en la unión europea. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016.

CORY, Nigel. *Cross-border data flows: where are the barriers, and what do they cost?*. Information Technology and Innovation Foundation,2017. Disponível em: < https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>. Acesso em 11 nov.2020.

CRAVO, Daniela Copetti; JOELSONS, Marcela. A importância do CDC no tratamento de dados pessoais de consumidores no contexto de pandemia e de *vacatio legis* da LGPD. Revista de Direito do Consumidor, vol. 131, p. 111-145, set-out, 2020.

CUNHA, Bruno Queiroz. Antagonismo, modernismo e inércia: a política regulatória brasileira em três atos. Cadernos EBAPE.BR, v.14, [s.n.], p.477, jul., 2016.

DELMAS-MARTY, Mireille. *Por um direito comum*. São Paulo: Martins Fontes, 2004.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, n.2, 2011.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. ed. São Paulo: Thompson Reuters, 2019.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Victor Rozatti (Org.). Direito Digital: direito privado e internet. São Paulo: Foco, 2019.

ENGELMANN, Wilson; SZINVELSKI, Mártin M.. Risco cibernético no tratamento de dados pessoais e autodeterminação informativa: reflexões à luz da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). In: Dóris Ghilardi; Liz Beatriz Sass. (Org.). *Temas Atuais de Direito Privado e Sociedade da Informação*: o direito na era digital. 1ed.Florianópolis: Habitus, 2020, p. 95-114.

EVERSON, Michelle. Independent agencies: hierarchy beaters?. *European Law Journal*, v. 1, n. 2, p. 180-204, 1995.

FENWICK, Mark; KAAL, Wulf; VERMEULEN, Erik P.M. Regulation Tomorrow: What Happens When Technology Is Faster than the Law?, *American University Business Law Review*, v. 6, n. 3, p.561-594, 2017.

FERNÁNDEZ ROJAS, Gabriel. Las administraciones independientes de regulación y supervisión en españa. *Vniversitas*, [S. l.], v. 54, n. 109, p. 419-460, 2005. Disponível em: https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/14710. Acesso em: 19 dez. 2020.

FISHER-LESCANO, Andreas; TEUBNER, Gunther. Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law. Michigan Journal of International Law, v.25, p.999-1045, 2004.

FLORIDI, Luciano. Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage, *Philos. Technol.* n.31, p.163–167, 2018.

FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? *Philosophical Transactions of the Royal Society*, v. 374, n. 2083, 2016. Disponível em: <https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360>. Acesso em 14 dez. 2020.

FONSECA CARVALHO, João Pedro Antunes Lima da. A natureza jurídica da autoridade nacional de proteção de dados à luz da teoria do estado regulador: há espaço para a adoção do conceito material de descentralização administrativa no brasil? *Revista De Direito, Estado e Telecomunicações*, vol. 12, n. 2, 118-130, 2020.

FRANCHINI, Claudio. Autonomia e independenza nell'amministrazione europea. *Diritto amministrativo*, v.16, n.1, p. 87-102, 2008.

FRANCHINI, Claudio. Mito e realtà delle autorità indipendenti. *Impresa e Stato*, n. 35, p. 34-[xx], 1996.

FRYDMAN, Benoit. *O fim do Estado de Direito*. Porto Alegre: Livraria do Advogado, 2016.

GARCÍA COSTA, Francisco Manuel. La independencia de las autoridades administrativas garantes del derecho de acceso a la información pública. Disponível em: <http://laadministracionaldia.inap.es/noticia.asp?id=1510342>. Acesso em 15 de dez. 2020.

GIUZIO, Graciela. Video-vigilancia: La jurisprudencia de la unidad reguladora y de control de datos personales (AGESIC). *Derecho Laboral*. Revista de doctrina, jurisprudencia e informaciones sociales, v. 56, n. 250, p. 355-368, 2013.

GOMES, Rodrigo Dias de Pinho. *Big data: desafios à tutela da pessoa humana na sociedade da informação*. Rio de Janeiro: Lumen Juris, 2017.

GROENLEER, Martijn. *The autonomy of European Union agencies*: A comparative study of institutional development. Eburon Uitgeverij BV, 2009.

GSMA. Flujos transfronterizos de datos. Materializando los beneficios y eliminando las barreras. Disponível em: < https://www.gsma.com/latinamerica/wp-content/uploads/2019/07/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_SPANISH-2.pdf.>. Acesso em 1 jan.2021.

GUERRA, Sérgio. Agências reguladoras e supervisão ministerial. In: ARAGÃO, Alexandre Santos de (Org.). Poder Normativo das Agências Reguladoras. Rio de Janeiro: Ed. Forense, 2006.

GUERRA, Sérgio; SALINAS, Natacha. O Congresso Nacional e a frágil autonomia das agências reguladoras. *Conjuntura Econômica (Rio De Janeiro)*, v. 74, p. 26-28, 2020.

GUERRA, Sérgio; SALINAS, Natacha; GOMES, Lucas As agências reguladoras em resposta à crise da COVID-19. *Revista de Administração Pública (Impresso)*, v. 54, p. 874-897, 2020.

GUIA para Técnicas Básicas de Anonimização de Dados do Gabinete para a Protecção de Dados Pessoais (GPDP) do Governo Governo da Região Administrativa Especial de Macau. Disponível em: <https://www.gpdp.gov.mo/uploadfile/2019/0417/20190417033911965.pdf>.Acesso em 16 dez. 2020.

GUIDI, Guilherme Berti de Campos. *Modelos regulatórios para proteção de dados pessoais*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2017. Disponível em: < https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 20 out. 2020.

HAN, Byung-Chul. *Sociedad de la Transparencia. Barcelona:* Herder, 2013.

HANS, Rosling. *Factfullne*ss: o hábito libertador de só ter opiniões baseados em fatos. 4ed. São Paulo: Record, 2020.

INSTITUTO TECNOLOGIA E SOCIEDADE. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Disponível em: < https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acesso em 1 dez. 2020.

INTERNACIONAL STANDARDS ON THE PROTECTION OF PERSONAL DATA AND PRIVACY. Resolução de Madrid. <http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf>. acesso em: 4 dez. 2020.

LA SPINA, Antonio. *Lo Stato Regolatore*. Bolonha: Il Mulino, 2000.

LACHAUD, Eric. The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument. *Computer Law & Security Review*, v. 34, n. 2, April 2018, p. 244-256. Disponível em: <https://doi.org/10.1016/j.clsr.2017.09.002>. 6 de abril de 2020.

LACHAUD, Eric. What GDPR tells about certification. *Computer Law & Security Review*, p.2-3, nov., 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105457. Acesso em 29 jan.2021.

LAITA, Inagcio. Independencia y régimen jurídico de la agencia española de protección de datos. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás (Org.). *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009. p.217-226.

LASH, Scott. *Critique of information*. Londres: Sage Publications, 2002.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999.

LIMA, Cíntia Rosa Pereira de. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados*: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n.

12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

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

LIMBERGER, Têmis. *Cibertransparência*: informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado Editora, 2016.

LIMBERGER, Têmis. Informação em rede: uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. In: MAGALHÃES MARTINS, Guilherme; LONGHI, João Victor Rozatti (Org.). Direito Digital: direito privado e internet. São Paulo: Foco, 2019. p.253-266.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado Editora, 2007.

LOHNER, Wolfrang. Tecnología de la información. Su impacto social y efectos legislativos. Algunas consideraciones. *Informática y Direito*: Revista iberoamericana de derecho informático, s.l., n.5, p.1427, 1994.

LOMBARTE, Antonio. De la libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, n.100, p.639-669, sep.-dez, 2017.

LOMBARTE, Artemi Rallo. Del derecho a la protección de datos a la garantía de nuevos derechos digitales. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.23-52.
LOMBARTE, Artemi Rallo. Las administraciones independientes: una aproximación constitucional. CHULVI, Cristina Pauner, MALLÉN, Beatriz Tomás (Org.). *Las Administraciones independientes*. Madrid: Tirant lo Blanch, 2009.p.11-20.

LÓPEZ, Manuel Valín. Las autoridades autonómicas de protección de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019.p.521-549.

LUCCA, Newton; LIMA, Cíntia Rosa P. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: Cíntia Rosa Pereira de Lima. (Org.). *Comentários à Lei Geral de Proteção de Dados*. 1ed.São Paulo: Almedina, 2020. p. 373-397.

MACHADO, Diego; DANILO, Doneda. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Caderno Especial - A Regulação da Criptografia no Direito Brasileiro*, vol. 1, p. 99-128, 2018.

MAGRANI, Eduardo. *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. 2. ed., Porto Alegre: Arquipélago Editorial, 2019.

MAJONE, Giandomenico. Do Estado positivo ao Estado regulador: causas e conseqüências de mudanças no modo de governança. *Revista do Serviço Público*, v. 50, n. 1, p. 5-36, 1999

MANTELERO, Alessandro. The future of data protection: gold standard vs. global standard. *Computer Law & Security Review*, p.1-5, nov., 2020. https://doi.org/10.1016/j.clsr.2020.105500. Acesso em 29 jan. 2021.

MAQUEO RAMÍREZ, María Solange; MORENO GONZÁLEZ, Jimena; RECIO GAYO, Miguel. Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho*, v. 30, n. 1, p. 77-96, 2017.

MAQUEO RAMÍREZ, María Solange; MORENO GONZÁLEZ, Jimena; RECIO GAYO, Miguel. Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho*, v. 30, n. 1, p. 77-96, 2017.

MARQUES NETO, Floriano Peixoto de Azevedo. As Agências Reguladoras Independentes e seu Enquadramento Legal: A Importância de Uma Lei Quadro. *Revista de Direito de Informática e Telecomunicações*, v. 1, p. 41-58, 2006.

MARR, Bernanrd. 20 fatos sobre a internet que você (provavelmente) não sabe. 1 out. 2015. https://forbes.com.br/fotos/2015/10/20-fatos-sobre-a-internet-que-voce-provavelmente-nao-sabe/#foto11. Acesso em 20 set. 2020.

MAYER-SCHONBERGER, V.; CUKIER, K. *Big data: a revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt: New York, 2013.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution that will transform how we live, work, and think. New York: Houghton Mifflin Harcourt, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555-587, nov-dez, 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*, vol. 1009, p. 173-222, nov, 2019.

MONSÁLEZ, Carlos Reusser. O que és la sociedade en red? In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.1231-1235.

MOREIRA, Egon Bockmann; CAGGIANO, Heloisa Conrado. O poder normativo das agências reguladoras na jurisprudência do STF - Mutação constitucional do princípio da legalidade? *Revista de Direito Público da Economia - RDPE*, Belo Horizonte, ano 11, n. 43, jul./set. 2013. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4222896/mod_resource/content/1/moreira%2C%20egon%20bockmann%3B%20caggiano%2C%20heloisa%20conrado%20-%20o%20poder%20normativo%20das%20ag%C3%AAncias%20....pdf>. Acesso 23 nov.2020.

MORENO, José. The economic value of information in the network society. *Observatorio*, Lisboa, v. 9, n. 2, p. 1-28, jun., 2015.

MOSCA, Javier Berdaguer. La imagen como dato personal.*Doctrina y jurisprudencia de derecho civil*, n. 6, p. 31-40, 2018.

NAHABETIÁN BRUNET, Laura. Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*, n. 39, p. 199-225, 2015.

NAVARRETE, Jesús Rubí. La agencia española de protección de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.491-520.

NOUGRÈRES, Ana Brian. El sistema legal uruguayo de protección de datos personales. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, n. 3, p. 1-30, 2007.

NORA, Simon; MINC, Alain. *A informatização da sociedade*. Rio de Janeiro: FGV, 1980.

OCDE. Exploring the economics of personal data: a survey of methodologies for measuring monetary value. *OECD Digital Economy Papers*, n. 220, OECD Publishing, Paris. Disponível em: <http://dx.doi.org/10.1787/5k486qtxldmq-en>. Acesso 25 nov.2020.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, n. 57, p. 1701-1777, 2010.

OLIVEIRA, Anderson; Haase, Lucas. Ordem econômica nacional: análise sobre as agências reguladoras brasileiras e a teoria da captura do interesse coletivo pelo interesse individual. *Revista de Direito do Consumidor*, v. 128, p. 101-116, mar-abr, 2020.

OLIVETTI, Miguel. Tensiones discursivas sobre la sociedad de la información, el caso de AGESIC Uruguay. *Políticas de Comunicación e Integración Económica Intercontinental*, p. 37-44, 2018.

OSÓRIO, Fábio Medina. *Direito Administrativo Sancionador*. 7.ed. São Paulo: Revista dos Tribunais, 2020

PAVÓN PÉREZ, Juan Antonio. La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, n.19-20, p.235-252, 2002. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/831270.pdf>. Acesso em 13 nov.2020.

PEIXOTO, Erick Lucena Santos; EHRHARDT JÚNIOR, Marcos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. EHRHARDT JÚNIOR, Marcos, LOBO, Fabíola Albuquerque (Org.). *Privacidade e sua compreensão no direito brasileiro*. Belo Horizonte: Fórum, 2019. p.33-54.

PÉREZ LUÑO, A.. Internet y los derechos humanos. *Anuario de Derechos Humanos*. Nueva Época, Norteamérica, n. 12, p.287-330, dic. 2011. Disponible en: <https://revistas.ucm.es/index.php/ANDH/article/view/38107/36859>. Acesso em: 23 out. 2020.

PÉREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. *Revista Brasileira de Políticas Pública,* Brasília, DF, v.4, n.2, p.8-46, 2014.

PÉREZ-LUNO, Antonio Enrique. Inteligencia artificial y posthumanismo. In: BRAVO, Alvaro S. (editor). *Derecho, Inteligencia Artificial y Nuevos Entornos Digitales*. Sevilla, 2020. p.9-22.

PETRLIC, Ronald. The General Data Protection Regulation: From a Data Protection Authority's (Technical) Perspective. *IEEE Security & Privacy*, vol. 17, no. 6, p. 31-36, nov-dec., 2019.

PIÑAR MAÑAS, José Luis. Administración electrónica y protección de datos personales, *Revista Jurídica da Universidade de Santiago de Compostela*, Santiago de Compostela, n.1, p.145-175, 2011.

PIÑAR MAÑAS, José Luis. Introducción. Hacia un nuevo modelo europeo de protección de datos. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016. p.15-22.

PIÑAR MAÑAS, José Luis. Sociedad, innovación y privacidad. *Información Comercial Española*, ICE: Revista de economía, Madrid, n. 897, p.67-76, jul./ago, 2017.

POMED SÁNCHEZ, Luis. Fundamento y naturaleza jurídica de las administraciones independientes. *Revista de Administración Pública*, Madrid, v.132, p.117-169, 1993.

PORTAL CPA WEBTRUST. Disponível em: <https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services>. Acesso em: 11 abril de 2020.

PORTAL DA AGENCE FRANÇAISE DE NORMALISATION (AFNOR). Disponível em: <https://www.afnor.org/>. Acesso em 14 dez. 2020.

PORTAL DA INTERTEK. Disponível em: <https://www.intertek.com/assurance/iso-27001/>. Acesso em 14 dez. 2020.

PORTAL DA TÜV RHEINLAND. Disponível em: < https://www.tuv.com/world/en/information-security.html?verbid=131>. Acesso em 14 dez. 2020.

PORTAL DA TÜV SÜD WEBSITE. Disponível em: <https://www.tuvsud.com/en/industries/consumer-products-and-retail/consumer-products-and-retail-listing>. Acesso em 14 dez. 2020.

PORTAL DO BRITISH STANDARDIZATION INSTITUTION. Disponível em: <https://www.bsigroup.com/pt-BR/Sobre-o-BSI/Orgao-Nacional-de-Normas-do-Reino-Unido/>. Acesso em 14 dez. 2020.

PORTAL DO BUREAU VERITAS BRASIL. Disponível em: <https://www.bureauveritascertification.com.br/ >. Acesso em 14 dez. 2020.

PORTAL DO EUROPRIVACY SEAL. Disponível em: <https://www.european-privacy-seal.eu/EPS-en/Home>. Acesso em 14 dez. 2020.

PORTAL DO PRIVACY BY DESIGN CERTIFICATION. Disponível em: <https://gpsbydesigncentre.com/privacy-by-design-certification/> Acesso em 14 dez. 2020.

PORTAL DO TRUST EPRIVACY CERTIFICATION. Disponível em: <https://trustarc.com/consumer-info/privacy-certification-standards/>. Acesso em 14 dez. 2020.

PUCCIELI, Oscar. El derecho de la protección de datos personales en perspectiva latino-americana. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.373-429.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018.

REDE IBEROAMERICANA DE PROTEÇÃO DE DADOS. *Standards de Proteção de Dados*. Disponível em: <https://www.dataguidance.com/sites/default/files/02.24.20_ibero-am_standards.pdf>. Acesso em: 30 nov. 2020.

REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.461-512.

REIGADA, Antonio Troncoso. Del principio de seguridad de los datos al derecho a la seguridad digital. *Economía industrial*, Madrid, [s.v.], n. 410, p.127-151, 2018.

REILLY, Marcelo Bauzá. Los estándares de protección de datos personales para los Estados iberoamericanos. *La justicia uruguaya: revista jurìdica*, v.79, n. 156, p. 93-96, 2018.

RICAHARDS, Neil M.; KING, Jonathan H. Three Paradoxes of Big Data. Disponível em: <https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/>. Acesso em: 20 jun. 2020.

RIFON, Nora J.; LAROSE, Robert; CHOI, Sejung Marina. Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of consumer affairs*, v. 39, n. 2, p. 339-362, 2005.

RODOTÀ, Stefano. *El derecho a tener derechos.* Madrid: Trotta, 2014.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet?. *Civilistica.com*, Rio de Janeiro, n. 2, jul./dez.2015. Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/. Acesso em: 20 out. 2020.

RODRIGUES JUNIOR, Otávio Luiz. *A mudança na jurisprudência alemã sobre vida privada*. Disponível em: <https://www.conjur.com.br/2012-jul-18/direito-comparado-mudanca-jurisprudencia-alema-vida-privada>. Acesso 4 jul. 2020.

RODRIGUES, Rowena; BARNARD-WILLS, David; WRIGHT, David [et all...]. *EU privacy seals projec*t. Luxemburg: Publications Office of the European Union, 2013.

RODRIGUES, Rowena; PAPAKONSTANTINOU, Vagelis (Org.). *Privacy and Data Protection Seals***.** Springer, Information Technology and Law Series, v. 28, 2018.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito* – UFPR, Curitiba, n.53, p.51-58, 2011.

RUBINSTEIN, Ira S. Big Data: The end of privacy or a new beginning?, *International Data Privacy Law*, v.2, n.3, p.74-82, 2013.

RUIZ, Cláudio. Privacy and security, the Latin American way. In: MAGRANI, Eduardo. *Digital rights: Latin America and the Caribbean*. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017. p.24-26.

SAARENPÄÄ, Ahti. Derechos Digitales. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.291-326.

SALDANHA, Jânia Maria Lopes. *Cosmopolitismo jurídico*: teorias e práticas de um direito emergente entre a globalização e mundialização. Porto Alegre: Livraria do Advogado, 2018.

SALINAS, Natasha Schmitt Caccia;GUERRA, Sérgio. Resolução eletrônicade conflitos em agências reguladoras.Revista Direito GV, v. 16, n. 1, jan./abr.2020, e1949. doi: http://dx.doi.org/10.1590/2317-6172201949.

SANTOS, Marina; CERQUEIRA, Norma; MENEGHETTI, Rayssa. Anonimização de dados como garantia ao direito à privacidade na internet das coisas (Internet of Things-IoT). *Revista Brasileira de Direito e Gestão Pública,* v. 8, n. 5, p. 1219-1229, 2020.

SCHERTEL MENDES, Laura; DONEDA, Danilo. Reflexões gerais sobre a nova lei de proteção de dados. Revista do Direito do Consumidor, Brasília, v.120, p.469-483, nov./dez. 2018.

SCHIAVI, Pablo. El derecho al olvido en tiempos de "google": primeras aproximaciones a su regulación en Uruguay. Revista de Direito Administrativo e Infraestrutura, v. 2, n. 7, p. 179-196, 2018.

SCHIAVI, Pablo. El derecho al ovido ya la protección de datos personales en Uruguay. *Revista de Direito Administrativo e Infraestrutura*, v. 1, n. 2, p. 309-331, 2017.

SCHIAVI, Pablo. La protección de los datos personales en las redes sociales. *Revista de Direito Administrativo e Constitucional*, v. 13, n. 52, p. 145-178, 2013.

SCHIAVI, Pablo. Primeras reflexiones sobre la nueva ley de telemedicina en Uruguay.*Revista de Direito Administrativo e Infraestrutura*, v. 5, n. 16, 2021.

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

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1814-1894, dec. 2011.

SHAPIRO, Martin. The problems of independent agencies in the United States and the European Union. *Journal of European Public Policy*, v. 4, n. 2, p. 276-277, 1997.

SILVEIRA, Sérgio Amadeu. Democracia e os códigos invisíveis: como algoritmos estão modulando comportamentos e escolhas políticas [e-book]. Rio de Janeiro: Editora Sesc, 2018.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. *Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai*. Disponível em: <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso 2 jul 2020.

SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. *Perspectivas em Ciência da Informação*, n. 4, v. 24, p. 132-144, 2019.

SZINVELSKI, Mártin; LIMBERGER, Têmis; SALDANHA, Jânia. Transnacionalização e selos de qualidade em proteção de dados: um novo campo na era digital. *Revista dos Tribunais*, v. 1020, p.143-162, out., 2020.

TEUBNER, Gunther. *Fragmentos Constitucionais*: constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

TLACUILO FUENTES, Itzayana. Legal Recognition of the Digital Trade in Personal Data. Mexican Law Review, [S.l.], p. 87-117, dec. 2019.

TORNARÍA, Felipe Rotondo. Protección de datos personales, autorregulación y transferencias internacionales de datos. *La justicia uruguaya: revista jurìdica*, n. 147, p. 63-69, 2013.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho (JO 2016, L 207, p. 1.) Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250>. Acesso em 23 nov. 2020.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. O Tribunal de Justiça declara inválida a Decisão de Execução 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf >.Acesso em 23 nov. 2020.

UNIÃO EUROPEIA. Article 29 Data Protection Working Party: Guidelines on Data Protection Officers. Disponível em: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44100> Aceso em 21 dez. 2020.

UNIÃO EUROPEIA. Autoridade Europeia para a Proteção de Dados. Relatório 2019. Disponível em:<https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_ex_sum_pt.pdf>. Acesso em 12 nov. 2020.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf> Acesso em 14 out. 2020.

UNIÃO EUROPEIA. *Convenção para a proteção de indivíduos com relação ao processamento automático de dados pessoais*. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em 8 nov. 2020.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>. Acesso em 25 nov. 2020.

UNIÃO EUROPEIA. Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Parecer 4/2007 sobre o conceito de dados pessoais.* Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>. Acesso em: 2 jul. 2020.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da Europa,* de 27 de abril de 2016. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 14 out. 2020.

UNIÃO EUROPEIA. Supervisor Europeu de Proteção de Dados. *Ditamen sobre el cumplimento efectivo de la legislación en la economía de la sociedad digital*. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018XX0704(01)&from=ES>. Acesso 30 de mar. 2020.

URUGUAI XXI. Oito Empresas Uruguaias Entre As Melhores Da Latam No Desenvolvimento De Aplicações Móveis. 8 de julho de 2020. Disponível em: <https://www.uruguayxxi.gub.uy/pt/noticias/artigo/ocho-empresas-uruguayas-entre-las-mejores-de-latam-en-desarrollo-de-apps-moviles/>.

URUGUAI. Comercio Electrónico en el Uruguay, da Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), 2014. Disponível em: < https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/1er-estudio-de-comercio-electronico-en-uruguay.>. Acesso em 15 nov. 2020.

URUGUAI. Decreto 64/020, Reglamentacion de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 1 set. 2020.

URUGUAI. Decreto n. 414/009, de 31 de agosto de 2009. Reglamentacion de la ley 18.331, relativo a la proteccion de datos personales. Disponível em: <https://www.impo.com.uy/bases/decretos/414-2009>.Acesso em 1 set. 2020.

URUGUAI. Decreto nº 664/008, de 22 de dezembro de 2008. Creacion del registro de bases de datos personales. Disponível em: https://www.impo.com.uy/bases/decretos/664-2008. Acesso em 1 set. 2020.

URUGUAI. Lei 17.250, de 2000. Defensa del Consumidor. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp3295160.htm>.Acesso 14 nov.2020.

URUGUAI. Lei 17.930, de 23 de dezembro de 2005. Presupuesto Nacional. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp3511048.htm>. Acesso em: 14 dez. 2020.

URUGUAI. Ley n. 18331, de 11 de agosto de 2008. Lei de Protección de Datos Personales. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 1 set. 2020.

URUGUAI. Resolución N° 68/017. Se resuelve aprobar el documento llamado “Criterios de disociación”, que obra como Anexo de la presente Resolución, con arreglo al Decreto N° 54/017, de 20 de febrero de 2017, reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015. Disponivel em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-68017>.Acesso em 10 dez. 2020.

URUGUAI. Resultados EUTIC2019: internet al alcance de todos en Uruguay, da Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. p.45-46. Disponível em: <https://www.ine.gub.uy/documents/10181/35704/Principales+resultados+de+la+Encuesta+de+Usos+de+Tecnolog%C3%ADas+de+la+Informaci%C3%B3n+y+la+Comunicaci%C3%B3n+2019/2488b09e-9cd5-453b-b6fc-7d66b2ba89ff>. Acesso em: 15 nov.2020.

URUGUAI. URCDP. *Buenas prácticas en protección de datos personales para el uso de formularios por entidades públicas*. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/buenas-practicas-proteccion-datos-personales-para-uso-formularios>. Acesso: 24 out. 2020.

URUGUAI. URCDP. *La protección de los datos personales*. Disponível em: <https://uruguayeduca.anep.edu.uy/recursos-educativos?combine=datos+personales&field_nivel_target_id=All&field_asignatura_o_especialidad_target_id=All&field_destinatarios_target_id=All&field_etiquetas_target_id=All&field_formato_target_id=All&field_palabrasclave_target_id= >.Acesso em 24 nov. 2020.

URUGUAI. URCDP. *Tus Datos Valen*. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/librillo%2Binstrucciones%2Bbaja%2B%281%29.pdf>. Acesso em 24 nov. 2020.

USTARÁN, Eduardo GARCÍA, Paula. Transferencias internacionales de datos. LOMBARTE, Artmi (Diretor). *Tratado de Protección de Datos*. Valência: Tirant lo Blanch, 2019. p.459-490.

VAN DIJK, Jan. *The network society*. SAGE: Publications Limited, 2006.

VAQUERO, Juan Pablo. El valor económico de un derecho fundamental: la monetización de los datos personales. In: REILLY, Marcelo Bauzá (Coord.). *El derecho de las TIC en Iberoamérica*. Montevideo: La Ley, 2019. p.1027-1036.

VARA, Ana María. A un año de la muerte de Ulrich Beck: De la sociedad del riesgo a la metamorfosis del mundo. *Rev. Iberoam. Cienc. Tecnol. Soc*., Ciudad Autónoma de Buenos Aires, v. 11, n. 32, p. 215-237, mayo, 2016.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 717-739.

VASCONCELOS, Beto; PAULA, Felipe de. Autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRASÃO, Ana; OLIVA, Milena. (Org.). *Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro*. 1ed.: Revista dos Tribunais, 2019. p. 717-740.

VILLELA SOUTO, Marcos Juruena. As agências reguladoras e os princípios constituicionais. *Revista de Direito Constitucional e Internacional*, v. 58, p. 220-234, jan-mar, 2007.

VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto N. G. de. Dados anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. In: TEPEDINO, Gustavo; FACHIN, Luiz E. (Org.). *Pensamento crítico do direito civil brasileiro*. Curitiba: Juruá, 2011.

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computers judge personalities better than humans. *Proceedings of the National Academy of Sciences*, n. 112, v. 4., p. 1036-1040, jan, 2015.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, v. 30, n. 1, p. 75-89, 2015.

ZUMBANSEN, Peer. Transnational Legal Pluralism. *Transnational Legal Theory*, [s.l.], v. 1, n.2, 2010, p.141-189. Disponível em: < https://doi.org/10.1080/20414005.2010.11424506 >. Acesso em 5 abril 2020.

ANEXO A – AGENDA REGULATÓRIA DA ANPD

§ 1º O atendimento ao disposto no **caput** deverá ocorrer por meio da implantação de infraestrutura de transporte de fibra óptica, com capacidade mínima de 10 **Gbps** (dez **gigabits** por segundo), do início ao fim do trecho utilizado para atendimento do respectivo Município, que permita conexão ao menos a partir de um ponto localizado no seu distrito sede a um ponto de troca de tráfego que se enquadre nas características definidas no Plano Geral de Metas de Competição aprovado pela Anatel.

§ 2º As sedes de Municípios, vilas, áreas urbanas isoladas e aglomerados rurais, indicados pela Anatel, que ainda não disponham dessa infraestrutura deverão ser atendidas por cada concessionária da seguinte forma:

I - no mínimo, dez por cento até 31 de dezembro de 2021;

II - no mínimo, vinte e cinco por cento até 31 de dezembro de 2022;

III - no mínimo, quarenta e cinco por cento até 31 de dezembro de 2023; e

IV - cem por cento até 31 de dezembro de 2024.

Art. 19. Nas sedes de Municípios atendidas por força do disposto no Decreto nº 6.424, de 2008, a concessionária deverá manter instalada a capacidade de **backhaul** estabelecida.

Art. 20. As concessionárias do STFC na modalidade local ficam obrigadas a disponibilizar o acesso à infraestrutura de **backhaul**, objeto das metas de universalização, nos termos de regulamentação específica, de maneira a atender, preferencialmente, a implementação de políticas públicas para as telecomunicações.

Parágrafo único. A Anatel pode desobrigar o compartilhamento de infraestrutura de **backhaul** caso seja verificada a existência de competição adequada no respectivo mercado relevante.

CAPÍTULO V
DAS METAS DE SISTEMA DE ACESSO FIXO SEM FIO PARA A PRESTAÇÃO DO SERVIÇO TELEFÔNICO FIXO COMUTADO

Art. 21. Nas localidades atendidas por força do Decreto nº 9.619, de 2018, a infraestrutura de suporte aos sistemas de acesso sem fio implantada até 31 de dezembro de 2020 deve ser mantida pela concessionária.

Art. 22. As concessionárias do STFC na modalidade local têm por obrigação disponibilizar o acesso à infraestrutura de acesso sem fio, nos termos da regulamentação aplicável, e atenderá, preferencialmente, a implementação de políticas públicas para as telecomunicações.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Art. 23. O **backhaul** para atendimento dos compromissos de universalização, bem como as estações rádio base e as redes de transporte implantadas especificamente para atendimento dos compromissos de universalização qualificam-se entre os bens de infraestrutura e equipamentos de comutação e transmissão reversíveis à União e devem integrar a relação de bens reversíveis.

Art. 24. A Anatel deverá, no prazo de três meses, contado da data de publicação deste Plano, publicar a lista de sedes de Municípios, vilas, áreas urbanas isoladas e aglomerados rurais que ainda não disponham da infraestrutura de **backhaul** e que sejam suficientes para a utilização do saldo previsto no art. 17.

Parágrafo único. A publicação da lista de que trata o **caput** tem o objetivo de permitir a plena participação social e assegurar a observância dos objetivos gerais das políticas públicas de telecomunicações, principalmente evitar a sobreposição involuntária de atendimento por infraestrutura de **backhaul**.

Art. 25. Enquanto não for publicada a regulamentação deste Plano, aplicam-se, no que couber, as disposições do regulamento do Decreto nº 9.619, de 2018.

Parágrafo único. A regulamentação deste Plano deverá ser editada pela Anatel, no prazo de doze meses, contado da data de publicação deste Decreto.

ANEXO II

TELEFONES DE USO PÚBLICO DAS CONCESSIONÁRIAS DO SERVIÇO TELEFÔNICO FIXO COMUTADO NA MODALIDADE LOCAL

SETORES DO PLANO GERAL DE OUTORGAS DE SERVIÇO DE TELECOMUNICAÇÕES PRESTADO NO REGIME PÚBLICO - PGO	QUANTITATIVO DE TELEFONE DE USO PÚBLICO -TUP EM LOCAIS SITUADOS NA ÁREA RURAL
1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 e 17	66.157

SECRETA

SECRETARIA DE

RET

Na Portaria que dispõe sobre Processos Disciplinares e do Sistema de Ge Entes Privados no âmbito da Presidência Diário Oficial da União de 6 de julho de 20 **onde se lê:** "Portaria nº 5, de 2 de julho d 2 de julho de 2020".

SECRETARIA

PORTARIA Nº 90, DE

Decla decre Repú Decr

O MINISTRO DE ESTADO CHEFE DA REPÚBLICA, no uso da atribuição que lh II, da Constituição Federal, e tendo em vist 28 de novembro de 2019, resolve:

Art. 1º Fica declarada a revoga

Portaria nº 15, de 15 de fevere
Portaria nº 16, de 15 de fevere
Portaria nº 62, de 5 de maio d
Portaria nº 268, de 5 de maio
Portaria nº 23, de 23 de março

Art. 2º Esta Portaria entra em

LUIZ

AUTORIDADE NACIONA

PORTARIA Nº 11, DE

Torna pública a agenda regulatória para o

O DIRETOR-PRESIDENTE DA AUT exercício das atribuições que lhe confere o a

CONSIDERANDO que a Agenda que agrega as ações regulatórias considera tratamento pela Autoridade durante sua v

CONSIDERANDO a deliberação Deliberativa nº 1, realizada em 20 de jane

CONSIDERANDO o constante do resolve:

Art. 1º Tornar pública a Agenda de Dados - ANPD para o biênio 2021-2022, Conselho-Diretor na Reunião Deliberativa n

Art. 2º Os Projetos de Regulam priorização nesta Agenda Regulatória:

Fase 1 - iniciativas da agenda acontecerá em até 1 ano;

Fase 2 - iniciativas da agenda

ANEXO I

AGENDA REGULATÓRIA - 2021-2022

Item	Tema	Descrição	Priorização	Previsão de início do	
				1º/2021	2º/2021
1	Regimento Interno da ANPD	Publicação do primeiro Regimento Interno da ANPD.	Fase 1	G	
2	Planejamento Estratégico da ANPD	Publicação do Planejamento Estratégico de 2021-2023, contendo os objetivos a serem alcançados pela ANPD e os seus respectivos prazos e as ações estratégicas vinculadas.	Fase 1	G	
3	Proteção de dados e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos	A LGPD prevê regulamentação diferenciada para microempresas e empresas de pequeno porte, com a edição de normativo sobre o assunto, conforme estabelece o art. 55-J da referida lei.	Fase 1	G	
4	Direitos dos titulares de dados pessoais	A LGPD estabelece os direitos dos titulares de dados pessoais, mas diversos pontos merecem regulamentação, que tratará desses direitos, incluindo, mas não limitado aos artigos 9º, 18, 20 e 23.	Fase 3		
5	Estabelecimento de normativos para aplicação do art. 52 e seguintes da LGPD	O art. 53 da LGPD prevê que a ANPD deve definir, via regulamento próprio sobre sanções administrativas a infrações da referida lei, as metodologias que orientarão o cálculo do valor-base das sanções de multa. A regulamentação também estabelecerá as circunstâncias e as condições para a adoção de multa.	Fase 1	G	
6	Comunicação de incidentes e especificação do prazo de notificação	De acordo com o art. 48 da LGPD, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações.	Fase 1	G	
7	Relatório de Impacto à Proteção de Dados Pessoais	De acordo com as competências estabelecidas pelo art. 55-J, inciso XIII, cabe a ANPD editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais.	Fase 1	G	
8	Encarregado de proteção de dados pessoais	Nos termos do art. 41, § 3º da LGPD, a ANPD pode estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.	Fase 2		
9	Transferência Internacional de Dados Pessoais	O art. 33, inciso I da LGPD, prevê que a transferência internacional de dados pessoais somente é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na referida lei. Por sua vez, o art. 34 explica que o nível de proteção de dados do país estrangeiro ou do organismo internacional poderá ser avaliado pela ANPD. O art. 35 da lei determina, ainda, que a definição do conteúdo de cláusulas-padrão contratuais, dentre outros, será realizada pela ANPD. Assim, é necessário regulamentar os arts. 33, 34 e 35 da LGPD, sem prejuízo dos demais temas tratados pelos artigos não mencionados neste texto.	Fase 2		
10	Hipóteses legais de tratamento de dados pessoais	Documento orientando o público sobre as bases e hipóteses legais de aplicação da LGPD sobre diversos temas, incluindo as hipóteses legais descritas no art. 7º mas não restritas a ele.	Fase 3		

Ministério da Agricultura, Pecuária e Abastecimento

GABINETE DA MINISTRA

PORTARIA MAPA Nº 25, DE 27 DE JANEIRO DE 2021

Torna sem efeito a Portaria nº 15, de 14 de janeiro de 2021, que dispõe sobre medidas para a abertura do mercado brasileiro para importação de produtos agropecuários.

A MINISTRA DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso das atribuições que lhe confere o art. 87, parágrafo único, inciso I, da Constituição

Parágrafo único. O Projeto de
página eletrônica do Ministério da
https://www.gov.br/agricultura/pt-br/acess
publicas.

Art. 2º As sugestões tecnicame
por meio do Sistema de Monitoramento d
Defesa Agropecuária - SDA
https://sistemasweb.agricultura.gov.br/sism

Parágrafo único. Para ter acesso
prévio no Sistema de Solicitação de Ace
https://sistemasweb.agricultura.gov.br/solic

Art. 3º Esta Portaria entra em

ANEXO B - PADRÕES DE PROTEÇÃO DE DADOS PESSOAIS PARA OS ESTADOS IBERO-AMERICANOS

PADRÕES DE PROTEÇÃO DE DADOS PESSOAIS

PARA OS ESTADOS IBERO-AMERICANOS

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

RED IBEROAMERICANA DE PROTECCION DE DATOS

PADRÕES DE
PROTEÇÃO DE DADOS PESSOAIS
PARA OS ESTADOS IBERO-AMERICANOS

No âmbito do XV Encontro Ibero-Americano de Proteção de Dados, a Rede Ibero-Americana de Proteção de Dados (RIPD ou a Rede) aprovou e apresentou oficialmente os denominados "Padrões de Proteção de Dados dos Estados Ibero-Americanos", 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.

O texto ora aprovado, tenta dar respostas para um dos eixos da estratégia acordada pela RIPD em novembro de 2016, em Montevidéu, plasmada no documento "RIPD 2020", que consiste em "encorajar e contribuir para o fortalecimento e a adequação dos processos regulatórios na região, mediante a elaboração de diretrizes que sirvam de parâmetro para futuras regulações ou para a revisão das já existentes."

Nesse sentido, 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.

Entre os objetivos dos Padrões Ibero-Americanos, destacam-se:

- 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.
- Garantir o efetivo exercício e tutela do direito à proteção de dados pessoais de qualquer pessoa física nos Estados Ibero-Americanos, mediante a determinação de regras comuns que assegurem o devido tratamento de seus dados pessoais.
- Facilitar o fluxo de dados pessoais entre os Estados Ibero-Americanos e fora de suas fronteiras, com o propósito de coadjuvar para o crescimento econômico e social da região.
- Encorajar a cooperação internacional entre as autoridades de controle dos Estados Ibero-Americanos com outras autoridades de controle não pertencentes à região, e autoridades e órgãos internacionais na matéria.

Como antecedentes diretos desses Padrões, por um lado, é possível mencionar a adoção pela própria RIPD, em 2007, no contexto do V Encontro Ibero-Americano de Proteção de Dados, das "Diretivas para a Harmonização da Proteção de Dados na Comunidade Ibero-Americana". Com elas, pretendia-se estabelecer um "contexto harmonizado" de referência para iniciativas regulatórias nacionais que pudessem surgir na região em matéria de proteção de dados. E, por outro, os padrões aprovados na Conferência Internacional de Autoridades de Privacidade e Proteção de Dados, celebrada em Madri, em 2009, os chamados "Padrões de Madri", que sem dúvida representaram um avanço na busca por soluções e disposições específicas "que poderiam ser aplicadas independentemente das diferenças que pudessem existir entre os diferentes modelos existentes de proteção de dados e privacidade".

Na elaboração dos Padrões Ibero-Americanos também foram tomados como referência outros instrumentos internacionais e emblemáticos em matéria de proteção de dados pessoais, como as Diretivas relativas à proteção da intimidade e da circulação transfronteiriça de dados pessoais da Organização para a Cooperação e Desenvolvimento Econômico; o Convênio número 108 do Conselho da Europa, para a proteção das pessoas respeito do tratamento automatizado de dados de caráter pessoal e seu Protocolo; o Marco de Privacidade do Fórum de Cooperação Econômica Ásia-Pacífico, e o Regulamento do Parlamento Europeu e do Conselho, relativo à proteção das pessoas físicas no que respeita ao tratamento de dados pessoais e à livre circulação desses dados, entre outros.

O percurso seguido na elaboração incluiu as seguintes etapas:

- Junho de 2016: no XIV Encontro Ibero-Americano de Proteção de Dados, celebrado em 08 de junho de 2016, em Santa Marta, Colômbia, acordou-se a elaboração dos Padrões Ibero-Americanos a cargo do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI), nesse momento em caráter de presidente da Rede.

- Novembro de 2016: no Seminário da RIPD no Centro de Cooperação Espanhola em Montevidéu, celebrado nos dias 08 e 09 de novembro em Montevidéu, Uruguai, o INAI apresentou aos membros presentes da Rede o anteprojeto de Padrões Ibero-Americanos. Nesse seminário, acordou-se que, durante todo o mês de dezembro de 2016, o anteprojeto de Padrões Ibero-Americanos estaria aberto para comentários e observações dos membros da Rede.

- Maio de 2017: na Oficina da RIPD no Centro de Cooperação Espanhola, em Cartagena de Índias, foi estudado e debatido, do ponto de vista técnico, a versão dos Padrões Ibero-Americanos resultado de todas as contribuições recebidas durante o mês de dezembro de 2016. Nessa oficina participaram as Autoridades membros da RIPD, uma representação do Supervisor Europeu de Proteção de Dados e da Organização dos Estados Americanos, bem como, mediante videoconferência, a Unidade de Fluxos Internacionais da Comissão Europeia.

- Junho de 2017: no XV Encontro Ibero-Americano de Proteção de Dados, celebrado entre 20 e 22 de junho de 2017, em Santiago do Chile, aprovou-se por unanimidade em sessão fechada do Encontro a versão que resultara dos trabalhos realizados durante a oficina de Cartagena de Índias, sendo formalmente proclamados em Sessão Aberta.

Com a aprovação desses Padrões, a RIPD possui uma ferramenta chave para poder enfrentar com rigor o seguimento e apoio dos futuros desenvolvimentos legislativos na Região, devido a que os Padrões Ibero-Americanos têm a característica de serem um modelo normativo que:

- Responde às necessidades e exigências nacionais e internacionais que demanda o direito à proteção de dados pessoais, em uma sociedade onde as tecnologias da informação e do conhecimento assumem cada vez maior relevância em todas as atividades da vida cotidiana.
- Inclui as melhores práticas nacionais e internacionais na matéria.
- Propõe uma série de padrões flexíveis que possam facilitar sua adoção entre os Estados Ibero-Americanos, sem infringir de qualquer maneira seu direito interno, de maneira tal que esse documento seja uma realidade viva e viável na região ibero-americana, em benefício do próprio titular.
- Garante um nível adequado de proteção dos dados pessoais na região ibero-americana, com o fim de não estabelecer barreiras para sua livre circulação nos Estados Ibero-Americanos e, em consequência, favorecer as atividades comerciais entre a região, bem como com outras regiões econômicas.

Por outro lado, e não menos importante, os Padrões Ibero-Americanos permitirão reforçar a posição da Rede no âmbito internacional. Para isso, iniciativas serão implementadas nos diversos fóruns internacionais (Comissão Europeia, Conferência Internacional de Autoridades de Proteção de Dados e Privacidade, Organização dos Estados Americanos, etc.), tentando procurar a maior difusão possível dos mesmos.

Em definitiva, o trabalho efetuado pelas entidades que integram a RIPD, que levou finalmente à aprovação dos citados Padrões, constitui uma experiência concreta de cooperação que, a nosso critério, pode ser de grande utilidade para outras organizações, por que ficam à inteira disposição de todas as entidades e profissionais que possam se beneficiar deles, em nome de garantir, da maneira mais eficaz, o possível exercício e tutela do direito à proteção de dados, tanto na região ibero-americana como no contexto internacional.

Estados Ibero-Americanos:

(1) Considerando a proteção das pessoas físicas, relativamente ao tratamento de seus dados pessoais, como direito fundamental reconhecido com categoria máxima na maioria das Constituições Políticas dos Estados Ibero-Americanos, na forma do direito de proteção dos dados pessoais ou *habeas data*, e que, nalguns casos, foi jurisprudencialmente definido por seus Tribunais ou Cortes Constitucionais;

(2) Determinando que o direito à proteção dos dados pessoais foi conceitualizado em alguns países Ibero-Americanos, legislativamente ou jurisprudencialmente, como direito de natureza diferente dos direitos à vida privada e familiar, à intimidade, à honra, ao bom nome e outros direitos semelhantes, que em conjunto garantem o livre desenvolvimento da personalidade da pessoa física, até se conformarem como direito autônomo, com características e dinâmicas próprias, cujo objeto é a preservação do poder de disposição e do controle que qualquer pessoa física tem respeito da informação que lhe diz respeito, especialmente atendendo ao emprego das tecnologias da informação e das comunicações, que cada vez assumem maior relevância em todos os aspectos da vida cotidiana;

(3) Assumindo que salvaguardar o direito das pessoas físicas respeito do tratamento de seus dados pessoais é compatível com o objetivo de garantir e proteger outros direitos, os quais são reconhecidos como indivisíveis e interdependentes entre si, e que requerem de proteção conforme para resguardar, em sua esfera mais ampla, às pessoas físicas contra intrusões ilegais ou arbitrárias, mesmo daquelas derivadas do tratamento de dados pessoais. O acima mencionado não impede que o direito à proteção dos dados pessoais seja aplicado às pessoas jurídicas, em cumprimento do estabelecido no direito interno dos Estados Ibero-americanos;

(4) Lembrando que a Rede Ibero-Americana de Proteção de Dados surgiu em virtude do acordo alcançado no Encontro Ibero-Americano de Proteção de Dados, celebrado em La Antigua, Guatemala, entre 01 a 06 de junho de 2003, com a presença de representantes de 14 países ibero-americanos. Esta iniciativa contou, desde o início, com o apoio político refletido na Declaração Final da XIII Cúpula de Chefes de Estado e de Governo dos países Ibero-Americanos, realizada em Santa Cruz de la Sierra, Bolívia, entre 14 e 15 de novembro de 2003, cientes do caráter da proteção de dados pessoais como direito fundamental;

(5) Tendo em conta que, devido à Resolução adotada na XXV Cúpula Ibero-Americana de Chefes de Estado e de Governo, que teve lugar em Cartagena de Índias, Colômbia, nos dias 28 e 29 de outubro de 2016, reafirmou-se que a adoção, elaboração e impulsionamento de diversos manuais, programas, iniciativas e projetos fortaleceriam a gestão e o impacto das ações de cooperação entre os países da Ibero-América;

(6) Assumindo que a Rede Ibero-Americana de Proteção de Dados se constitui como fórum permanente de intercâmbio de informação aberto a todos os países membros da Comunidade Ibero-Americana e que possibilita o envolvimento dos setores público, privado e social, com o fim de encorajar desenvolvimentos normativos necessários para garantir uma regulação avançada do direito de proteção dos dados pessoais num contexto democrático e global;

(7) Lembrando que, em virtude da reunião celebrada em Santa Cruz de la Sierra, Bolívia, entre os dias 03 e 05 de maio de 2006, elaborou-se o documento denominado Diretrizes para a Harmonização da Proteção de Dados na Comunidade Ibero-Americana, que estabelece um conjunto de disposições cujo objeto é contribuir para a elaboração das iniciativas regulamentares de proteção de dados que possam surgir na Comunidade Ibero- Americana, constituindo-se em referência para o desenvolvimento dos presentes Padrões;

(8) Considerando que a União Europeia tem adotado um novo quadro normativo na matéria, com o objetivo de modernizar suas disposições e garantir maior solidez e coerência na proteção efetiva do direito fundamental à proteção dos dados pessoais na União Europeia e para gerar confiança na sociedade em geral e, por sua vez, facilitar o desenvolvimento da economia digital, tanto no mercado interior como em suas relações globais; quadro normativo que se posiciona como referência obrigatória e determinante na elaboração das legislações nacionais de proteção de dados na Ibero- América;

(9) Reconhecendo a existência da falta de harmonização nos Estados Ibero-Americanos respeito do reconhecimento, adoção, definição e desenvolvimento das figuras, princípios, direitos e procedimentos que dão conteúdo ao direito de proteção de dados pessoais em suas legislações nacionais, o qual, sem dúvida, dificulta na atualidade enfrentar os novos desafios na proteção desse direito, derivados da contínua e vertiginosa evolução tecnológica e da globalização em diversos âmbitos;

(10) Tornando urgente, no âmbito da contínua inovação tecnológica, a adoção de instrumentos regulamentares que, por um lado, garantam a proteção das pessoas físicas

em relação ao tratamento de seus dados pessoais e, pelo outro, o livre fluxo dos dados pessoais, que atualmente conformam a base para o desenvolvimento, fortalecimento e intercâmbio de bens e serviços, em uma economia global e digital, sobre os quais são erigidas as economias dos Estados Ibero-Americanos;

(11) Acordando que, para garantir um alto nível de proteção dos direitos e liberdades das pessoas físicas, entre outras questões, por sua vez, requer-se de nível uniforme e elevado de proteção às pessoas físicas respeito de sua informação pessoal, que responda às necessidades e exigências atuais em um contexto global, com o objetivo de não estabelecer barreiras à livre circulação dos dados pessoais nos Estados Ibero-Americanos e, em consequência, encorajar atividades comerciais entre a região, bem como em outras regiões econômicas;

(12) Aceitando que, com o propósito de ampliar e fortalecer o regime de proteção às pessoas físicas respeito do tratamento de seus dados pessoais, é imperioso estabelecer um equilíbrio entre os interesses de todos os atores do setor público, privado e social e titulares envolvidos, incluindo o estabelecimento de exceções por questões de interesse público razoáveis e compatíveis com os direitos e liberdades, a fim de evitar incorrer em restrições ou limitações injustificadas ou desproporcionadas, que não estejam em conformidade com os fins perseguidos em sociedades democráticas;

(13) Cientes dos riscos potenciais que poderiam derivar da esfera das pessoas físicas em função do tratamento de seus dados pessoais em grande escala, efetuado por órgãos públicos e privados e, em particular, considerando a especial vulnerabilidade de crianças e adolescentes, que demandam garantias adequadas e suficientes de proteção perante usos indevidos ou arbitrários de sua informação pessoal, preservando, então, seu interesse superior, o livre desenvolvimento de sua personalidade, sua segurança e outros valores que objeto de máxima proteção por parte dos Estados Ibero-Americanos;

(14) Acordando que o desenvolvimento tecnológico facilita o tratamento de novas categorias de dados pessoais que apresentam riscos específicos, especialmente o uso inadequado dos mesmos; assim, resulta altamente relevante alcançar um consenso mínimo respeito das categorias de dados pessoais consideradas de caráter sensível ou especialmente protegidas, bem como das regras de tratamento, considerando que as consequências e ingerências negativas que podem derivar do uso indevido deste tipo de dados pessoais podem produzir condições injustas ou discriminatórias para as pessoas físicas;

(15) Admitindo que nem todos os Estados Ibero-Americanos contam com uma legislação na matéria, situação que pode afetar a preservação e tratamento da informação pessoal, se considerado o acelerado uso das tecnologias da informação que facilitam e possibilitam a comunicação massiva de dados pessoais de maneira imediata e quase ilimitada;

(16) Estabelecendo que as legislações em matéria de proteção de dados pessoais dos Estados Ibero-Americanos devem adotar as referências contidas nos presentes Padrões, para contar com um contexto regulamentar harmonizado, que ofereça um nível de proteção às pessoas físicas respeito do tratamento de seus dados pessoais e, por sua vez, garantindo o desenvolvimento comercial e econômico da região;

(17) Admitindo que, atualmente, as bases jurídicas que legitimam qualquer órgão de caráter público ou privado que tratar dados pessoais em seu poder são o consentimento do titular; o cumprimento de uma disposição legal; o cumprimento de ordem judicial, resolução ou mandado fundado e motivado de autoridade pública competente; o exercício de faculdades próprias das autoridades públicas; o reconhecimento ou defesa dos direitos do titular perante autoridades públicas competentes; a execução de contrato ou pré-contrato em que o titular for parte; o cumprimento de obrigação legal aplicável ao responsável; a proteção dos interesses vitais do titular ou de outra pessoa física; o interesse legítimo do órgão público ou privado, ou por razões de interesse público;

(18) Salientando a necessidade de que os Estados Ibero- Americanos tratem os dados pessoais com os mesmos padrões e regras homogêneas que oferecem aos titulares as mesmas garantias de proteção, através do estabelecimento de um catálogo de princípios de cumprimento obrigatório, que responda aos atuais padrões nacionais e internacionais na matéria, bem como às exigências que demanda um efetivo exercício e respeito desse direito fundamental;

(19) Reconhecendo que, com o propósito de garantir de maneira efetiva o direito à proteção dos dados pessoais, é preciso adotar um contexto regulamentar que reconheça a qualquer pessoa física, no caráter de titular de seus dados pessoais, a possibilidade de exercer, por regra geral de maneira gratuita e excepcional com custos associados por razões naturais de reprodução, o envio, certificação ou outras, os direitos de acesso, retificação, cancelamento, oposição e portabilidade, inclusive no contexto de tratamentos de dados pessoais efetuados por motores ou buscadores da Internet; direitos que complementam as condições necessárias para que os titulares possam exercer de maneira plena seu direito à autodeterminação informativa;

(20) Destacando a importância e o papel fundamental desempenhado pelos prestadores de serviços, que tratam dos dados pessoais em nome e por conta do responsável, incluindo aqueles que prestam serviços de cômputo na nuvem e outras matérias, resultando que os Estados Ibero-Americanos devam adotar, em um mundo globalizado, um regime que permita regular este tipo de serviços, com a finalidade de estabelecer uma série de garantias para a proteção dos dados pessoais que devido a seu encargo possuem e tratam, sem isentar o responsável de suas obrigações e responsabilidades que possui perante titulares e autoridades de controle;

(21) Considerando que o desenvolvimento das novas tecnologias da informação e das comunicações, bem como dos serviços desenvolvidos no contexto da economia digital, contribuem para o crescimento contínuo dos fluxos transfronteiriços de dados pessoais no âmbito da sociedade global, é inescusável a obrigação de estabelecer uma base mínima que facilite e permita a responsáveis e encarregados, como exportadores, realizar transferências internacionais de dados pessoais com total respeito dos direitos dos titulares;

(22) Tendo em conta que, através da Internet, é possível acessar e obter informação disponível em qualquer país, bem como efetuar seu tratamento, coletar dados de milhões de pessoas sem domicílio físico, circunstância que não deveria constituir fator de impedimento para a efetiva proteção dos direitos e liberdades das pessoas no ciberespaço;

(23) Reconhecendo a importância de adotar medidas preventivas que permitam ao responsável responder de maneira proativa perante possíveis problemas relacionados com o direito à proteção de dados pessoais, como à adoção de esquemas de autorregulação vinculante ou sistemas de certificação na matéria; à designação de um oficial de proteção de dados pessoais; à elaboração de avaliações de impacto da proteção de dados pessoais e da privacidade de forma predeterminada e por projeto, entre outras, o que resulta essencial no âmbito das tecnologias da informação e das telecomunicações;

(24) Admitindo a necessidade imperiosa de que cada Estado Ibero- Americano conte com autoridade de controle independente e imparcial em suas faculdades, cujas decisões somente possam ser recorríveis pelo controle judicial, alheia a qualquer influência externa, com poderes de supervisão e investigação em matéria de proteção de dados pessoais, e encarregada de zelar pelo cumprimento da legislação nacional na matéria, que possua recursos humanos e materiais suficientes para garantir o exercício de seus poderes e o desempenho efetivo de suas funções;

(25) Reconhecendo que os Estados Ibero-Americanos são obrigados a adotar um regime que garanta aos titulares um conjunto de mecanismos e procedimentos para apresentar suas reclamações perante a autoridade de controle, quando considerarem vulnerados seus direitos à proteção de dados pessoais, bem como de ser indenizados se tiverem sofrido danos e prejuízos como consequência da violação de seu direito;

(26) Salientando a importância de estabelecer uma base mínima de cooperação internacional entre as autoridades de controle latino-americanas, e entre elas e as de terceiros países, com a finalidade de favorecer e facilitar a aplicação da legislação na matéria e a efetiva proteção dos titulares;

Convieram em adotar os presentes Padrões como máxima prioridade na Comunidade Ibero-Americana para que, com o caráter de diretrizes orientadoras, contribuam para a emissão de iniciativas regulamentares de proteção de dados pessoais na região dos países que ainda não contam com esses ordenamentos, ou no caso, sirvam de referência para a modernização e atualização das legislações existentes, favorecendo a adoção de um contexto regulamentar harmonizado, que ofereça um nível adequado de proteção às pessoas físicas respeito do tratamento de seus dados pessoais e garantindo, por sua vez, o desenvolvimento comercial e econômico da região, em função do seguinte:

Capítulo I

Disposições gerais

1. Objeto

1.1. Os presentes Padrões têm como objetivo:

a. Estabelecer um conjunto de princípios e direitos de proteção de dados pessoais que os Estados Ibero-Americanos poderão adotar e desenvolver em sua legislação nacional, com o fim de garantir o correspondente tratamento dos dados pessoais e contar com regras homogêneas na região.

b. Aumentar o nível de proteção das pessoas físicas relativamente ao tratamento de seus dados pessoais, bem como entre os Estados Ibero-Americanos, para responder às necessidades e exigências internacionais demandas pelo direito à proteção de dados pessoais em uma sociedade onde as tecnologias da informação e do conhecimento assumem cada vez maior relevância em todos os momentos da vida cotidiana.

c. Garantir o efetivo exercício e tutela do direito à proteção dos dados pessoais de qualquer pessoa física nos Estados Ibero-Americanos, mediante o estabelecimento de regras comuns que assegurem o devido tratamento de seus dados pessoais.

d. Facilitar o fluxo dos dados pessoais entre os Estados Ibero-Americanos e além de suas fronteiras, com o propósito de coadjuvar no crescimento social e econômico da região.

e. Impulsionar o desenvolvimento de mecanismos de cooperação internacional entre as autoridades de controle dos Estados Ibero-Americanos, autoridades de controle não pertencentes à região e autoridades e entidades internacionais na matéria.

2. Definições

2.1. Aos efeitos dos presentes Padrões se entenderá por:

a. Anonimização: aplicação de medidas de qualquer natureza voltadas a impedir a identificação ou reidentificação de pessoa física sem esforços desproporcionados.

b. Consentimento: manifestação da vontade, livre, específica, inequívoca e informada do titular, através da qual aceita e autoriza o tratamento dos dados pessoais que lhe dizem respeito.

c. Dados Pessoais: qualquer informação referente a uma pessoa física identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou de qualquer outro tipo. Considera-se que uma pessoa é

identificável quando sua identidade pode ser determinada direta ou indiretamente, sempre que isso não demandar prazos ou atividades desproporcionadas.

d. **Dados pessoais sensíveis**: aqueles referidos à esfera íntima do titular ou cuja utilização indevida possa originar discriminação ou derivar em risco grave para ele. De maneira enunciativa, consideram-se sensíveis aqueles dados pessoais que podem revelar aspectos como origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, à vida, preferência ou orientação sexual, dados genéticos ou dados biométricos dirigidos a identificar, de maneira unívoca, uma pessoa física.

e. **Encarregado**: prestador de serviços, que com o caráter de pessoa física ou jurídica ou autoridade pública, alheia à organização do responsável, trata dos dados pessoais em nome e por conta dele.

f. **Exportador**: pessoa física ou jurídica de índole privada, autoridade pública, serviços, órgão ou prestador de serviços localizado no território de um Estado que efetuar transferências internacionais de dados pessoais, conforme estabelecido nos presentes Padrões.

g. **Responsável**: pessoa física ou jurídica de índole privada, autoridade pública, serviços ou órgão que, só ou em conjunto com outros, determina fins, médios, alcance e outras questões relacionadas com o tratamento de dados pessoais.

h. **Titular**: pessoa física a quem diz respeito os dados pessoais.

i. **Tratamento**: qualquer operação ou conjunto de operações efetuada mediante procedimentos físicos ou automatizados, realizadas sobre dados pessoais, relacionadas, de maneira enunciativa mais não limitativa, com a obtenção, acesso, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração, transferência, difusão, poder, aproveitamento e, em geral, quaisquer usos ou disposições de dados pessoais.

3. Âmbito de aplicação subjetivo

3.1. Os presentes Padrões serão aplicáveis às pessoas físicas ou jurídicas de índole privada, autoridades e órgãos públicos, que tratem dados pessoais no exercício de suas atividades e funções.

4. Âmbito de aplicação objetivo

4.1. Os presentes Padrões serão aplicáveis ao tratamento de dados pessoais que estejam em suportes físicos, automatizados total ou parcialmente, ou em ambos suportes, independente da forma ou da modalidade de sua criação, tipo de suporte, processamento, armazenamento e organização.

4.2. Como regra geral, os presentes Padrões serão aplicáveis aos dados pessoais de pessoas físicas, o que não impede que os Estados Ibero- Americanos, em sua legislação nacional, disponham que a informação das pessoas jurídicas seja salvaguardada segundo o direito à proteção dos dados pessoais, em cumprimento do estabelecido em seu direito interno.

4.3. Os Padrões não serão de aplicação nas seguintes situações:

a. Quando os dados pessoais estiverem destinados a atividades exclusivamente no âmbito da vida familiar ou doméstica da pessoa física, isto é, quando da utilização de dados pessoais em ambiente de amizade, parentesco ou grupo pessoal próximo, e quando não tiverem como propósito divulgação ou utilização comercial.

b. A informação anônima, isto é, aquela que não estiver relacionada com uma pessoa física identificada ou identificável, bem como os dados pessoais submetidos a processo de anonimização, de forma tal que o titular não possa ser identificado ou reidentificado.

4.4. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer categorias de dados pessoais nas quais não poderá ser aplicado o regime de proteção previsto nos presentes Padrões, em cumprimento do direito interno.

5. Âmbito de aplicação territorial

5.1. Os Padrões serão de aplicação no tratamento de dados pessoais efetuado:

a. Por responsável ou encarregado estabelecido em território dos Estados Ibero-Americanos.

b. Por responsável ou encarregado não estabelecido em território dos Estados Ibero-Americanos, quando as atividades do tratamento estiverem relacionadas com a oferta de bens ou serviços dirigidos aos residentes dos Estados Ibero-Americanos, ou, relacionadas com o controle de seu comportamento, na medida em que este acontecer nos Estados Ibero-Americanos.

c. Por responsável ou encarregado não estabelecido em um Estado Ibero-Americano, mas que lhe for aplicável a legislação nacional desse Estado, derivado da celebração de contrato ou em virtude do direito internacional público.

d. Por responsável ou encarregado não estabelecido em território dos Estados Ibero-Americanos e que utilizar ou empregar meios, automatizados ou não, localizados nesse território para tratar dados pessoais, exceto que esses meios sejam utilizados somente com fins de trânsito.

5.2. Aos efeitos dos presentes Padrões, se entenderá por estabelecimento o lugar da administração central ou principal do responsável ou encarregado, que deverá ser determinado em função de critérios objetivos e compreender o exercício efetivo e real das atividades de gestão que determinem as principais decisões, quanto aos fins e meios do tratamento de dados pessoais que realizar através de modalidades estáveis.

5.3. A presença e utilização de meios técnicos e tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituirão, em si mesmas, um estabelecimento principal e não serão consideradas critérios determinantes para a definição do estabelecimento principal do responsável ou encarregado.

5.4. Quando for realizado o tratamento de dados pessoais por grupo empresarial, o estabelecimento principal da empresa que exercer o controle deve ser considerado o estabelecimento principal do grupo empresarial, exceto quando os fins e meios do tratamento forem efetivamente determinados por outra das empresas do grupo.

6. Exceções gerais ao direito à proteção de dados pessoais.

6.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá limitar o direito à proteção de dados para preservar a segurança nacional, a segurança pública, a proteção da saúde pública, a proteção dos direitos e das liberdades de terceiros, bem como por questões de interesse público.

6.2. As limitações e restrições serão reconhecidas de maneira expressa na lei, com o propósito de oferecer certeza suficiente aos titulares sobre a natureza e alcance da medida.

6.3. Qualquer lei que tiver como propósito limitar o direito à proteção de dados pessoais conterá, no mínimo, disposições relativas:

a. À finalidade do tratamento.

b. Às categorias de dados pessoais correspondentes.

c. Ao alcance das limitações estabelecidas.

d. Às garantias adequadas para evitar acessos ou transferências ilícitas ou desproporcionadas.

e. Á determinação do responsável ou responsáveis.

f. Aos prazos de conservação dos dados pessoais.

g. Aos possíveis riscos para os direitos e liberdades dos titulares.

h. Ao direito dos titulares a serem informados sobre a limitação, salvo que for prejudicial ou incompatível com os fins desta.

6.4. As leis serão as necessárias, adequadas e proporcionais em uma sociedade democrática, e deverão respeitar os direitos e as liberdades fundamentais dos titulares.

7. Consideração do direito de proteção de dados pessoais

7.1. Os Estados Ibero-Americanos poderão isentar, em seu direito interno, do cumprimento dos princípios e direitos previstos nos presentes Padrões, exclusivamente na medida em que for necessário conciliar o direito à proteção de dados pessoais com outros direitos e liberdades fundamentais.

7.2. Essa isenção demandará um exercício de consideração, com a finalidade de determinar a necessidade, idoneidade e proporcionalidade da restrição ou exceção, conforme as regras e critérios que estabeleçam os Estados Ibero-Americanos em seu direito interno.

8. Tratamento de dados pessoais de crianças e adolescentes

8.1. No tratamento de dados pessoais relativos a crianças e adolescentes, os Estados Ibero-Americanos privilegiarão a proteção do interesse superior deles, conforme a Convenção sobre os Direitos da Criança e outros instrumentos internacionais que procurem seu bem-estar e proteção integral.

8.2. Os Estados Ibero-Americanos encorajarão, na formação acadêmica das crianças e adolescentes, o uso responsável, adequado e seguro das tecnologias da informação e comunicação, e os eventuais riscos que enfrentam em ambientes digitais respeito do tratamento inadequado de seus dados pessoais, bem como o respeito de seus direitos e liberdades.

9. Tratamento de dados pessoais de caráter sensível

9.1. Por regra geral, o responsável não poderá tratar dados pessoais sensíveis, exceto em quaisquer das seguintes hipóteses:

a. Que forem estritamente necessários para o exercício e cumprimento das atribuições e obrigações expressamente previstas nas normas que regulam sua atuação.

b. Dar cumprimento a um mandado legal.

c. Contar com o consentimento expresso e por escrito do titular.

d. Forem necessários por motivos de segurança nacional, segurança pública, ordem pública, saúde pública ou salvaguarda de direitos e liberdades de terceiros.

9.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer exceções, garantias e condições adicionais para garantir o devido tratamento dos dados pessoais sensíveis, conforme seu direito interno.

Capítulo II

Princípios de proteção de dados pessoais

10. Princípios aplicáveis ao tratamento de dados pessoais

10.1. No tratamento dos dados pessoais, o responsável respeitará os princípios de legitimação, licitude, lealdade, transparência, finalidade, proporcionalidade, qualidade, responsabilidade, segurança e confidencialidade.

11. Princípio de legitimação

11.1. Como regra geral, o responsável só poderá tratar dados pessoais quando surgir alguma das seguintes hipóteses:

a. O titular brindar seu consentimento para uma ou várias finalidades específicas.

b. O tratamento for necessário para cumprir ordem judicial, resolução ou mandado fundado e motivado de autoridade pública competente.

c. O tratamento for necessário para o exercício de faculdades próprias das autoridades públicas ou realizado em virtude de habilitação legal.

d. O tratamento for necessário para o reconhecimento ou defesa dos direitos do titular perante autoridade pública.

e. O tratamento for necessário para a execução de contrato ou pré- contrato, em que o titular for parte.

f. O tratamento for necessário para cumprir uma obrigação legal aplicável ao responsável.

g. O tratamento for necessário para proteger interesses vitais do titular ou de outra pessoa física.

h. O tratamento for necessário por motivos de interesse público estabelecidos ou previstos na lei.

i. O tratamento for necessário para atender aos interesses legítimos perseguidos pelo responsável ou por terceiros, sempre que sobre esses interesses não prevaleçam os interesses ou direitos e liberdades fundamentais do titular que requer da proteção de dados pessoais, especialmente quando o titular for criança ou adolescente. O acima mencionado não será aplicável em tratamentos de dados pessoais realizados por autoridades públicas no exercício de suas funções.

11.2. Tratando-se desse último inciso, entender-se-á amparado pelo interesse legítimo o tratamento de dados pessoais de contato imprescindíveis para a localização de pessoas físicas que prestam serviços ao responsável, com a finalidade de manter qualquer tipo de relação com esta.

12. Condições para o consentimento

12.1. Quando for necessário obter o consentimento do titular, o responsável demonstrará, de maneira indubitável, que o titular ofereceu seu consentimento, seja através de declaração ou de ação afirmativa clara.

12.2. Sempre que for preciso consentimento para tratamento de dados pessoais, o titular poderá revogá-lo em qualquer momento. Para esse fim, o responsável estabelecerá mecanismos simples, ágeis, eficazes e gratuitos.

13. Consentimento para tratamento de dados pessoais de crianças e adolescentes

13.1. Na obtenção do consentimento de crianças e adolescentes, o responsável obterá a autorização do titular do poder familiar ou tutela, conforme disposto nas regras de representação previstas no direito interno dos Estados Ibero-Americanos, ou no caso, solicitará diretamente autorização ao menor de idade, se o direito interno de cada Estado Ibero- Americano estabelecer idade mínima para a concessão direta e sem qualquer representação do titular do poder familiar ou tutela.

13.2. O responsável realizará esforços razoáveis para verificar se o consentimento foi concedido pelo titular do poder familiar ou tutela, ou então, pelo menor diretamente atendendo sua idade de acordo com o direito interno de cada Estado Ibero-Americano considerando a tecnologia disponível.

14. Princípio de licitude

14.1. O responsável tratará os dados pessoais que estiverem em seu poder com rigoroso apego e cumprimento do previsto no direito interno do Estado Ibero-Americano que for aplicável, do direito internacional e dos direitos e liberdades das pessoas.

14.2. O tratamento de dados pessoais realizado por autoridades públicas ficará sujeito às faculdades ou atribuições que o direito interno do Estado Ibero-Americano correspondente lhes conferir expressamente, além do previsto no número acima nos presentes Padrões.

15. Princípio de lealdade

15.1. O responsável tratará os dados pessoais que estiverem em seu poder priorizando

a proteção dos interesses do titular e se abstendo de tratá-los através de meios enganosos ou fraudulentos.

15.2. Aos efeitos dos presentes Padrões, serão considerados desleais os tratamentos de dados pessoais que envolvam discriminação injusta ou arbitrária contra os titulares.

16. Princípio de transparência

16.1. O responsável informará ao titular sobre a existência e características principais do tratamento a que serão submetidos seus dados pessoais, a fim de poder tomar decisões informadas ao respeito.

16.2. O responsável proporcionará ao titular, no mínimo, a seguinte informação:

a. Identidade e dados de contato.

b. As finalidades do tratamento que receberão seus dados pessoais.

c. Comunicações nacionais ou internacionais de dados pessoais que tencione realizar, incluindo destinatários e finalidades que motivam sua realização.

d. A existência, forma e mecanismos ou procedimentos através dos quais exercerá os direitos de acesso, retificação, cancelamento, oposição e portabilidade.

e. No caso, a origem dos dados pessoais quando o responsável não os obtiver diretamente do titular.

16.3. A informação proporcionada ao intitular deve ser suficiente e de fácil acesso, bem como redigida e estruturada em linguagem clara, simples e de fácil compreensão para os titulares aos quais estará dirigida, especialmente se tratando de crianças e adolescentes.

16.4. Todo responsável contará com políticas transparentes para os tratamentos de dados pessoais que realizar.

17.Princípio de finalidade

17.1. Todo tratamento de dados pessoais estará limitado ao cumprimento de finalidades determinadas, explícitas e legítimas.

17.2. O responsável não poderá tratar os dados pessoais em seu poder com fins diferentes dos que motivaram seu tratamento original, exceto pela ocorrência de alguma das causas que possibilitam um novo tratamento dos dados, conforme o princípio de legitimação.

17.3. O tratamento posterior de dados pessoais com fins de arquivamento, pesquisa científica e histórica, ou com fins estatísticos, todos eles em favor do interesse público, não será considerado incompatível com as finalidades iniciais.

18. Princípio de proporcionalidade

18.1. O responsável somente tratará os dados pessoais que forem adequados, pertinentes e limitados para o mínimo necessário em relação às finalidades que justifiquem seu tratamento.

19. Princípio de qualidade

19.1. O responsável adotará as medidas necessárias para manter exatos, completos e atualizados os dados pessoais em seu poder, de maneira tal a não alterar sua veracidade, conforme requerido para o cumprimento das finalidades que motivaram o tratamento.

19.2. Quando os dados pessoais já não sejam necessários para o cumprimento das finalidades que motivaram o tratamento, o responsável os suprimirá ou eliminará de seus arquivos, registros, bases de dados, dossiês ou sistemas de informação, ou no caso, deverá submetê-los a um procedimento de anonimização.

19.3. Na supressão dos dados pessoais, o responsável implementará métodos e técnicas orientadas à sua eliminação definitiva e segura.

19.4. Os dados pessoais somente serão conservados durante o prazo necessário para o cumprimento das finalidades que justifiquem seu tratamento, ou aquelas relacionadas com exigências legais aplicáveis ao responsável. Porém, a legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer exceções respeito do prazo de conservação dos dados pessoais, respeitando totalmente os direitos e garantias do titular.

20. Princípio de responsabilidade

20.1. O responsável implementará os mecanismos necessários para demonstrar o cumprimento dos princípios e obrigações estabelecidas nos presentes Padrões, bem como prestará contas sobre o tratamento de dados pessoais em seu poder para o titular e a autoridade de controle, para o que poderá empregar padrões, melhores práticas nacionais ou internacionais, esquemas de autorregulação, sistemas de certificação ou quaisquer outros mecanismos que determinar adequado para tais fins.

20.2. O acima mencionado corresponderá quando os dados pessoais forem tratados por encarregado em nome e por conta do responsável, bem como no momento de realizar transferências de dados pessoais.

20.3. Entre os mecanismos que o responsável poderá adotar para cumprir com o princípio de responsabilidade encontram-se, de maneira enunciativa mais não limitativa, os seguintes:

a. Alocação de recursos para instrumentação de programas e políticas de proteção de dados pessoais.

b. Implementação de sistemas de gestão de riscos associados com o tratamento de dados pessoais.

c. Elaboração de políticas e programas de proteção de dados pessoais obrigatórios e exigíveis ao interior da organização do responsável.

d. Pôr em prática um programa de capacitação e atualização do pessoal sobre obrigações em matéria de proteção de dados pessoais.

e. Rever de maneira periódica as políticas e programas de segurança de dados pessoais, para determinar as modificações requeridas.

f. Estabelecer um sistema de supervisão e vigilância interna e/ou externa, incluindo auditorias, para verificar o cumprimento das políticas de proteção de dados pessoais.

g. Estabelecer procedimentos para receber e responder dúvidas e reclamações dos titulares.

20.4. O responsável conferirá e avaliará em forma permanente os mecanismos que, para tal efeito, adotar voluntariamente para cumprir com o princípio de responsabilidade, com o objeto de medir seu nível de eficácia quanto ao cumprimento da legislação nacional aplicável.

21. Princípio de segurança

21.1. O responsável estabelecerá e manterá, independentemente do tipo de tratamento que efetuar, medidas de índole administrativa, física e técnica suficientes para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.

21.2. Para a determinação das medidas citadas no número acima, o responsável considerará os seguintes fatores:

a. O risco para os direitos e liberdades dos titulares, em particular, pelo valor potencial quantitativo e qualitativo que pudessem ter os dados pessoais tratados para terceiras pessoas não autorizadas para sua posse.

b. O estado da técnica.

c. Os custos de aplicação.

d. A natureza dos dados pessoais tratados, especialmente dados pessoais sensíveis.

e. Alcance, contexto e finalidades do tratamento.

f. Transferências internacionais de dados pessoais realizadas ou que pretendam ser realizadas.

g. Número de titulares.

h. Possíveis consequências para os titulares derivadas de vulneração.

i. Vulnerações prévias acontecidas no tratamento de dados pessoais.

21.3. O responsável realizará um conjunto de ações visando garantir o estabelecimento, implementação, operação, monitoração, revisão, manutenção e melhoria contínua das medidas de segurança aplicáveis ao tratamento dos dados pessoais, de maneira periódica.

22. Notificação de vulnerações na segurança dos dados pessoais

22.1. Quando o responsável tiver conhecimento de vulneração na segurança dos dados pessoais acontecida em qualquer fase do tratamento, entendida como qualquer dano, perda, alteração, destruição, acesso, e em geral, qualquer uso ilícito ou não autorizado de dados pessoais, mesmo quando acontecer de maneira acidental, notificará à autoridade de controle e aos titulares afetados nesse acontecimento imediatamente.

22.2. O acima mencionado não resultará aplicável quando o responsável puder demonstrar, atendendo ao princípio de responsabilidade proativa, a improbabilidade de vulneração da segurança acontecida, ou que ela não representa risco para os direitos e liberdades dos titulares envolvidos.

22.3. A notificação realizada pelo responsável para os titulares afetados estará redigida em linguagem clara e simples.

22.4. A notificação referida nos números acima conterá, no mínimo, a seguinte informação:

a. Natureza do incidente.

b. Dados pessoais comprometidos.

c. Ações de correção realizadas de forma imediata.

d. Recomendações para o titular sobre medidas que poderia adotar para proteger seus interesses.

e. Meios disponíveis para o titular para obter mais informações sobre a questão.

22.5. O responsável documentará qualquer vulneração à segurança de dados pessoais acontecida em qualquer fase do tratamento, identificando, de maneira enunciativa mais não limitativa, a data em que aconteceu; o motivo da vulneração; os fatos relacionados e seus efeitos e medidas corretivas implementadas de forma imediata e definitiva, que estarão à disposição da autoridade de controle.

22.6. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá os efeitos das notificações de vulnerações de segurança realizadas pelo responsável à autoridade de controle, no referente a procedimentos, forma e condições de intervenção, com o propósito de preservar os interesses, direitos e liberdades dos titulares afetados.

23. Princípio de confidencialidade

23.1. O responsável estabelecerá controles ou mecanismos para que quem intervir em qualquer fase do tratamento dos dados pessoais mantenha e respeite sua confidencialidade, obrigação que continuará, inclusive, após finalizar sua relação com o titular.

Capítulo III

Direitos do titular

24. Direitos ARCO

24.1. Em todo momento, o titular ou seu representante poderão solicitar ao responsável o acesso, retificação, cancelamento, oposição e portabilidade dos dados pessoais relacionados.

24.2. O exercício de quaisquer dos direitos referidos no número acima não é requisito prévio, nem impede o exercício de outro.

25. Direito de acesso

25.1. O titular terá direito de solicitar o acesso a seus dados pessoais em poder do responsável, bem como de conhecer qualquer informação relacionada com as condições gerais e específicas de seu tratamento.

26. Direito de retificação

26.1. O titular terá direito de obter do responsável a retificação ou correção de seus dados pessoais, quando esses resultarem inexatos, incompletos ou não se encontrarem atualizados.

27. Direito de cancelamento

27.1. O titular terá direito de solicitar o cancelamento ou supressão de seus dados pessoais de arquivos, registros, processos e sistemas do responsável, a fim de que já não estejam em seu poder e deixem de ser tratados por este último.

28. Direito de oposição

28.1. O titular poderá se opor ao tratamento de seus dados pessoais quando:

a. Existir razão legítima derivada de situação particular.

b. O tratamento de seus dados pessoais tiver como objetivo marketing direto, incluída a elaboração de perfis, na medida em que estiver relacionada com essa atividade.

28.2 Tratando-se do inciso acima, quando o titular se opuser ao tratamento com fins de marketing direto, seus dados pessoais deixarão de ser tratados para esses fins.

29. Direito a não ser objeto de decisões individuais automatizadas

29.1. O titular terá direito de não ser objeto de decisões que possam produzir efeitos jurídicos ou o afetem de maneira significativa, baseados somente em tratamentos automatizados destinados a avaliar, sem intervenção humana, determinados aspectos pessoais ou analisar ou predizer, em particular, seu rendimento profissional, situação econômica, estado de saúde, preferências sexuais, confiabilidade ou comportamento.

29.2. O previsto no número acima não será aplicável quando o tratamento automatizado de dados pessoais for necessário para a celebração ou execução de contrato entre o titular e o responsável; estiver autorizado pelo direito interno dos Estados Ibero-Americanos, ou tiver como base o consentimento demonstrável do titular.

29.3. Contudo, quando for necessário para a relação contratual ou o

titular tiver manifestado seu consentimento, terá direito de obter intervenção humana; receber uma explicação sobre a decisão tomada; expressar seu ponto de vista e impugnar a decisão.

29.4. O responsável não poderá realizar tratamentos automatizados de dados pessoais que tiverem como efeito a discriminação dos titulares por origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, à vida, preferência ou orientação sexual, bem como dados genéticos ou dados biométricos.

30. Direito à portabilidade dos dados pessoais

30.1. Ao tratar dados pessoais por via eletrônica ou meios automatizados, o titular terá direito de obter cópia dos dados pessoais que informou ao responsável ou que são alvo de tratamento, em formato eletrônico estruturado, de uso comum e leitura mecânica, que permita continuar utilizando-os e transferi-los para outro responsável, em caso necessário.

30.2. O titular poderá solicitar que seus dados pessoais sejam transferidos diretamente de responsável para responsável, quando isso for tecnicamente possível.

30.3. O direito à portabilidade dos dados pessoais não afetará negativamente os direitos e liberdades de outros.

30.4. Sem prejuízo de outros direitos do titular, o direito à portabilidade dos dados pes-

soais não resultará procedente quando for informação inferida, derivada, criada, gerada ou obtida a partir da análise ou tratamento efetuado pelo responsável com base nos dados pessoais informados pelo titular, como o caso dos dados pessoais submetidos a um processo de personalização, recomendação, categorização ou criação de perfis.

31. Direito à limitação do tratamento dos dados pessoais

31.1. O titular terá direito a que o tratamento dos dados pessoais se limite ao armazenamento durante o período decorrido entre uma solicitação de retificação ou oposição até a resolução pelo responsável.

31.2. O titular terá direito à limitação do tratamento de seus dados pessoais quando esses forem desnecessários para o responsável, mas precisar deles para formular uma reclamação.

32. Exercício dos direitos ARCO e de portabilidade

32.1. O responsável estabelecerá meios e procedimentos simples, rápidos, acessíveis e gratuitos que permitam ao titular exercer seus direitos de acesso, retificação, cancelamento, oposição e portabilidade.

32.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá requerimentos, prazos, termos e condições nos quais os titulares poderão exercer seus direitos de acesso, retificação, cancelamento, oposição e portabilidade, bem como as causas de improcedência no exercício que podem ser, de maneira enunciativa mais não limitativa:

a. Quando o tratamento for necessário para cumprir um objetivo importante de interesse público.

b. Quando o tratamento for necessário para exercer as funções próprias das autoridades públicas.

c. Quando o responsável consignar que possui motivos legítimos para que o tratamento prevaleça sobre interesses, direitos e liberdades do titular.

d. Quando o tratamento for necessário para cumprir com disposição legal.

e. Quando os dados pessoais forem necessários para manter ou cumprir uma relação jurídica ou contratual.

32.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá reconhecer que pessoas físicas, vinculadas com falecidos ou designados por eles, possam exercer os direitos referidos no presente padrão, respeito dos dados pessoais de falecido que lhes digam respeito.

32.4. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria reconhecerá o direito do titular de não concordar ou impugnar respostas concedidas pelo responsável

perante uma solicitação de exercício dos direitos aludidos no presente número, ou perante sua falta de resposta junto a autoridade de controle e, no caso, perante instâncias judiciais, conforme o direito interno de cada Estado Ibero-Americano.

Capítulo IV

Encarregado

33. Alcance do encarregado

33.1. O encarregado realizará atividades de tratamento dos dados pessoais sem possuir nenhum poder de decisão sobre o seu alcance e conteúdo, bem como limitará suas atuações aos termos previstos pelo responsável.

34. Formalização da prestação de serviços do encarregado

34.1. A prestação de serviços entre o responsável e o encarregado será formalizada mediante assinatura de contrato ou qualquer outro instrumento jurídico que considerarem os Estados Ibero-Americanos na legislação nacional aplicável na matéria.

34.2. O contrato ou instrumento jurídico estabelecerá, no mínimo, o objeto, alcance, conteúdo, duração, natureza e finalidade do tratamento; tipo de dados pessoais; categorias dos titulares, bem como obrigações e responsabilidades do responsável e encarregado.

34.3. O contrato ou instrumento jurídico estabelecerá, no mínimo, as seguintes cláusulas gerais relacionadas com os serviços prestados pelo encarregado:

a. Realizar o tratamento dos dados pessoais conforme as instruções do responsável.

b. Abster-se de tratar dados pessoais para fins diferentes dos instruídos pelo responsável.

c. Implementar medidas de segurança conforme os instrumentos jurídicos aplicáveis.

d. Informar o responsável do acontecimento de vulneração nos dados pessoais que tratar por suas instruções.

e. Preservar a confidencialidade dos dados pessoais tratados.

f. Suprimir, devolver ou comunicar para um novo encarregado designado pelo responsável os dados pessoais objeto de tratamento, uma vez cumprida a relação

jurídica com o responsável ou por instruções desse, exceto que disposição legal exigir a conservação dos dados pessoais ou que o responsável autorizar sua comunicação a outro encarregado.

g. Abster-se de transferir dados pessoais, salvo no caso em que o responsável assim estabelecer, ou a comunicação derivar de uma subcontratação, ou por pedido expresso da autoridade de controle.

h. Permitir ao responsável ou autoridade de controle inspeções e verificações no local.

i. Gerar, atualizar e conservar a documentação necessária e que permita a acreditação de suas obrigações.

j. Colaborar com o responsável em tudo o relativo ao cumprimento da legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

34.4. Quando o encarregado descumprir as instruções do responsável e decidir por si mesmo sobre o alcance, conteúdo, meios e outras questões do tratamento dos dados pessoais assumirá o caráter de responsável, conforme a legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

35. Subcontratação de serviços

35.1. Por sua vez, o encarregado poderá subcontratar serviços que compreendam o tratamento de dados pessoais, sempre que existir autorização prévia por escrito, específica ou geral do responsável, ou for estipulado expressamente no contrato ou instrumento jurídico subscrito entre este e o encarregado.

35.2. O subcontratado assumirá o caráter de encarregado, nos termos estipulados pela legislação nacional do Estado Ibero-Americano aplicável na matéria.

35.3. O encarregado formalizará a prestação de serviços do subcontratado através de contrato ou de quaisquer outros instrumentos jurídicos determinados pela legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

35.4. Quando o subcontratado descumprir suas obrigações e responsabilidades respeito do tratamento dos dados pessoais, conforme instruído pelo encarregado, assumirá o caráter de responsável segundo a legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

Capítulo V

Transferências internacionais de dados pessoais

36. Regras gerais para transferências de dados pessoais

36.1. O responsável e o encarregado poderão realizar transferências internacionais de dados pessoais em quaisquer dos seguintes casos:

a. O país, parte de seu território, setor, atividade ou organização internacional destinatária dos dados pessoais tiver sido reconhecido com nível adequado de proteção de dados pessoais por parte do país transferente, conforme a legislação nacional desse que resultar aplicável na matéria, ou então, o país destinatário ou vários setores dele consignarem condições mínimas e suficientes para garantir um adequado nível de proteção dos dados pessoais.

b. O exportador ofereça garantias suficientes do tratamento dos dados pessoais no país destinatário, e este, por sua vez, acreditar o cumprimento das condições mínimas e suficientes estabelecidas na legislação nacional de cada Estado Ibero-Americano aplicável na matéria.

c. Exportador e destinatário subscreverem cláusulas contratuais ou qualquer outro instrumento jurídico que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, das obrigações e responsabilidades assumidas pelas partes e dos direitos dos titulares. A autoridade de controle poderá validar cláusulas contratuais ou instrumentos jurídicos segundo determinar na legislação nacional dos Estados Ibero-Americanos aplicável na matéria.

d. Exportador e destinatário adotarem um esquema de autorregulação vinculante ou mecanismo de certificação aprovado, sempre que seja conforme as disposições previstas na legislação nacional do Estado Ibero-Americano aplicável na matéria, que o exportador estará obrigado a observar.

e. A autoridade de controle do Estado Ibero-Americano do país do exportador autorizar a transferência, em termos da legislação nacional que for aplicável na matéria.

36.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer expressamente limites às transferências internacionais de categorias de dados pessoais por razões de segurança, segurança pública, proteção à saúde pública, proteção dos direitos e liberdades de terceiros, bem como questões de interesse público.

Capítulo VI

Medidas proativas no tratamento de dados pessoais

37. Reconhecimento de medidas proativas

37.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá reconhecer e estabelecer medidas que promovam o melhor cumprimento de sua legislação e coadjuvem no fortalecimento e aumento dos controles de proteção de dados pessoais implementados pelo responsável, entre os quais poderão se encontrar as indicadas abaixo no presente Capítulo.

38. Privacidade por projeto e privacidade por defeito

38.1. O responsável aplicará, a partir do projeto, na determinação dos meios de tratamento dos dados pessoais, durante e antes de solicitar os dados pessoais, medidas preventivas de diversa natureza que permitam aplicar de maneira efetiva princípios, direitos e outras obrigações previstas na legislação nacional do Estado Ibero-Americano que lhe for aplicável.

38.2. O responsável garantirá que seus programas, serviços, sistemas ou plataformas informáticas, aplicações eletrônicas ou qualquer outra tecnologia que impliquem tratamento de dados pessoais, cumpram por defeito ou se ajustem aos princípios, direitos e outras obrigações previstas na legislação nacional do Estado Ibero-Americano que lhe for aplicável. Especificamente, somente com o fim de serem objeto de tratamento os mínimos dados pessoais e limitar a acessibilidade deles, sem a intervenção do titular, a um número indeterminado de pessoas.

39. Oficial de proteção de dados pessoais

39.1. O responsável designará um oficial de proteção de dados pessoais ou figura equivalente, nos casos estabelecidos pela legislação nacional dos Estados Ibero-Americanos aplicável na matéria e quando:

a. For autoridade pública.

b. Realizar tratamentos de dados pessoais que tiverem como objeto a observação habitual e sistemática da conduta do titular.

c. Realizar tratamentos de dados pessoais onde for provável um alto risco de afetação do direito à proteção de dados pessoais dos titulares, considerando, entre outros fatores e de maneira enunciativa mais não limitativa, categorias de dados pessoais tratados, especialmente se tratando de dados sensíveis; transferências efetuadas; número de titulares; alcance do tratamento; tecnologias de informação utilizadas ou finalidades destes.

39.2. O responsável que não se encontrar nalguma das causas previstas no número acima, poderá designar um oficial de proteção de dados pessoais, se assim estimar conveniente.

39.3. O responsável estará obrigado a apoiar o oficial de proteção de dados pessoais no desempenho de suas funções, facilitando os recursos necessários para seu desempenho e para a manutenção de seus conhecimentos especializados e a atualização desses.

39.4. O oficial de proteção de dados pessoais terá, no mínimo, as seguintes funções:

a. Assessorar o responsável respeito dos temas submetidos a sua consideração em matéria de proteção de dados pessoais.

b. Coordenar, no interior da organização do responsável, políticas, programas, ações e outras atividades que correspondam com o cumprimento da legislação nacional do Estado Ibero-Americano que resultar aplicável na matéria.

c. Supervisionar no interior da organização do responsável o cumprimento da legislação nacional do Estado Ibero-Americano que resultar aplicável na matéria.

40. Mecanismos de autorregulação

40.1. O responsável poderá se aderir, de maneira voluntária, a esquemas de autorregulação vinculante, cujos objetos forem, entre outros, contribuir para a correta aplicação da legislação nacional do Estado Ibero- Americano que resultar aplicável na matéria e estabelecer procedimentos de resolução de conflitos entre o responsável e o titular, sem prejuízo de outros mecanismos estabelecidos pela legislação nacional da matéria aplicável, considerando as características específicas dos tratamentos de dados pessoais realizados, bem como o efetivo exercício e respeito dos direitos do titular.

40.2. Aos efeitos do número acima, será possível desenvolver, entre outros, códigos deontológicos e sistemas de certificação e seus respectivos selos de confiança, que contribuam para os objetivos assinalados no presente número.

40.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regras que correspondam para a validação, confirmação ou reconhecimento dos mecanismos de autorregulação aludidos.

41. Avaliação de impacto na proteção de dados pessoais

41.1. Quando o responsável pretenda realizar um tipo de tratamento de dados pessoais que, por sua natureza, alcance, contexto ou finalidades, envolva a probabilidade de um alto risco de afetação do direito à proteção de dados pessoais dos titulares, realizará, de maneira prévia à implementação, uma avaliação do impacto na proteção dos dados pessoais.

41.2. A legislação nacional dos Estados Ibero-Americanos que for aplicável na matéria assinalará aqueles tratamentos que demandem avaliação de impacto na proteção de dados pes-

soais; o conteúdo dessas, as hipóteses nas quais corresponder a apresentação do resultado perante autoridade de controle, bem como os requerimentos da apresentação, entre outras questões.

Capítulo VII

Autoridades de controle

42. Natureza das autoridades de controle e supervisão

42.1. Em cada Estado Ibero-Americano deverá existir uma ou mais autoridades de controle em matéria de proteção de dados pessoais com plena autonomia, conforme a legislação nacional aplicável na matéria.

42.2. As autoridades de controle poderão ser órgãos unipessoais ou pluripessoais; atuarão com caráter imparcial e independente em seus poderes, bem como serão alheias a qualquer influência externa, seja direta ou indireta, e não solicitarão nem admitirão ordem nem instrução alguma.

42.3. O membro ou os membros dos órgãos de direção das autoridades de controle contarão com experiência e aptidões, especialmente respeito do âmbito de proteção de dados pessoais, necessários para cumprir suas funções e exercer seus poderes. Serão nomeados, mediante procedimento transparente em virtude da legislação nacional aplicável, e somente poderão ser removidos por causas graves estabelecidas no direito interno de cada Estado Ibero-Americano, conforme as regras do devido processo.

42.4. A legislação nacional dos Estados Ibero-Americanos que resultar aplicável na matéria deverá conceder às autoridades de controle poderes suficientes de investigação, supervisão, resolução, promoção, sanção e outros que resultarem necessários para garantir seu efetivo cumprimento, bem como o exercício e respeito efetivo do direito à proteção de dados pessoais.

42.5. As decisões das autoridades de controle somente estarão sujeitas ao controle jurisdicional, conforme os mecanismos estabelecidos na legislação nacional dos Estados Ibero-Americanos que for aplicável na matéria e seu direito interno.

42.6. As autoridades de controle contarão com os recursos humanos e materiais necessários para o cumprimento de suas funções.

Capítulo VIII

Reclamações e Sanções

43. Regime de reclamações e imposição de sanções

43.1. Todo titular terá direito de apresentar sua reclamação perante uma autoridade de controle, bem como de recorrer da tutela judicial para tornar efetivos seus direitos, conforme a legislação nacional do Estado Ibero-Americano aplicável na matéria.

43.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regime que permitirá ao titular apresentar uma reclamação perante a autoridade de controle quando considerar que o tratamento de seus dados pessoais infringe o regulamento nacional na matéria, assim como solicitar tutela judicial.

43.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regime que permita adotar medidas corretivas e sancionar condutas que contravenham o disposto nas legislações nacionais correspondentes, indicando, no mínimo, o limite máximo e os critérios objetivos para fixar as correspondentes sanções a partir da natureza, gravidade, duração da infração e suas consequências, bem como as medidas implementadas pelo responsável para garantir o cumprimento de suas obrigações na matéria.

Capítulo IX

Direito de indenização

44. Reparação do dano

44.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria 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.

44.2. O direito interno dos Estados Ibero-Americanos indicará a autoridade competente para receber este tipo de ações apresentadas pelo titular afetado, bem como prazos, requerimentos e termos através dos quais será indenizado, em caso de corresponder.

Capítulo X

Cooperação internacional

45. Estabelecimento de mecanismos de cooperação internacional

45.1. Os Estados Ibero-Americanos poderão adotar mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais correspondentes na matéria, os quais poderão compreender, de maneira enunciativa mais não limitativa:

a. O estabelecimento de mecanismos que permitam reforçar a assistência e cooperação internacional na aplicação das respectivas legislações nacionais na matéria.

b. A assistência entre as autoridades de controle através da notificação e remissão de reclamações, assistência em investigações e intercâmbio de informação.

c. A adoção de mecanismos voltados para o conhecimento e intercâmbio das melhores práticas e experiências em matéria de proteção de dados pessoais, inclusive no relativo a conflitos de jurisdição com terceiros países.