



Instituto  
de Tecnologia  
& Sociedade  
do Rio

# **Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais**

**O estudo foi elaborado por:**

Chiara Spadaccini de Teffé e Mario Viola.

**Contribuíram com o estudo:**

Jaqueline Simas de Oliveira, Fabro Steibel,  
Eduardo Magrani e Giovana Carneiro.

---

## Sumário Executivo

1. O veto à Autoridade Nacional de Proteção de Dados, na Lei n. 13.709/2018, representou uma significativa perda para a estrutura de proteção dos dados pessoais das pessoas naturais no País, bem como atingiu diretamente a efetividade da mencionada norma, a fiscalização de seu cumprimento e sua devida aplicação pelas instituições. Com o veto, foi esvaziado todo o capítulo IX da Lei, o qual tratava da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Arts. 55-59). Diante disso, além das pessoas naturais disporem de garantias e de instrumentos reduzidos para a tutela de seus dados pessoais e privacidade, as empresas não gozarão de facilidades e orientações que uma Autoridade poderia lhes proporcionar.

2. Como será analisado ao longo do relatório, o estabelecimento de uma autoridade verdadeiramente independente, autônoma e com corpo técnico qualificado é fundamental para que a regulação do tema ocorra de forma apropriada, privilegiando a pessoa natural, e em linha com o Regulamento Geral Europeu sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR). Como a Autoridade deve ter, entre suas funções, a possibilidade de monitorar tanto o Estado quanto sujeitos privados, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas.

3. A experiência de outros países mostra a relevância da existência de uma Autoridade nacional específica para a aplicação eficiente de suas respectivas leis de proteção de dados pessoais. Reino Unido, França, Itália, Argentina e Uruguai são exemplos significativos no tema e, como será apontado, devem servir de inspiração para o modelo brasileiro. Não há dúvidas de que uma maior compatibilidade entre os diferentes sistemas facilitará, por exemplo, os fluxos internacionais de dados, o que beneficiará os mais diversos setores e poderá ser utilizado para variados fins, como comerciais e para a cooperação entre

entidades públicas.

4. A existência de uma Autoridade Nacional independente e com elevada autonomia é um dos requisitos para que o Brasil e sua legislação sejam reconhecidos como adequados ao modelo de tratamento de dados pessoais estabelecido na Europa por meio do GDPR. Na América do Sul, apenas Argentina e Uruguai receberam essa chancela até o momento. A mencionada análise, ao verificar a situação da autoridade nacional de proteção de dados no País, levará em conta especialmente sua independência em aspectos como estrutura/organização, exercício de funções/atribuições e poderes da autoridade, devendo tanto o legislador brasileiro quanto o Presidente da República, portanto, observarem com cuidado tais requisitos no momento de constituir a Autoridade Nacional.

5. Vindo por meio de lei ou de medida provisória, o importante é que a mencionada Autoridade Nacional brasileira para a proteção de dados seja estabelecida nos moldes do que havia sido proposto no Projeto de Lei da Câmara n. 53/18, o qual se encontrava alinhado com excelentes modelos e práticas internacionais, bem como havia sido objeto de amplo debate público, democrático e multissetorial. Esse é, vale ressaltar, o entendimento majoritário dos diversos setores da sociedade que vêm discutindo a regulação do tratamento de dados pessoais no País, nos últimos anos. Debate esse que o ITS Rio, seus diretores, pesquisadores e associados vêm participando há mais de 10 anos.

6. Para que o Brasil alcance um patamar elevado de proteção aos direitos humanos e de desenvolvimento enquanto nação, defende-se a necessidade da criação de uma Autoridade Nacional de Proteção de Dados Pessoais que goze de autonomia, seja amplamente independente, apresentando as disposições presentes no PLC n. 53/18, e detenha características semelhantes às aquelas preconizadas na norma europeia de proteção de dados.

# Sumário

<b>1. Do veto relativo à Autoridade Nacional de Proteção de Dados</b>	<b>6</b>
<b>2. A Autoridade Nacional de proteção de dados no Projeto de Lei da Câmara n. 53/18</b>	<b>13</b>
<b>3. Modelos estrangeiros de Autoridades para a proteção de dados pessoais</b>	<b>22</b>
3.1 Normas do Regulamento Geral Europeu sobre a Proteção de Dados relativas às Autoridades garantidoras	22
3.2 Autoridade Europeia para a Proteção de Dados	24
3.3 Autoridade do Reino Unido para a proteção de dados (Information Commissioner's Office – ICO)	26
3.4 Autoridade italiana para a proteção de dados de pessoais (Garante per la protezione dei dati personali)	30
3.5 A Autoridade nacional francesa encarregada pela proteção de dados (Commission Nationale de l'Informatique et des Libertés – CNIL)	33
3.6 A agência argentina de acesso à informação pública	37
<b>4. Considerações finais</b>	<b>40</b>
<b>5. Para saber mais</b>	<b>42</b>

## **1. Do veto relativo à Autoridade Nacional de Proteção de Dados**

O veto à Autoridade Nacional de Proteção de Dados representou a questão mais polêmica e significativa na fase de sanção presidencial à Lei n. 13.709/2018, que dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965/2014 (conhecida como Marco Civil da Internet). Com o veto, foi esvaziado todo o capítulo IX da Lei, o qual tratava da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Arts. 55-59).

Ainda que as referências à Autoridade Nacional apareçam na Lei brasileira de proteção de dados 51 vezes, elas no momento não gozam de efetividade, o que prejudica tanto a fiscalização e a aplicação da mencionada norma quanto diminui a possibilidade de uma maior proteção da privacidade e dos dados pessoais das pessoas naturais. Como se não bastasse, determinados dispositivos da Lei por dependerem de regulamentação pela Autoridade Nacional<sup>1</sup> acabam por prejudicar, também, os setores produtivos, já que sem a intervenção da Autoridade todas as empresas, independente do seu tamanho ou atividade, terão que cumprir a integralidade das normas, sem a possibilidade de flexibilização. Não à toa, diversas organizações e setores<sup>2</sup> têm defendido a

---

<sup>1</sup> Como, por exemplo, a norma prevista no parágrafo 3º, do artigo 41, da Lei: “Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. (...) § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.”

<sup>2</sup> Recordar-se que a “Coalizão direitos na rede” redigiu carta em defesa da Autoridade de Proteção de Dados Pessoais, a qual foi assinada por diversos membros do terceiro setor, academia, setor empresarial e setor público. Os principais assinantes foram: Actantes, Casa da Cultura Digital Porto Alegre, Centro de Estudos da Mídia Alternativa Barão de Itararé, Coding Rights, Coletivo Digital, Coolab - Laboratório Cooperativista de Tecnologias Comunitárias, Instituto Beta: Internet & Democracia, Instituto Brasileiro de Defesa do Consumidor, Instituto Nupef, Instituto de Tecnologia e Equidade (IT&E), Internet Sem Fronteiras, Intervozes — Coletivo Brasil de Comunicação Social, Movimento Mega Não, Prioridade Absoluta - Instituto Alana, Proteste - Associação de Consumidores, Open Knowledge, Instituto Alana, Instituto Update, Labhacker, Associação Brasileira das Empresas de Software – ABES, Associação Brasileira das Empresas de Tecnologia da Informação e da Comunicação – BRASSCOM, Associação Brasileira de Provedores de Internet e Telecomunicações – ABRINT, Associação Brasileira Online to Offline – ABO2O, Associação Brasileira de Crédito Digital – ABCD, Associação Brasileira da Indústria Inovadora em Saúde – ABIIS, Câmara Brasileira de Comércio Eletrônico - Camara-e.net, Grupo de

importância da criação de uma Autoridade Nacional de Proteção de Dados Pessoais funcionalmente independente no País, nos moldes do que havia sido estabelecido no PL e preferencialmente com características semelhantes às do modelo estabelecido pelo Regulamento Geral Europeu sobre a Proteção de Dados.

Uma autoridade verdadeiramente independente, autônoma e com corpo técnico qualificado é fundamental para que a regulação do tema não seja fracionada nas mais diversas instâncias que passarão a aplicar a lei nos níveis federal, estadual e municipal. Como a Autoridade deve ter entre suas funções a possibilidade de monitorar o próprio Estado, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas. A entidade exerceria uma função uniformizadora, orientando a fiscalização do cumprimento da nova lei.<sup>3</sup> Além disso, a Autoridade Nacional poderia também oferecer orientações sobre como interpretar os dispositivos legais. Sem ela, são elevadas as chances de que os indivíduos comecem a levar ao Judiciário os direitos que a lei nova traz e que

---

Estudos em Direito, Tecnologia e Inovação do Mackenzie, Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação/GPoPAI-USP, Instituto de Tecnologia e Sociedade do Rio de Janeiro/ITS-Rio, Rede latina-americana de estudos sobre vigilância, tecnologia e Sociedade /LAVITS, Laboratório de Tecnologias Livres da UFABC, Instituto Igarapé, Instituto de Referência em Internet e Sociedade/IRIS, Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público/CEDIS, IP.Rec - Instituto de Pesquisa em Direito e Tecnologia do Recife e Ministério Público do Distrito Federal e Territórios. A carta acima encontra-se disponível em:

<<https://direitosnarede.org.br/c/em-defesa-da-autoridade-independente-de-protecao-de-dados/>> Acesso em: 24.09.18. Além da assinatura da Carta, tais instituições redigiram artigos e textos institucionais defendendo o não veto da Autoridade na Lei. O ITS Rio publicou o artigo *Lei de Dados Pessoais precisa de uma Autoridade independente*, em seu canal no Medium. Disponível em: <<https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64>> Acesso em: 24.09.18.

<sup>3</sup> O risco de não ter uma Autoridade Nacional é de que os outros entes federativos comecem a criar as suas próprias autoridades estaduais ou municipais, visando dar efetividade à Lei. Neste sentido já há projeto de lei em tramitação na Assembleia Legislativa do Estado de São Paulo, o Projeto de Lei nº 598, de 5 de setembro de 2018, que se propõe a suplementar a lei federal e prevê a criação de uma autoridade estadual com competência concorrente com a Autoridade Nacional. Nos termos do PL, essa autoridade estadual seria “órgão da administração pública direta e/ou indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.” Disponível em: <<https://www.al.sp.gov.br/propositura/?id=1000230528>> Acesso em: 24.09.2018. Igualmente já foi aprovada a primeira lei municipal sobre a proteção de dados pessoais, Lei Complementar n. 161, de 05 de julho de 2018, do Município de Vinhedo, que cria a figura do Ouvidor da Proteção de Dados Pessoais, com competência para zelar pela implementação e fiscalização da Lei. Em verdade, essa lei municipal foi aprovada antes mesmo da aprovação pelo Senado Federal da Lei nº 13.709/18, mas em grande medida copia dispositivos da lei federal. Disponível em: <<http://consulta.siscam.com.br/camaravinhedo/arquivo?Id=129711>> Acesso em: 03.10.2018.

isso começa a gerar os mais variados entendimentos nos tribunais brasileiros, tribunais esses que não têm o conhecimento técnico especializado que a matéria exige, havendo então a possibilidade de interpretações diametralmente opostas sobre um mesmo tema, o que poderá gerar uma enorme insegurança jurídica. Pela experiência prática, sabe-se que serão necessários pelo menos três anos de vigência da lei para que as discussões comecem a chegar aos tribunais superiores, quando, só então, os entendimentos começarão a ser uniformizados.

A experiência de outros países mostra a relevância da existência de uma Autoridade Nacional específica para a aplicação eficiente de suas respectivas leis de proteção de dados. O mecanismo permite alcançar uma tutela efetiva da privacidade dos cidadãos, enquanto propicia segurança jurídica na interpretação e aplicação da lei. Na Europa, por exemplo, desde 2000, a proteção de dados pessoais assegurada por uma autoridade independente é considerada direito fundamental, conforme previsto no artigo 8º da Carta dos Direitos Fundamentais da União Europeia. Vale recordar também que, desde a aprovação da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, já existia a obrigação para os Estados-membros da União Europeia de estabelecerem autoridades de proteção de dados que teriam a função de fiscalizar a aplicação no seu território das disposições adotadas pelos Estados-membros nos termos da referida Diretiva.<sup>4</sup> Essa prática foi estendida a outros 17 países integrantes do Conselho da Europa e a 6 países não integrantes dessa organização regional (notadamente, Cabo Verde, Maurício, México, Senegal, Tunísia e Uruguai), por meio do protocolo adicional à Convenção 108 de 1981, no tocante a autoridades de controle e fluxo transfronteiriço de dados, aprovado em 08 de novembro de 2001.<sup>5</sup>

---

<sup>4</sup> Disponível em:

<<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>> Acesso em: 24.09.2018.

<sup>5</sup> Disponível em:

<[https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p\\_auth=YUz9nmn3](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=YUz9nmn3)> Acesso em: 24.09.2018.



Além disso, nos últimos anos, diversos países vêm adotando nova legislação ou atualizando legislações existentes em matéria de proteção de dados para aproveitarem as diversas oportunidades oferecidas pela economia digital, bem como para elevarem a segurança dos dados e a proteção da privacidade das pessoas naturais. Uma maior compatibilidade entre os diferentes sistemas pode facilitar, por exemplo, os fluxos internacionais de dados, o que beneficiaria os mais diversos setores e poderia ser utilizado para fins variados, como comerciais e para a cooperação entre entidades públicas. Apenas a título exemplificativo, uma vez reconhecida a adequação do sistema de proteção de dados do Brasil pela Comissão da União Europeia, empresas portuguesas poderiam transferir seus *call centers* para o Brasil, já que a transferência internacional de dados entre Portugal e Brasil seria facilitada e não dependeria de maiores arranjos contratuais, como ocorre hoje em dia. O mesmo poderia acontecer com *data centers* ou mesmo provedores de computação na nuvem, já que as barreiras impostas pelo GDPR à transferência internacional de dados para países que não têm nível adequado de proteção de dados não se aplicariam ao Brasil, o que, como consequência, atrairia não apenas novos investimentos para o Brasil, mas também possibilidade de expansão dos negócios existentes, em razão da possibilidade de atender a todo o mercado da União Europeia.

O impacto de uma lei de dados pessoais é abrangente. Ela afeta não apenas empresas de tecnologia, mas qualquer outra entidade ou organização pública ou privada que trabalhe com dados. Com a sanção, o Brasil torna-se um dos mais de cem países que dispõem de uma legislação sobre a temática. A inspiração para a lei brasileira veio diretamente da norma europeia de proteção de dados, o *General Data Protection Regulation* (GDPR) ou, em português, o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016).<sup>6</sup>

A existência de uma autoridade independente é um dos requisitos para que o Brasil tenha reconhecida a adequação de suas normas sobre o tema em

---

<sup>6</sup> Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679>> Acesso em: 23.08.18

comparação com o tratamento oferecido na Europa pelo GDPR.<sup>7</sup> Na América do Sul, apenas Argentina e Uruguai<sup>8</sup> receberam essa chancela<sup>9</sup> até o momento. A análise de adequação, ao verificar a situação da autoridade nacional de proteção de dados no País, levará em conta especialmente sua independência em aspectos como: estrutura/organização, exercício de funções/atribuições e poderes.

A existência de uma autoridade independente também pode facilitar o ingresso do Brasil na Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Para que os países possam fazer parte de tal organização, eles devem se obrigar a cumprir as normas estabelecidas pela OCDE, inclusive no tocante à proteção da privacidade e fluxos transfronteiriços de dados pessoais.<sup>10</sup>

No Brasil, os principais argumentos que embasaram o veto à Autoridade na Lei n. 13.709/18 envolveram, essencialmente, a possibilidade de vício de

---

<sup>7</sup> Recorda-se, aqui, o artigo 45(2)(b) do GDPR: “**Transferências com base numa decisão de adequação** 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica. 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos: (...) b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros;”

<sup>8</sup> Alguns países na América Latina têm legislações específicas para a proteção de dados desde o início dos anos 2000, como, por exemplo, Chile, Argentina, Uruguai e Colômbia. Na Argentina, a Lei de Proteção de Dados Pessoais foi aprovada em 2000 (Lei nº 25.326 de 2000 - <http://www.protecciondedatos.com.ar/ley25326.htm> ). No Uruguai, a Lei nº 18.331, que trata da proteção de dados pessoais e da ação de habeas data, está publicada desde o ano de 2008 (<https://legislativo.parlamento.gub.uy/temporales/leytemp3267832.htm> ).

<sup>9</sup> De acordo com documento institucional, “The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with South Korea. The adoption procedure of the adequacy decision concerning Japan was launched on 5 September 2018.”

Disponível em:

<[https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)> Acesso em: 28.09.18.

<sup>10</sup> Disponível em:

<<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> Acesso em: 20.08.18.

iniciativa e questões orçamentárias. Alegou-se que uma iniciativa do Legislativo não poderia criar um órgão como a mencionada Autoridade. Isso só poderia ser feito pelo Executivo, com base nos artigos 61, §1º, II, e 37, XIX, da Constituição Federal de 1988.<sup>11 12</sup> Afirmou-se também que o projeto não poderia criar gastos não previstos no orçamento, uma vez que a Autoridade geraria despesas para a sua implementação e funcionamento. Além disso, vale lembrar que a lei foi aprovada pelo Senado em 10 de julho de 2018, data próxima ao período eleitoral, o que possivelmente gerou e vem gerando um desafio ainda maior para a criação da entidade.

A respeito do vício de iniciativa, entre a aprovação do Senado e a efetiva sanção da Lei, vozes se levantaram afirmando que ele poderia ser superado, em virtude da redação aprovada no PLC n. 53/18 se valer fortemente de projeto de lei apresentado pelo Poder Executivo em 2016 (PL n° 5.276/16) e dos debates e consultas que vinham sendo realizados desde 2010.<sup>13</sup> Destaca-se que a proposta do Executivo, mesmo que não criasse explicitamente a Autoridade nos moldes aprovados, já previa a designação de um órgão competente para a proteção de dados pessoais no País.

Todavia, por questão de respeito estrito às regras constitucionais, o governo preferiu vetar a Autoridade na Lei. Quem concordou com o veto, alegou, entre outras afirmações, que a primeira empresa que sofresse uma sanção recorreria ao argumento de que tal Autoridade seria inconstitucional, o

---

<sup>11</sup> Art. 37 (...) XIX - somente por lei específica poderá ser criada autarquia e autorizada a instituição de empresa pública, de sociedade de economia mista e de fundação, cabendo à lei complementar, neste último caso, definir as áreas de sua atuação; Art. 61. A iniciativa das leis complementares e ordinárias cabe a qualquer membro ou Comissão da Câmara dos Deputados, do Senado Federal ou do Congresso Nacional, ao Presidente da República, ao Supremo Tribunal Federal, aos Tribunais Superiores, ao Procurador-Geral da República e aos cidadãos, na forma e nos casos previstos nesta Constituição. § 1º São de iniciativa privativa do Presidente da República as leis que: II - disponham sobre: e) criação e extinção de Ministérios e órgãos da administração pública, observado o disposto no art. 84, VI;

<sup>12</sup> Na razão dos vetos aos dispositivos relativos à Autoridade, o Presidente afirmou que: “Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, §1º, II, “e”, cumulado com o artigo 37, XIX da Constituição.”

<sup>13</sup> V. a título exemplificativo parecer do ministro aposentado do Supremo Tribunal Federal (STF), Ilmar Nascimento Galvão, e do professor da Universidade de Brasília (UnB), Jorge Octávio Lavocat Galvão, disponível em:

<<https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018>> Acesso em: 24.09.2018.

que traria insegurança jurídica e uma complexa demanda ao Judiciário.<sup>14</sup> Na cerimônia de sanção da Lei, no dia 14 de agosto de 2018, o Presidente anunciou que enviaria ao Congresso projeto de lei para a criação da Autoridade. Nos bastidores, há quem afirme que o Governo pode, até mesmo, editar uma Medida Provisória para criar a Autoridade. De toda forma, a lei de dados apenas entrará em vigor no País após decorridos 18 (dezoito) meses de sua publicação oficial, ou seja, em 16 fevereiro de 2020.

Nesse momento, está nas mãos do Presidente uma relevante ponderação de interesses que envolve segurança pública, privacidade, proteção de dados pessoais e questões econômicas. Fica o anseio de que seja levado em consideração todo o avanço conquistado por meio da ampla discussão pública que norteou a aprovação do Projeto de Lei da Câmara n. 53/18 e que seja considerada a importância da criação de uma Autoridade Nacional de Proteção de Dados Pessoais autônoma, independente e nos moldes do que havia sido estabelecido no PL, sob pena de se prejudicar a efetividade e a aplicação da Lei de Dados Pessoais brasileira.

Importante destacar que já se passaram alguns meses desde a sanção presidencial da Lei n. 13.709/2018 e, até o momento<sup>15</sup>, o Exmo. Sr. Presidente da República, Michel Temer, não enviou qualquer projeto de lei ou medida provisória ao Congresso Nacional, o que pode significar que o tema ficará para a próxima legislatura, situação essa que poderá nos levar à uma situação de elevada incerteza, já que o novo presidente pode optar por não enviar tal texto ao Congresso e/ou os novos integrantes do legislativo federal podem ter uma posição distinta daquela manifestada tanto na Câmara dos Deputados quanto no Senado Federal, quando da aprovação do Projeto de Lei da Câmara n. 53/18, que deu origem à Lei n. 13.709/18, tema do qual trataremos a seguir.

---

<sup>14</sup> V. por exemplo, a manifestação da SUCESU – Sociedade de Usuários de Tecnologia em sua "NOTA DE ESCLARECIMENTO E POSICIONAMENTO ACERCA DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD". Disponível em <http://sucusu.org.br/2018/09/26/nota-de-esclarecimento-e-posicionamento-a-cerca-da-lei-geral-de-protecao-de-dados-lgpd/>> Acesso em: 08.11.18.

<sup>15</sup> Estudo concluído em 11 de novembro de 2018.

## **2. A Autoridade Nacional de proteção de dados no Projeto de Lei da Câmara n. 53/18**

Segundo a versão do Projeto aprovada pelo Senado, a Autoridade Nacional teria natureza de autarquia especial, estaria vinculada ao Ministério da Justiça e gozaria de independência administrativa. Além disso, haveria ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. Essa estrutura foi mantida na Lei n. 13.709/2018, sendo positivado em seu artigo 5º, inciso XIX, que a Autoridade Nacional será “órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.”

No rol de suas atribuições, a Autoridade deveria, por exemplo, zelar pela proteção dos dados pessoais; estimular a adoção de padrões técnicos bem como de serviços e produtos que facilitem o exercício de controle pelos titulares sobre seus dados pessoais; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; solicitar às entidades do poder público, que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado e realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o poder público.

Os artigos 55, 56 e 57 tratavam especificamente sobre a Autoridade Nacional de Proteção de Dados (ANPD) e apresentavam a seguinte redação:

**Art. 55.** Fica criada a Autoridade Nacional de Proteção de Dados - ANPD, integrante da administração pública

federal indireta, submetida a regime autárquico especial e vinculado ao Ministério da Justiça.

§ 1º A ANPD deverá ser regida nos termos previstos na Lei no 9.986, de 18 de julho de 2000.

§ 2º A ANPD será composta pelo Conselho Diretor, como órgão máximo, e pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação desta Lei.

§ 3º A natureza de autarquia especial conferida à ANPD é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira.

§ 4º O regulamento e a estrutura organizacional da Autoridade serão aprovados por decreto do Presidente da República.

§ 5º O Conselho Diretor será composto por 3 (três) conselheiros e decidirá por maioria.

§ 6º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos.

§ 7º Os mandatos dos primeiros membros do Conselho Diretor serão de 3 (três), 4 (quatro), 5 (cinco) anos, a serem estabelecidos no decreto de nomeação.

§ 8º É vedado ao ex-conselheiro utilizar informações privilegiadas obtidas em decorrência do cargo exercido, sob pena de incorrer em improbidade administrativa.

**Art. 56.** A ANPD terá as seguintes atribuições:

I – zelar pela proteção dos dados pessoais, nos termos da legislação;

II – zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III – elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação,

mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V – atender petições de titular contra controlador;

VI – promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII – promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, que deverão levar em consideração especificidades das atividades e o porte dos responsáveis;

IX – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos comercial e industrial;

XI – solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII – elaborar relatórios de gestão anuais acerca de suas atividades;

XIII – editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante, assim como prestar contas sobre suas atividades e planejamento;

XV – arrecadar e aplicar suas receitas e publicar no relatório de gestão a que se refere o inciso XII do *caput* deste artigo o detalhamento de suas receitas e despesas; e

XVI – realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o poder público.

§ 10 Ao impor condicionamentos administrativos ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

§ 20 Os regulamentos e normas editados pela ANPD devem necessariamente ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

**Art. 57.** Constituem receitas da ANPD:

I – o produto da execução da sua dívida ativa;

II – as dotações consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos;

III – as doações, legados, subvenções e outros recursos que lhe forem destinados;

IV – os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade;

V – os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo;

VI – o produto da cobrança de emolumentos por serviços prestados;

VII – os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais e internacionais;

VIII – o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.



A previsão contida no vetado artigo 55 era de se ter um órgão da administração indireta, regido pela Lei n. 9.986/2000 (que dispõe acerca da gestão de recursos humanos das Agências Reguladoras), que gozaria de autonomia financeira e não teria subordinação hierárquica. Essa disposição buscava assegurar a necessária autonomia e independência que a Autoridade Nacional deveria dispor, visto que, entre suas atribuições, ela tinha como função fiscalizar tanto o setor público quanto o setor privado. Caso tal órgão fosse estruturalmente subordinado, ainda que apenas financeiramente, a outro órgão da administração pública, sua autonomia e independência certamente restariam prejudicadas, ao menos no que toca à fiscalização das atividades de tratamento de dados realizadas pelo órgão público ao qual estivesse subordinado.

Essa preocupação com a independência e autonomia foi complementada, no mencionado PL, com a previsão de mandatos com prazos distintos para os primeiros membros do Conselho Diretor da Autoridade — prazos esses não concomitantes com o de Presidente da República —, devendo eles gozar também de mandatos fixos e de estabilidade, disposições que visavam certamente limitar pressões políticas advindas do Governo Federal.<sup>16</sup> A previsão de mandatos distintos impediria, por exemplo, que cada novo Presidente eleito modificasse toda a composição da agência durante o seu mandato e buscasse com isso determinadas facilidades.

Além disso, como destacado no PL, mostra-se de grande relevância o estabelecimento de um dever de confidencialidade quanto às informações privilegiadas obtidas em decorrência de cargo no Conselho Diretor, ainda que

---

<sup>16</sup> Caso semelhante existe na Anatel (Agência Nacional de Telecomunicações). Seu Conselho Diretor (Órgão máximo) é integrado por cinco conselheiros escolhidos e nomeados pelo Presidente da República, após aprovação pelo Senado Federal. Seus membros são brasileiros de reputação ilibada, formação universitária e elevado conceito no campo de sua especialidade. **Os conselheiros têm mandato de cinco anos, com vencimento sequencial, a fim de que as substituições sejam paulatinas e saia apenas um conselheiro por ano. Busca-se com isso evitar a perda repentina da memória e da cultura organizacional no âmbito das decisões da Agência.** Informações disponíveis em: <<http://www.anatel.gov.br/institucional/institucional-menu/estrutura-organizacional/87-lei-de-acesso-a-informacao/institucional/162-conselho-diretor-organograma>> Acesso em: 28.09.18.

após o término do mandato. Essa disposição visava a evitar que, eventualmente, tais sujeitos fossem cooptados por algum setor, em razão das informações privilegiadas às quais tivessem tido acesso em função do mandato. Dispunha o PL que, caso ex-conselheiro utilizasse informações privilegiadas obtidas em decorrência do cargo exercido, ele poderia responder por improbidade administrativa.

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, previsto nos também vetados artigos 58 e 59<sup>17</sup>, teria o papel de trazer o aspecto do debate multissetorial para a proteção de dados pessoais, inspirando-se na bem sucedida experiência do Comitê Gestor da Internet no Brasil (CGI.br). Tendo em vista que a proteção de dados pessoais, ou melhor, a Lei Geral de Proteção de Dados afeta todos os setores, indistintamente, mostra-se de extrema relevância discutir, em um fórum consultivo — como seria o CNPDP —, as especificidades dos distintos setores regulados pela ANPD, a fim de que esta última possa, quando concretizada, aplicar corretamente a lei, considerando-se os desafios e peculiaridades dos diversos tipos de atividades por ela reguladas.

---

<sup>17</sup> Art. 58. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por 23 (vinte e três) representantes titulares, e seus suplentes, dos seguintes órgãos: I – 6 (seis) representantes do Poder Executivo federal; II - 1 (um) representante indicado pelo Senado Federal; III - 1 (um) representante indicado pela Câmara dos Deputados; IV – 1 (um) representante indicado pelo Conselho Nacional de Justiça; V – 1 (um) representante indicado pelo Conselho Nacional do Ministério Público; VI – 1 (um) representante indicado pelo Comitê Gestor da Internet no Brasil; VII – 4 (quatro) representantes da sociedade civil com atuação comprovada em proteção de dados pessoais; VIII – 4 (quatro) representantes de instituição científica, tecnológica e de inovação; e IX – 4 (quatro) representantes de entidade representativa do setor empresarial afeto à área de tratamento de dados pessoais. § 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação, e terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. § 2º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público, não remunerada. § 3º Os representantes referidos nos incisos I, II, III e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades. § 4º Os representantes referidos nos incisos VII, VIII e IX do caput deste artigo e seus suplentes serão indicados na forma do regulamento e não poderão ser membros da entidade mencionada no inciso VI do caput deste artigo.

Art. 59. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e de atuação da Autoridade Nacional de Proteção de Dados; II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III – sugerir ações a serem realizadas pela 40 Autoridade; IV – realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e V – disseminar o conhecimento sobre proteção de dados pessoais e da privacidade à população em geral.

Já as atribuições conferidas à ANPD pelo vetado artigo 56 têm a primordial função de fazer com que a referida Autoridade possa exercer plenamente seus deveres. Diversos são os dispositivos da Lei n. 13.709/18 que exigem ou possibilitam a intervenção da ANPD, seja para regulamentá-los, seja para flexibilizá-los de acordo com as particularidades de alguns tratamentos de dados ou de controladores, de forma a dar maior efetividade para a aplicação da referida Lei.

O artigo 38, *caput*, por exemplo, estabelece que a “A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial”. Já o artigo 40 confere à Autoridade Nacional a possibilidade de “(...) dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência”.

Existe igualmente a previsão de possibilidade de edição de “normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados” (artigo 41, § 3º). Sem a existência da Autoridade Nacional qualquer controlador terá que estabelecer um encarregado para o tratamento de dados pessoais, independente do seu tamanho ou das atividades de tratamento de dados pessoais que realizar. Aqui, a Autoridade teria o papel de flexibilizar a norma de acordo com as especificidades dos distintos controladores.

Da mesma forma, é fundamental a criação da Autoridade para que seja dada efetividade à Lei n. 13.709/18. Seu artigo 53 prevê que “A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa”,

ou seja, sem a autoridade não haverá regulamento da Lei e nenhuma das sanções nela previstas poderá ser aplicada, o que importa dizer que eventuais infrações cometidas não serão penalizadas ou combatidas adequadamente porque não existirá sanção aplicável, a não ser que as infrações se enquadrem em infrações previstas em outras leis.

Da mesma forma, cabe à Autoridade estabelecer as “normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados” (artigo 63). Aqui, mais uma vez, sem a criação da Autoridade não será possível regulamentar essa matéria e os bancos de dados já em funcionamento, quando da entrada em vigor da Lei, ficarão em uma espécie de “limbo” jurídico.

A Autoridade Nacional “estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais” (artigo 51) e poderá ainda reconhecer e divulgar regras de boas práticas e de governança adotadas por distintos controladores e operadores (artigo 50, § 3º).

Poderá igualmente a Autoridade “dispor sobre padrões técnicos mínimos relativos a medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, a serem adotadas pelos controladores” (artigo 46, § 1º).

Esses são alguns exemplos de dispositivos da Lei n. 13.709/18 que demonstram como é fundamental a criação da Autoridade Nacional e que ela seja efetivamente independente. Resta evidente, portanto, que a Autoridade nos moldes propostos pelo PL apresentava elementos essenciais para sua autonomia e independência, devendo eventual lei ou medida provisória oriunda do Executivo replicar integralmente o texto e a estrutura acima desenhados pelo Legislativo e demais atores que participaram de sua construção ampla e democrática. Para a adequada promoção e proteção da privacidade e dos dados pessoais, assim como para se estabelecer o equilíbrio necessário à promoção da

inovação e da livre iniciativa, é necessário que a Autoridade Nacional seja organizada de modo a não sofrer influências ou pressões externas.

Além disso, mostra-se relevante que ela disponha de recursos humanos, técnicos, financeiros e de infraestrutura adequados para o efetivo desempenho de suas atividades; que não seja controlada financeiramente por outro órgão; que seus membros não estejam sujeitos ou subordinados à influência de terceiros; e que demonstre efetivamente que goza de poderes investigativos, corretivos e consultivos. Isso exige um compromisso do Executivo em elaborar uma norma que mantenha de forma integral as disposições previamente discutidas no PL nº 53/18.

De forma a complementar os estudos relativos à Autoridade e sua estrutura, bem como a justificar a referência ao modelo europeu, mostra-se necessário analisar tanto os dispositivos do *General Data Protection Regulation* (GDPR) quanto modelos estrangeiros de Autoridades para a proteção de dados pessoais, em razão dos mesmos já terem um tempo razoável de consolidação, mostrarem-se estáveis e serem citados de forma recorrente pela doutrina especializada como estruturas independentes e com elevado grau de autonomia.

### **3. Modelos estrangeiros de Autoridades para a proteção de dados pessoais**

Neste eixo do estudo, serão analisados modelos estrangeiros de Autoridades específicas para a proteção de dados pessoais, notadamente as Autoridades do Reino Unido, Itália, França e Argentina, as quais atuam em nível nacional, com vistas a demonstrar o grau de afinidade entre os dispositivos que foram vetados na nossa Lei n. 13.709/18, que versavam sobre a Autoridade Nacional de Proteção de Dados, e as disposições estabelecidas nos mencionados países. Além disso, serão tecidos comentários sobre a Autoridade Europeia para a Proteção de Dados (AEPD), que atua junto às instituições integrantes da União Europeia — órgãos e agências —, bem como acerca das normas do novo Regulamento Geral Europeu sobre a Proteção de Dados (GDPR) que tratam das autoridades garantidoras.

#### **3.1 Normas do Regulamento Geral Europeu sobre a Proteção de Dados relativas às Autoridades garantidoras**

O Regulamento Geral Europeu sobre a Proteção de Dados dispõe, em seu capítulo VI, acerca das Autoridades de controle independentes, que são compreendidas como “uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51” (Artigo 4º, 21). Elas deverão defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados na União.<sup>18</sup>

Estabeleceu-se que as autoridades de controle deverão agir com total independência na prossecução de suas atribuições e no exercício dos poderes que lhes são atribuídos; que seu pessoal deverá gozar de garantias, para que não

---

<sup>18</sup> Informações e dados das Autoridades nacionais europeias:  
<[http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48619](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48619)> Acesso em: 31.08.18.

sofra influências indevidas, e ter deveres específicos que garantam sua imparcialidade; e que elas deverão ter ampla independência nas áreas humanas, técnicas e financeiras. Há também elevada preocupação com o procedimento de nomeação de cada membro das respectivas autoridades de controle, bem como com a constituição das mesmas. Além disso, o Regulamento estabelece poderes e atribuições para as Autoridades. Todas essas previsões guardam elevada semelhança com os dispositivos vetados na nossa Lei n. 13.709/18.

O artigo 55 da nossa lei estabelecia, em seu parágrafo 3º, que a Autoridade deveria ser “caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira.” Já o GDPR, nos parágrafos de seu artigo 52, prevê que as Autoridades de Proteção de Dados “agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do presente regulamento”. Além disso, os “membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem”. O GDPR exige também que os Estados-Membros assegurem 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.”

Da mesma forma, guardam muita semelhança os dispositivos dos dois instrumentos normativos no que toca às atribuições da autoridade de proteção de dados, notadamente o artigo 56 da Lei n. 13.709/18 e o artigo 57 do GDPR. Dentre as atribuições contidas nos dois diplomas legais estão as de fiscalizar e aplicar sanções em casos de tratamentos de dados realizados em descumprimento à legislação; analisar as reclamações apresentadas por qualquer titular de dados; promover a sensibilização e a compreensão do

público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade; e elaborar relatórios anuais.

Entende-se que a reinserção das atribuições da Autoridade Nacional — previstas no artigo 56, que foi objeto de veto, e complementadas por outros dispositivos da LGPD, os quais preveem outras atribuições e competências à Autoridade — colocará o Brasil alinhado com bons exemplos internacionais e, em especial, com o modelo da União Europeia, que é aquele que vem sendo adotado na grande maioria dos países, o que facilitará não apenas o fluxo internacional de dados e o comércio internacional, mas também reduzirá barreiras para a cooperação entre o Brasil e a Europa, por exemplo, com relação à cooperação judiciária.

### **3.2 Autoridade Europeia para a Proteção de Dados**

A Autoridade Europeia para a Proteção de Dados (AEPD) tem como função principal garantir que todas as instituições e organismos da União Europeia (UE) respeitem o direito à privacidade dos cidadãos quando processarem seus dados pessoais.<sup>19</sup> Ela foi criada em 2004 e tem sede em Bruxelas (Bélgica).<sup>20</sup> A AEPD é chefiada por um supervisor e um supervisor-assistente e apoiada por um gabinete (secretariado) de advogados experientes, especialistas em TI e administradores. Atualmente, Giovanni Buttarelli é o supervisor europeu de proteção de dados e Wojciech Wiewiórowski é o supervisor assistente da AEPD. Os dois foram nomeados por

---

<sup>19</sup> Disponível em: <[https://edps.europa.eu/edps-homepage\\_en?lang=pt](https://edps.europa.eu/edps-homepage_en?lang=pt)> Acesso em: 27.08.18.

<sup>20</sup> A autoridade independente de controle (adiante designada Autoridade Europeia para a proteção de dados) foi criada pelo Regulamento (CE) n. 45/2001, do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000. A norma também estabeleceu as regras de proteção de dados nas instituições da UE, bem como as funções, os poderes e a independência institucional da Autoridade. Em 10 de janeiro de 2017, a Comissão Europeia adotou uma proposta que revoga o mencionado Regulamento e o alinha com o Regulamento Geral de Proteção de Dados (GDPR). Regulamento (CE) n. 45/2001 disponível em: <<https://edps.europa.eu/node/2995>>



decisão conjunta do Parlamento Europeu e do Conselho, em 4 de dezembro de 2014, para um mandato de cinco anos (2015-2019).<sup>21</sup>

No exercício de suas funções, as instituições e os organismos da UE realizam o tratamento de dados pessoais dos cidadãos, o que inclui a sua coleta, registro, armazenamento, extração e envio, por exemplo. Compete à Autoridade Europeia para a Proteção de Dados zelar pelo respeito às regras de privacidade que regem tais atividades. No rol das atribuições da AEPD estão: a) o controle do tratamento dos dados pessoais, a fim de garantir o cumprimento das regras de privacidade; b) o aconselhamento das instituições e organismos da UE sobre todos os aspetos do tratamento dos dados pessoais, das políticas e da legislação neste domínio; c) o monitoramento das novas tecnologias capazes de impactar a proteção de dados pessoais; d) intervir junto do Tribunal de Justiça da UE para prestar aconselhamento especializado sobre a interpretação da legislação em matéria de proteção de dados; e, e) cooperar com as autoridades nacionais de supervisão e outros órgãos de supervisão para melhorar a coerência na proteção das informações pessoais.

Como valores fundamentais da Autoridade, são destacadas a imparcialidade, devendo a Autoridade ser independente e objetiva, encontrando o equilíbrio certo entre os interesses em jogo; a integridade, havendo o compromisso em manter os mais altos padrões de comportamento e fazendo o que é certo, mesmo que seja impopular; a transparência, devendo a Autoridade explicar o que faz e por qual razão, em linguagem clara e acessível a todos; e o pragmatismo, sendo necessário então que o órgão busque entender as necessidades dos *stakeholders* e encontre soluções que funcionem na prática.<sup>22</sup>

Seu objetivo central é servir como um centro de excelência imparcial para aplicar e reforçar os padrões de privacidade e proteção de dados na UE.

---

<sup>21</sup> European Data Protection Supervisor. Vacancy for the European Data Protection Supervisor. COM/2014/10354. 2014/C 163 A/02. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3AC2014%2F163A%2F02>> Acesso em: 27.08.18.

<sup>22</sup> Disponível em: <[https://edps.europa.eu/sites/edp/files/publication/18-03-15\\_annual\\_report\\_2017\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-15_annual_report_2017_en.pdf)> Acesso em: 27.08.18

Juntamente com o requisito básico de independência, o mandato da AEPD inclui: desenvolver e comunicar uma visão geral, pensando em termos globais e propondo recomendações concretas e soluções práticas; fornecer orientações para o enfrentamento de novos desafios e imprevistos na área de proteção de dados; e operar nos níveis mais altos e desenvolver relações com uma comunidade diversificada de partes interessadas em outras instituições da UE, Estados-Membros, países não pertencentes à UE e outras organizações nacionais ou internacionais.

É importante salientar que, em 10 de janeiro de 2017, com vistas a adequar tal norma ao GDPR, a Comissão Europeia apresentou “proposta de Regulamento do Parlamento Europeu e do Conselho”, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n. 45/2001 e a Decisão n. 1247/2002/CE.<sup>23</sup> Esse documento foi recentemente aprovado pelo Parlamento Europeu com algumas emendas,<sup>24</sup> em 13 de setembro de 2018. No momento, segundo documento disponível na página do Conselho da União Europeia <sup>25</sup>, ele está aguardando posicionamento do próprio Conselho.

### **3.3 Autoridade do Reino Unido para a proteção de dados (*Information Commissioner's Office – ICO*)**

O Gabinete do Comissário de Informação é um órgão independente do Reino Unido criado para defender os direitos de informação de acordo com o interesse público, promovendo abertura pelos órgãos públicos e a privacidade

---

<sup>23</sup> Disponível em:

<<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017PC0008&from=EN>> Acesso em: 04.10.2018.

<sup>24</sup> Disponível em: <<http://data.consilium.europa.eu/doc/document/PE-31-2018-INIT/pt/pdf>> Acesso em: 09.10.2018.

<sup>25</sup> Disponível em: <<http://data.consilium.europa.eu/doc/document/ST-12221-2018-INIT/en/pdf>> Acesso em: 04.10.2018.

de dados para os indivíduos.<sup>26</sup> Ele é um órgão público executivo não departamental, que se reporta diretamente ao Parlamento e é financiado pelo Departamento responsável pelos setores digital, cultural, midiático e esportivo. Sua sede principal é em Wilmslow, na cidade de Cheshire (Inglaterra) e, desde 2016, Elizabeth Denham encontra-se no cargo de comissário de informação (*Information Commissioner*).

Hoje, o Gabinete conta com mais de 500 funcionários que estão empregados em escritórios em Wilmslow, Irlanda do Norte, Escócia e País de Gales, lidando com mais de 16.000 reclamações relacionadas a proteção de dados, 5.000 reclamações sobre liberdade de informação e mais de 200.000 chamadas de ajuda.<sup>27</sup> O Reino Unido, diferente das demais Autoridades de Proteção de Dados dos países membros da União Europeia, tem seu orçamento composto apenas por receitas oriundas de uma taxa cobrada dos distintos controladores de dados, o que, de alguma forma, fragiliza sua independência financeira.<sup>28</sup> O modelo adotado pelo legislador brasileiro é similar àqueles adotados por Malta e Luxemburgo, que além de serem totalmente financiados pelo Estado conseguem aumentar suas receitas por meio, por exemplo, de multas impostas a controladores, em razão do cometimento de infrações por descumprimento da lei de proteção de dados.<sup>29</sup> Isso é o que se conclui pela leitura dos incisos I, II e VII do artigo 57 da nossa Lei n. 13.709/18, igualmente objeto de veto presidencial.

Em termos históricos, recorda-se que, em 12 de julho de 1984, a Lei de Proteção de Dados do Reino Unido (*Data Protection Act*) recebeu a aprovação real. A Lei estabeleceu oito princípios<sup>30</sup>, como um código de boas práticas para a manipulação de informações, os quais os usuários de dados registrados seriam

---

<sup>26</sup> Disponível em: <<https://ico.org.uk/>> Acesso em: 04.09.18

<sup>27</sup> Disponível em: <<https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/>> Acesso em: 04.09.18

<sup>28</sup> Cf. Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), 2010, p. 20. Disponível em: <<http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>> Acesso em: 26.09.2018.

<sup>29</sup> v. Ibid.

<sup>30</sup> Disponível em: <<http://www.legislation.gov.uk/ukpga/1984/35/schedule/1/enacted>> Acesso em: 04.09.18

obrigados a cumprir.<sup>31</sup> Essa lei foi recentemente atualizada pelo *Data Protection Act 2018*, de forma a se adequar ao GDPR.<sup>32</sup> De acordo com seu artigo 115, o Comissário deve ser a autoridade de supervisão no Reino Unido para efeitos do artigo 51 do GDPR<sup>33</sup>.<sup>34</sup> Suas funções gerais serão conferidas por disposições como os artigos 57 e 58 do GDPR, os quais tratam das atribuições e poderes das autoridades garantidoras.

Relativamente à proteção de dados<sup>35</sup>, o Gabinete dispõe de várias ferramentas e poderes para alterar o comportamento de organizações e indivíduos que coletam, usam e mantêm informações pessoais. Esses poderes foram desenhados para promover a conformidade de instituições e pessoas com as leis relacionadas à proteção de dados. Eles incluem, por exemplo, processo criminal, penalidades monetárias, aplicação e fiscalização do cumprimento da lei e, em algumas circunstâncias, auditoria. O comissário de informações também tem o poder de aplicar multa monetária em um controlador de dados. As ferramentas não são mutuamente exclusivas, podendo ser aplicadas de forma combinada, a depender do caso.

As principais ações que o Gabinete pode realizar são: a) exigir que organizações forneçam ao Gabinete informações específicas dentro de um

---

<sup>31</sup> Disponível em: <<https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/>> Acesso em: 04.09.18

<sup>32</sup> Disponível em: <<https://www.gov.uk/government/collections/data-protection-act-2018>> Acesso em: 26.09.2018.

<sup>33</sup> **Artigo 51. Autoridade de controlo** 1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»). 2.As autoridades de controlo contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de controlo cooperam entre si e com a Comissão, nos termos do capítulo VII. 3. Quando estiverem estabelecidas mais do que uma autoridade de controlo num Estado-Membro, este determina qual a autoridade de controlo que deve representar essas autoridades no Comité e estabelece disposições para assegurar que as regras relativas ao procedimento de controlo da coerência referido no artigo 63, sejam cumpridas pelas autoridades. 4. Os Estados-Membros notificam a Comissão das disposições do direito nacional que adotarem nos termos do presente capítulo, até 25 de maio de 2018 e, sem demora, de qualquer alteração posterior a essas mesmas disposições.

<sup>34</sup> Disponível em: <[http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga\\_20180012\\_en.pdf](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf)> Acesso em 28.09.18.

<sup>35</sup> Disponível em: <<https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>> Acesso em: 04.09.18

determinado período de tempo; b) emitir compromissos que imponham que uma organização realize determinadas condutas, a fim de melhorar sua conformidade com a legislação; c) apresentar avisos de execução e ordens de "parar agora", se houver uma violação, exigindo que as organizações tomem (ou se abstenham de) etapas específicas, a fim de garantir que cumpram a lei; d) realizar avaliações consensuais (auditorias) para verificar se as organizações estão cumprindo com suas obrigações; e) realizar auditorias obrigatórias para avaliar se as organizações que processam dados pessoais seguem boas práticas; f) aplicar multas financeiras por violações graves da Lei de Proteção de Dados; g) processar aqueles que cometerem infrações penais; e h) reportar ao Parlamento questões de interesse. Enfim, atribuições e poderes que encontram grande semelhança com aqueles contidos na nossa Lei nº 13.709/18 e que foram objeto de veto.

Uma vez que seu objetivo é garantir que as informações pessoais sejam protegidas adequadamente, o Gabinete tem como compromisso desempenhar suas atividades de forma transparente, responsável, proporcional e consistente. Além disso, tais atividades devem ser direcionadas apenas a casos em que a ação seja necessária. Vale ressaltar que o site do Gabinete apresenta uma formatação fácil de ser compreendida, dispõe de áreas que de forma simples ressaltam a importância da proteção dos dados pessoais e quais direitos as pessoas têm e, por fim, oferece um canal onde qualquer um pode realizar reclamações e pedir ajuda.<sup>36</sup> Sem dúvida, essa ferramenta encontra-se alinhada com orientação positivada no GDPR, em que se afirma a necessidade da “promoção da sensibilização do público para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais”<sup>37</sup>. Nesse sentido dispunha o inciso VI, do artigo 56, do PLC n. 53/18, que afirmava que uma das atribuições da ANPD seria “promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança”.

---

<sup>36</sup> Disponível em: <<https://ico.org.uk/make-a-complaint/>> Acesso em: 04.09.18

<sup>37</sup> Considerando n. 122 do GDPR.

A busca pela adequação de sua legislação de proteção de dados com o GDPR é um tema que vem preocupando o Reino Unido, especialmente com a proximidade da concretização de sua saída da União Europeia (*Brexit*), o que levou o país a aprovar recentemente uma nova lei sobre a proteção de dados pessoais (*Data Protection Act 2018*). Essa preocupação com a adequação do Reino Unido ao modelo europeu já foi manifestada, inclusive, pela Comissária de Informação,<sup>38</sup> o que só ressalta, ainda mais, a importância de um país como o Brasil estar alinhado com o cenário internacional nesta temática.

### **3.4 Autoridade italiana para a proteção de dados de pessoais (*Garante per la protezione dei dati personali*)**

O responsável/garantidor italiano pela proteção de dados pessoais é uma autoridade administrativa independente<sup>39</sup>, estabelecida pela chamada lei de privacidade (Lei n. 675, de 31 de dezembro de 1996)<sup>40</sup> e depois disciplinada pelo Código relativo à proteção de dados pessoais (Decreto Legislativo de 30 de junho de 2003, n. 196<sup>41</sup>, recentemente modificado pelo Decreto Legislativo n. 101, de 10 de agosto de 2018, com vistas à sua adequação ao GDPR).<sup>42</sup>

As funções da Autoridade estão definidas no Regulamento (UE) 2016/679 e no Código de Proteção de Dados Pessoais (Decreto Legislativo de 30 de junho de 2003, n. 196), adaptado às disposições do mencionado

---

<sup>38</sup> Cf.

<<http://amberhawk.typepad.com/amberhawk/2018/05/european-commission-rejects-governments-approach-for-personal-data-transfers-as-ico-doubts-the-uk-wi.html>> Acesso em: 26.09.2018.

<sup>39</sup> Disponível em: <<https://www.garanteprivacy.it/>>

<<https://www.garanteprivacy.it/web/guest/home/autorita>> Acesso em: 03.09.18.

<sup>40</sup> Disponível em:

<<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>> Acesso em: 03.09.18.

<sup>41</sup> Disponível em:

<<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248>>. Acesso em: 03.09.18.

<sup>42</sup> Disponível em

<[http://www.gazzettaufficiale.it/atto/serie\\_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true](http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true)> Acesso em 26.09.2018.

Regulamento por meio do Decreto legislativo de 10 de agosto de 2018, n. 101, bem como em vários outros atos normativos italianos e internacionais. A Autoridade atua em todas as áreas nas quais é necessário garantir um adequado tratamento dos dados e o respeito pelos direitos das pessoas quanto à utilização de suas informações pessoais.

Além de independente, a autoridade foi elaborada de forma a ser autônoma e transparente. A transparência, aqui, é compreendida como a acessibilidade total das informações relativas à organização e atividade do garantidor. Com isso, visa-se facilitar o controle sobre as funções institucionais e o uso dos recursos a ela atribuídos. Atualmente, o Gabinete do responsável é composto pelo Secretário Geral, o Dr. Giuseppe Busia<sup>43</sup>, e pelos vice-secretários-gerais, os doutores Daniele De Paoli e Claudio Filippi.

Entre outras atribuições, a Autoridade se ocupa de: a) adotar as medidas previstas na legislação quanto à proteção de dados pessoais; b) examinar as reclamações recebidas; c) colaborar com as outras autoridades de proteção de dados e prestar assistência mútua para garantir atuação e aplicação coerente do Regulamento; d) informar, também por iniciativa própria, o Parlamento e outros organismos e instituições sobre a necessidade de se adotar atos normativos e administrativos relativos à proteção de dados pessoais; e) formular pareceres sobre propostas de atos normativos e administrativos; f) participar de discussões sobre iniciativas legislativas em audiências no Parlamento; g) elaborar relatório anual sobre a atividade desenvolvida e sobre o estado de implementação da legislação em matéria de privacidade; h) participar das atividades do setor na União Europeia e em âmbito internacional, inclusive nas funções de controle e assistência em sistemas como da Europol, Schengen e VIS; i) cuidar das informações e desenvolver a conscientização do público e dos titulares em relação à importância da proteção de dados pessoais, com especial atenção à tutela dos menores; j) manter registros internos acerca das violações

---

<sup>43</sup> Disponível em:

<<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4518544>> Acesso em: 03.09.18

mais relevantes e impor sanções pecuniárias quando exigido pelo Regulamento e pela legislação nacional; l) envolver, sempre que previsto, cidadãos e todas as partes interessadas em consultas públicas cujos resultados sejam tomados em consideração para a preparação de medidas gerais; m) verificar se o tratamento de dados pessoais está em conformidade com o Regulamento, bem como com as leis e regulamentos nacionais, e prescrever, quando necessário, aos titulares ou aos responsáveis pelo tratamento de dados as medidas a serem tomadas para a realização do tratamento de forma adequada, respeitando os direitos e liberdades fundamentais dos indivíduos; e, n) no caso de tratamentos que violem as disposições do Regulamento, endereçar avisos ao titular ou ao responsável pelo tratamento e solicitar o cumprimento das disposições do Regulamento; impor uma limitação provisória ou definitiva sobre o tratamento; ou ordenar a retificação, o cancelamento de dados pessoais ou a limitação do tratamento. Vale lembrar que muitas dessas atribuições foram também contempladas nos dispositivos da Lei brasileira de Proteção de Dados Pessoais que foram objeto de veto presidencial.

O garantidor da proteção de dados pessoais segue um modelo de organização e comportamento baseado no respeito aos princípios da lealdade, imparcialidade, integridade, confidencialidade e cumprimento adequado dos deveres. Ele também atua na prevenção contra todas as formas de corrupção. O Código de Ética do garantidor<sup>44</sup> — adotado desde 1998 — define os critérios e procedimentos que todos os funcionários, consultores e demais pessoas autorizadas a comparecer ao escritório do garantidor devem respeitar no seu trabalho, de acordo com a posição de independência reconhecida à autoridade e com as tarefas de garantia que lhe são confiadas. A atividade desses sujeitos deve respeitar a posição de independência reconhecida ao garantidor, com as tarefas de garantia que lhe são confiadas, com a imparcialidade e transparência da atividade administrativa, bem como com o cumprimento das obrigações de confidencialidade. Aqui, mais uma vez, vislumbra-se o acerto do legislador

---

<sup>44</sup> Disponível em: <<https://www.garanteprivacy.it/web/guest/home/autorita/codice-etico>> Acesso em: 03.09.18



brasileiro que, no §7º, de seu artigo 55, vedou “ao ex-conselheiro [da Autoridade Nacional] utilizar informações privilegiadas obtidas em decorrência do cargo exercido, sob pena de incorrer em improbidade administrativa”, justamente com o fim de cumprir suas obrigações de confidencialidade e de assegurar a independência da Autoridade Nacional.

### **3.5 A Autoridade nacional francesa encarregada pela proteção de dados (Commission Nationale de l'Informatique et des Libertés – CNIL)**

A França é historicamente reconhecida como um Estado atento à proteção dos direitos e liberdades individuais de seus cidadãos. Assim, não por acaso, a autoridade nacional encarregada pela proteção de dados pessoais naquele país, a CNIL (*Commission Nationale de l'Informatique et des Libertés*), foi instituída em 1978, ou seja, há nada menos que quatro décadas.<sup>45</sup>

A implementação da referida autoridade se deu por meio da Lei n. 78-17 de janeiro de 1978<sup>46</sup>, conhecida como a *Loi Informatique et Libertés*. Tal diploma legal sofreu diversas alterações com o passar dos anos para se adaptar a novas demandas e textos legais, bem como para se adequar ao Regulamento Europeu sobre a Proteção de Dados.<sup>47</sup>

A CNIL é classificada como uma autoridade administrativa de controle independente, conforme estabelecido pelo *caput* do artigo 11<sup>48</sup> da Lei 78-17, o que pressupõe que o desempenho de suas funções deve ocorrer de forma

---

<sup>45</sup> Item desenvolvido por Jaqueline Simas de Oliveira.

<sup>46</sup> Disponível em:

<<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20180201>> Acesso em: 24.08.18.

<sup>47</sup> Recentemente, foram aprovados a Lei n° 2017-55, de 20 de janeiro de 2017, sobre o estatuto geral das autoridades administrativas e públicas independentes e o seu decreto regulamentador, Decreto n° 2018-232, de 30 de março de 2018. Disponíveis em

<<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033897475&categorieLien=id>> e

<[https://www.legifrance.gouv.fr/affichTexte.do?jsessionid=6C6FD743D9DEBF4A4DCF71EDEAFF0367.tplgfr31s\\_1?cidTexte=JORFTEXT000036757777&dateTexte=20180401](https://www.legifrance.gouv.fr/affichTexte.do?jsessionid=6C6FD743D9DEBF4A4DCF71EDEAFF0367.tplgfr31s_1?cidTexte=JORFTEXT000036757777&dateTexte=20180401)> Acesso em: 26.09.2018.

<sup>48</sup> *Article 11. La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante.*

totalmente autônoma das demais atividades desempenhadas pelo Estado francês.

A autonomia da CNIL também é evidenciada pela leitura do artigo 21<sup>49</sup> do referido diploma, o qual estabelece que os ministros, autoridades públicas, dirigentes de empresas públicas ou privadas, chefes de quaisquer grupos e, de maneira genérica, os responsáveis pelo tratamento ou arquivamento de dados pessoais não podem se opor à ação da comissão ou de seus membros e devem tomar todas as medidas cabíveis a fim de facilitar sua atividade.

As funções e objetivos da CNIL são muito amplos e encontram-se dispostos no supramencionado artigo 11, podendo ser agrupados da seguinte forma:

a) Informar e educar - a CNIL possui como objetivo precípua informar a todas as partes abarcadas pela Lei 78-17 sobre seus direitos e obrigações. A CNIL atende às demandas e questionamentos dos cidadãos e dos profissionais que tratam dados pessoais. Ademais, a autoridade promove ações de conscientização na imprensa, em seu website e em suas redes sociais, a fim de disponibilizar ferramentas pedagógicas que possam ser utilizadas no âmbito da proteção de dados pelos interessados.

b) Proteger os direitos dos cidadãos - qualquer pessoa pode entrar em contato com a CNIL para exercer seus direitos, notadamente para viabilizar o acesso aos seus dados pessoais tratados ou coletados por terceiros.

c) Aconselhar entidades públicas e privadas e propor regulamentações - as atividades de aconselhamento e regulamentação da CNIL são amplas e traduzem-se, por exemplo, na emissão de opinião sobre projetos de lei relativos à proteção de dados pessoais e na participação em audiências parlamentares relativas a temas de sua alçada. No âmbito dessa missão, a CNIL busca soluções que permitam às entidades públicas e privadas perseguir seus objetivos legítimos respeitando os direitos e liberdades dos cidadãos. Em 2017, a CNIL atendeu diversos questionamentos de autoridades públicas e desenvolveu trabalhos para facilitar a adaptação das entidades ao RGPD.

---

<sup>49</sup> Article 21. *Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche.*

d) Antecipar e inovar - no âmbito de sua atividade de inovação e prospecção, a CNIL conta com um laboratório para detectar e analisar novas tecnologias e aplicativos que possam impactar a vida privada<sup>50</sup>. Nesse sentido, ela contribui para o desenvolvimento de soluções tecnológicas que protejam a privacidade de seus usuários, incentivando as empresas desenvolvedoras de tecnologia a desempenharem suas funções pela lógica do *privacy by design*.

e) Controlar e sancionar - por fim, a CNIL realiza um controle *a posteriori* a fim de verificar o cumprimento da legislação de proteção de dados pelas entidades públicas e privadas e sancioná-las no caso de descumprimento das regras concernentes ao tema. As sanções previstas são diversas, podendo ser: (i) notificação prévia pelo descumprimento, (ii) limitação temporária ou definitiva das atividades de tratamento de dados da entidade infratora, (iii) suspensão dos fluxos de dados, (iv) determinação do cumprimento das regras de proteção de dados pessoais, (v) determinação da retificação, limitação ou exclusão de dados coletados indevidamente e, por fim, (vi) aplicação de sanções pecuniárias, em consonância com o estabelecido pelo RGPD. A sanção aplicada dependerá do tipo de descumprimento e do grau da ofensa perpetrada.

As funções da CNIL são desempenhadas pela sua direção, composta por 18 membros que são, em sua maioria, eleitos por assembleia ou pelas jurisdições das quais eles advêm, bem como pelos 198 agentes contratuais<sup>51</sup> da autoridade, os quais são responsáveis por executar as decisões e orientações da direção.

A direção da CNIL se reúne semanalmente em sessões plenárias, sob uma ordem do dia estabelecida pelo presidente da entidade. Uma parte importante dessas sessões é realizar o exame de projetos de lei ou de decretos submetidos pelas autoridades públicas à análise da CNIL, enquanto outra parte atua no estudo do impacto de novas tecnologias na vida privada e na privacidade dos cidadãos.

Ademais, a CNIL também é composta por um Comitê Restrito, formado por 05 membros da sua direção e por um presidente. O Comitê é o órgão

---

<sup>50</sup> Mais informações sobre o laboratório e sobre os trabalhos desenvolvidos pelo mesmo podem ser encontradas em: <<https://linc.cnil.fr/>>. Disponível apenas em francês. Acesso em: 05.09.18.

<sup>51</sup> Agentes contratuais são indivíduos que exercem a função pública e tem suas obrigações e direitos estabelecidos por um contrato, de tempo determinado ou indeterminado, com o Estado francês.

responsável por sancionar indivíduos e empresas que tratam dados pessoais e descumprem a legislação, a nível Europeu e nacional, concernente ao tema.

Como forma de comprovar sua efetividade, a autoridade publica anualmente um relatório de prestação de contas demonstrando resumidamente os serviços prestados naquele ano. Apenas à título exemplificativo, em 2017 a CNIL atendeu à 8.360 denúncias de cidadãos que alegaram ter seus direitos violados, autorizou 2.964 transferências de dados para fora da União Europeia, se pronunciou 177 vezes sobre projetos de lei, certificou 123 entidades que estavam de acordo como o RGPD, aplicou 9 sanções financeiras (das quais 03 à entidades públicas) e notificou 79 entidades para que se adequassem à legislação de proteção de dados<sup>52</sup>.

Pela análise do modelo francês, verifica-se que o legislador brasileiro seguiu na direção correta e dotou a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade com todas as características e atribuições necessárias ao correto funcionamento de uma Autoridade do tipo, seguindo a melhor experiência internacional, já que a CNIL, conforme salientado anteriormente, é considerada como uma das principais Autoridades de Proteção de Dados do Mundo, justificando-se, portanto, o pleno restabelecimento dos dispositivos que foram objeto de veto pelo Presidente da República, no que toca à Autoridade Nacional de Proteção de Dados (ANPD) e ao Conselho Nacional de Proteção e Dados Pessoais e da Privacidade.

Vale ressaltar que alguns estudos apontaram que a CNIL não possuiria plena independência financeira,<sup>53</sup> uma vez que seu orçamento provém do

---

<sup>52</sup> O relatório de 2017 pode ser encontrado em: <[https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_en\\_bref\\_2018.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_en_bref_2018.pdf)>. Disponível apenas em francês. Acesso em: 05.09.18.

<sup>53</sup> Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), 2010, p. 20. Disponível em: <<http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>> Acesso em: 26.09.2018.

Estado e é votado anualmente pelo Parlamento francês,<sup>54</sup> o que a deixaria em desconformidade com a normativa europeia. Em relação a esse ponto específico, parece que os dispositivos propostos na Lei nº 13.709/18 e que foram objeto de veto, notadamente o artigo 57 e seus incisos, quanto à receita da ANPD<sup>55</sup>, proporcionam uma maior independência e autonomia financeiras à instituição do que o modelo francês ou mesmo do que o modelo inglês, conforme já salientado. Isso demonstra que o legislador nacional estava ciente das experiências estrangeiras e buscou solucionar os problemas nelas identificados, com relação à atuação das autoridades de proteção de dados pessoais, por meio de solução que assegurasse a plena independência política, técnica e financeira à Autoridade brasileira. Nesse sentido, entende-se que o modelo previsto nos artigos 55-57 da Lei nº 13.709/18, os quais foram objeto de veto por parte do Presidente da República, deva ser efetivamente incorporado ao ordenamento jurídico brasileiro, a fim de se garantir uma correta aplicação da referida lei e tornar o Brasil um país com um nível adequado de proteção de dados pessoais, ficando inclusive em conformidade com as normas do GDPR.

### **3.6 A agência argentina de acesso à informação pública**

A Argentina foi o primeiro país latino-americano a receber o reconhecimento, pela Comissão da União Europeia, da adequação de seu sistema de proteção de dados pessoais.<sup>56</sup> De 2001 a 2017, a autoridade

---

<sup>54</sup> Disponível em: <<https://www.data.gouv.fr/fr/datasets/budget-de-la-cnll-1/>>. Disponível apenas em francês. Acesso em: 05.09.18.

<sup>55</sup> Art. 57. Constituem receitas da ANPD: I – o produto da execução da sua dívida ativa; II – as dotações consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; III – as doações, os legados, as subvenções e outros recursos que lhe forem destinados; IV – os valores auferidos na venda ou aluguel de bens móveis e imóveis de sua propriedade; V – os valores auferidos em aplicações no mercado financeiro das receitas previstas neste artigo; VI – o produto da cobrança de emolumentos por serviços prestados; VII – os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; VIII – o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

<sup>56</sup> 2003/490/CE: Decisão da Comissão, 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://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32003D0490&from=EN>> Acesso em: 04.10.2018.

competente para fiscalização do cumprimento da Lei de proteção de dados<sup>57</sup> foi a Direção Nacional de Proteção de Dados (*Dirección Nacional de Protección de Datos Personales*), órgão vinculado ao Ministério da Justiça e dos Direitos Humanos, mas com a ressalva, em lei, de que o Diretor da autoridade somente poderia ser exonerado pelo Poder Executivo por mal desempenho das suas funções.<sup>58</sup>

O fato de a Direção Nacional de Proteção de Dados Pessoais ser órgão da administração direta vinculado a um ministério foi objeto de críticas quanto à sua real independência.<sup>59</sup> Não por acaso, em 2017,<sup>60</sup> após a aprovação do GDPR,<sup>61</sup> a autoridade de controle Argentina tornou-se a Agência de Acesso à Informação Pública (*Agencia de Acceso a la Información Pública*), criada sob o regime de autarquia, com todas as características de uma autoridade independente, o que inclui autonomia funcional e financeira, diretor com mandato fixo e pessoal técnico e administrativo dedicado.<sup>62</sup>

Dentre as atribuições da Agência, estão a de estabelecer normas e regulamentos para o correto desempenho das atividades previstas na lei de proteção de dados pessoais, fiscalizar a integridade e segurança dos bancos de dados alcançados por tal lei, solicitar informações a entidades públicas e privadas a respeito dos tratamentos de dados por elas conduzidos, impor sanções administrativas por descumprimentos da referida lei, iniciar ações penais por violações da lei de proteção de dados e assistir e assessorar titulares

---

<sup>57</sup> Lei n. 25.326/2000. Disponível em espanhol em:

<<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>> Acesso em: 04.10.2018.

<sup>58</sup> Artigo 29 da Lei nº 25.326/2000.

<sup>59</sup> V. DELGADO, Lucrecio Rebollo; SALTOR, Carlos Eduardo. *El derecho a la protección de datos en España y Argentina: Orígenes y regulación vigente*. Dykinson: Madrid, 2013. p. 159.

<sup>60</sup> Decreto n. 899/2018. Disponível em espanhol em:

<<https://www.argentina.gob.ar/normativa/decreto-899-2017-285903/texto>> Acesso em: 04.10.2018.

<sup>61</sup> Ainda com vistas à adequação da legislação sobre proteção de dados ao novo regime jurídico estabelecido pelo GDPR, o Governo Argentino enviou, em 19 de setembro de 2018, ao parlamento daquele país novo projeto de lei de proteção de dados. Disponível em espanhol em: <[https://www.argentina.gob.ar/sites/default/files/mensaje\\_ndeg\\_147-2018\\_datos\\_personales.pdf](https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf)> Acesso em: 04.10.2018.

<sup>62</sup> V. Lei n. 27.275/16. Disponível em espanhol em:

<<http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>> Acesso em: 04.10.18.

dos dados com vistas à defesa dos direitos que a lei de proteção de dados pessoais lhes garante.<sup>63</sup>

Vale lembrar também que a lei argentina também estabelece limites para a transferência internacional de dados para países que não possuem um nível adequado de proteção de dados.<sup>64</sup>

Vê-se, assim, que nosso vizinho também optou por um modelo de Autoridade de controle independente e autônomo, inspirado na legislação europeia de proteção de dados pessoais. Não há dúvidas de que a criação da Autoridade Nacional no Brasil terá impacto também no fluxo de dados intra-mercosul, facilitando o comércio e a cooperação internacional tanto com a Argentina quanto com o Uruguai, outro Estado membro desse bloco econômico que também já possui o “selo” de adequação de sua legislação sobre proteção de dados com o modelo europeu.<sup>65</sup>

---

<sup>63</sup> Artigo 26(1) da Lei n. 25.326/2000.

<sup>64</sup> Artigo 12 da da Lei n. 25.326/2000.

<sup>65</sup> DECISÃO DE EXECUÇÃO DA COMISSÃO, de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados [notificada com o número C(2012) 5704].

Disponível em:

<<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=EN>> Acesso em: 04.10.2018.

## 4. Considerações finais

O veto à Autoridade Nacional de Proteção de Dados, na Lei n. 13.709/2018, representou uma grande perda para a estrutura de proteção de dados pessoais brasileira, atingindo diretamente a efetividade, a fiscalização e a aplicação de suas normas. Além das pessoas naturais disporem de garantias e de instrumentos reduzidos de proteção, as empresas não gozarão das facilidades e orientações que uma Autoridade poderia lhes proporcionar.

Como enfatizado ao longo do relatório, o estabelecimento de uma autoridade verdadeiramente independente, autônoma e com corpo técnico qualificado é fundamental para que a regulação do tema ocorra de forma apropriada, privilegiando a pessoa natural e em linha com o *General Data Protection Regulation* (GDPR). Como a Autoridade deve ter entre suas funções a possibilidade de monitorar tanto o Estado quanto sujeitos privados, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas.

A experiência de outros países mostra a relevância da existência de uma Autoridade nacional específica para a aplicação eficiente de suas respectivas leis de proteção de dados. Reino Unido, França, Itália e Argentina são exemplos significativos no tema e, como apontado, devem servir de inspiração para o modelo brasileiro. Não há dúvidas de que uma maior compatibilidade entre os diferentes sistemas pode facilitar, por exemplo, os fluxos internacionais de dados, o que beneficiaria os mais diversos setores e poderia ser utilizado para fins variados, como para facilitar práticas comerciais e para a cooperação entre entidades públicas.

Inclusive, a existência de uma autoridade independente é um dos requisitos para que o Brasil tenha reconhecida a adequação de suas normas em comparação com o tratamento oferecido ao tema na Europa pelo GDPR. Na América do Sul, apenas Argentina e Uruguai receberam essa chancela até o momento. A mencionada análise, ao verificar a situação da autoridade nacional de proteção de dados no País, levará em conta especialmente sua independência



em aspectos como estrutura/organização, exercício de funções/atribuições e poderes da autoridade, devendo tanto o legislador brasileiro quanto o Presidente da República, portanto, observarem com cuidado tais requisitos no momento de constituir a Autoridade Nacional.

Vindo por meio de Lei ou de Medida Provisória, o importante é que a mencionada Autoridade seja estabelecida nos moldes do que havia sido proposto no Projeto de Lei da Câmara n. 53/18, o qual se encontrava amplamente alinhado com bons modelos e práticas internacionais, bem como havia sido objeto de amplo debate público e democrático. Esse é, vale ressaltar, o entendimento majoritário dos diversos setores da sociedade que vêm discutindo a regulação do tratamento de dados pessoais no País, nos últimos anos. Para que o Brasil alcance um patamar elevado de proteção aos direitos humanos e de desenvolvimento, faz-se necessário criar uma Autoridade Nacional de Proteção de Dados Pessoais que goze de autonomia, seja funcionalmente independente e detenha características semelhantes àquelas preconizadas na norma europeia de proteção de dados.

## 5. Para saber mais

- Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), 2010. Disponível em: <<http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>> Acesso em: 26.09.2018.
- National Data Protection Authorities. Disponível em: <[http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612080](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)> Acesso em: 26.09.2018.
- What are Data Protection Authorities (DPAs)? Disponível em: <[https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en)> Acesso em: 26.09.2018.
- Ronaldo Lemos. Lei de dados nasceu desgovernada. Disponível em: <<https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/08/lei-de-dados-nasceu-desgovernada.shtml>> Acesso em: 26.09.2018.
- Ronaldo Lemos. Começa uma nova era para o tratamento de dados no Brasil. Disponível em: <<https://www1.folha.uol.com.br/mercado/2018/07/comeca-uma-nova-era-para-o-tratamento-de-dados-no-brasil.shtml>> Acesso em: 26.09.2018.
- Carlos Affonso Souza. Entenda os vetos do Presidente na Lei de Proteção de Dados. Disponível em: <<https://tecfrent.blogosfera.uol.com.br/2018/08/14/entenda-os-vetos-do-presidente-na-lei-de-protecao-de-dados/>> Acesso em: 26.09.2018.
- Chiara de Teffé, Eduardo Magrani e Mario Viola. 5 pontos sobre a importância de uma Autoridade Nacional de Proteção de Dados. Disponível em: <[https://medium.com/@ITSriodejaneiro/5-pontos-sobre-a-import%C3%A2ncia-de-uma-autoridade-nacional-de-prote%C3%A7%C3%A3o-de-dados-4cf8137cf59e?fbclid=IwAR3Mnzi\\_FaXRq-l1P4yEleMtqhGlabqQWs7YWM6msYrXLftETUVrvZiOA](https://medium.com/@ITSriodejaneiro/5-pontos-sobre-a-import%C3%A2ncia-de-uma-autoridade-nacional-de-prote%C3%A7%C3%A3o-de-dados-4cf8137cf59e?fbclid=IwAR3Mnzi_FaXRq-l1P4yEleMtqhGlabqQWs7YWM6msYrXLftETUVrvZiOA)> Acesso em: 07.11.18.
- Chiara Spadaccini de Teffé e Ana Lara Mangeth. Lei de Dados Pessoais precisa de uma Autoridade independente. Disponível em: <<https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64>> Acesso em: 26.09.2018.
- Danilo Doneda. O que está em jogo com a nova Autoridade Nacional de Proteção de Dados. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018>> Acesso em: 26.09.2018.
- Laura Schertel Mendes e Danilo Doneda. Lei de proteção de dados não pode morrer na praia. Disponível em: <<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>> Acesso em: 26.09.2018.



**ITS Rio**

[its@itsrio.org](mailto:its@itsrio.org)

+55 (21) 3486-0390