



**CENTRO UNIVERSITÁRIO DE LAVRAS
CURSO DE GRADUAÇÃO EM DIREITO**

**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: ANÁLISE DA SUA
ESTRUTURA ATRAVÉS DE UMA PERSPECTIVA DE DIREITO COMPARADO**

LUCAS DE SOUZA GIMENES

**LAVRAS-MG
2020**

LUCAS DE SOUZA GIMENES

**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: ANÁLISE DA SUA
ESTRUTURA ATRAVÉS DE UMA PERSPECTIVA DE DIREITO COMPARADO**

Monografia apresentado ao Centro
Universitário de Lavras, como parte das
exigências do curso de Bacharelado
em Direito.

ORIENTADOR

Prof. Me. Guilherme Scodeler de Souza Barreiro

**LAVRAS-MG
2020**

Ficha Catalográfica preparada pelo Setor de Processamento Técnico
da Biblioteca Central do UNILAVRAS

G491a Gimenes, Lucas de.
 Autoridade Nacional de Proteção de Dados: análise de
sua estrutura através de uma perspectiva de Direito
Comparado; orientação de Guilherme Scodeler de Souza
Barreiro. -- Lavras: Unilavras, 2020.
 62 f.

 Monografia apresentada ao Unilavras como parte das
exigências do curso de graduação em Direito.

 1. Direito Digital. 2. Proteção de Dados. 3. Autoridades de
Proteção de Dados. I. Barreiro, Guilherme Scodeler de
Souza (Orient.). II. Título.

LUCAS DE SOUZA GIMENES

**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: ANÁLISE DA SUA
ESTRUTURA ATRAVÉS DE UMA PERSPECTIVA DE DIREITO COMPARADO**

Monografia apresentado ao Centro
Universitário de Lavras, como parte das
exigências do curso de Bacharelado
em Direito.

APROVADO EM: 21/10/2020

ORIENTADOR

Prof. Me. Guilherme Scodeler de Souza Barreiro / UNILAVRAS

MEMBRO DA BANCA

Prof. Pós-Dr. Denilson Victor Machado Teixeira / UNILAVRAS

**LAVRAS-MG
2020**

À minha mãe, Nívea.

*Vais ficar a olhar?
Começa por baixo
Começa com teu braço direito
O caminho até o topo é estreito
Mas tu vais lá chegar
E quando isso acontecer
Começa de novo.*

(Na vitrine de uma loja em Lisboa)

RESUMO

Introdução: As sociedades atuais são demarcadas pelo crescente avanço tecnológico e, em decorrência a isso, pelo aumento exponencial de informações pertencentes a uma pessoa, em especial aquelas atreladas à internet. Na busca pela proteção de todos esses dados, diversos países tem se prontificado a estabelecer legislações que efetivem a privacidade dos indivíduos no uso da rede, e, afim de efetivar isso, tais legislações também buscaram a criação de entidades públicas que fiscalizassem a aplicação da lei frente aos organismos públicos e privados enquanto esses tratassem os dados das pessoas físicas, essas estruturas são chamadas de Autoridades de Proteção de Dados. **Objetivo:** analisar as disposições relativas as Autoridades de Proteção de Dados existentes no ordenamento argentino, uruguaio, europeu e também no brasileiro a fim de que se possa observar as semelhanças e diferenças entre estes. **Metodologia:** A pesquisa é eminentemente qualitativa, e baseia-se em uma revisão bibliográfica e documental a respeito da Proteção de Dados e da Privacidade, utilizando-se eminentemente de uma análise de direito comparado. **Resultados:** Constatou-se que as Autoridades de Proteção de Dados devem, para ter uma atuação efetiva, gozar de independência, dessa maneira, foi observado que em muitos aspectos a Autoridade Nacional de Proteção de Dados parece com da Argentina e do Uruguai e também com o modelo europeu, mas que também demonstra características que poderá estar fatalmente subordinada às vontades do poder executivo federal. **Conclusão:** Apesar de que várias disposições da Lei Geral de Proteção de Dados Pessoais demonstrarem que os trabalhos legislativos tentaram resguardar uma atuação autônoma e independente para a autoridade brasileira, na prática, muitos debates e reformulações legislativas serão necessárias para que isso ocorra.

Palavras-chave: Autoridade Nacional de Proteção de Dados; Direito Digital; Privacidade; Proteção de Dados; Tecnologia;

LISTA DE SIGLAS

AGESIC	<i>Agencia de Gobierno Eletronico y Sociedad de la informacion y del Conocimiento</i>
ANPD	Autoridade Nacional de Proteção de Dados
APD	Autoridade de Proteção de Dados
ARPA	Advanced Research Project Agency
DPA	<i>Data Protection Authority</i>
EUA	Estados Unidos da América
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
RGPD	Regulamento Geral de Proteção de Dados
URSS	União das Repúblicas Socialistas Soviéticas
WWW	<i>World Wide Web</i>

SUMÁRIO

1 INTRODUÇÃO.....	9
2 REVISÃO DA LITERATURA	11
2.1 A NOVA SOCIEDADE INFORMATIZADA: BREVE HISTÓRICO DO SURGIMENTO DA INTERNET E DA DISSEMINAÇÃO DE INFORMAÇÕES PELA TECNOLOGIA.....	12
2.2 A INCIDÊNCIA DO DIREITO SOBRE A TECNOLOGIA: AS NOVAS REGULAMENTAÇÕES.....	15
2.3 HISTÓRICO SOBRE A PROTEÇÃO DOS DADOS PESSOAIS.....	20
2.3.1 A proteção de dados no contexto europeu: do seu surgimento a criação do Regulamento Geral de Proteção de Dados.....	21
2.3.2 A criação do sistema de proteção de dados pessoais na sociedade brasileira: considerações sobre a LGPD.....	24
2.4. AUTORIDADES DE PROTEÇÃO DE DADOS	27
2.4.1 As autoridades de Proteção de Dados Europeias: análise do modelo europeu e de sua contribuição para os demais países.....	28
2.4.2 Autoridade de Proteção de Dados no Contexto Argentino ...	32
2.4.3 Autoridade de Proteção de Dados no Contexto Uruguaio	36
2.4.4 Autoridade Nacional de Proteção de Dados Brasileira.....	40
2.5 COMPARATIVO ENTRE AS ATIVIDADES DESEMPENHADAS PELAS AUTORIDADES DE PROTEÇÃO DE DADOS: COMO ESTÁ A AUTORIDADE BRASILEIRA FRENTE AS DEMAIS AUTORIDADES DE PROTEÇÃO DE DADOS?	46
3 CONSIDERAÇÕES GERAIS.....	52
4 CONCLUSÃO	55
REFERÊNCIAS	57

1 INTRODUÇÃO

O avanço tecnológico é uma figura demarcada pela dialética, de um lado, significa a quebra das barreiras temporais e territoriais, facilitando a comunicação e a disseminação de informações, enquanto, de outra parte, é sinônimo da maior exposição das pessoas e de seus dados pessoais frente aos provedores de aplicação ou às tecnologias empregadas nas *smart cities*, diminuindo drasticamente a intimidade.

Nesse escopo, diversos países têm se dedicado a criação de leis que objetivam a garantia da proteção dos dados pessoais de seus indivíduos, de maneira que, para isso, surgiram autoridades públicas de caráter regulatório e fiscalizatório sobre a matéria.

Enquanto países vizinhos, como a Argentina e o Uruguai, possuem uma cultura de proteção de dados enraizada há mais tempo, o Brasil tem dado seus passos iniciais na matéria e na estruturação da Autoridade Nacional de Proteção de Dados, de modo que o seu papel e a importância de suas funções é ainda muito abstrato.

Essa pesquisa traz como seu objetivo analisar se as autoridades nacionais de proteção de dados do Brasil, da Argentina, do Uruguai, assim com o modelo constituído na União Europeia, se assemelham em suas funções, objetivos e também em sua estrutura administrativa dentro de seus países de forma a criar um modelo a respeito da proteção de dados em escopo mundial.

Dessa forma, a problemática que se traz ao trabalho pode ser traduzida através da seguinte pergunta: estará a Autoridade Nacional de Proteção de Dados em conformidade com as demais Autoridades a fim de promover a Proteção de Dados Pessoais?

Tem-se como a hipótese a de que a Autoridade Nacional de proteção de Dados irá guardar acentuada correspondência com os modelos criados nos demais países aqui analisados, de maneira que se mostrará apta ao exercício de suas atribuições a fim de efetivar a proteção de dados e de também viabilizar as transferências internacionais de dados.

Em razão de que a proteção de dados torna-se uma preocupação cada vez mais acentuada para todos os países do globo, a presente pesquisa se justifica sobre o fato de que pensar a respeito das possíveis correlações existentes entre a Autoridade Nacional de Proteção de Dados brasileira e a dos demais países aqui elen-

cados irá permitir tecer considerações sobre a atuação e o caminho que a ANPD irá traçar ao longo de seus primeiros anos como principal instrumento para garantir a eficácia da Lei.

Quanto aos principais elementos metodológicos que constituem a presente pesquisa, é preciso destacar que sua abordagem é de natureza qualitativa, buscando compreender o fenômeno em si,

De outro liame, sua natureza é de pesquisa aplicada, já que seu interesse é na solução de um problema de pesquisa local o qual seja a compreensão da estruturação e das funções da Autoridade Nacional de Proteção de Dados.

Trata-se de uma pesquisa com viés exploratório, já que através dos métodos aqui empregados busca-se obter maior familiaridade com o problema apresentado, além de no decorrer de sua execução, torna-lo mais explicito.

No que concerne aos procedimentos empregados, esse pesquisa científica é demarcada majoritariamente por uma revisão bibliográfica onde serão analisados desde as doutrinas a cerca da proteção de dados e da privacidade e também por meio de artigos científicos de estudiosos dessas temáticas de autores provenientes do Brasil, Argentina, Uruguai e União Europeia, bem como livros e texto científicos que tratem a respeito do direito regulatório.

É preciso também destacar que todo estudo aqui realizado se apresentará através de uma metodologia de direito comparado, de maneira que passará ao estudo pormenorizado das legislações da União Européia, argentina, uruguaia e também brasileira a respeito da Proteção de Dados Pessoais e Privacidade bem como sobre suas Autoridades de Proteção de Dados.

No primeiro capítulo, busca-se delimitar os conceitos de tecnologia da informação e levantar um histórico a cerca do surgimento da internet, de sobremaneira se possa caracterizar a sociedade de informação, tão essencial para as determinações sobre a Proteção de Dados.

No segundo capítulo, o que se pretende trazer reflexões a respeito da relação existente entre a Tecnologia e o Direito, e os feitos que produzem um ao outro. Dá-se enfoque especial para os debates que surgiram a cerca da regulação estatal sob o domínio da internet ainda na década de 1990.

O terceiro capítulo deste trabalho irá realizar um resgate histórico da evolução legislativa a respeito da Proteção de Dados Pessoais e Privacidade, tanto na União Européia quanto no Brasil.

O primeiro item será destinado a análise das leis sobre a Proteção de Dados na Europa a partir da década de 1950, vendo diversos tratados e regulamentos que foram positivados sobre a matéria, até que se faça uma análise do atual Regulamento Geral de proteção de Dados, referenciando a técnica legislativa sobre a matéria.

O segundo item dedica-se a analisar as leis que tratam da a respeito dos dados no ordenamento jurídico brasileiro e, em seguida, passa ao estudo do processo legislativo para a criação da legislação e corrente estudo da Lei Geral de Proteção de Dados

No quarto capítulo, busca-se construir o conceito que abarca a Autoridade de Proteção de Dados nos diferentes cenários e, em especial, dar corpo e forma para ANPD, de maneira a conhecer de seu funcionamento e da sua eficácia em um método comparativo.

Para isso, no primeiro item tem-se por finalidade delimitar a sistemática envolvendo as autoridades no conceito europeu, tão fundamental a ponto de ser o predecessor e a inspiração das estruturas regulatórias desenvolvidas em outros países. determinando as características que serão essenciais para a constituição de uma Autoridade de Proteção de Dados.

No segundo e terceiro item serão analisados, respectivamente, as figuras existentes no cenário da Argentina e do Uruguai, delimitando o contexto legislativo da proteção de dados nesses países e também analisando estruturalmente as APDs, a fim de que se possa traçar futuramente o quadro comparativo entre ambas os organismos e a Autoridade brasileira.

Já no último item pretende-se traçar exhaustivamente a figura da Autoridade Nacional de Proteção de Dados, compreendendo inicialmente os debates legislativos que cercaram a sua criação e após disso, a análise de suas características essenciais nos ditames da lei.

O último capítulo terá a aplicação preponderante do método de Direito Comparado, fazendo a análise das disposições dos diversos ordenamentos aqui estudados sobre as autoridades de Proteção de Dados.

2 REVISÃO DA LITERATURA

2.1 A NOVA SOCIEDADE INFORMATIZADA: BREVE HISTÓRICO DO SURGIMENTO DA INTERNET E DA DISSEMINAÇÃO DE INFORMAÇÕES PELA TECNOLOGIA

A sociedade moderna, demarcada pela acentuada evolução tecnológica e também pela hiperconexão a rede, é uma construção plural fruto dos mais diversos acontecimentos e invenções oriundas do século anterior, e, mais precisamente, das tecnologias destinadas a transmissão de comunicações e informações que foram surgindo e se aprimorando.

A formação de todo o aparato tecnológico que individualiza tão profundamente bem a civilização atual, tem sua origem em um ponto um pouco mais remoto da história humana, retomando aos primórdios da criação dos primeiros aparelhos de transposição das informações por meio da utilização de cabos e de ondas sonoras.

No século XVII, a invenção de Samuel Finley Breese Morse foi a primeira do gênero ao permitir a transmissão de mensagens por intermédio de um telégrafo entre linhas fixada nas cidades de Baltimore e Washington-DC, nos Estados Unidos da América (LEWIS, 2003 *apud* MARINELI, 2019).

Alexander Graham Bell, anos depois, faria surgir o primeiro aparelho telefônico, permitindo que se transmitisse sons de voz através de uma rede de cabos que conectavam um ponto a outro (LEWIS, 2003 *apud* MARINELI, 2019).

Esses inventos culminaram nas atuais formas de comunicação e disponibilização de informações conhecidas atualmente, afinal, computadores, *tablets* e *smartphones*, especialmente quando conectados as redes de internet, são os atuais aparelhos que demarcam a sociedade de informação.

Sobre o conceito de internet, Marcello Pova (2000) delimita-a como se tratando de uma rede formada por pessoas que produzem conteúdos e, por meio de computadores, destinam-os para outras pessoas, que, através de outras máquinas, se conhecem e também criam seus próprios conteúdos.

Já Corrêa (2000) conceitua internet como sendo um sistema de nível global, que permite às pessoas que se comuniquem e transfiram arquivos de um computador para outro. Para o autor, a internet possibilitaria o intercâmbio capaz de

criar diversos novos mecanismos de relacionamento, já que a transferência de informações ocorreria através da rede de maneira rápida e eficiente, sem se limitar com as fronteiras territoriais.

Por outro lado, Pinheiro (2012) observa que a internet é bem mais do que apenas a comunicação e a transferência de mídias entre sistemas de computador, mas, em especial, formada por indivíduos que a ela integram, sejam estas pessoas físicas ou jurídicas, como governos, instituições filantrópicas ou empresas.

Lemos (2005, p.16), observa que a estrutura da rede é composta pelo "conjunto de computadores que a compõem e pelos meios físicos que os interconectam, como fibras ópticas, linhas telefônicas, ondas de rádio, etc."

Dessa forma, a internet deve ser compreendida como um uma ferramenta de comunicação, um método de transmissão de informações, ideias e experiências entre seus usuários em um ambiente virtual, mas que para seu acesso depende do uso de máquinas e equipamentos de hardware.

Entretanto, por mais que a "era *on-line*" hoje signifique avanço, progresso e até um sinal de felicidade para todos aqueles que dela participam, o seu surgimento, diferente de tudo isso, foi demarcado pela instabilidade política provocada pela tensão existente entre os Estado Unidos da América e a URSS durante o período de Guerra Fria.

Dessa maneira, a internet apareceu primeiro como um invento do governo dos EUA, cuja finalidade maior era de interligar as diversas bases militares norte-americanas em um sistema de comunicação único, de tal maneira que em um ataque de mísseis inimigos, as informações existentes naquela base não se perdessem por causa da destruição (MARINELI, 2019).

Foi na década de 1960 que a Advanced Research Project Agency, denominada pela sigla ARPA, que tinha como função a realização de diversos projetos militares, acabou criando o sistema nomeado de ARPANet, composto por cabos subterrâneos interligados que formavam uma rede de transmissão de informações capaz de ligar as instalações militares estadunidenses aos centros de pesquisa do governo americano (MARINELI, 2019).

Contudo, somente em meados da década de 1980 que o sistema desenvolvido pela ARPA seria liberado para uso em universidades norte-americanas,

entretanto, naquele momento, restringia-se a divulgações e troca de conhecimento acadêmico produzidos naquelas mesmas universidades (PINHEIRO, 2012).

A internet, da maneira como se conhece hoje, surgiria no ano de 1987, sendo uma derivação do sistema ARPANet, com o propósito de uso para finalidade comerciais e civis. Popularizando-se ainda mais na década de 1990, com o surgimento do *World Wide Web* (www)¹ (PINHEIRO, 2012).

Na atualidade, a internet é demarcada pela sua caracterização universal e aberta, a qual permite, dentro da autossuficiência da rede, a constante troca de informações, sem que para isso se faça necessária a participação de um ente central supervisor (CARVALHO, 2018).

Consoante Ferraro (2018) a internet conseguiu romper todas as barreiras que lhe foram impostas quando definido seu objetivo de criação e, hoje é presente na sociedade de maneira a alterar as relações educacionais, trabalhistas, o próprio mercado e também hábitos e questões culturais dos povos e países que ela se posiciona.

Enquanto fenômeno disruptivo que é, a internet se mostra o prelúdio da revolução tecnológica que se veria a partir dos anos 2000, e também para propulsionar uma nova forma de organização social, denominada de sociedade da informação.

A respeito desse conceito, o estudo intitulado de "A sociedade de informação no Brasil - Livro verde", organizado pelo Ministério da Ciência e Tecnologia, destaca que:

A sociedade de 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, afetada pela infraestrutura de informações disponível. É também acentuada a sua dimensão político-econômica, decorrente da contribuição da infraestrutura de informações para que as regiões sejam mais ou menos atraentes em relação a 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 de seu elevado potencial de promover a integração, ao reduzir a distancia entre as pessoas e aumentar o seu nível de informação (BRASIL, 2000, p. 5).

¹ Ainda que os termos Internet e Word Wide Web possam parecer sinônimos para a maioria das pessoas, é preciso notar que eles não se confundem. Conforme a doutrina de Marcel Leonardi (2019), enquanto a internet deve ser entendida como um sistema, uma rede de comunicação e de transmissão de informações, o WWW é apenas a maneira que se usa para ter acesso a essa rede.

O que se tem aqui é uma espécie de revolução digital, por meio da qual se permite um maior armazenamento das informações em um único local, ao passo que também se facilita o acesso a esses mesmos dados, tudo de uma maneira que se organize a dar vida a esse novo modelo social e de uma nova economia (BIONI, 2019).

Não somente isso, o avanço tecnológico, cada vez mais abrangente, chega a fazer com que se tornem factíveis ideias que há tempos pareciam ilusórias, como, por exemplo, o uso recorrente da inteligências artificial para diversas atividades, tais como ditar um texto à um software para que esse seja transcrito em palavras ou então analisar o *score* de crédito de uma pessoa que se submete a aquisição de um cartão de crédito.

Magrani (2018) assevera que atualmente permite-se, em larga escala, que diversos dispositivos tecnológicos possam tomar decisões e realizar avaliações e tantas outras ações que antes eram somente realizadas pelos humanos, de tal maneira que as implicações éticas decorrentes disso ainda necessitam serem analisadas em virtude de quão recente são tais fenômenos.

A tecnologia expandiu-se também para o campo das políticas públicas de tal maneira que é possível que inúmeros governos busquem aplicar as tecnologias dentro do ambiente público das cidades de forma que se faz possível melhorar a qualidade de serviços públicos, manejar com maior efetividade os recursos e receitas do estado e também ampliar a relação existente entre o governo e os seus governados (ZATARAIN, 2018).

Frente a tantas mudanças, o cenário tecnológico torna-se uma preocupação para diversos ramos da ciências humanas, os quais buscam estudar desde a sua origem até seus efeitos que serão causa de transformações profundas na estrutura social. Entre elas está o Direito.

2.2 A INCIDÊNCIA DO DIREITO SOBRE A TECNOLOGIA: AS NOVAS REGULAMENTAÇÕES

Álvaro Vieira Pinto (2005, p.41) definindo o conceito de tecnologia, asseverou que esta seria capaz de “embriagar a consciência das massas, fazendo-as crer que

têm a felicidade momentânea de viver nos melhores tempos jamais desfrutados pela humanidade”.

Não seria difícil concordar com o proposto pelo autor, afinal, é uma presunção quase que absoluta que o progresso tecnológico é, ao mesmo tempo, também o progresso social, e que com isso as novas tecnologias tornarão mais fácil a vida de seus usuários e, conseqüentemente, criarão uma sensação de bem-estar e comodidades nunca vista antes na história.

Ocorre que, o avanço das tecnologias produzem uma série de conseqüências em decorrência do seu surgimento, de sobremaneira que daí resultam uma série de questões jurídicas, onde, devido a falta de regulação estatal, associada juntamente a ignorância legislativa a respeito da matéria, trazem efeitos desastrosos, que no mais podem impedir o uso livre dessas novas ferramentas ou então criar um estado de insegurança a ponto de que não se proteja efetivamente os direitos de seus usuários. Isso, pode-se dizer, seria uma espécie de mal-estar, quase que como um efeito colateral do avanço da tecnologia.

Assim, a possibilidade da transformação do direito tenta trazer maior estabilidade a essas questões, de forma que a positivação de regulamentações para as novas técnicas permite nortear os efeitos que poderão causar na esfera patrimonial ou dos direitos da personalidade.

Concomitante a isso, percebe-se que são as vontades sociais que irão coordenar a feitura de tais normas, e na seara do direito digital e das questões relativas a internet, esse interesse comum faz-se primordial para garantir a elaboração de novas leis (PINHEIRO, 2012).

Marcel Leonardi (2011) atesta que a internet não exige apenas que surjam novas soluções para os problemas relativos a internet e as tecnologias, mas que também é preciso considerar que a forma que se analisará os problemas e as respostas jurídicas também deve ser repensada.

Para Doneda (2019) é necessário que se tenha como ponto de partida a conscientização dos efeitos das tecnologias perante a sociedade, seguida da reflexão a respeito da importância do ordenamento jurídico como garantidor e defensor de valores fundamentais que estão em jogo no uso de tais inventos tecnológicos.

Essas considerações, não obstante, remontam há uma antiga discussão iniciada ainda na década de 1990, quando a internet veio a popularizar-se e a tornar-se parte do dia a dia da maioria das pessoas. Foi, então, nesse período histórico que se iniciou a primeira discussão a respeito da possibilidade de regulamentar ou não a internet.

Surgiram nessa época duas vertentes: uma, que acreditava que a regulação da rede se daria pela atuação dos próprios provedores de serviço e de mecanismos existentes na própria internet, através de parâmetros e normas internas dessas próprias organizações; e a outra corrente, defensora de que apenas uma regulação estatal seria genuinamente eficiente para barrar qualquer violação que ocorresse dentro da rede.

Mais precisamente, esses grupos eram denominados, respectivamente, de Liberais e Realistas (CARVALHO, 2018).

Para os primeiros - os liberais- a internet deveria ser entendida como um lugar único, diferente até mesmo dos países. Seria, dessa forma, o ciberespaço, respaldando-se unicamente pelo seu próprio código de conduta e resolvendo seus conflitos de maneira rápida e célere através de mecanismos que os próprios agentes da rede iriam construir e efetivar.

Em 1996, foram publicados as primeiras obras (BARLOW, 1996; JHONSON; POST, 1996) que proclamariam a independência da rede contra as regulações advindas dos Estados nacionais, e também de organismos supranacionais.

Entre eles, o documento denominado de Declaração de Independência do Ciberespaço, que fora escrito por John Perry Barlow, tinha como finalidade a de quase ser um manifesto anarquista, o qual pregava a necessária abstenção estatal no que concernia a regulamentação do ambiente da internet.

Nos parágrafos iniciais, Barlow orienta seu discurso a ordenar aos estados que não interferissem na internet:

Governos do Mundo Industrial, vocês, gigantes desgastados de carne e aço, eu venho do Ciberespaço, o novo lar da Mente. Em nome do futuro, peço a vocês do passado para nos deixar em paz. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nos reunimos. Não temos um governo eleito, nem é provável que tenhamos um, por isso lhes dirijo com maior autoridade do que aquela com a qual a própria liberdade sempre fala. Declaro que o espaço social global que estamos construindo é naturalmente independente das tiranias que vocês pretendem impor sobre nós. Vocês não têm o direito moral de nos governar nem possuem quaisquer métodos de coação sobre os quais tenhamos real motivo para temer. (BARLOW, 1996 - Tradução nossa)

Barlow, então, trouxe em suas reflexões duros questionamentos a respeito da possibilidade de atuação dos Estados e das organizações de caráter internacional dentro da Internet.

Para ele, a atuação desses organismos se consubstanciaria em uma manifestação completamente tirânica, na qual os países nada mais seriam do que governantes apóstatas que tomariam o controle de uma estrutura a qual não os pertence e que não poderiam controlar. Dessa maneira, essa regulação seria muito semelhante a uma ditadura como aquelas que a humanidade já enfrentou.

Na mesma linha do pensamento liberal, David Johnson e David Post, argumentam no artigo *Law and Borders – The rise of the law in Cyberspace*, que a regulamentação estatal sobre a internet seria uma ideia limitada, e incapaz de conseguir ser bem sucedida:

Esta nova fronteira define um ciberespaço distinto, que pode e precisa criar sua própria lei e instituições legais. Legisladores e autoridades de aplicação da lei delimitadas territorialmente veem este novo ambiente como profundamente ameaçador. Mas essas autoridades ainda podem reconhecer os esforços de autorregulação dos participantes do ciberespaço que se preocupam mais com o novo mercado digital em ideias, informações e serviços. Separadas das doutrinas ligadas às jurisdições territoriais, novas regras surgirão para governar uma ampla gama de novos fenômenos que não têm um paralelo claro no mundo não virtual. Estas novas regras irão desempenhar o papel de lei, definindo a personalidade jurídica e a propriedade, resolvendo disputas e consolidando uma conversa coletiva sobre os valores centrais dos participantes online (JHONSON; POST, 1996, p. 1367)

Dessa maneira, a rede seria capaz de criar mecanismos próprios de controle, garantindo a boa convivência entre os próprios usuários. O Estado, por sua vez, apenas dificultaria esse processo, tornando-o mais caro e mais demorado na solução de conflitos, além de, obviamente, não resolver os problemas das fronteiras nacionais e nem dirimir qual legislação seria a pertinente para julgar conflitos que sejam de características transnacionais.

É simples delimitar até onde vão os limites dos ordenamentos jurídicos das nações, em especial na época em que as únicas delimitações que os países conheciam eram suas próprias fronteiras geográficas, no entanto, a partir do momento que a internet permitiu que ocorressem as trocas informacionais entre pessoas de diferentes países, culturas e convicções, os impactos das condutas realizadas e ideias exprimidas no ambiente on-line passaram a poder ser sentidas em qualquer lugar do globo.

Ocorre que, o sistema político-jurídico tradicional de governar é posto em confronto frente a natureza transfronteiriça da internet, visto que, nesse ambiente, os limites da aplicabilidade da lei não se confundem com os limites dos territórios dos estados nacionais (CARVALHO, 2018).

Outra corrente que surgiu nesse período foi a dos chamados realistas, estes, conforme já fora mencionado, defendiam que o controle estatal era o melhor caminho a ser seguido, sendo que este deveria se dar através da atuação das nações no ambiente virtual a fim de regulamenta-la.

A estrutura que se formou dentro da rede, segundo a visão de tal corrente, não orientava a internet para um caminho da liberdade, ou de uma regulação eficaz que fosse feita pelos próprios usuários da internet, já que tais institutos só poderiam ser alcançados através da imposição de normas e sanções provenientes dos próprios estados.

A corrente dos realistas ganhava cada vez mais força visto que esses acreditavam que a internet, desde sua origem, não era um ambiente livre e aberto para qualquer valor, mas sim que sua codificação e toda a sua formação foram enviesadas politicamente a um fim.

Escolhas entre valores, escolhas sobre a regulação, sobre o controle, escolhas sobre a definição de espaços de liberdade – tudo isso constitui assunto da política. O código codifica valores e, não obstante, de forma surpreendente, a maior parte das pessoas fala como se o código fosse apenas uma questão de engenharia (LESSIG, 2006, p. 78 - tradução nossa).

Tal questão é facilmente observada, por exemplo, quando se defronta com o surgimento da Internet em plena guerra fria, onde o governo estadunidense formara a ARPANet com o intuito apenas de proteger os dados militares de suas estações de inteligência e de pesquisa.

O viés político na utilização da rede se perpetua até hoje, a exemplo do caso envolvendo as eleições presidenciais dos Estados Unidos da América no ano de 2016, onde a empresa Cambridge Analytica foi acusada de manipular dados de mais de 50 milhões de pessoas em favor da eleição de Donald Trump (DIÁRIO DE NOTÍCIAS, 2018).

Assim, a crítica realista baseia-se em ideias como o pluralismo de culturas e as mais diversas origens históricas de formação dos estados nacionais para legitimar a tese da regulação estatal da internet (CARVALHO, 2018).

Ainda que muitos acreditem até hoje na teoria liberalista, defendendo fortemente o fim da intervenção estatal na internet para que o ciberespaço pudesse vir a se regular de maneira autônoma, é plenamente perceptível a vitória da teoria realista através das diversas legislações existentes em todo o mundo as quais almejam garantir a neutralidade da rede durante o uso dos jurisdicionados.

2.3 HISTÓRICO SOBRE A PROTEÇÃO DOS DADOS PESSOAIS

A proteção de Dados e a privacidade quando pensadas frente a sociedade da informação, demandam uma nova releitura, adequando-se aquilo que as pessoas efetivamente querem ver tutelado pela seara jurídica. Dessa maneira, passam a serem analisadas no cenário impregnado pelo desenvolvimento tecnológico e pela busca por delimitar os novos espaços os quais serão submetidos a ao império regulatório da Lei.

Assim, se tanto a privacidade quanto a proteção de dados pessoais são compreendidas como assuntos a serem discutidos em colóquios científicos, no poder legislativo e também nos tribunais, é por causa da nova orientação dada a estrutura do ordenamento jurídico de maneira a permear à atuação eficaz dos direitos fundamentais (DONEDA, 2019).

Frente a esse cenário, intensificou-se a busca por medidas que coibissem a utilização indevida de dados pessoais e violassem a privacidade dos usuários das redes.

Exemplos como o Marco Civil da internet e a Lei Geral de Proteção de Dados Pessoais, ambos no Brasil, além dos diplomas internacionais como o *General Data Protection Regulation* da União Europeia apenas demonstram que a intervenção estatal, através da regulação, é cada vez mais frequente no ambiente da internet, bem como necessária a fim de preservar direitos fundamentais.

Este capítulo, tratará a respeito da evolução do conceito de proteção de dados pessoais ao longo da história, observando a formulação do conceito de privacidade, passando pelos fundamentos de proteção de dados na união europeia, principal expoente sobre a temática no mundo, e culminando na análise do instituto frente ao ordenamento jurídico nacional.

2.3.1 A proteção de dados no contexto europeu: do seu surgimento a criação do Regulamento Geral de Proteção de Dados

O principal expoente quando se discute a respeito da evolução do tema de proteção de dados é a legislação que se formou na União Europeia ao longo do século XX. A relevância prática das normas ali estatuídas serviu de inspiração para tantas outras legislações, como a Argentina, Uruguai e a recente Lei Geral de Proteção de Dados promulgada no Brasil.

A privacidade também ganhou novos contornos em virtude de acontecimentos políticos e sociais que se sucederam ao longo do século, de maneira que a sua relevância prática como um direito aumentou profundamente ao longo dos anos seguintes.

Assim, compreender as questões atinentes a proteção de dados que surgiram primeiro no Direito europeu é de extrema importância, visto que, além de significar o estudo da origem desse direito, é também uma forma de delimitação da matéria e também do que se espera a respeito das legislações de tantos outros países.

As primeiras legislações são datadas de logo após o fim da 2ª Grande Guerra, quando cerca de 10 países se reuniram a fim de criarem o Conselho da Europa (CdE), e, dessa maneira, promoverem juntos o Estado de Direito, a democracia, e os direitos humanos (SALDANHA, 2018).

O primeiro documento firmado sobre a temática, fruto das deliberações do CdE, foi a Convenção Europeia dos Direitos Humanos que surgiu no ano de 1953. O diploma legal estatuiu em seu art. 8º o direito ao respeito pela vida privada e familiar, dispondo no item 1 desse artigo que “qualquer pessoa tem o direito de respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência” (UNIÃO EUROPEIA, 1953).

O que se esperava era que o estado deixasse o cidadão em sua privacidade, de maneira que toda intervenção que ocorresse em sua vida fosse por motivo justificável, em especial, pela lei. Além disso, também se esperava uma atuação positiva por parte dos estados para que garantissem ativamente a proteção e o respeito pela vida privada e familiar (SALDANHA, 2018).

A convenção 108 de 1981, também chamada de convenção da Eslováquia, foi o primeiro documento a tratar a respeito de dados pessoais quando em caráter automatizado. O artigo primeiro do documento prevê que:

A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados») (UNIÃO EUROPEIA, 1981).

Pioneiro em sua temática, foi o primeiro documento com eficácia legal a prever medidas para a proteção de dados, sendo tratado como um instrumento de proteção internacional, de maneira que todos os países poderiam ratificá-lo, não havendo a necessidade de serem obrigatoriamente integrantes da união europeia para fazerem isso.

As disposições da convenção possuem efeitos vinculantes, obrigando que todos aqueles que a assinavam a promover a proteção de dados e as garantias referentes ao tratamento automatizado de dados pessoais dos particulares.

Todas as normas definidas na convenção, possuem aplicabilidade tanto para o setor privado quanto para o setor público, bem como nos procedimentos realizados pelas autoridades judiciárias e polícias. O objetivo era proteger os titulares quando no tratamento de seus dados, e também regular a transferência de dados entre os países signatários (SALDANHA, 2019).

A proteção de dados, conforme se observa, é um desdobramento do direito a privacidade e que tomou forma como um direito autônomo com a passar dos anos em virtude da crescente conscientização sobre o tema da proteção de dados.

Assim, enquanto a privacidade é compreendida como um conceito maior, mais profundo e complexo, dizendo a respeito da vida privada e familiar de uma pessoa e também de sua intimidade, o direito a proteção de dados é, na verdade, uma vertente mais objetiva e incisiva de sua incidência, sendo considerado sempre que se tratar a respeito de informações pessoais de alguém, que a identifique ou de detalhes de sua personalidade.

Atualmente a União Europeia possui todo um sistema orientado para trabalhar a questão da proteção de dados pessoais dos cidadãos europeus, trata-se do *General Data Protection Regulation*, mais comumente chamado GDPR, ou na tradução ao português de RGPD (Regulamento Geral de proteção de dados).

No entanto, o atual regulamento fora antecedido pela Diretiva nº 46 de 1995 (UNIÃO EUROPEIA, 1995), que foi o primeiro diploma legal a tratar especificamente sobre a proteção de dados. Ocorre que as diretivas emanadas pela União Europeia não tem uma eficácia impositiva, servindo apenas como uma orientação.

Pode-se dizer que as diretivas tratam a respeito de um entendimento existente na União Europeia onde os estados membros que a compõe, por sua vez, legislarão sobre ele no âmbito interno de seus países, orientando-se pela tese que fora firmada pela diretiva. No entanto, a Diretiva 95/46/CE acabou por ocasionar uma série de divergências na aplicação em virtude das diversas legislações setoriais oriundas de cada um dos 28 países da União Europeia, e, além disso, acabou gerando uma séria insegurança jurídica e um entrave para o avanço econômico na Europa (SALDANHA, 2018).

Não havia consenso, por exemplo, nos critérios de aplicação de multa por vazamentos de dados, e tampouco uma padronização dos valores destas quando aplicadas.

Buscando sanar os problemas gerados pela antiga legislação, foi proposto no ano de 2012 o Regulamento Geral de Proteção de Dados, e após 4 anos de amadurecimento e debates no parlamento europeu, foi finalmente promulgado no ano de 2016 como *Regulation 2016/679*, atingindo sua eficácia plena em 25 de maio de 2018 (UNIÃO EUROPEIA, 2016).

Convém destacar que, pela sistemática jurídica da união europeia, o Regulamento possui força de lei, e dessa maneira, aplica-se em eficácia vertical a todos os países que compõem a *European Economic Area*.

Assim, diferente do que dispõe a diretiva, o regulamento é de aplicação direta, não sendo necessário que seja transposto para o ordenamento interno dos países membros (SALDANHA, 2018).

Logo, o regulamento busca efetivar o direito relativo a proteção dos dados, e, mais que isso, dá corpo a um regramento contundente na busca pela mitigação de riscos, vazamentos e incidentes que permeiam estes dados durante todo o tempo do tratamento, isso é, desde a coleta até seu descarte quando estes não forem mais úteis.

A sistemática de proteção de dados criada na união Europeia é de relevância para todos os países que se importam com o tratamento dos dados e os direitos de

seus titulares, de maneira que, para muitos, um país só pode ser considerado com uma legislação adequada quando a união europeia o sinaliza como seguro para a troca de dados e a realização de tratativas econômicas. Atualmente, apenas 13 países foram considerados adequados em matéria de proteção de dados, sendo que na América do Sul apenas Argentina e Uruguai se encaixam na presente categoria (COMISSÃO EUROPÉIA).

2.3.2 A criação do sistema de proteção de dados pessoais na sociedade brasileira: considerações sobre a LGPD

Como demonstrado acima, faz-se necessário o estudo do regramento europeu para que se possa compreender a questão do direito a proteção dos dados nos demais países do mundo.

Primeiro, porque toda a sistemática envolvendo o próprio direito a proteção dos dados pessoais se originou e evoluiu dentro do contexto europeu, e, segundo, as atuais leis que visam proteger os dados pessoais estão intimamente balizadas pelos dispostos na legislação europeia.

O Brasil é atrasado na regulação jurídica de tal matéria, e muito disso se deve ao fato de não existir uma cultura referente a proteção dos dados pessoais, seja dentro de empresas, ou até mesmo na própria esfera pública.

Ademais, soma-se a isso o fato de que a proteção de dados só fora tratada no Brasil através de legislações esparsa, e de maneira muito difusa, em alguns artigos de uma ou de outra lei.

O primeiro diploma jurídico a tratar especificamente a respeito da proteção de dados foi a lei da Política Nacional de Informática, nela, imbricou-se em criar mecanismos que garantissem a proteção de dados de pessoas físicas ou jurídicas cuja os quais se houvessem interesse no resguardo do sigilo, bem como previu a lei a possibilidade de retificação dos dados pessoais quando se encontrassem errados ou incompletos (BRASIL, 1984).

Também o Habeas Data recebeu status de remédio constitucional, com previsão no artigo 5º LXXII, e posteriormente regulamentado pela Lei 9.507 de 1997, para:

- a) assegurar o conhecimento de informações relativas à pessoa impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988).

Já o Código de Defesa do consumidor estatui a possibilidade de que os consumidores tenham acesso a seus dados que estejam em poder dos fornecedores de serviços ou produtos, quer estejam essas informações presentes em fichas, cadastros ou outros tipos de registros, digital ou físico (BRASIL, 1990).

Em 2011, a Lei do Cadastro Positivo regulamentou o processo de acesso e consulta aos bancos de dados de informações financeiras e de adimplemento, para fins de formação do histórico de *credit score* (BRASIL, 2011).

O Marco Civil da Internet, ao estabelecer uma série de normas para o uso da internet, em especial diversos deveres para os provedores de acesso à rede, previu expressamente a necessidade de proteção aos dados pessoais dos usuários da internet, bem como quais seriam os direitos destes (BRASIL, 2014).

Apesar da existência dessas primeiras previsões a respeito dos dados no âmbito nacional, o Brasil nunca possuiu efetivamente uma consciência ou uma cultura efetiva a respeito da proteção de dados, em especial no âmbito corporativo,.

Assim, não era comum que se adotassem boas práticas de governança ou então políticas de segurança da informação. A legislação, dessa forma, não era de todo respeitada.

Acaba que, inclusive, operavam-se largamente os efeitos do chamado capitalismo de vigilância, onde as empresas buscavam o monitoramento constante dos usuários para a coleta de suas informações e também a sua mercantilização.

Sobre esse aspecto, salienta Frazão:

Do ponto de vista econômico, dados importam a medida que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Conseqüentemente, os dados precisam ser processados para que possam gerar valor. (2019a, p.26)

Buscando a alteração desse paradigma, e tentando tornar a proteção de dados mais prestigiada e efetiva no contexto brasileiro, o Congresso Nacional recebeu diversos projetos de lei que buscavam regular a proteção de dados.

Acabou, por sorte, em aprovar aquele que tinha maior familiaridade com o Regulamento europeu, e que conferiria mais respeitabilidade perante o cenário internacional.

No ano de 2010, o Ministério da Justiça, juntamente com o Observatório Brasileiro de Políticas Digitais da Internet, lançaram a primeira consulta pública

sobre a necessidade de uma Lei de Proteção de Dados. Tal procedimento durou 5 meses e recebeu 800 contribuições e mais de 14 mil visitas no site (PAULA; VASCONCELOS, 2019).

Acabou que em virtude dos acontecimentos que se sucederam nos anos seguintes, como as denúncias de Edward Snowden a respeito da espionagem realizada pelo governo estadunidense em países como Alemanha e Brasil, e a consequente promulgação do Marco Civil da Internet, os debates acerca da lei que ocorriam tanto no executivo quanto no congresso foram engavetados.

Apenas no ano de 2015 que se voltaria a discutir um anteprojeto para a proteção de dados no âmbito do executivo federal. A consulta pública realizada dessa vez contou com mais de 1.100 participações e teve cerca de 50 mil visitas diferentes ao site do anteprojeto, de maneira que culminou no Projeto de Lei nº 5.276 de 2016 (PAULA; VASCONCELOS, 2019).

Tal projeto, encaminhado pelo Ministério da Justiça e da Cidadania à Casa Civil da Presidência da República, foi de imediato enviado à Câmara do Deputados, onde após a aprovação pela comissão especial designada para a sua análise e também para a realização dos debates, foi aprovado pelo plenário da respectiva casa e também do Senado Federal, seguiu para aprovação da presidência da república como PLC nº 53/18 (DONEDA, 2019).

No ano de 2016, acabou sendo promulgada a Lei nº 13.709/2019, conhecida como Lei Geral de Proteção de Dados, ou pelo seu acrônimo LGPD.

A sistemática prevista na Lei é, basicamente, a de buscar formas de mitigar riscos e fazer com que aqueles que tratam dados trabalhem com um regramento bem definido sobre o que podem e como podem fazer (VAINZOF, 2019).

Para Frazão (2019a) a Lei Geral de Proteção de Dados tem um importante papel em reforçar a autodeterminação informativa dos titulares e dar a estes o devido controle sobre seus seus próprios dados, reprimindo a economia baseada na coleta e tratamento de informações.

A lei é também um agente transformador do modelo do capitalismo de vigilância que todos os titulares estão submetidos, bem como ferramenta que limita a extração de dados de maneira desregrada, que é feita sem o consentimento ou a ciência dos usuários (FRAZÃO, 2019b).

Já Siqueira (2019) assevera que a LGPD surge com o objetivo de permitir aos titulares de dados que tenham o controle e a autonomia sobre as suas informações. Também só permite que a coleta e o tratamento de tais dados sejam feitos dentro dos limites estabelecidos pela lei, bem como observando o princípio da finalidade e também se enquadrando em alguma das bases legais que servem para legitimar o tratamento de dados.

Não só isso, a lei trás logo nos seus artigos iniciais os valores e fundamentos que justificam a sistemática de proteção de dados que ela planeja dar corpo no cenário jurídico-econômico brasileiro, entre eles, destaca no artigo 2º os fundamentos de respeito a privacidade, da autodeterminação informativa e da inviabilidade da intimidade, da honra e da imagem (BRASIL, 2018).

Siqueira (2019) também destaca que a LGPD possui entre seus objetivos o de proteger os direitos fundamentais de liberdade, e que também se destina ao livre desenvolvimento da personalidade da pessoa natural, em seu sentido jurídico.

O que a LGPD cria, acima de tudo, é um terreno fértil para a consciência de que a proteção de dados é, na verdade, um direito autônomo, expressão dos direitos de dignidade e de liberdade, e profundamente relacionado com o fato de que os indivíduos não podem simplesmente serem transformados em objetos de vigilância (FRAZÃO, 2019b).

2.4. AUTORIDADES DE PROTEÇÃO DE DADOS

A própria sistemática legal, por si só, não serve para dar efetividade máxima à proteção de dados pessoais e à privacidade. Para que seja efetivamente garantido o *enforcement* da Lei faz-se preciso que se socorra a estruturas regulatórias e fiscalizadoras, capazes de observar se os organismos públicos e privados os quais realizam o tratamento dos dados pessoais estão cumprindo as exigências impostas pela lei.

Além disso, muitas das normas de proteção de dados, como é o caso da legislação brasileira, deixam uma série de pontos os quais precisam ser regulamentados pela autoridade supervisora, por dois motivos:

O primeiro deles se deve ao fato de que muitas dessas regulamentações precisam ser emanadas de um corpo técnico, altamente especializado em matérias

como proteção e dados, privacidade, segurança de informação e tecnologia, não podendo deixar que isso se sujeite ao processo legislativo do congresso nacional, visto que, além do baixo conhecimento das temáticas, é também lento, em virtude de seu formalismo, e não tem a capacidade de criar novos regulamentos legais no mesmo passo em que surgem as novas tecnologias.

A segunda questão a ser considerada aqui é a de que as mudanças tecnológicas são acentuadas e ocorrem com certa frequência. Dessa forma, os debates em matéria de proteção de dados pessoais não se esgotam, sendo tão constantes quanto as transformações que nela ocorrem em razão de tal avanço. (DONEDA, 2019)

Dessa maneira, as Autoridades de Proteção de Dados, que podem ser renomeadas sobre a Sigla de APD, existem enquanto entidades da administração pública e, atuando de maneira independente e extremamente técnica, expedem diversas regulamentações sobre a temática de proteção de dados a fim de adequar a atuação dos agentes de tratamento.

Os subcapítulos abaixo buscarão compreender as figuras das Autoridades no contexto europeu, argentino, uruguaio e também no brasileiro, a fim de que possam ser futuramente comparadas elencando semelhanças e diferenças.

2.4.1 As autoridades de Proteção de Dados Européias: análise do modelo europeu e de sua contribuição para os demais países.

A convenção de 1981 (UNIÃO EUROPÉIA, 1981), também denominada de Convenção de Estrasburgo, é um marco no tocante ao conteúdo da Proteção de Dados Pessoais, sendo este, inclusive, o primeiro documento jurídico a delimitar a existência da Autoridade de Proteção de Dados e a desenhar as suas funções, ainda que o modelo aqui proposto na norma não guardasse considerável semelhança com a Autoridade atual desenhada pelo Regulamento.

Na convenção, a proteção de dados efetiva estava atrelada com os deveres de fiscalização e regulamentação através da imposição das normas presentes nos seus mais diversos dispositivos, tudo isso sendo garantido por intermédio da figura denominada de *Supervisory Authorities*, já demarcada pela independência nas suas funções (CASTRO, 2019).

A questão das Autoridades de Proteção de Dados seria melhor aprofundada dentro do contexto Europeu com a promulgação do Regulamento nº 2016/679 (UNIÃO EUROPÉIA, 2016), que buscou substancialmente aprimorar todas as funções e competências a serem realizadas pelas APDs.

Estas Autoridades de Controle são definidas pelo Regulamento Geral de Proteção de Dados como autoridades públicas independentes criadas por cada um dos estados membros, e que guardam a função de fiscalizar a aplicação das normas do regulamento e também de sancionar aqueles que cometem violações (UNIÃO EUROPÉIA, 2016).

Ainda assim, é preciso que exista a certeza de que estas instituições as quais tem como dever primordial regular o tratamento de dados e definir critérios técnicos de sua proteção deverão agir de maneira imparcial e desinteressada, de forma que suas decisões não estarão submetidas a influências ou pressões externas, seja de entes públicos ou privados (CASTRO, 2019).

Para Bieker (2019) é importante que as Autoridades de Proteção de Dados conservem o distanciamento necessário dos estados membros os quais fazem parte, visto que a existência de uma relação de dependência ou submissão não seria capaz de garantir a segurança e a neutralidade necessária para a sua atuação em prol da proteção dos dados pessoais.

É por isso que o Regulamento nº 2016/679, de maneira similar ao que dispunha a antiga Diretiva nº 96/45, prevê no artigo 51 que a Autoridade de Controle deverá atuar com total independência durante a aplicação das normas ali dispostas, defendendo os direitos e liberdades fundamentais dos titulares e também garantindo a circulação dos dados pessoais por toda o Território da União Europeia (UNIÃO EUROPÉIA, 2016).

O que se observa é que a característica fundamental de toda Autoridade de Proteção de Dados é a capacidade de que essa possa realizar as suas atribuições com a completa independência, de maneira que seus membros não estão sujeitos a influências internas ou externas, diretas ou indiretas, não sendo obrigados, para o exercício de suas funções, solicitar ou receber ordens de ninguém (SALDANHA, 2018).

Essa independência precisa se realizar de três formas distintas: financeira, estrutural e funcional. Todas essas dispostas ao longo dos itens do artigo 52 do Regulamento Geral de Proteção de dados.

A independência financeira que se busca está garantida pelo GDPR no fato de que incumbe aos estados membros da União Européia a separação de um montante de seu orçamento público anual para a APD de forma que possa desempenhar as suas atribuições sem conflito com o restante da administração. Aliás o item 6 do artigo 52 do regulamento prevê que até mesmo o controle fiscalizatório que for realizado sobre a utilização do orçamento pela autoridade deverá ser feito sem que isso demonstre uma intervenção estatal que busque ajudar ou prejudicar outros setores (UNIÃO EUROPÉIA, 2016).

Podendo o orçamento dos entes públicos ser considerado como a característica essencial para que mantenham o desempenho de suas funções, a previsão da independência financeira é uma das formas mais eficazes de diminuir o controle do estado sobre as decisões emanadas pela autoridade, seja no tocante a beneficiar-se com informações comerciais, conceder benefícios econômicos ou até privilégios, e para ser desidioso com as condutas ilegais de empresas e demais organizações (CASTRO, 2019).

No que se refere a sua independência estrutural, ainda no artigo 52 do regulamento, tem-se que:

Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comité (UNIÃO EUROPÉIA, 2016).

Logo, a estrutura que deve se encontrar a sua disposição é aquela necessária ao correto desempenho de todas as suas funções, sem que isso signifique a necessidade de socorrer-se constantemente ao poder público superior, a fim de requisitar bens e postos de trabalho. O Regulamento também prevê a necessidade de que a autoridade possua corpo de funcionários próprio, encontrando-se unicamente submetidos a direção dos membros da Autoridade de Proteção de Dados Pessoais.

Ademais, em comparação com a antiga Diretiva, houve no artigo nº 58 do Regulamento o alargamento considerável dos poderes concedidos as Autoridades de Controle, os quais se subdividem em Poderes de Investigação, de Correção e Consultivos.

Dessa forma, poderá a Autoridade, no exercício de suas atribuições, utilizar-se de seus poderes para realizar investigações sob a forma de auditorias; notificar o responsável pelo tratamento de violações frente ao regulamento europeu; fazer advertências aos controladores e operadores em relação a forma como tratam os dados; ordenar ao responsável pelo tratamento que preste comunicações ao titular dos dados de uma violação que tenha ocorrido nas constâncias do tratamento ou então de responder-lhe alguma petição; emitir pareceres e aprovar projetos de códigos de conduta; emitir pareceres que tenham como destino os órgãos máximos da administração pública do respectivo estado membro, bem como a outras instituições e organismos, e até mesmo para o público, sobre qualquer assunto relacionado com a proteção de dados pessoais (UNIÃO EUROPÉIA, 2016).

Resta, pois, compreender as características que delimitam a independência funcional das Autoridades de Proteção de Dados, em especial com relação aos membros que a compõem.

O Regulamento prevê formas de ingresso e a necessidade corrente de capacitação na matéria de proteção de dados daqueles que integram as APDs, ademais, no artigo nº 52, item 3 do GDPR, fica a previsão de que os membros devem abster-se de atos ou do exercício de funções incompatíveis com suas atribuições frente as autoridades de controle, independente serem estas remuneradas ou não (UNIÃO EUROPÉIA, 2016).

O Regulamento Geral de Proteção de Dados também prevê a necessidade de delimitação do tempo de mandato dos membros que compõem a Autoridade, sendo este nunca inferior a quatro anos, também orienta a obrigação de sigilo profissional durante e após o mandato de todas as informações que tenham recebido durante seu exercício.

Aliás, a fim de garantir ainda mais a estabilidade dos dirigentes, o regulamento somente autoriza a exoneração, conforme o Artigo 53, item 4, em casos de "falta grave ou se tiverem deixado de cumprir as condições exigidas para o exercício das suas funções". (UNIÃO EUROPÉIA, 2016)

A respeito disso, Arantes e Blum (2018) observam que a estabilidade funcional é um ponto extremamente relevante na garantia do bom desempenho dos funcionários, privando de pressões externas, como as oriundas da política, ou então

internas, como o posicionamento diferente dentro da autoridade de proteção de dados.

A sistemática efetiva de proteção de dados pessoais depende da lei, de uma cultura de privacidade implementada pelas organizações e também seguida pelas pessoas para a proteção de seus próprios dados, mas, como demonstra a experiência desenhada na União Europeia, uma Autoridade de fiscalização é primordial para garantir que o respeito a lei, desde que, é claro, essa Autoridade possua independência e autonomia, assim como tenha seus poderes e atribuições bem delimitados para tornar real a proteção de dados pessoais.

Elencadas as características essenciais de uma autoridade que servem a configurar a independência de sua atuação, resta observar como tais características foram estruturadas nas APDs da Argentina e do Uruguai, e como isso tem sido trabalhado para a construção da Autoridade Nacional de Proteção de Dados através da Lei nº 13.853/2019 no Brasil

2.4.2 Autoridade de Proteção de Dados no Contexto Argentino

A Argentina foi o primeiro país da América do Sul a sancionar uma lei a respeito da proteção de dados ainda nos anos 2000. A norma emanada pelo poder legislativo possuía uma forte influência das disposições contidas na Diretiva 96/45/CE e também na legislação de proteção de dados espanhola.

Além disso, foi também o primeiro país na América do Sul a conseguir a chancela da União Europeia a fim de que fosse considerado adequado para o tratamento e transmissão internacional de dados com os países europeus.

Na decisão da Comissão nº 2003/490/CE, o grupo de trabalho responsável pelo parecer a respeito da adequação legislativa para a proteção de dados na Argentina decidiu que:

(14) A lei argentina abrange todos os princípios básicos necessários para assegurar um nível adequado de protecção das pessoas singulares, embora também preveja excepções e limitações de modo a salvaguardar interesses públicos importantes. A aplicação destas normas é garantida por uma reparação judicial rápida específica para a protecção de dados pessoais, conhecida como habeas data, juntamente com as reparações judiciais gerais. A lei prevê a criação de um organismo de controlo responsável pela protecção de dados encarregado de realizar todas as acções necessárias para dar cumprimento aos objectivos e às disposições da lei e dotado das competência de investigação e de intervenção. Nos termos do regulamento, a Direcção Nacional de Protecção de Dados Pessoais foi criada como organismo de controlo. A lei argentina prevê sanções dissuasivas eficazes

de natureza tanto administrativa como penal. Por outro lado, as disposições da lei argentina no que respeita à responsabilidade civil (contratual e extra-contratual) aplicam-se no caso de tratamento ilícito prejudicial para as pessoas em causa.

[...]

(16) Deve assim considerar-se que a Argentina assegura um nível adequado de protecção dos dados pessoais, nos termos da Directiva 95/46/CE (UNIÃO EUROPEIA, 2003).

Assim, a Lei 25.326 de 2000 (Argentina, 2000b) foi a norma responsável por criar toda a sistemática a respeito da protecção de dados na Argentina, incluindo ainda a figura da Autoridade de Protecção de Dados, denominada na lei de *Órgano de Controlo*.

No entanto, toda as disposições legais a respeito da APD criada na Argentina fora vetada no decreto presidencial nº 995/2000, em virtude de que a estrutura criada violaria pressuposto de iniciativa do Presidente da República Argentina, por se tratar de uma entidade da administração pública indireta cuja criação faria incorrer em aumento de despesas para o governo (Argentina, 2000a).

Assim, no ano de 2001, foi emanado pelo Presidente Argentino o Decreto nº 1.558/2001 (ARGENTINA, 2001), que, entre outras disposições, regulamentou a Autoridade de Protecção de dados Argentina, denominada como *Dirección Nacional de Protección de Datos Personales*.

Ela ficou demarcada, nos moldes da nova redacção dada ao artigo 29 da Lei 25.326/2000, como sendo um órgão da administração direta vinculado ao Ministério da Justiça e dos Direitos Humanos do governo federal (ARGENTINA, 2000b).

Isso significava que a Autoridade de Controle carecia de real independência em sua atuação, de forma que estaria subordinada financeira e estruturalmente a outros órgãos da administração. Ainda que a Lei de Protecção de Dados previsse que, no caso do diretor, por exemplo, esse exerce suas funções com plena independência e que não estaria sujeito a controle de qualquer outra autoridade pública, não foi assim que boa parte da doutrina entendia.

A respeito disso, traz-se a seguinte passagem:

Neste tema, muito se tem que ver com relação a falta de autonomia e independência da Autoridade de Controle em respeito ao poder executivo argentino. Sem autonomia e independência a autoridade de controle perde a eficácia em suas funções (DELGADO; SALTOR, 2011, p. 159 - tradução).

Essa subordinação a qual a Autoridade de Protecção de Dados estava submetida na argentina foi alvo também de críticas por parte dos Organismos da

União Européia, os quais observavam uma certa instabilidade na atuação da APD enquanto órgão da administração Direta:

No entanto, o Grupo de Trabalho chama a atenção para o fato de o chefe da autoridade supervisora de proteção de dados ser nomeado e poder ser demitido pelo Ministro da Justiça e Direitos Humanos, que também decide sobre o pessoal da autoridade. A autoridade está integrada na estrutura do Ministério da Justiça. O Grupo de Trabalho considera que esta situação não garante que a autoridade possa agir com total independência e, portanto, insta à criação dos elementos necessários para esse fim, incluindo modalidades modificadas de nomeação e destituição do chefe da autoridade (UNIÃO EUROPÉIA, 2003).

Dessa maneira, reacendeu na Argentina, após a promulgação do GDPR, a discussão a respeito da natureza da Autoridade de Controle, sendo que por meio do Decreto 899 de 2017, restou configurado que a *Agencia de Acceso a la Información Pública*, Autoridade responsável pelos direitos da lei de Acesso a Informação, ficaria também responsável por garantir a eficácia da Lei de proteção de dados argentina.

A mudança foi de certa forma benéfica, isso porque a Agência é, na verdade, uma Autarquia constituinte da Administração indireta, e assim, possui maior independência financeira, estrutural e funcional do que a antiga direção, conforme demonstra a redação do artigo 19 da Lei 27.257 de 2017 (ARGENTINA, 2017).

Com relação à independência financeira que caracteriza a Agência de Acesso a Informação, ela não mais necessita de depender dos recursos advindos da presidência da república para executar suas atribuições, mas sim possui a liberdade para desenhar e executar seu próprio orçamento, a ser apresentado ao Congresso Nacional argentino anualmente para que seja aprovado nas diretrizes constantes da Lei de Orçamento da Administração Nacional (IDEC, 2019).

A mudança de paradigma, aliada com a maior quantidade de recursos no próprio orçamento, faz com que seja mais fácil para a Autoridade de Proteção de dados, no exercício de suas atribuições, trabalhar com maior eficiência e maior presteza, fazendo valer a aplicação das normas previstas na lei de Proteção de dados no que concerne as suas funções e a proteção dos direitos dos titulares de dados.

Ja no que concerne a respeito da independência estrutural do modelo Autárquico da Agência, há uma evolução significativa para a garantia deste do que quando se tratava de um órgão integrante do Ministério da Justiça e Direitos Humanos Argentino.

Assim, além de toda uma estrutura física e recursos financeiros muito melhor que a tornam mais preparada para garantir a lei de Proteção de Dados, o Artigo 25 da lei 27.275 estabelece que Agência possui todo um corpo técnico e administrativo especializado para promover a eficácia das balizas existentes na Lei (ARGENTINA, 2017).

Assim, simetricamente, os agentes que compõe a Autoridade estão completamente voltados a promover a cultura da proteção de dados e a realizar as diligências de fiscalização e sancionatórias a fim de garantir o adequado tratamento de dados por parte das organizações públicas e privadas.

A autonomia funcional presente na Agência é também fator fundamental na sua configuração como um ente independente. Ela é presente desde a forma de escolha dos diretores a sua estabilidade, bem como a forma como compõe todo o corpo de colaboradores da instituição.

A nomeação de um diretor da Agência inicia-se pelo processo de indicação pelo Poder executivo, aqui, devem ser observados inúmeros requisitos como a idoneidade e a dedicação exclusiva dos candidatos. É aberto prazo para uma audiência pública onde o candidato será sabatinado por diversos atores da sociedade civil e também por organizações. Somente após todo esse processo é que o Governo poderá confirmar o candidato como Diretor da Agência ou então vir a propor outro nome (ARGENTINA, 2017).

É de suma importância Salientar que o mandato dos diretores é fixo, com duração de 5 anos e possibilidade de uma única recondução. Além disso, sua estabilidade garante o direito de só ser exonerado nos casos de mal desempenho, delito no exercício de suas funções ou então de crimes comuns, conforme disposição do Artigo 27 (ARGENTINA, 2017).

O Diretor da Agência também possui total autonomia para a escolha dos funcionários que comporão a Autoridade. Assim, ele é capaz de propor e desenhar toda a estrutura funcional da entidade, evitando que sejam colocados funcionários que possam, eventualmente, apresentar conflitos de interesse da DPA com outras organizações (IDEC, 2019).

Com relação aos poderes da respectiva autoridade, eles podem ser classificados como: investigativos, normativos, consultivos e também de intervenção.

A ela incumbe criar normas e regulamentos para o desempenho das atividades previstas na Lei de maneira adequada, bem como elaborar códigos de conduta, fiscalizar os bancos de dados, no que concerne a sua segurança e integridade, receber reclamações de titulares quanto ao tratamento de seus dados e também de investigar eventuais violações de dados (IDEC, 2019).

Ademais, é fundamental destacar que a autoridade também possui um papel educativo de extrema relevância a fim de que se expanda o conhecimento a respeito dos ditames da lei, conscientizando a população a respeito dos direitos dos titulares de dados e também de qual o seu papel enquanto autoridade central e reguladora.

2.4.3 Autoridade de Proteção de Dados no Contexto Uruguaio

A preocupação no Uruguai a respeito da temática de proteção de dados vem de antes da promulgação de qualquer lei nacional sobre o assunto, visto que o país é um dos 51 signatários da Convenção nº 108, a qual tratava do tratamento automatizado de dados, sendo, dessa maneira, o único país da América Latina a ter ratificado o documento (SALDANHA, 2018).

O que mais chama atenção a respeito da formação e evolução do direito a proteção de dados no ordenamento uruguaio advém, em especial, por causa dos movimentos de reafirmação e expansão dos direitos e garantias fundamentais durante o processo de reabertura democrática após o período ditatorial que tantos países viveram na América do Sul (GUIDI, 2018).

Assim, o que se queria era impedir que governos, organizações ou qualquer outra entidade pudesse se aproveitar dos dados pessoais de uma ou mais pessoas e utiliza-los de maneira ardilosa, e, em se tratando no caso de regimes ditatoriais, uma arma contrária àqueles que fossem considerados como revolucionários.

Dessa forma, O Uruguai foi o segundo país na América Latina a possuir uma legislação focada em proteção de Dados, através da Lei nº 18.331 de 11 de agosto de 2008 (URUGUAI, 2008), também chamada de *Ley de Protección de Datos Personales y Acción de Habeas Data*.

A partir dela, foi criada toda a sistemática legal e administrativa focada na proteção dos direitos dos titulares de dados. E, de tal maneira, estatuiu diversas

disposições a respeito do tratamento de dados, adequação das organizações frente aos ditames da lei, entre outros.

Além disso, a lei criou a Autoridade de Proteção de Dados bem como redigiu certas orientações para a realização de transferências de dados internacionais com todos os países do bloco europeu.

Ainda que o arcabouço normativo vigente no país seja diversificado, composto pela Lei Geral, decretos do poder executivo federal e também por diversas resoluções e notas técnicas emitidas pela Autoridade de Proteção de Dados, não é tão complexo quanto os textos legislativos europeus ou então toda a estrutura formada no âmbito da administração pública europeia, embora seja esta a sua fonte de inspiração primária em especial a Diretiva nº 95/46/CE.

A Lei de Proteção de Dados vigente foi regulamentada através do Decreto nº 414 de 31 de agosto de 2009, o qual buscou clarificar diversos de seus pontos e ainda delimitar a forma de organização, os poderes e o funcionamento da Autoridade de Controle do País, denominada de *Unidad Reguladora y de Control de Datos Personales* (URUGUAI, 2009).

Ainda assim, parecem existir mais alguns empecilhos na realização pela Autoridade de suas funções, em especial sobre os elementos caracterizadores de uma entidade independente, autônoma e desinteressada.

Quando se observa a sua posição dentro da administração pública, o que se nota é que a *Unidad* é um componente da administração direta, visto ser integrante da *Agencia de Gobierno Eletronico y Sociedad de la informacion y del Conocimiento* (AGESIC) órgão pertencente a presidência da república, conforme disposição do Artigo 31 da Lei de Proteção de Dados (URUGUAI, 2008).

Essa questão impacta diretamente no orçamento que encontra-se a sua disposição para o exercício de suas atribuições enquanto órgão regulador, e também traz consequências para que se possa afirmar ser possuidor de qualquer autonomia financeira, nos moldes da legislação europeia, por exemplo.

Isso porque a proposta orçamentária anual da Autoridade acaba sendo somada ao Orçamento da AGESIC que, no final, é parte integrante do orçamento da presidência da república, apresentados ao congresso nacional (URUGUAI, 2008).

Assim, a APD depende do repasse desses valores para sua manutenção e persecução de seus objetivos, o que, conforme a pesquisa realizada para o IDEC

(2019), representa para sociedade civil um entrave para a eficácia da atuação da Autoridade, sendo que para muitos o Governo Federal deveria dar maior importância para o órgão.

Com relação a sua estrutura funcional, pode-se afirmar que a diretoria da *Unidad* é composto por um Conselho Diretor e um Conselho Consultivo.

O primeiro tem na sua composição 3 membros, um deles é o diretor da própria AGESIC, que é nomeado pelo presidente uruguaio, e os outros são indicados pelo poder executivo. Esses dois possuem mandatos com duração de 4 anos, e só perderão seus cargos em virtude de inaptidão, omissão ou crime, desde que observado o devido processo legal para a sua exoneração (URUGUAI, 2008).

Ainda que o motivo de o conselho diretor ser integrado pelo Diretor Geral da AGESIC seja o de manter certa conformidade na visão e projetos desenvolvidos tanto pela Agência quanto pela *Unidad*, a sociedade civil observa mais como um causador de conflitos de interesse entre o papel fiscalizador/regulador que a Autoridade desempenha e com os projetos políticos de executivo, devendo, na verdade, haver distanciamento entre ambos (IDEC, 2008).

Logo, parece que não existe de fato uma independência funcional na autoridade de Controle em virtude de uma possível intervenção quase que direta do poder executivo nela, o que, inclusive, chega a ser empecilho a própria fiscalização da administração pública.

Embora a Lei preveja que todos os diretores ajam com total independência no plano técnico, não recebendo ordens nem instruções (URUGUAI, 2008), é um pouco forçoso acreditar que isso se concretize simplesmente por causa da previsão legal.

Ademais, para garantir a efetividade e completude de suas atribuições encontram-se uma série de poderes disponíveis para a Autoridade: como poderes investigativos para analisar bases de dados públicas ou privadas, intimar os controladores de dados a comparecer perante a *Unidad*, poderes de intervenção de modo a poder aplicar as sanções como multas, suspensão ou encerramento da base de dados e também poderes consultivos assessorando o poder executivo na formulação de novas leis ou respondendo consultas de organizações ou dos próprios titulares de dados (URUGUAI, 2008).

A legislação também garante poderes normativos à Autoridade, a fim de que possa emitir notas técnicas e recomendações, no entanto, conforme observa Guidi,

o Decreto Regulamentador nº 441 parece insuficiente por não ter buscado disciplinar o poder normativo que a Autoridade de Controle possui, de forma que acabou "deixando em aberto os temas a serem objeto de tais orientações ou mesmo o peso jurídico de tais documentos" (2018, p. 101).

Além disso, ela possui o poder de receber queixas dos cidadãos uruguaios, mas, não possui prerrogativas de tomar uma conduta impositiva a fim obrigar as organizações a adotarem um comportamento específico. Dessa forma, ele pode até sancionar as empresas com multas, observações ou então suspensão da base de dados, no entanto, não pode obriga-las a nada, de maneira que sempre acabaram aconselhando aos titulares a buscarem a via jurisdicional para maior presteza (GUIDI, 2018).

Ainda sobre essa temática, a própria lei obriga que para o encerramento das bases de dados é preciso que a Autoridade de Proteção de Dados socorra-se da via jurisdicional para que seja feito (URUGUAI, 2008).

Por fim, é importante destacar que a lei não disciplinou qualquer poder educativo a ser desempenhado pela APD, embora a maior parte da população uruguaia conheça seus direitos e a existência da Lei de Proteção de Dados (IDEC, 2019).

Não obstante, é preciso destacar que ainda assim o Uruguai é reconhecido como um país adequado para a transferencia internacional de dados conforme decisão da comissão Europeia. Coloca-se abaixo um pequeno excerto que demonstra tal afirmação:

(6) As normas de proteção dos dados pessoais da República Oriental do Uruguai baseiam-se em grande medida nas normas da Diretiva 95/46/CE e encontram-se estabelecidas na Lei n.º 18.331 de proteção dos dados pessoais e ação de *habeas data* (*Ley n.º 18.331 de protección de datos personales y acción de habeas data*), de 11 de agosto de 2008, que é aplicável tanto às pessoas singulares como às pessoas coletivas.

(7) A referida lei é regulamentada pelo Decreto n.º 414/009, de 31 de agosto de 2009, aprovado no intuito de clarificar diversos elementos da lei e regular a organização, os poderes e o funcionamento da autoridade nacional de proteção de dados. O preâmbulo deste decreto indica que, quanto a esta questão, a ordem jurídica nacional deve ser adaptada ao regime jurídico comparável mais comumente aceite, sobretudo o estabelecido pelos países europeus através da Diretiva 95/46/CE.

(8) Também existem disposições de proteção de dados em algumas leis especiais que criam e regulam bases de dados, nomeadamente leis que regulam determinados registos públicos (escrituras notariais, propriedade industrial e marcas, atos pessoais, direitos reais, atividade mineira ou informação financeira). A Lei n.º 18.311 aplica-se supletivamente às questões que não são especificamente regidas por esses diplomas específicos, nos termos do artigo 332.º da Constituição.

(9) As normas de proteção de dados aplicáveis na República Oriental do Uruguai cobrem todos os princípios básicos necessários para assegurar um

nível adequado de proteção das pessoas singulares e preveem também exceções e limitações de modo a salvaguardar interesses públicos importantes. Estas normas de proteção de dados e as exceções referidas refletem os princípios consagrados na Diretiva 95/46/CE (UNIÃO EUROPEIA, 2012).

Dessa forma, as considerações a respeito da estrutura criada dentro do Uruguai, por parecer carecer de maior independência no gozo de suas atribuições, é de vital importância quando da análise da figura da Autoridade Nacional de Proteção de Dados, de forma a pensar a sua estrutura e funções quando estiver na persecução de seus objetivos.

2.4.4 Autoridade Nacional de Proteção de Dados Brasileira

Da mesma forma que se deu na União Europeia e nos demais países que já internalizaram uma cultura a respeito da Proteção de Dados, o Brasil também reconheceu a impossibilidade de que a autodeterminação informativa fosse completa simplesmente de acordo com as disposições da lei geral e com as ações conscientes do próprio titular dos dados.

Recentemente, o Governo Federal veio a editar o Decreto nº 10.474 de 26 de agosto de 2020 o qual aprovou a Estrutura Regimental e o Quadro de cargos em comissão e funções de confiança da Autoridade Nacional de Proteção de Dados (BRASIL, 2020), logo após o Senado Federal aprovar a conversão em lei da Medida Provisória nº 959 de 2020 a qual deu vigência imediata a Lei Geral de Proteção de Dados (OLIVEIRA, 2020).

No entanto, os debates em torno da necessidade de uma Autoridade de Proteção de dados iniciaram conjuntamente com as primeiras consultas legislativas propostas a respeito da criação da lei.

Acontece que o anteprojeto nº 5.276/16 do poder executivo acabou não prevendo expressamente a existência da Autoridade Nacional de Proteção de Dados e nem sequer delimitou a estrutura ou competências de um órgão regulador, apesar de que no item nº 16 da exposição de motivos da referida lei reconhecer a sua importância para garantir a eficácia da LGPD.

Com o objetivo de dar efetividade à regulamentação sugerida, a proposta prevê um órgão competente para a proteção de dados pessoais no país. Será sua responsabilidade elaborar diretrizes de uma Política Nacional de Proteção de Dados Pessoais e Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança, estimular a adoção de

padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, entre outras medidas (BRASIL, 2016).

A esse respeito, Doneda (2019) observa que a lei, por diversas vezes, referiu-se a um órgão competente a fim de operacionalizar garantias legais e os mecanismos de tutela necessários a proteção dos titulares de dados, os quais só poderiam ser efetivados através da atuação do respectivo órgão.

Dessa forma, devido a inércia do poder executivo em delimitar especificamente qual seria o órgão regulador, acabou que no PLC nº 53/18 fora acrescentado pela Câmara dos Deputados a figura da ANPD, como uma autarquia federal a partir do artigo 55 da LGPD (BRASIL, 2018).

Acertadamente, o Presidente da república acabou por vetar todos os artigos da lei que dispunham a respeito da criação da Autoridade Nacional de Proteção de Dados, em virtude de existir vício de iniciativa da propositura do projeto de lei, visto ter extrapolado a competência privativa a qual dispõe o presidente da república para a criação de órgãos e entidades na administração pública federal (PAULA; VASCONCELOS, 2019).

É preciso destacar que o veto presidencial foi a decisão mais prudente a ser tomada a respeito da criação da autoridade, uma vez que se caracterizava como grave afronta ao texto constitucional, ferindo as disposições presentes nos artigos 37, XIX e 62, §1º, II, e da Constituição da República Federativa do Brasil (BRASIL, 1998).

Essa inconstitucionalidade presente no texto da lei seria capaz de colocar em cheque a atuação da ANPD, bem como fragilizar toda a sistemática de proteção de dados que a ela incumbe criar, visto que, por exemplo, a primeira multa que a Autoridade viesse a aplicar em uma empresa poderia ser o estopim para o questionamento de sua constitucionalidade em virtude do vício existente na sua criação.

Após o veto, o governo federal se comprometeu em legislar uma norma que viesse a delimitar toda a estruturação da Autoridade Nacional de Proteção de Dados, de forma que no final do Ano de 2018 editou a Medida Provisória nº869/18 a qual fora convertida na Lei nº 13.853 no ano de 2019 (DONEDA,2019).

Ocorreu que, diferentemente da estrutura pensada pela Câmara dos Deputados, a qual instituiu a ANPD como uma entidade da Administração Pública

Indireta, transformou-a em um órgão subordinado à Presidência da República, que impactou consideravelmente nos elementos caracterizadores de sua independência.

Primeiro, na análise a respeito da existência de uma autonomia estrutural no que concerne a Autoridade Nacional de Proteção de Dados, é preciso notar que o fato de a redação legal tê-la tornado como um órgão da administração pública direta é vista com maus olhos pela maioria dos doutrinadores nacionais. Para estes, o modelo autárquico antes desenhado pela Câmara dos Deputados resguardava uma maior autonomia da entidade pública, bem como lhe permitira uma atuação desinteressada.

Castro (2019) observa que a existência da Autoridade enquanto órgão da administração direta faria com que funcionasse apenas como uma extensão do poder executivo, que, no exercício de suas funções, poderia muito bem vir apenas a aplicar as orientações e vontades advindas dos órgãos hierarquicamente superiores.

Doneda (2019), inclusive, pontua que um órgão que desempenhasse as mesmas competências as quais incumbe a ANPD, jamais poderia estar vinculado diretamente a qualquer outro órgão da administração pública, em virtude das severas consequências que a ausência de independência poderia acarretar no desempenho de suas funções.

Ademais, em que pese o artigo 55-B da Lei Geral de Proteção de Dados prever que está resguardada a autonomia técnica e decisória da ANPD (BRASIL, 2018), a mera previsão legal não é garantia de sua aplicabilidade prática, em especial se for considerado que a hierarquia em que está subordinado e também a possibilidade de controle de orçamento.

Nesse aspecto, é importante que se teça comentários a respeito da inexistência de uma autonomia financeira da ANPD, afinal, pela forma de constituição enquanto órgão da administração direta, tem-se que seus recursos financeiros irão constituir o montante do orçamento destinado a presidência da república, e assim, as receitas necessárias ao exercício das atividades da autoridade dependerão do repasse feito pelo governo federal.

Tal previsão está pactuada no artigo 55-L da Lei 13.709/18, no entanto, é interessante notar que não apenas essas serão suas fontes de recursos financeiros, podendo ainda buscar a venda de bens móveis e imóveis, o resgate de valores aplicados no mercado financeiro, ou então de doações e subrogações, entre outras

hipóteses (BRASIL, 2018). É importante destacar que a lei não permitiu, semelhante as legislações internacionais, que as multas pudessem integrar seu orçamento.

No entanto, o que se tem é que a maioria dos recursos financeiros da Autoridade serão aqueles que vierem a ser repassados pela União, dessa forma, a ANPD será primordialmente custeada pelos valores que forem autorizados pela lei do orçamento anual, ademais, a falta de recursos que vierem a ocorrer durante seu exercício poderá ser suprida com a realocação de recursos ou por outros ainda que não previstos na Lei orçamentária (CASTRO, 2019).

Não obstante, uma questão que precisa ser considerada, e que, de certa forma, até justifica a escolha de seu arranjo institucional e também da limitação quanto a sua autonomia financeira tem a ver com o momento político experienciado durante o período de sua criação, demarcado por uma acentuada busca pela contenção de gastos do poder público.

Sobre isso, Paula e Vasconcelos (2019, p. 726) observam que o processo de construção da Autoridade:

Reside no peso de um momento de intensa restrição orçamentária e financeira que constrangia as decisões governamentais. A luta pela criação de uma nova entidade poderia prolongar o debate interno no Governo Federal, carregando riscos inerentes a eventual nova paralização do tramite da proposta.

Logo, a implementação da Autoridade Nacional de Proteção de Dados como órgão integrante da Presidência da República foi a solução encontrada frente as barreiras que impediam que o poder executivo criasse uma entidade que gerasse mais despesas ao Tesouro Nacional, frente as limitações que imperavam graças a Lei de Responsabilidade Fiscal (DONEDA, 2019).

No entanto, pelo que pode ser entendido da própria lei, a natureza atual da autoridade é transitória, de sobremaneira que se determinou, em um período máximo de dois anos da sua criação, que seja discutido a respeito da sua transformação em outro organismo público, seja uma autarquia ou uma agência reguladora² (BRASIL, 2018).

² Nesse aspecto, faz-se importante uma pequena diferenciação a respeito dessas figuras. Nos ensinamentos de DI PIETRO (2019) a autarquia deve ser entendida como uma pessoa jurídica de direito público, capaz de se auto-administrar e assim realizar o serviço público a qual se destina, além disso, a autarquia é criada por lei e sofre influencia do controle administrativo exercido pela administração direta. Já a agência reguladora (DI PIETRO, 2019) é um organismo da administração direta ou indireta a qual é demarcado pela especificidade em determinada temática, devendo a agência reguladora organizar o setor afeto as suas competências e fiscalizar as entidades a sua atuação submetidas.

Assim, é crível a possibilidade de reformulação da ANPD de sobremaneira que isso possa acarretar, futuramente, uma maior autonomia e independência para uma atuação desinteressada de suas funções, por não estar vinculada a nenhum outro órgão da administração públicas e por possuir orçamento próprio para desenvolver suas funções com maior eficácia.

No que concerne a respeito da existência de uma independência funcional dos membros componentes da autoridade, é preciso notar que, em que pese estar atualmente rotulada como um órgão, a ANPD teve seu corpo de funcionários e diretores estruturado de maneira muito similar a de uma Autarquia federal, seja no desempenho de suas funções ou então na existência de estabilidades e demais garantias.

A primeira constatação a ser feita aqui tem relação com as limitações financeiras que a autoridade passa em virtude da contenção de despesas. Dessa maneira, a LGPD aduz que a o provimento de cargos e de funções da ANPD está condicionada a prévia e expressa previsão na Lei Orçamentária Anual e também nas demais diretrizes orçamentárias (BRASIL, 2018).

Ademais, a Lei Geral de Proteção de Dados prevê que os cargos em comissão e as funções de confiança devem ser remanejados de outros órgão e entidades componentes da administração federal (BRASIL, 2018). Dessa maneira, em virtude da ausência de quadros próprios, poderá também faltar-lhe servidores que atuem com a devida *expertise* e o grau de técnica o qual a matéria de proteção de dados necessita.

Isso, mais uma vez, é uma corroboração com as ideias de que a Autoridade foi criada em um momento de contenção de despesas do poder público, visto que a transferência de cargos em comissão ou funções de confiança na ANPD não gera gastos para administração pública, visto estes já possuírem previsão orçamentária (ARMELIN; TEIXEIRA, 2019).

Com relação aos diretores que comporão a Autoridade Nacional, a lei se preocupou exaustivamente em replicar as disposições legais destinadas aos diretores de autarquias especiais, a fim de garantir-lhes uma maior autonomia em seu cargo e na condução da ANPD durante a persecução de seus objetivos.

O processo de escolha daqueles que comporão o Conselho Diretor está preceituado no artigo 55-D, parágrafo 1º da LGPD (BRASIL, 2018), para que a

escolha seja efetivada, deverá ocorrer a nomeação do candidato pelo Presidente da República logo após sua aprovação pelo Senado Federal.

O procedimento mais complexo é de todo útil, pois mitiga a possibilidade que o executivo busque colocar no comando da ANPD pessoas que sirvam aos interesses do poder público federal ou então de empresas do setor privado. Além disso, a medida ajuda a aumentar a autonomia dos Diretores para o exercício de suas funções.

A lei também garante a estabilidade funcional aos dirigentes da ANPD, ao permitir que a sua saída do cargo diretivo ocorra, quando não se tratar do termo final do mandato, somente em casos de renúncia, demissão por processo administrativo disciplina ou por condenação judicial transitada em julgado, conforme o artigo 55-E da Lei Geral de Proteção de Dados (BRASIL, 2018).

Positivando a estabilidade dos diretores, a LGPD amplia a possibilidade de uma atuação autônoma e desinteressada dos dirigentes, de maneira que estes poderão deliberar quanto às medidas para a efetivação da Lei sem qualquer vinculação com interesses ou decisões que não sejam técnicas (ARMELIN; TEIXEIRA,2019).

A Lei Geral de Proteção de Dados também dispõe a respeito do dever de sigilo em relação as informações que os diretores tomarem conhecimento durante seu mandato, para isso, a LGPD aplica o artigo 6º da Lei nº 12.813 de 2013 (BRASIL, 2018).

Não obstante, é pertinente a crítica feita por Castro (2019) a respeito da estabilidade dos membros diretores da ANPD, isso porque, como será composta em maioria por membros de cargos em comissão, aquela se torna passível de questionamento, o que poderá acarretar a nomeação de membros que não são estáveis e assim tenham sua autonomia reduzida.

Resta também discutir a respeito dos poderes concedidos a Autoridade para que possa realizar suas atribuições e também garantir a correta aplicação da lei de maneira efetiva, sem ser coibida por quaisquer outros entes públicos ou privados para, por exemplo, aplicar ou não determinada sanção.

O artigo 55-J da LGPD atribui a ANPD uma série de competências e atribuições, dentro o rol de 24 incisos, ele estabelece que a Autoridade Nacional possuirá poderes normativos, ao criar a Política Nacional de Proteção de Dados e

também de poder, na esfera administrativa, interpretar a LGPD e a legislação sobre o tema. Além disso, ela também poderá editar regulamentos e procedimentos a serem observados sobre o tratamento de dados e também sobre o Relatório de Impacto à Proteção de Dados (BRASIL, 2018).

A Autoridade Nacional de Proteção de Dados também possui poderes de fiscalização, podendo realizar auditorias em casos de denúncias a respeito de violações a Lei durante o tratamento de dados, também será possível que venham aplicar multas e outras sanções sobre as empresas e o poder público quando houver sido constatado qualquer ilegalidade no tratamento (BRASIL, 2018).

Exerce também poderes consultivos, devendo responder a consultas dos titulares de dados e também emitir opiniões e notas técnicas para o poder público quando solicitada. A Autoridade também possui um importantíssimo papel educativo, devendo promover o conhecimento das normas e políticas públicas em matéria de privacidade e proteção de dados para toda a população (BRASIL, 2018).

2.5 COMPARATIVO ENTRE AS ATIVIDADES DESEMPENHADAS PELAS AUTORIDADES DE PROTEÇÃO DE DADOS: COMO ESTÁ A AUTORIDADE BRASILEIRA FRENTE AS DEMAIS AUTORIDADES DE PROTEÇÃO DE DADOS?

É preciso destacar que quanto maior a semelhança que o organismo criado no Brasil possuir com o da União Europeia, maior será a respeitabilidade brasileira no cenário internacional de proteção de dados, vendo o país como uma nação séria e comprometida com a preservação dos direitos dos titulares e também um local atrativo economicamente e propício a transferência internacional de dados entre empresas e organizações da Europa e de outros países que estejam implementando legislações sobre a temática

Além disso, uma Autoridade de Proteção de Dados forte e independente é também de enorme valia para o fluxo de dados na constância do Mercosul, visto que, em especial tratando-se tanto da Argentina quanto do Uruguai, fomentará o comércio e poderá intensificar a cooperação internacional entre os países formadores do Bloco (ITSRIO, 2018).

Delimitada cada uma das Autoridades de Proteção de Dados da Argentina e do Uruguai, e também traçado o Modelo de DPA que vigora na União Europeia,

resta agora fazer o comparativo destas com a futura Estrutura da Autoridade Nacional de Proteção de Dados, a fim de se demonstrar as semelhanças e diferenças entre esses organismos públicos.

Através da aplicação de uma metodologia de Direito Comparado, planeja-se neste capítulo assimilar os pontos existentes dos modelos uruguaio e argentino com aqueles que a lei brasileira delimitou para a ANPD a fim de ver quão parecidas ou diferentes essas entidades públicas são.

Para isso, utilizar-se-á todos os dados analisados no capítulo anterior construído o raciocínio científico com base nas quatro variações de autonomia esperadas de uma Autoridade de Proteção de Dados: financeira, estrutural, funcional e seus poderes.

Com relação independência financeira, o Regulamento europeu preceitua que as APDs deverão possuir um orçamento próprio para a realização de suas funções, este é destinado dos recursos públicos do estado membro e não integra as receitas de nenhum dos poderes ou de outros órgãos (UNIÃO EUROPÉIA, 2016).

Não obstante, essa forma não foi adotada na sua integralidade pelas autoridades dos países sul americanos, o que mais se aproximou dessa estrutura foi a Argentina quando passou a autoridade para ser componente da *La Agencia*, no entanto, apesar da autarquia possuir orçamento próprio, as receitas destinada ao órgão de controle e proteção de dados estão juntas as demais receitas, de sobremaneira que se faz necessária que a própria agência destine recurso para sua atuação (IDEC, 2019).

O modelo de autonomia financeira da ANPD, dessa forma, está mais próximo daquele idealizado para a Autoridade uruguaia, onde esta é vista como um órgão pertencente à Administração Pública Federal Direta, com suas receitas totalmente integrantes desta (URUGUAI, 2008).

Apesar da previsão que a Autoridade Nacional de Proteção de Dados irá elaborar sua própria proposta orçamentária, ela ainda irá ser integrante do orçamento da presidência da república (BRASIL, 2018) ficando inclusive sujeita aos ditames da legislação orçamentária (CASTRO, 2019).

Sobre a estrutura que deve ser concedida às Autoridades de Controle, como já elencado, o GDPR criou uma estrutura nos moldes de uma Autarquia, estando distanciada de todos os demais entes da administração pública federal,

além disso, o regulamento ordena que essas Autoridades tenham a sua disposição bens e pessoal qualificado para que possam exercer suas atividades (UNIÃO EUROPÉIA, 2016).

Nesse sentido, o que mais se aproxima da figura europeia é a Autoridade Argentina, visto integrar uma autarquia federal, não obstante, da mesma forma que ocorre com seu orçamento, ela utiliza os próprios bens da Agência no desempenho de suas funções e também o pessoal da entidade. Ademais, o fato de não possuir um corpo técnico especializado para a realização de suas funções tem sido visto como um entrave pela população do país (IDEC, 2019).

Já os modelos uruguaio (URUGUAI, 2008) e brasileiro (BRASIL, 2018) adotaram a estrutura como integrante da administração direta e totalmente vinculada a presidência da república, de maneira que, além da explícita subordinação a que esses órgão estarão submetidos ao governo federal de seus respectivos países, dependem da disponibilização de uma estrutura/ambiente para a realização de suas atividades.

A esse respeito, é ainda difícil ver o que espera para a ANPD, nem sequer constituída e também sem previsão dentro o orçamento do governo federal, o que se pode afirmar no presente momento é que todos os bens serão integralmente fornecidos pela presidência da república, o que pode dificultar sua atuação e, na pior hipótese, obrigá-la a se submeter as vontades exteriores primeiro para que receba equipamentos e demais itens de trabalho.

A respeito da autonomia financeira e estrutural que cerca as Autoridades de Proteção de Dados, há algumas constatações que são pertinentes quanto a isso.

Para muitos doutrinadores, a forma como foi constituída a Autoridade Nacional de Proteção de Dados acaba sendo um ponto negativo, visto que além da possibilidade de intervenção da administração federal em sua atuação, representa uma dissonância em relação ao modelo europeu, dificultando o reconhecimento do país como adequado em relação a proteção de dados e também gerar entraves econômicos e comerciais (PAULA; VASCONCELOS, 2019).

Existe sim certa similitude com os modelos adotados pelo Uruguai e pela Argentina nesse aspecto, no entanto, é preciso lembrar que a própria União Europeia liberou no ano de 2003 recomendação a respeito dessa forma de estruturação (UNIÃO EUROPÉIA, 2003), e que desde a promulgação do GDPR,

esses países latino americanos tem repensado a sua estrutura de proteção de dados e inclusive pensado em novas leis de proteção de dados.

O que mais assemelha todos os modelos de Órgão de Controle, tanto da União Europeia quanto com os modelos de Autoridades de proteção de Dados da América do Sul, e aqui inclui-se a ANPD, tem a ver com a autonomia funcional, na parte que concerne aos Diretores desses organismos.

Primeiro, todas as leis estabeleceram um procedimento complexo para a nomeação destes, envolvendo mais de um dos poderes, normalmente o executivo federal e uma ou mais casas do poder legislativo. Há certas variações como ocorre na legislação Argentina de uma consulta pública a respeito do dirigente indicado para compor a diretoria (IDEC, 2019).

As legislações também são positivas no que diz respeito a delimitar a duração dos mandatos dos dirigentes, sempre estabelecendo prazos para isso. É também comum a presença de instrumentos que garantam a estabilidade dos dirigentes das APDs, dessa forma, antes do término do mandato, os diretores só poderão ser exonerados, via de regra dessas legislações, quando houver renúncia, processo administrativo disciplinar, ou sentença transitada em julgado.

A questão negativa em relação a ANPD reside na crítica já elucidada por Castro (2019) a qual reside na possibilidade de ser discutida a estabilidade dos membros em comissão que estarão compondo a Autoridade Brasileira.

Logo, sendo derrubada a estabilidade dos dirigentes, a APD brasileira irá se destoar das demais existentes e isso poderá, drasticamente, impedir o reconhecimento de sua eficácia no cenário internacional e travar as relações comerciais e de transferência de dados tanto na América do Sul quanto com países europeus.

Além dessas questões, há um ponto positivo em relação a ANPD com as demais Autoridades, residindo no fato de que está também positivado o dever dos dirigentes de guardarem sigilo durante e após o mandato das informações que tomarem conhecimento (BRASIL, 2019).

Essa é uma medida de enorme importância, afinal, frente a uma economia movida a base de dados pessoais, que fomenta e também dá origem a diversos modelos de negócio delimitar restrições ao uso das informações demonstra a importância que o tema tem para a política brasileira.

No entanto, a ANPD possui uma grave falha a respeito de seu corpo técnico, visto que, diferente dos demais países que orientam que as Autoridades de Proteção de Dados tenham um pessoal próprio para o exercício de todas as funções ali dentro, a autoridade brasileira terá seus servidores remanejados de outros órgãos da Administração Direta Federal (BRASIL, 2018), em virtude dos debates a respeito do corte de gastos que se encontra em debate entre os poderes.

Assim, é preciso entender que os funcionários não serão um corpo técnico especializado em matérias como tecnologia e privacidade e proteção de dados, o que pode configurar um entrave quando no exercício de suas funções fiscalizatórias e normativas.

Por fim, o último item que precisa ser discutido tem relação com os poderes destinados a Autoridade Nacional de Proteção de Dados. A primeira constatação a ser feita em relação a isso é positiva, visto que ela contempla todos os poderes que o Regulamento europeu positivou para suas APDs, e, inclusive, até mais quando comparado com a Autoridade do Uruguai, a qual não possui um poder educativo (IDEC, 2019).

No geral, nos 24 incisos que a lei nº 13.709/2016 estabeleceu as competências da ANPD, vemos desde os poderes básicos como os de fiscalização dos procedimentos de tratamento e também de aplicar sanções nos casos de violação de tratamento de dados (BRASIL, 2018).

A legislação chega inclusive a inovar frente as demais, como na possibilidade de criar abrandamentos nas exigências da lei para micro e pequenas empresas, podendo retirar, por exemplo, a necessidade de sempre terem um encarregado de proteção de dados (BRASIL, 2019), o que se demonstra como uma enorme vantagem ao favorecer a livre iniciativa e a liberdade econômica no país.

O que pode se mostrar mais difícil na prática tem relação com o direito de petição dos titulares a autoridade, visto que, enquanto a legislação europeia (UNIÃO EUROPEIA, 2016) possibilita que os envolvidos no tratamento de dados adotem determinada conduta, a entidade brasileira se assemelha ao modelo do Uruguai (GUIDI, 2019), onde somente poderá intimá-los para que venham a corrigir um problema ou realizar uma conduta, mas jamais obrigá-los a adotar certo comportamento.

Ainda que todos os poderes caminhem para demonstrar uma efetiva atuação da ANPD, é preciso ressaltar novamente que a forma como foi estruturada e também as disposições a respeito de seu orçamento não são de todos benéficas a sua atuação, de forma que os óbices que ali estiverem presentes irão refletir no desenvolvimento de suas competências.

3 CONSIDERAÇÕES GERAIS

A fim de que se pudesse trazer respostas ao problema de pesquisa, foi construído um raciocínio a partir da análise da evolução tecnológica e das transformações acentuadas pela qual as diversas sociedades do mundo tem passado, em virtude da comunicação e troca de informações que se dão de maneira ininterrupta.

Após isso, passou-se a analisar como o direito tem se mostrado frente a essas transformações, com ênfase especial, no primeiro momento, nas tendências regulatórias que surgiram em relação a internet e logo após debruçou-se sobre a formação do pensamento a respeito da proteção de dados pessoais e privacidade na modernidade em virtude do acentuado compartilhamento e disponibilização de informações na rede.

Para muitos, os dados já são considerados como que um novo petróleo, sendo capazes de movimentar toda a economia mundial. Afinal, a quantidade insondável de informações que uma pessoa tem, que variam desde dados financeiros como o *score* bancário e os números do cartão de crédito, até informações deixadas como rastros na internet por meio da utilização de buscadores e de sites de *e-commerce* que podem ser estudadas através das técnicas de *profiling*, montando um perfil sócio-econômico dos usuários e assim permitindo o oferecimento de produtos e serviços especializados.

Em um primeiro olhar, a prática das empresas de explorar dados a fim de garantir ofertas de acordo com os interesses de cada uma das pessoas poderia parecer uma conduta muito benéfica se não fosse pelo fato de que a exploração dessas informações se deu, por um longo tempo, sem o menor consentimento dos usuários.

No entanto, o tratamento de dados ocorria sem que as empresas perguntassem se aqueles que utilizavam seu serviços se encontravam de acordo com esse recolhimento, sem que expusessem os reais motivos pelos quais tratavam os dados, e também, muitas das vezes, a coleta era realizada além da própria aplicação acessando informações de outros locais dos dispositivos, como o gerenciador de arquivos e a câmera.

Isso ensejou dos governos de diversos países que buscassem a criação de legislações que viessem a tratar a respeito da proteção dos dados e garantissem o direito a autodeterminação informativa dos usuários dentro da rede.

Ocorre que a legislação precisa ser implementada pelos países de alguma maneira, da mesma forma, é preciso a frequente fiscalização dos estamentos e garantias elencados pela lei, e para isso que foram criadas as Autoridades de Proteção de Dados pelos países que estabeleceram tais leis.

Na análise de cada uma das figuras criadas pelos países aqui pesquisados, é notório a quantidade de semelhanças que essas possuem quanto a sua estruturação e suas atribuições.

O modelo definido na Europa tem sido a base de todo e qualquer outra sistemática de proteção de dados que tenha surgido em outros países, como dito, as leis setoriais europeias balizara fortemente a criação do sistema não só do Uruguai e da Argentina, mas de tantos outros países que transformaram a privacidade e a Proteção de Dados em uma pauta política urgente.

Da mesma forma, a figura da Autoridade de Proteção de Dados ganhou posição de destaque nessas discussões, a autonomia do ente administrativo para o exercício das suas atividades de fiscalização e regulatórias.

Não é possível que se pense o aprimoramento da proteção de dados e o desenvolvimento de novas normativas que estejam aptas para a abarcarem a diversidade de situações de tratamentos de dados sem que se permita a atuação de um órgão independente de influencias externas e munido de um corpo técnico especializado. Espera-se que estes órgãos administrativos realmente sirvam como entes fiscalizadores das disposições da lei e que possuam uma atuação totalmente autônoma, não estando submetidos a interesses do governo ou de instituições privadas.

No entanto, a atuação de uma APD não se limita a proteção de dados por intermédio da aplicação de sanções cometidas pelos controladores, mas também possui o papel de regular praticas de tratamento de dados a fim de preservar o avanço tecnológico e de não estagnar a economia ou o comércio internacional.

A Lei Geral de Proteção de Dados foi criada com forte inspiração das normas existentes na União Européia, e, nesse mesmo diapasão ocorreu a estruturação da Autoridade Nacional.

Assim, o texto legal foi claro e preciso no que concerne as atribuições e incumbências da ANPD, inclusive achou por bem normalizar a previsão de que a Autoridade possui autonomia técnica para o exercício de seu mister.

Não obstante, conforme tudo o que já foi previamente destacado, normativas legais não tem, por si só, o poder de tornar suas previsões efetivas na realidade, dessa maneira, parece difícil crer que a ANPD conseguirá ser plenamente independente e desinteressada ao realizar suas atribuições de fiscalização, sanção e de regulamentação.

O fato de a Autoridade Nacional encontrar-se plenamente dependente do poder executivo federal, tanto nas questões financeiras quanto na parte do fornecimento de equipamentos e pessoal técnico, destoa-se bastante do modelo adotado nos outros países analisados, e, além disso, pode vir a ser considerado como um forte entrave para o reconhecimento do Brasil como um país adequado a proteção de dados e para as transferências internacionais.

Por todo estudo aqui feito, é visível a existência dessas modalidades de independência na legislação européia e a presença de boa parte desses atributos frente as Autoridades criadas no Uruguai e na Argentina, no entanto, na análise da futura ANPD, o que se pode constatar é um grave problema de que se conseguirá ser independente na sua atuação.

4 CONCLUSÃO

A presente pesquisa se propôs ao longo de toda a sua revisão de literatura analisar as principais estruturas de Autoridades de Proteção de Dados existentes realizando posteriormente um comparativo destas com a futura ANPD, órgão regulador da administração pública brasileira, através de uma metodologia de direito comparado a fim de levantar as semelhanças e diferenças entre esses entes regulatórios.

Durante todo o desenvolvimento desse trabalho buscou-se corroborar com a hipótese apresentada de que a ANPD possuiria larga compatibilidade com o modelo europeu de proteção de dados e também com as Autoridades desenhadas no Uruguai e também na Argentina e que isso seria capaz de criar uma espécie de unicidade entre esses organismos a fim de a ANPD, no exercício de suas atribuições, pudesse fiscalizar o cumprimento da lei por parte das organizações públicas e privadas que realizam o tratamento dos dados pessoais e também de garantir os direitos titulares frente as violações e vazamentos que vierem a ocorrer.

Em que pese que a Autoridade Nacional de Proteção de Dados ainda não esteja operacional, embora o Governo Federal já tenha dado o primeiro passo ao promulgar o decreto o qual institui a Autoridade, já é possível que se compreenda como se dará sua atuação e até mesmo traçar considerações a respeito da relevância prática e jurídica que este organismo público terá.

Acima de qualquer outra coisa, a principal conclusão a que se chega é que para a Autoridade de Proteção de Dados possa ser um órgão eficiente e respeitado durante sua atuação e também de que ele garanta o fiel cumprimento da Lei Geral de Proteção de Dados pelas organizações dependerá da sua identificação como um organismo autônomo e independente.

Ademais, além de instrumento de proteção dos direitos dos titulares de Dados Pessoais, a ANPD servirá para incluir o Brasil na economia movida a dados que gradualmente se torna presente em todos os países bem como permitirá que tomem corpo as transferências de dados tanto com a União Europeia, países latino americanos e demais nações que vão aos poucos incluindo em seus ordenamentos jurídicos normas a respeito da Proteção de Dados.

Não obstante, o que mais se parece é que o Brasil encontra-se distante de construir sua autoridade como uma instituição totalmente autônoma, em que pese que boa parte de suas características estejam presentes nas Autoridades de outros países, além da vasta similitude com o organismo uruguaio questões como pertencer a administração pública direta não parecem, até o presente momento, suficientes para garantir a melhor atuação da ANPD em Proteção de Dados Pessoais.

Espera-se que a autoridade venha a ser revista logo em seus primeiros, bem como demanda a lei para que se analise a possível conversão em uma entidade da administração indireta, de sobremaneira que afaste-se o controle do poder executivo em sua atuação e que se confira maior independência para a tutela efetiva dos Dados pessoais/

Dessa forma, a Autoridades terá um papel fundamental dentro do *enforcement* da lei o qual só poderá ser atingido dentro de um escopo de independência estrutural, financeira, funcional e técnica de sua atuação.

REFERÊNCIAS

ARANTES, Camila Rioja; BLUM, Renato Opice. Autoridades de Controle, Atribuições e Sanções. *in*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) **Comentários ao GDPR** - Regulamento Geral de Proteção de Dados da União Européia. São Paulo: Revista dos Tribunais; 2018. p. 227-253.

ARGENTINA. **Decreto** nº 995 de 02 de novembro de 2000a. Disponível em: <<https://bit.ly/2YycxQW>>. Acesso em 24 jun. 2020

_____. **Decreto** nº 1.588 de de 29 de novembro de 2001. Disponível em: <<https://bit.ly/3dB3liF>>. Acesso em: 24 jun. 2020

_____. **Ley** nº 25.326 de 02 de novembro de 2000b. Disponível em: <<https://bit.ly/37Zuyuh>>. Acesso em: 24 jun. 2020.

_____. **Ley** nº 27.275 de 29 de setembro de 2017. Disponível em: <<https://bit.ly/3esiTqm>>. Acesso em: 24 jun. 2020.

ARMELIN, Ruth Maria Guerreiro da Fonseca; TEIXEIRA, Tarcisio. **Lei Geral de Proteção de Dados comentada artigo por artigo**. 1. ed. Salvador: JusPofivm; 2019.

BARLOW, John Perry. A declaration of Independence of cyberspace. **EFF**, 1996. Disponível em<<https://bit.ly/2N8pJpU>>. Acesso em: 19 jun. 2020.

BARRETO, Ana Maria Menna. A Proteção de Dados Pessoais no Brasil. In: HISSA, Carmina Bezerra; LIMA, Ana Paula M. Canto de; SALDANHA, Paloma Mendes. **Direito Digital** – Debates Contemporâneos. São Paulo: Revista dos Tribunais; 2019.

BIEKER, Felix. *Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice*. **HAL**. Disponível em:< <https://bit.ly/2EWXqsE>>. Acesso em: 01 set. 2020

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense; 2019.

BRASIL. **Constituição da República Federativa do Brasil** de 05 de outubro de 1988. Disponível em: <<https://bit.ly/2JLDdFT>>. Acesso em: 02 jun. 2020

_____. **Decreto** nº 10.474 de 26 de agosto de 2020. Disponível em: <<https://bit.ly/3kIMLaD>>. Acesso em: 14 set. 2020

_____. **Lei** nº 7.232 de 29 de outubro de 1984. Disponível em: <<https://bit.ly/36v2bTw>>. Acesso em: 02 jun. 2020.

_____. **Lei** nº 8.078 de 11 de setembro de 1990. Disponível em: <<https://bit.ly/2WDpcz6>>. Acesso em: 02 jun. 2020.

_____. **Lei** nº 12.414 de 9 de Junho de 2011. Disponível em: <<https://bit.ly/2NAE2T1>>. Acesso em: 02 jun. 2020.

_____. **Lei** nº 12.965 de 23 de abril de 2014. Disponível em: <<https://bit.ly/2prCjrk>>. Acesso em: 02 jun. 2020.

_____. **Lei** nº 13.709 de 14 de agosto de 2018. Disponível em: <<https://bit.ly/3gWpeLG>>. Acesso: 12 jul. 2020.

_____. **Projeto de Lei** nº 5276/2016. Disponível em: <<https://bit.ly/2QNnDN8>>. Acesso em: 02 set. 2020.

_____. Ministério da Ciência e Tecnologia. **Sociedade de Informação no Brasil - Livro Verde**. Brasília: Ministério da Ciência e da Tecnologia; 2000.

CASTRO, Maria Eugênia Bordinassi de. A estrutura e a natureza jurídica da Autoridade Nacional de Proteção de Dados com base na lei nº 13.853/2019. In: MAGRO, Américo Ribeiro; TEIXEIRA, Tarcísio (coords.). **Proteção de Dados - Fundamentos Jurídicos**. 1. ed. Salvador; JusPODIVM; 2019. p. 199 - 227.

CARVALHO, Lucas Borges de. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. **Revista Brasileira de Direito**, Passo Fundo, v. 11, n. 2, p. 213-235, mai./ago. 2018. Disponível em <<https://bit.ly/2PKXlqd>>. Acesso em: 02 nov. 2019.

COMISSÃO EUROPEIA. **Adequacy Decisions** - How the EU determines if a non-EU country has a adequate level of data protection. Disponível em <<https://bit.ly/3eiDkGf>>. Acesso em: 19 jun. 2020.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva; 2000.

DELGADO, Lucrecio Rebollo; SALTOR, Carlos Eduardo. **El Derecho a a Protección de Datos en España y Argentina - Orígenes y Regulación Vigente**. Madrid: Editorial DYKINSON; 2011.

DIÁRIO DE NOTÍCIAS. **O documento que explica como a Cambridge Analytica ajudou a eleger Trump**. Diário de notícias. 2018. Disponível em <<https://bit.ly/3hMiYHq>>. Acesso em: 19 jun. 2020.

DONEDA, Danilo. **Da Privacidade à Proteção dos Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 2. ed. rev. e atual. São Paulo: Thomson Reuters Brasil; 2019.

FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais - Noções Introdutórias para a compreensão da Importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, ANA; OLIVA, Milena; TEPEDINO, Gustavo (Coords.). **Lei Geral de Proteção de Dados Pessoais e a suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters do Brasil; 2019a. p. 23-52.

_____. Objetivos e Alcance da Lei Geral de Proteção de Dados. *In*: FRAZÃO, ANA; OLIVA, Milena; TEPEDINO, Gustavo (Coords.). **Lei Geral de Proteção de Dados Pessoais e a suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters do Brasil; 2019b. p. 99-129.

GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. *in*: BRANCO, Sérgio; TEFFÉ, Chiara de (Org.). **Privacidade em perspectivas**. Rio de Janeiro: *Lumen Iuris*; 2018. P. 85-109.

IDEC - INSTITUTO BRASILEIRA DE DEFESA DO CONSUMIDOR. **Autoridade de Proteção de Dados na América Latina - Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai**. São Paulo: Idec; 2019.

ITSRIO - INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Proposta para a criação da Autoridade Brasileira de Proteção de Dados Pessoais**. Rio de Janeiro: ITSRIO; 2018.

JOHNSON, David; POST, David. Law and Borders: the rise of. law in cyberspace. **Stanford Law Review**, [S.l.], v. 48, n. 5, p. 1367-1402, mai. 1996. Disponível em <<https://bit.ly/2PEmmbS>>. Acesso em 02 nov. 2019.

LEMOS, Ronaldo. **Direito, tecnologia e cultura**. 1. ed. Rio de Janeiro: Editora FGV; 2005.

LEORNADI, Marcel. **Fundamentos de Direito Digital**. São Paulo: Revista dos Tribunais; 2019.

_____. **Tutela e privacidade na internet**. São Paulo: Saraiva; 2011.

LESSIG, Lawrence. **Code: version 2.0**. New York: Basic Books, 2006.

MAGRANI, Eduardo. **A internet das Coisas**. Rio de Janeiro: FGV Editora, 2018.

MARINELI, Marcelo Romão. **Privacidade e rede sociais virtuais**. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais; 2019.

OLIVEIRA, Felipe. Senado decide que LGPD entra em vigor agora, mas prazo depende da sanção. UOL. Disponível em: <<https://bit.ly/33rXZDE>>. Acesso em: 14 set. 2020

PAULA, Felipe de; VASCONCELOS, Beto. A Autoridade Nacional de Proteção de Dados. In: FRAZÃO, ANA; OLIVA, Milena; TEPEDINO, Gustavo (Coords.). **Lei Geral de Proteção de Dados Pessoais e a suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters do Brasil; 2019. p. 717-737.

PERRARO, Amanda Garcia. Sociedade Digital: Novos Desafios para o Direito. In: CAMARGOS, Coriolano Almeida; SANTOS, Cleórbete (Coords.). **Direito Digital: novas teses jurídicas**. Rio de Janeiro: Lumen Juris; 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. rev. atual. e ampl. São Paulo: Saraiva; 2012.

PINTO, Álvaro Vieira. **O conceito de Tecnologia**. Rio de Janeiro: Contraponto, 2005.

PÓVOA, Marcello. **Anatomia da Internet**. Rio de Janeiro: Casa da Palavra; 2000.

SALDANHA, Nuno. **Novo Regulamento Geral de Proteção de Dados - O que é? A quem se Aplica? Como Implementar?**. 1. ed. Lisboa: FCA - Editora de Informática; 2018.

SIQUEIRA, Antônio Henrique Albani. Disposições preliminares. In: SIQUEIRA, Antônio Henrique Albani; FEIGELSON, Bruno (Coords.). **Comentários à Lei Geral de Proteção de Dados – Lei 14.709/2018**. São Paulo: Revista dos Tribunais, 2019. p. 15-58.

UNIÃO EUROPÉIA. **Convenção Europeia de Direitos Humanos** de 1953. Disponível em <echr.coe.int>. Acesso em: 19 jun. 2020.

_____. **Convenção 108** de 1981; Disponível em: <<https://bit.ly/2WAtibi>>. Acesso em: 19 jun. 2020.

_____. **Decisão** nº 2003/490/CE de 30 de Junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina. Disponível em: <<https://bit.ly/2A0DLWK>>. Acesso em: 24 jun. 2020.

_____. **Decisão** nº 2012/484/UE de de 21 de agosto de 2012, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Disponível em < <https://bit.ly/3IGjJUw>>. Acesso em: 01 set. 2020.

_____. **Directiva** nº 96/45CE. Disponível em: <<https://bit.ly/2oFp1XE>>. Acesso em: 19 jun. 2020.

_____. **Regulamento Geral de Proteção de Dados** 2016/679. Disponível em: <<https://bit.ly/2JJYHmK>>. Acesso em: 19 jun. 2020.

URUGUAI. **Decreto** nº 414 de 31 de agosto de 2009. Disponível em: <<https://bit.ly/3dBfEvE>>. Acesso em: 25 jun. 2020

_____. **Ley** nº 18.331 de 18 de agosto de 2008. Disponível em: <<https://bit.ly/2NsuAlb>>. Acesso em: 24 jun. 2020

VAINZOF, Rony. Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) **LGPD** – Lei Geral de Proteção de Dados Comentada. São Paulo: Revista dos Tribunais; 2018. p.19-176.

ZATARAIN, Jesús Manuel Niebla. Smart Cities and personal data: balancing innovation, technology and the law. **Direito, Estado e Sociedade**, Rio de Janeiro, [S.l.], n. 53, p. 205-223, jul./dez. 2018. Disponível em: <<https://bit.ly/2pzzgxa>>. Acesso: 25 jun. 2020