OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Janeiro 2022

Autoridades de Proteção de Dados

Recursos, natureza jurídica e autonomia

Quem somos?

Fundado em 1997, o Opice Blum, Bruno e Vainzof Advogados Associados é escritório pioneiro em Direito Digital no país. Vimos nascer tendências, participamos delas e nos posicionamos sempre na vanguarda. Inovamos, perseguimos a excelência e ampliamos nossas frentes de atuação para atender, de forma ainda mais completa, nossos clientes.

Nossa atuação é reconhecida no Brasil e no exterior em rankings como Chambers & Partners, Who's Who Legal, The Legal 500, Best Lawyers, Leaders League, Análise Advocacia 500, entre outros.

PROTEÇÃO DE DADOS

Nossa área de Proteção de Dados oferece:

***DPO as a Service*:** atuamos com terceirização da função completa do DPO (*Data Protection Officer*) ou Encarregado de Proteção de Dados Pessoais, na condição de pessoa jurídica perante a ANPD (Autoridade Nacional de Proteção de Dados) e os titulares de dados, para desenvolver, entre outras atividades, (i) monitoramento da conformidade da empresa com a LGPD; (ii) elaboração do Relatório de Impacto à Proteção de Dados Pessoais; (iii) monitoramento de leis e normas; e (iv) apoio técnico-jurídico no desenvolvimento de novas iniciativas (*Privacy by Design*). Além disso, oferecemos assessoria para o exercício interno da função de DPO, bem como assessoria jurídica empresarial.

Consultivo em Proteção de Dados: nossa equipe atua com a identificação de situações pertinentes à privacidade e proteção de dados, por meio das seguintes etapas: mapeamento das contingências; investigação dos riscos de privacidade; análise de incidentes de segurança anteriores; e revisão das práticas de privacidade adotadas. Com isso, possibilitamos que a organização esteja em conformidade com a LGPD, prezando pela segurança das informações dos seus clientes.

M&A: na área societária e de fusão/aquisição, nossa atuação ocorre a partir da análise de viabilidade e riscos do negócio, bem como por meio da aplicação de *Due Diligence* em proteção de dados e privacidade, que representa análise interna e externa quanto a brechas no negócio que possam impactar na segurança dos dados da empresa e dos clientes.

Adequação à LGPD: atuamos com a elaboração de projetos de adequação à LGPD para empresas e órgãos públicos, bem como de pareceres, consultas e memorandos de temas relacionados à proteção de dados. Trabalhamos com análise e elaboração de documentos, como contratos, cláusulas contratuais, políticas de privacidade e demais instrumentos. Fazemos a gestão de terceiros e de direitos dos titulares de dados; treinamento e capacitação de colaboradores e prestadores de serviços; além de atuarmos administrativamente junto a entidades reguladoras, a exemplo da ANPD, Senacon e Anatel.

Índice

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Introdução

A fim de garantir na prática um nível adequado de proteção de dados, a existência de uma autoridade supervisora independente, com poderes para monitorar e fazer cumprir regras relativas ao tema, é fundamental. A autoridade em questão deve atuar com total independência e imparcialidade no desempenho de suas funções e no exercício de seus poderes. Esses requisitos de independência, imparcialidade e autonomia se traduzem em diversas características, como estrutura e natureza jurídica da autoridade, seu quadro de pessoal, seus recursos financeiros, entre outras.

Há alguns anos, pensar na figura de uma autoridade de proteção de dados era algo distante. Desde 2006, quando foi estabelecido pelo Comitê de Ministros da Europa o Dia Internacional da Proteção de Dados em 28 de janeiro, tivemos muitos avanços em relação ao tema, inclusive no Brasil com o início da vigência da Lei Geral de Proteção de Dados em setembro de 2020 e a posterior estruturação da ANPD (Autoridade Nacional de Proteção de Dados). No segundo semestre do ano passado, em agosto, entraram em vigor as sanções administrativas de competência exclusiva da ANPD. A celebração anual do Dia Internacional da Proteção de Dados tem, portanto, o objetivo principal de relembrar que privacidade e proteção de dados pessoais são fundamentais e, por isso, indispensáveis.

O dia foi escolhido em referência a 28 de janeiro de 1981, ocasião em que se estabeleceu a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao tratamento automatizado de dados pessoais, considerado o primeiro instrumento internacional juridicamente vinculativo sobre a questão da proteção de dados pessoais.

Neste Dia Internacional da Proteção de Dados, reconhecemos a relevância da LGPD, que trouxe segurança jurídica para o Brasil, seguindo os passos do GDPR na União Europeia. Essas inovações legislativas, que resultaram na constituição da ANPD e de outras autoridades de proteção de dados em todo o mundo, demonstram a preocupação dos países com a privacidade dos cidadãos.

Nesse contexto, este estudo, elaborado pelo Opice Blum, Bruno e Vainzof Advogados Associados, tem por objetivo analisar a estrutura e a natureza jurídica das autoridades supervisoras de proteção de dados, seu quadro de pessoal e seus recursos financeiros, entre outras características, sobretudo no contexto europeu. Para tanto, serão examinados os recursos financeiros e pessoais disponibilizados a essas autoridades nos últimos anos, bem como sua estrutura e composição. Em seguida, os requisitos de independência e autonomia serão destrinchados para orientar eventual mudança futura na estrutura da ANPD.

Autoridades de Proteção de Dados da União Europeia

Recursos disponíveis

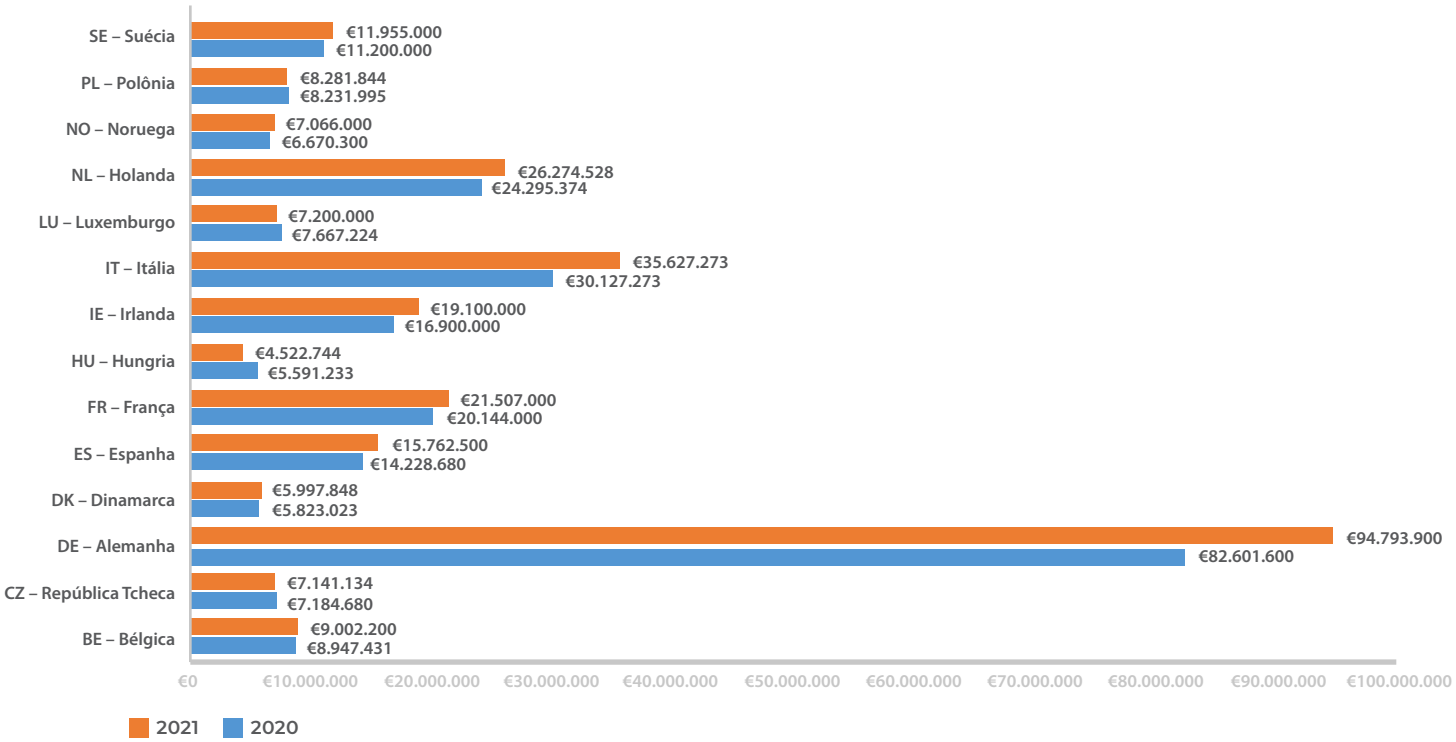
Em relatório de agosto de 2021 elaborado pelo *European Data Protection Board* (EDPB) sobre os recursos disponibilizados pelos Estados-membros da União Europeia para suas respectivas Autoridades de Proteção de Dados[1], é possível avaliar orçamentos repassados por cada Estado, recursos humanos existentes nas autoridades, número de pessoal envolvido nas áreas de fiscalização e sanções, e satisfação das autoridades com os recursos atualmente à sua disposição.

Essa análise é fundamental, uma vez que, conforme o próprio EDPB destaca, para que o direito fundamental à proteção de dados tenha verdadeiro significado e efeito na vida dos cidadãos da União Europeia, é necessária uma supervisão robusta – que apenas pode existir quando as Autoridades de Proteção de Dados estão devidamente equipadas com pessoal e recursos, a fim de supervisionar o cumprimento do GDPR (*General Data Protection Regulation*).

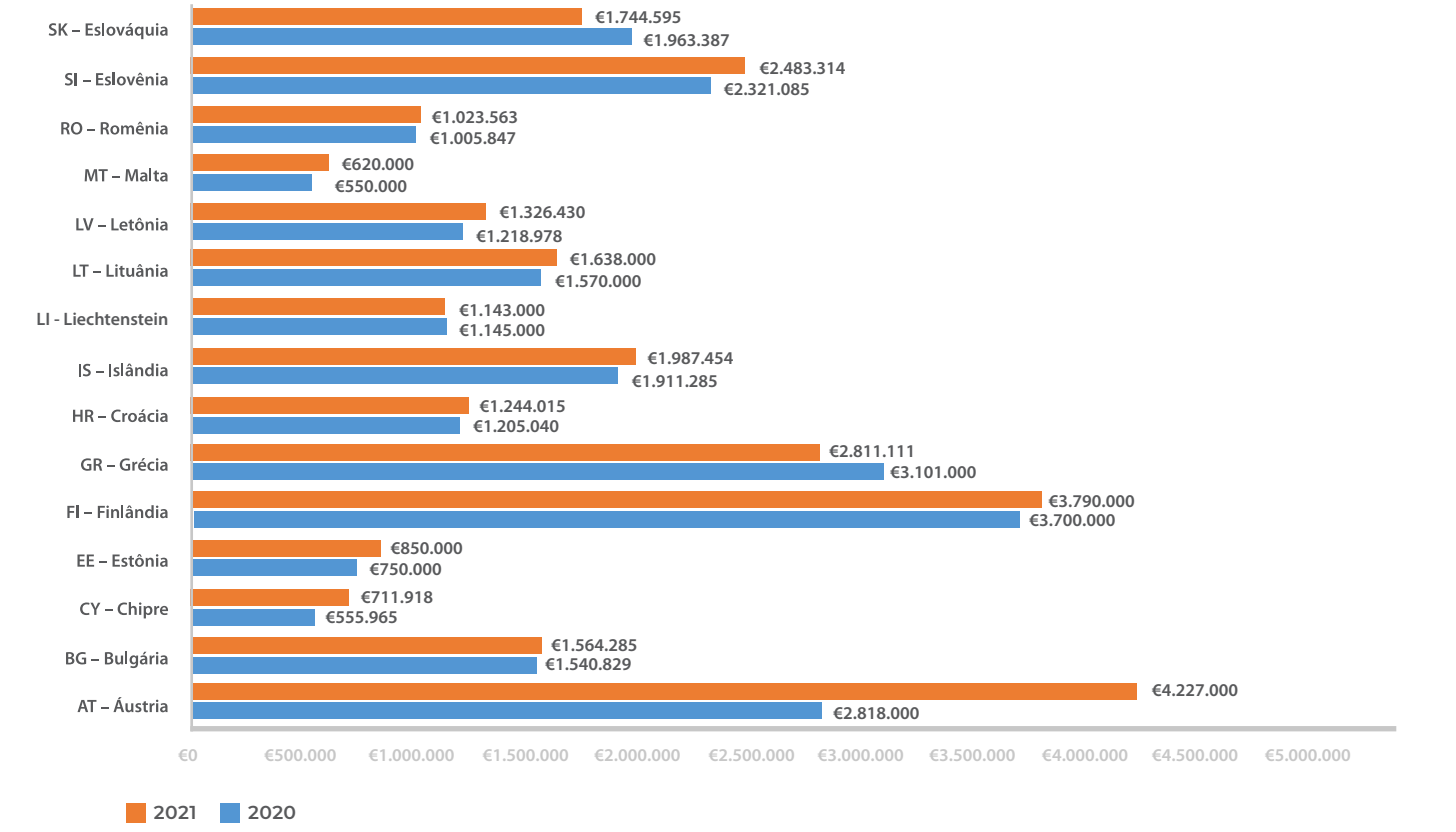
Recursos financeiros

Os gráficos abaixo, que fornecem informações sobre o orçamento disponibilizado às Autoridades em 2020 e 2021, devem ser interpretados à luz de possíveis diferenças no âmbito de competências, atividades e responsabilidades financeiras a nível nacional.

[1] UNIÃO EUROPEIA. *European Data Protection Board. Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities.* 05 ago. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en. **Acesso em: 10 de dezembro de 2021.**



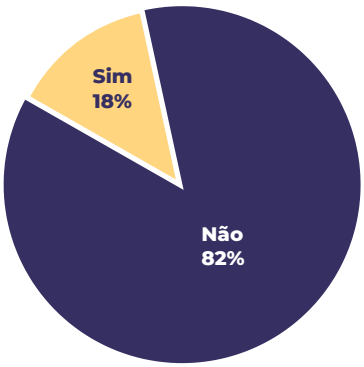
***Fonte:** European Data Protection Board, 2021.*



***Fonte:** European Data Protection Board, 2021*

A maioria das Autoridades **(82%) afirma** explicitamente que não tem recursos suficientes, embora exista uma minoria **(18%) que não vê necessidade** de incremento de recursos financeiros atualmente.

O orçamento alocado é suficiente para realizar as atividades das Autoridades?



Sim: AT, HU, LI, LU, CY

Não: BG, DE, FI ,GR, IS, MT, RO, SI, BE, IE, IT, CZ, EE, FR, HR, LV, PL, SK, LT, SE, NL, ES

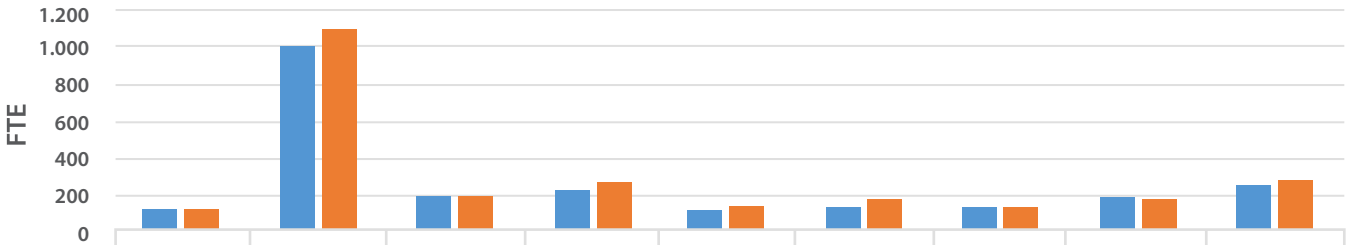
SI (Eslovênia): Não respondeu.

***Fonte:* European Data Protection Board, 2021.**

Recursos humanos

Os gráficos abaixo, que fornecem informações sobre os recursos humanos colocados à disposição das Autoridades de Proteção de Dados em 2020 e 2021, devem ser interpretados à luz de possíveis diferenças no âmbito das competências, atividades e responsabilidades financeiras a nível nacional[2].

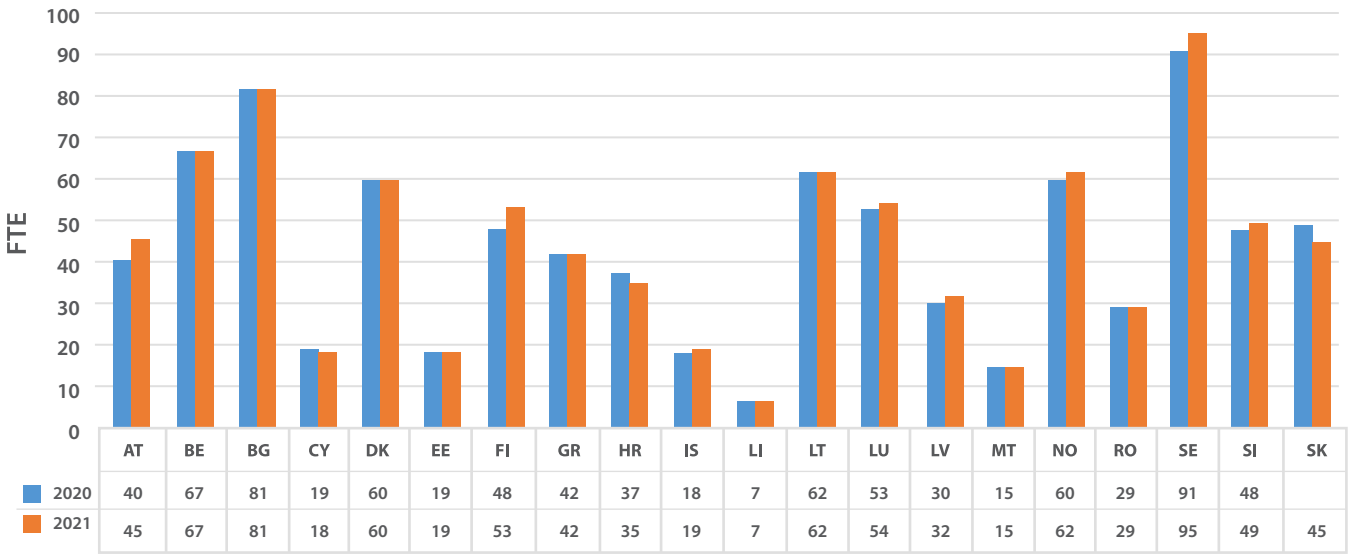
Número de empregados
para Autoridades acima de 100 FTE (*Full-time equivalent*)



	CZ	DE	ES	FR	HU	IE	IT	NL	PL
2020	115	1004	189	225	114	145	134	180	243
2021	112	1083	189	245	117	175	133	175	271

[2] A sigla "FTE", utilizada nos gráficos, significa "*full-time equivalent*": unidade que indica a carga de trabalho de um empregado para que as cargas de trabalho sejam comparáveis em diversos contextos.

Número de empregados
para Autoridades abaixo de 100 FTE (*Full-time equivalent*)



	AT	BE	BG	CY	DK	EE	FI	GR	HR	IS	LI	LT	LU	LV	MT	NO	RO	SE	SI	SK
2020	40	67	81	19	60	19	48	42	37	18	7	62	53	30	15	60	29	91	48	
2021	45	67	81	18	60	19	53	42	35	19	7	62	54	32	15	62	29	95	49	45

***Fonte:* European Data Protection Board, 2021.**

*DK 2021 (até 1° de julho)

Mais uma vez, a maioria das Autoridades **(86%)** declarou explicitamente que não tem recursos humanos suficientes, embora algumas não vejam necessidade de recursos humanos adicionais no momento **(14%)**.

Em sua visão, os recursos humanos alocados são suficientes para dar conta de suas atividades?

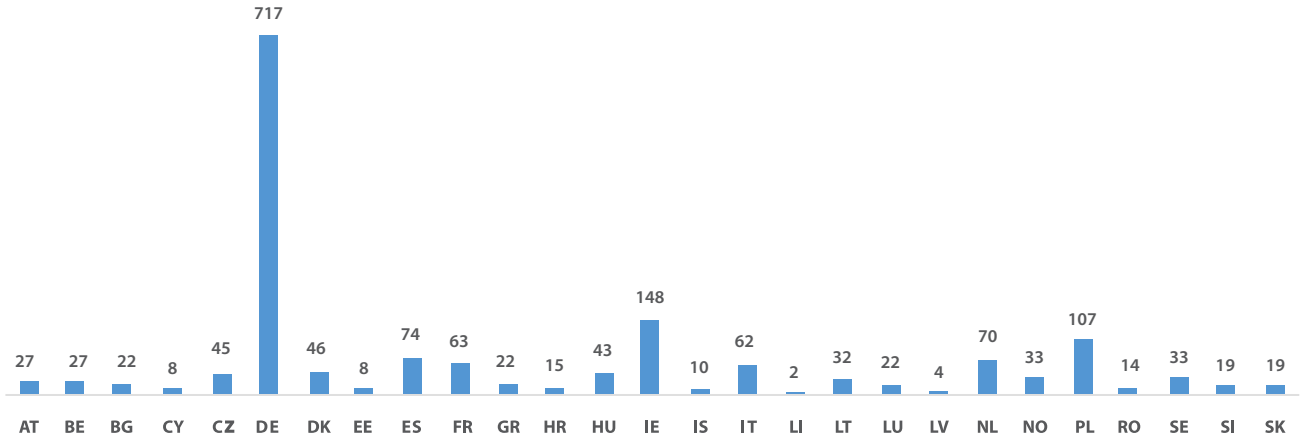
Sim: AT, HU, LI, CY

Não: BG, DE, FI ,GR, IS, MT, RO, SI, BE, IE, IT, CZ, EE, FR, HR, LV, PL, SK, LT, SE, NL, ES

***Fonte:* European Data Protection Board, 2021.**

O gráfico abaixo, por sua vez, revela o número de funcionários em cada Autoridade Nacional trabalhando com reclamações, sanções e *enforcement* em 01/01/2021.

Número de pessoas trabalhando com reclamações, *enforcement* e sanções (FTE) em 01/01/2021



***Fonte:** European Data Protection Board, 2021.*

Autoridades de Proteção de Dados da União Europeia: natureza jurídica e estrutura

Garante per la Protezione dei Dati Personali

O Garante per la Protezione dei Dati Personali é uma autoridade administrativa independente instituída pela Lei de Privacidade (Lei 31 de dezembro de 1996, n. 675), então regida pelo Código de Proteção de Dados Pessoais (Decreto legislativo de 30 de junho de 2003, n. 196), alterado pelo Decreto Legislativo de 10 de agosto de 2018, n. 101. Este último confirmou que o Garante é a autoridade de controle designada também para efeitos de aplicação do GDPR (nos termos do artigo 51 do Regulamento).

A Lei 31 de dezembro de 1996, n. 675, além de criar o Garante (art. 30, 1), determina a sua operação com total autonomia e independência de julgamento e avaliação (art. 30, 2), estabelecendo, ainda, sua formação como órgão colegiado composto por quatro membros, dois eleitos pela Câmara dos Deputados e dois pelo Senado da República com votos limitados. Eles elegem um presidente entre eles, cujo voto prevalece em caso de empate.

Os membros são escolhidos entre pessoas que asseguram a sua independência e são especialistas com reconhecida competência nas áreas do direito ou das tecnologias da informação, garantindo a presença de ambas as habilitações (art. 30, 3). O Regulamento 1/2000 sobre organização e funcionamento do gabinete do Garante traz as demais normas relativas à estrutura do órgão.

As despesas de funcionamento do Garante são imputadas a um fundo destinado a essa finalidade no orçamento do Estado, registrado em capítulo específico do orçamento do Tesouro. O relatório de gestão financeira está sujeito ao controle do Tribunal de Contas (art. 33, 2, Lei n. 675). O Garante elabora relatórios anuais sobre suas atividades e aplicação atual da legislação de privacidade, que são submetidos ao Parlamento e ao Governo.

De acordo com o Código de Privacidade (Decreto Legislativo de 30 de junho de 2003, n. 196), as despesas operacionais do Garante são cobradas a um fundo alocado no orçamento do Estado e registrado em uma missão específica e programa de gastos do Ministério da Economia e Finanças. Entre elas, o legislador menciona explicitamente aquelas relacionadas aos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessárias ao cumprimento das atribuições e ao exercício das competências da autoridade, incluindo a participação em processos de cooperação com terceiros.

Em nota complementar à Lei de Orçamento para o triênio 2020-2022, uma seção é dedicada aos direitos sociais, às políticas sociais e à família, entre os quais se encontram os repasses correntes para o Garante. A exigência identificada para a Autoridade é igual a € 30.127.273 para cada um dos três anos (2020, 2021 e 2022) e resulta da análise de regulamentos, acordos e/ou convenções, e de um acompanhamento rigoroso dos montantes efetivamente pagos.

Além desse valor já destinado, o fundo é alimentado com parte do valor pago a título de multas aplicadas pela autoridade: 50% do valor total é alocado às atividades de sensibilização, fiscalização e implementação do GDPR.

Agencia Española de Protección de Datos (AEPD)

A Agência Espanhola de Proteção de Dados é uma autoridade administrativa independente a nível estadual, entre as previstas na Lei 40/2015, de 1 de outubro, sobre o Regime Jurídico do Setor Público. Ela possui personalidade jurídica própria e plena capacidade pública e privada, atuando com total independência dos poderes públicos no exercício de suas funções.

O mesmo é definido no Título VII da Lei Orgânica 3/2018, de 5 de dezembro, que trata da Proteção de Dados Pessoais e Garantia dos Direitos Digitais. A legislação define que a Agência se configure como uma autoridade administrativa independente, de acordo com a Lei 40/2015, que se relaciona com o Governo por meio do Ministério da Justiça.

A Presidência da Agência e seu Vice-Presidente são nomeados pelo Governo, sob proposta do Ministério da Justiça, entre pessoas de reconhecida competência profissional, designadamente em matéria de proteção de dados. O Decreto-Real 389/2021, de 1º de junho, aprovou o Estatuto da Agência Espanhola de Proteção de Dados.

A Agência está sujeita à legislação administrativa tanto no exercício de suas atribuições quanto no seu regime patrimonial e contratual: Lei 39/2015 (Procedimento Comum das Administrações Públicas), Lei 33/2003 (Patrimônio das Administrações Públicas), Lei 9/2017 (Contratos do Setor Público).

Commission Nationale de L'Informatique et des Libertés (CNIL)

Criada em 1978 pela Lei francesa de Proteção de Dados (Lei 78-17, 1978), a CNIL é uma autoridade administrativa independente, composta por um Colégio de 18 membros e uma equipe de agentes contratuais do Estado. Quanto aos membros, 12 entre os 18 são eleitos ou nomeados pelas assembleias ou jurisdições a que pertencem. Ministros, autoridades públicas, líderes empresariais, públicos ou privados, não podem se opor à sua ação.

O Presidente da CNIL recruta livremente seus colaboradores, e, atualmente, a autoridade conta com 225 agentes e orçamento de 20,1 milhões de euros[4]. Entre os agentes, 24% estão alocados na Diretoria de *Compliance* (*Direction de la Conformité*) e 31% na Diretoria de Proteção de Direitos e Sanções (*Direction de la Protection des Droits et des Sanctions*)[5].

[3] ESPANHA. Decreto-Real 389, de 1º de Junho de 2021.

[4] FRANÇA. *Commission Nationale de L'Informatique et des Libertés*. 2021. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_cnil_en_bref_2021.pdf. Acesso em: 10 de dezembro de 2021.

[5] Informações referentes ao ano de 2020.

Entre os 18 membros multidisciplinares, há **4 parlamentares** (2 deputados, 2 senadores); **2 membros do Conselho Econômico, Social e Ambiental**; **6 representantes dos tribunais superiores** (2 vereadores de estado, 2 vereadores do Tribunal de Cassação, 2 vereadores do Tribunal de Contas); **5 personalidades qualificadas** nomeadas pelo Presidente da Assembleia Nacional (1 personalidade), **Presidente do Senado** (1 personalidade) e **Conselho de Ministros** (3 personalidades); e o **Presidente da Comissão de Acesso aos Documentos Administrativos** (CADA). O mandato dos comissários é de 5 anos ou, para os parlamentares, de duração igual ao mandato eletivo.

A CNIL é uma autoridade administrativa independente (AAI), ou seja, um organismo público que atua em nome do Estado sem que esteja sob autoridade do governo ou de um ministro. A Comissão apresenta anualmente ao Presidente da República e ao Primeiro-Ministro um relatório público que dá conta do cumprimento da sua missão (art. 8, 5°, II, Lei 78-17, 1978).

Uma autoridade administrativa independente (AAI) é um órgão responsável por regulamentar certos setores em nome do Estado, tendo a particularidade de não estar sujeita à autoridade hierárquica de um ministro e, portanto, não estar sujeita à autoridade governamental. Com isso, não recebe ordens nem conselhos das autoridades públicas e atua com total independência. As AAIs devem, no entanto, apresentar relatório de atividades ao Governo e ao Parlamento todos os anos antes de 1° de junho.

Uma AAI tem poder real para fazer recomendações, tomar decisões, mas também regula e sanciona o setor pelo qual é responsável. Seu papel é assegurar a regulação de um setor específico no qual o Governo não quer intervir diretamente. A lei orgânica de 20 de janeiro de 2017 exige que as autoridades administrativas independentes sejam criadas por lei.

Existem 2 categorias de autoridades administrativas independentes:

- **instituições responsáveis pela regulação das atividades econômicas** e
- **instituições responsáveis pela proteção dos direitos dos cidadãos** (categoria na qual a CNIL se encaixa).

Federal Commissioner for Data Protection and Freedom of Information (BfDI- Alemanha)

A instituição do Federal Commissioner for Data Protection and Freedom of Information foi criada em 1978. Por proposta do Governo Federal Alemão, o Comissário Federal é eleito sem debate pelo *Bundestag* (Parlamento da Alemanha) com maioria simples, tendo mandato de cinco anos, renovável uma vez.

O Comissário Federal é totalmente independente no desempenho de suas funções e está apenas sujeito à lei, sendo apoiado, no entanto, por cerca de 270 funcionários em Bonn e Berlim[6].

Como autoridade supervisora em nível federal, o Comissário Federal tem um papel especial a desempenhar na aplicação da lei de proteção de dados. As disposições legais relevantes podem ser encontradas nos Artigos 51 a 59 do GDPR (Regulamento Geral de Proteção de Dados) e nas Seções 8 a 19 do BDSG (Lei Federal de Proteção de Dados).

Segundo o capítulo IV, seção 12 (1) do BDSG: "*The Federal Commissioner shall, in accordance with this Act, have official federal status under public law*" (O Comissário Federal deverá ter status oficial federal de acordo com a lei pública).

Outra atribuição do Comissário Federal é o dever de elaborar relatório anual de atividades, que pode conter uma lista dos tipos de violações comunicadas e os tipos de medidas tomadas, incluindo sanções e medidas em conformidade com o Regulamento (UE) 2016/679. Ele deverá, ainda, apresentar o relatório ao *Bundestag* alemão, ao *Bundesrat* (órgão constitucional) e ao Governo Federal, devendo colocá-lo à disposição do público, da Comissão Europeia e do Conselho Europeu para a Proteção de Dados (capítulo IV, seção 15 do BDSG).

O Comissário também está sujeito ao *Dienstaufsicht* (supervisão administrativa/hierárquica) do Ministro Federal do Interior, bem como ao *Rechtsaufsicht* (supervisão legal) do Governo Federal. Além disso, desde 2006, o Comissário Federal observa o cumprimento da Lei de Liberdade de Informação, que dá a todos o direito de acesso às informações de autoridades federais e outros órgãos do Estado na medida em que realizam atividades administrativas federais.

[6] ALEMANHA. BfDI. 2021. Disponível em: https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/DieBehoerde/diebehoerde_node.html. Acesso em: 11 de dezembro de 2021.

Information Commissioner's Office (ICO)[7]

O Information Commissioner's Office é um órgão público independente, sendo o Departamento de Mídia Digital, Cultura e Esporte (DCMS) o seu patrocinador dentro do Governo. O Information Commissioner é uma corporação unipessoal ("*corporation sole*")[8], conforme estabelecido no Data Protection Act de 2018, 12, 1 (1).

O GDPR exige que todos os Estados-Membros estabeleçam uma autoridade supervisora independente para regular a legislação de proteção de dados e, conforme estabelecido no Artigo 52 do Regulamento, o Information Commissioner deve ser totalmente independente, permanecer livre de influências externas, diretas ou indiretas, e não solicitar nem aceitar instruções no desempenho de suas funções e poderes como autoridade supervisora nacional. De acordo com esses requisitos, foi elaborado um Acordo de Gestão pelo Departamento de Digital, Cultura, Mídia e Esporte (DCMS) em consulta com o Information Commissioner, válido até 31 de março de 2022. O IC é diretamente responsável perante o Parlamento, sendo que o Secretário de Estado e outros membros da Equipe Ministerial do DCMS representarão os interesses do IC no Parlamento, quando apropriado.

Como uma empresa unipessoal, todos os poderes e deveres formais do IC recaem sobre a figura do Comissário, não havendo exigência legal para que o IC tenha um Conselho. Contudo, para ajudar a cumprir suas responsabilidades, devido à escala e à complexidade do papel e do mandato, o Comissário optou por constituir um Conselho de Administração composto por Diretores Executivos e Não Executivos, e delegou formalmente a responsabilidade pela definição da direção estratégica do IC ao Conselho de Administração, que o Comissário preside[9].

O IC é financiado principalmente por organizações que pagam taxa de proteção de dados, que representa cerca de 85% a 90% do orçamento anual do órgão[10]. Isso é complementado por subsídios do governo para financiar a regulamentação do IC de várias outras leis (*Freedom of Information Act, Network and Information Systems Regulations, Electronic Identification and Trust Services, Investigatory Powers Act*).

[7] Embora não mais pertencente à União Europeia, para os fins do presente estudo, optou-se por incluir as informações referentes à Autoridade de Proteção de Dados do Reino Unido.

[8] Trata-se de pessoa jurídica consistente em um único cargo, ocupado por uma única pessoa: a corporation sole is a legal entity consisting of a single ("*sole*") incorporated office, occupied by a single ("*sole*") natural person.

[9] REINO UNIDO. *Information Commissioner's Office*. 2021. Disponível em: https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/. Acesso em: 11 de dezembro de 2021.

[10] Idem.

Interpretação dos Critérios de Autonomia e Independência

As autoridades supervisoras são organismos a serviço do interesse público, com base nas respectivas funções de supervisão. Para evitar possíveis conflitos de interesse e apoiar a supervisão e a tomada de decisão, considerações adequadas devem ser feitas não apenas para o cumprimento dos objetivos principais, mas para a governança em torno dos processos de supervisão e funcionamento da autoridade.

A boa governança é, portanto, necessária para a forma como os supervisores são gerenciados, avaliados e responsabilizados. Além disso, a independência adequada é uma ferramenta crucial para reduzir a probabilidade de influência indevida da indústria e de interferência política.

Anteriormente, viu-se que, de acordo com o art. 15 do GDPR, as autoridades de supervisão devem atuar com total independência e imparcialidade no desempenho de suas funções e no exercício de seus poderes e, ao fazê-lo, não solicitar nem aceitar instruções. Cada Estado deve assegurar que as autoridades de supervisão sejam dotadas de recursos necessários ao desempenho eficaz de suas funções e ao exercício de seus poderes.

O GDPR define a independência das autoridades de supervisão da seguinte forma (art. 52):

> ***Independência***
>
> ***1.*** *As autoridades de controle agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhes são atribuídos nos termos do presente regulamento.*
> ***2.*** *Os membros das autoridades de controle 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.*
> ***3.*** *Os membros da autoridade de controle abstêm-se de qualquer ato incompatível com suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.*
> ***4.*** *Os Estados-Membros asseguram que cada autoridade de controle 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 Comitê.*

5. *Os Estados-Membros asseguram que cada autoridade de controle selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controle interessada.*

6. *Os Estados-Membros asseguram que cada autoridade de controle fique sujeita a um controle financeiro que não afete a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional.*

Os artigos 53 e 54, por sua vez, fornecem requisitos para garantir a independência das autoridades de supervisão:

Condições gerais aplicáveis aos membros da autoridade de controle

• Os Estados-Membros estabelecem que cada membro das respetivas autoridades de controle seja nomeado por procedimento transparente:

- pelo Parlamento,
- pelo Governo,
- pelo Chefe de Estado, ou
- por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro.

• Cada membro possui habilitações, experiências e conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados pessoais, ao desempenho das suas funções e ao exercício dos seus poderes.

• As funções dos membros da autoridade de controle cessam ao final do seu mandato, com sua exoneração ou aposentadoria compulsória, nos termos do direito do Estado-Membro em causa.

• Os membros da autoridade de controle só serão exonerados se tiverem cometido falta grave ou deixado de cumprir as condições exigidas para o exercício das suas funções.

Regras aplicáveis à constituição da autoridade de controle

• Os Estados-Membros estabelecem, por via legislativa:

a) Constituição de cada autoridade de controle;

b) Qualificações e condições de elegibilidade necessárias para a nomeação dos membros de cada autoridade de controle;

c) Regras e procedimentos de nomeação dos membros de cada autoridade de controle;

d) Duração do mandato dos membros de cada autoridade de controle, que não será inferior a quatro anos, salvo no caso do primeiro mandato após 24 de maio de 2016, e ser mais curta quando for necessário proteger a independência da autoridade de controle através de um procedimento de nomeações escalonadas;

e) Se, e em caso afirmativo, por quantos mandatos os membros de cada autoridade de controle podem ser renomeados;

f) Condições que regem as obrigações dos membros e do pessoal de cada autoridade de controle, proibição das ações, funções e benefícios que com elas são incompatíveis durante o mandato e após o seu termo e regras que regem a cessação da relação de trabalho.

Para além dos requisitos estabelecidos pelo GDPR, é importante analisar como o requisito da independência foi definido em outros contextos regulatórios, especialmente no âmbito internacional.

Inicialmente, as "Características de Credenciamento de Autoridades de Proteção de Dados" do ICDPPC[11], adotadas em 25 de setembro de 2001 durante a 23ª Conferência Internacional realizada em Paris, propõem que deve ser garantido à autoridade de proteção de dados grau adequado de autonomia e independência para o desempenho de suas funções.

A autonomia requer que uma autoridade tenha poderes, tanto de forma legal quanto prática, para iniciar e realizar ações adequadas sem ter de buscar permissão de terceiros. A independência é importante para que as agências possam operar livres de interferência política ou governamental e resistir à influência de terceiros interessados. As garantias típicas incluem:

- Nomeação por prazo determinado;
- Remoção apenas por incapacidade de exercer o cargo, negligência com os deveres do cargo, ou falta grave;
- O poder de reportar diretamente ao chefe do executivo ou legislativo e de falar publicamente sobre assuntos de interesse;
- Imunidade contra ações judiciais pessoalmente direcionadas aos dirigentes, por atos praticados no âmbito de suas funções oficiais;
- Poder para iniciar investigações.

[11] ICDPPC. *Resolution on Accreditation Features of Data Protection Authorities*, 2015.

O tema da independência de autoridades de supervisão foi tratado também pelas Nações Unidas nos chamados Princípios de Paris[12], um conjunto de normas internacionais adotadas pela Assembleia Geral em 1993 que define papel, composição, status e funções das Instituições Nacionais de Direitos Humanos:

- A instituição nacional deve dispor de infraestrutura adequada ao bom desenvolvimento de suas atividades, em particular de financiamento adequado, que tem por objetivo permitir que a instituição tenha pessoal e instalações próprias, de forma a ser independente do Governo e não estar sujeita a controle financeiro que possa afetar sua independência;
- A fim de assegurar aos membros da instituição nacional um mandato estável, sem o qual não pode haver verdadeira independência, a sua nomeação efetua-se por ato oficial que fixa a duração específica do mandato, podendo ser renovável, desde que garantido o pluralismo de membros da instituição.

Sob o título "Métodos de operação", os Princípios de Paris afirmam ainda que a instituição nacional deve:

- Considerar livremente quaisquer questões que sejam de sua competência, mesmo aquelas apresentadas pelo Governo ou por este levantadas sem encaminhamento a uma autoridade superior, sob proposta de seus membros ou de qualquer peticionário;
- Ouvir qualquer pessoa e obter todas as informações e documentos necessários à avaliação das situações da sua competência;
- Dirigir-se à opinião pública, diretamente ou por meio de qualquer órgão de imprensa, especialmente para divulgar suas opiniões e recomendações.

Em relatório de 2016 intitulado *Being an Independent Regulator*[13], a Organização para Cooperação e Desenvolvimento Econômico (OCDE) observa que, em comparação com alocações orçamentárias plurianuais, as alocações anuais para os reguladores podem aumentar o risco de influência indevida. A OCDE também alerta contra o risco de **"**portas giratórias**"** e conflitos de interesse com a indústria, quando não são estabelecidas restrições pré ou pós-contratação de pessoal profissional.

[12] European Network of National Human Rights Institutions. *UN Paris Principles & Accreditation*, 2021.

[13] Organização para Cooperação e Desenvolvimento Econômico (OCDE). *Being an Independent Regulator*, 2016. Disponível em: https://www.oecd.org/publications/being-an-independent-regulator-9789264255401-en.htm. Acesso em: 12 de dezembro de 2021.

Em orientações de 2017 intituladas **"**Criando uma Cultura de Independência: Orientação prática contra a influência indevida**"**[14], a OCDE descreve cinco dimensões para uma cultura de independência:

- Clareza do papel para evitar influência indevida;
- Transparência para promover credibilidade e confiança nas decisões e processos do regulador, e responsabilidade para permitir a prestação de contas;
- Independência financeira;
- Independência de liderança, sendo o chefe de um regulador provavelmente exposto a pressões; e
- Comportamento da equipe, criando-se uma cultura de independência que tem por objetivo promover um ambiente que ajuda a equipe a produzir o conselho imparcial necessário e a rejeitar influências indevidas.

Mais recentemente, em 2018, o Conselho da Europa adotou a "Convenção 108+" (Convenção para a Proteção de Indivíduos no que diz respeito ao Tratamento de Dados Pessoais)[15]. O Protocolo de Alteração da Convenção 108 exige que as seguintes disposições tenham efeito na lei das partes signatárias:

> **Artigo 15 - Autoridades de supervisão**
> **1.** Cada Parte estabelecerá que uma ou mais autoridades serão responsáveis por garantir o cumprimento das disposições desta Convenção.
> **[...]**
> **5.** As autoridades de supervisão atuam com total independência e imparcialidade no desempenho das suas funções e no exercício dos seus poderes e, ao fazê-lo, não solicitam nem aceitam instruções.
> **6.** Cada Parte assegurará que as autoridades de supervisão sejam dotadas dos recursos necessários ao desempenho eficaz de suas funções e ao exercício de seus poderes.

[14] Organização para Cooperação e Desenvolvimento Econômico (OCDE). Criando uma Cultura de Independência: Orientação prática contra a influência indevida, 2017. Disponível em: https://www.oecd.org/gov/regulatory-policy/independence-of-regulators.htm.*

[15] UNIÃO EUROPEIA. Comissão Europeia. *Convention* 108+, 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.*

* Acessados em: 12 de dezembro de 2021.

Decisões de adequação tomadas pela Comissão Europeia

A Comissão Europeia tem o poder de determinar, com base no artigo 45 do Regulamento (UE) 2016/679, se um país fora da União Europeia oferece nível adequado de proteção de dados com base nos parâmetros exigidos pelo GDPR. A adoção de uma decisão de adequação envolve:

a. proposta da Comissão Europeia;
b. parecer do Conselho Europeu de Proteção de Dados;
c. aprovação de representantes de países da EU; e
d. adoção da decisão pela Comissão Europeia.

A qualquer momento, o Parlamento Europeu e o Conselho podem solicitar à Comissão Europeia que mantenha, altere ou retire decisão de adequação, alegando que seu ato excede as competências de execução previstas no regulamento.

O efeito de uma decisão de adequação é que os dados pessoais podem fluir da União Europeia (bem como Noruega, Liechtenstein e Islândia) para o país terceiro sem que seja necessária qualquer salvaguarda adicional. Em outras palavras, as transferências para o país serão equiparadas a transmissões de dados entre países da União Europeia.

A Comissão Europeia reconheceu até agora Andorra, Argentina, Canadá, Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça, Reino Unido e Uruguai como países que fornecem esse nível adequado de proteção.

A análise de algumas decisões de adequação, sobretudo em relação às características das Autoridades Nacionais de Proteção de Dados consideradas como relevantes pela Comissão, é capaz de revelar requisitos fundamentais a serem adotados por demais autoridades que também buscam mesmo grau de adequação em matéria de proteção de dados.

Para fins de análise, optou-se pela seleção de duas decisões mais recentes da Comissão (referentes ao Japão e ao Reino Unido) e de duas decisões ainda sob a égide da Diretiva 95/46/CE (referentes ao Uruguai e a Israel, em virtude da estrutura de suas Autoridades de Proteção de Dados).

Japão

Na decisão de implementação do sistema de proteção de dados japonês[16], de 23 de janeiro de 2019, a Comissão Europeia ressaltou que a adoção da decisão de adequação tem de se basear numa análise abrangente da ordem jurídica do país terceiro, no que diz respeito às regras aplicáveis aos importadores de dados e às limitações e salvaguardas ao acesso aos dados pessoais por parte das autoridades públicas.

A avaliação deve determinar se o país terceiro em questão garante nível de proteção essencialmente equivalente ao garantido na União Europeia (Considerando 104 do Regulamento (UE) 2016/679). Conforme esclarecido pelo Tribunal de Justiça da União Europeia, **"**essencialmente equivalente**"** não significa um nível de proteção idêntico. Em especial, os meios a que o país terceiro recorre podem ser diferentes dos utilizados na União Europeia, mas serão adequados desde que se revelem, na prática, eficazes para garantir a proteção adequada.

A norma de adequação não exige, portanto, uma réplica, ponto a ponto, das regras da União. Em vez disso, o teste consiste em saber se, por meio da substância dos direitos de privacidade e de sua implementação, supervisão e fiscalização eficazes, o sistema estrangeiro como um todo oferece o nível de proteção necessário.

A Comissão, ao analisar legislação e prática, concluiu que o Japão garante nível adequado de proteção dos dados pessoais transferidos para organizações abrangidas pela aplicação da Lei sobre a Proteção de Informações Pessoais ("*Act on the Protection of Personal Information*" ou APPI).

Especificamente no que tange à autoridade supervisora, tem-se que no Japão a autoridade incumbida de supervisionar e aplicar a APPI é a *Personal Information Protection Commission* (PPC), constituída por um presidente e oito comissários, designados pelo primeiro-ministro mediante aprovação de ambas as câmaras da Dieta, todos com mandato de cinco anos, com possibilidade de recondução (artigo 64 da APPI). Os comissários só podem ser destituídos com justa causa, num conjunto limitado de circunstâncias excepcionais[17], não podendo envolver-se ativamente em atividades políticas.

[16] UNIÃO EUROPEIA. Comissão Europeia. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information. 2019. Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2019/419/oj. Acesso em: 11 de dezembro de 2021.

[17] Nos termos do artigo 65 da APPI, a destituição contra a vontade do comissário só é possível com um dos seguintes fundamentos: **i)** abertura de um processo de falência; **ii)** condenação por violação da APPI ou da Lei relativa à utilização de números de identificação; **iii)** condenação a uma pena de prisão sem possibilidade de prestação de trabalho ou a uma pena ainda mais severa; **iv)** incapacidade para executar os seus deveres por motivos de distúrbio mental ou físico, ou de conduta reprovável.

Além disso, nos termos da APPI, os comissários a tempo integral devem abster-se de exercer outras atividades remuneradas ou de caráter comercial, estando igualmente sujeitos a normas internas que os impedem de participar nas deliberações em caso de conflito de interesses. A PPC é assistida por um secretariado, chefiado por um secretário-geral, criado para fins de execução das tarefas que lhe incumbem (artigo 70 da APPI). Tanto os comissários quanto os demais funcionários do secretariado estão vinculados por regras estritas de confidencialidade (artigos 72 e 82 da APPI).

Os poderes da PPC são exercidos com total independência (artigo 62 da APPI) e definidos principalmente nos artigos 40, 41 e 42 da APPI. Nos termos do artigo 40, a PPC pode solicitar aos agentes de tratamento (*Personal Information Handling Business Operators*, ou PIHBOs) que comuniquem informações ou apresentem documentos sobre as operações, podendo igualmente proceder a inspeções tanto no local quanto nos livros e outros documentos.

Na medida do necessário à aplicação da APPI, a PPC pode ainda formular orientações ou conselhos aos agentes relativamente à gestão das informações pessoais. A PPC já exerceu poderes que lhe são conferidos pelo artigo 41 da APPI quando formulou orientações dirigidas ao Facebook, na sequência das revelações efetuadas no âmbito do caso Facebook/Cambridge Analytica.

Mais importante ainda, a PPC tem competência, quer dando seguimento a uma queixa, quer atuando por sua própria iniciativa, para emitir recomendações e ordens destinadas a fazer aplicar a APPI e outras normas vinculativas (incluindo normas complementares) em casos concretos. Essas competências são definidas no artigo 42 da APPI.

Nos termos do artigo 42, n. 1, da APPI, se entender haver necessidade de proteger direitos e interesses de pessoa natural em casos de violação de disposições específicas da APPI, a PPC pode emitir recomendação de suspensão do ato ou de tomada de outras medidas necessárias para retificar a violação, que não é vinculativa, mas abre caminho à ordem vinculativa em conformidade com o artigo 42, n. 2, da APPI.

Com base nessa disposição, se a recomendação não for acatada "sem que existam motivos legítimos" e a PPC "entender que está iminente uma violação grave a direitos e interesses de uma pessoa natural", pode ordenar ao controlador que tome medidas consonantes com a recomendação. As normas complementares clarificam e reforçam poderes de execução coerciva da PPC.

Mais concretamente, nos casos que envolvam dados importados da União Europeia, a PPC considera sempre ausência imotivada da tomada de medidas por um controlador, em conformidade com recomendação emitida pela APPI, como violação grave iminente dos direitos e interesses de um titular, e, consequentemente, como infração que justifique a emissão de ordem vinculativa.

Por outro lado, a PPC apenas aceita como **"**motivo legítimo**"** para não cumprir a recomendação uma **"**ocorrência de natureza extraordinária [que impeça o cumprimento] fora do controle [do controlador], que não pode ser razoavelmente prevista (catástrofes naturais)**"** ou casos em que a necessidade de tomar medidas na sequência de uma recomendação **"**tenha deixado de existir porque [o controlador] tomou medidas alternativas para pôr termos à violação**"**.

A Comissão analisou também a atuação da PPC no que diz respeito à fiscalização e ao *enforcement* de autoridades governamentais, concluindo que os mecanismos existentes de supervisão, reforçados pela possibilidade de os titulares desencadearem a intervenção da PPC, na qualidade de autoridade de controle independente, proporcionam garantias adequadas contra risco de abusos pelas autoridades japonesas dos seus poderes no domínio da segurança nacional e contra eventual coleta ilícita de informações eletrônicas.

Em sua conclusão, a Comissão julga que APPI e normas complementares, juntamente com declarações, garantias e compromissos oficiais apresentados pelo Governo japonês, asseguram nível de proteção dos dados pessoais transferidos da União Europeia essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679. A Comissão considera, ainda, que os mecanismos de controle e as vias de recurso previstos na legislação japonesa permitem, no seu conjunto, identificar e sancionar na prática violações pelos agentes de tratamento, proporcionando vias judiciais aos titulares dos dados para garantir seus direitos previstos na APPI.

Finalmente, com base nas informações disponíveis sobre o quadro jurídico japonês, incluindo declarações, garantias e compromissos governamentais, a Comissão entende que qualquer ingerência das autoridades públicas japonesas nos direitos fundamentais dos titulares, cujos dados pessoais sejam transferidos da União Europeia para o Japão, para fins de interesse público, designadamente, para efeitos de aplicação do direito penal e de segurança nacional, será limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra essa ingerência.

Reino Unido

No Reino Unido, supervisão e aplicação do cumprimento do GDPR e do DPA 2018 são realizadas pelo Comissário da Informação (*Information Commissioner*). Conforme visto anteriormente, o Comissário de Informação é uma "*sole corporation*": entidade legal com personalidade jurídica própria, constituída em uma única pessoa. O Comissário é apoiado em seu trabalho por um escritório que, em 31 de março de 2020, contava com 768 funcionários permanentes[18].

A independência do Comissário está explicitamente estabelecida no artigo 52 do GDPR do Reino Unido, que não altera de forma substantiva o artigo 52, 1 a 3, do GDPR. Ele deve agir com total independência no desempenho de suas tarefas e no exercício de seus poderes, permanecendo livre de influências externas, diretas ou indiretas, e não solicitar nem aceitar instruções de terceiros. Também deve se abster de qualquer ação incompatível com suas funções e não deve, durante o exercício do cargo, exercer qualquer atividade incompatível, remunerada ou não.

As condições para nomeação e destituição do Comissário são estabelecidas no Anexo 12 do DPA 2018. Ele é nomeado por Sua Majestade por recomendação do Governo no âmbito de um concurso justo e aberto. O candidato deve ter qualificações, habilidades e competência adequadas. De acordo com o Código de Governança sobre Nomeações Públicas, uma lista de candidatos designáveis é feita por painel consultivo de avaliação. Antes que o Secretário de Estado do Departamento de Mídia Digital, Cultura e Esporte (DCMS) finalize sua decisão, o Comitê Seleto do Parlamento pertinente deve realizar um escrutínio prévio à nomeação. A posição do Comitê é tornada pública.

O Comissário da Informação exerce funções por período máximo de sete anos, sendo que uma pessoa não pode ser nomeada como Comissário mais de uma vez. Ele pode ser destituído do cargo por Sua Majestade após um discurso de ambas as Casas do Parlamento. No entanto, nenhum pedido de demissão do Comissário pode ser apresentado a qualquer das Casas do Parlamento, a menos que um Ministro tenha apresentado um relatório declarando que está convencido de que o Comissário é culpado de falta grave e/ou não preenche mais as condições exigidas para o desempenho das funções.

[18] UNIÃO EUROPEIA. Comissão Europeia. *Commission Implementing Decision of* 28.6.2021 *pursuant to Regulation* (EU) 2016/679 *of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*. 2021. Disponível em: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en. Acesso em: 11 de dezembro de 2021.

O financiamento do Comissário vem de três fontes:

(i) taxas de proteção de dados pagas pelos controladores, equivalentes a 85% - 90% do orçamento anual;
(ii) concessão de ajuda paga pelo Governo ao Comissário, utilizada principalmente para financiar os custos de funcionamento no que diz respeito às tarefas não relacionadas com a proteção de dados; e
(iii) taxas cobradas pelos serviços (no momento, essas taxas não são aplicadas).

As funções gerais do Comissário da Informação em relação ao tratamento de dados pessoais a que se aplica o GDPR do Reino Unido são estabelecidas no artigo 57, refletindo de perto as regras correspondentes do Regulamento (UE) 2016/679. Suas funções incluem monitoramento e aplicação do GDPR do Reino Unido, promoção da conscientização pública, tratamento de reclamações apresentadas pelos titulares dos dados, realização de investigações, entre outras.

Além disso, a Seção 115 do DPA 2018 estabelece outras funções gerais do Comissário, que incluem o dever de aconselhar o Parlamento, o governo e outras instituições e órgãos sobre medidas legislativas e administrativas relacionadas à proteção dos direitos e às liberdades dos indivíduos, e o poder de emitir, por iniciativa do próprio Comissário ou a pedido, pareceres ao Parlamento, ao governo ou a outras instituições e órgãos, bem como ao público, sobre qualquer questão relacionada à proteção de dados pessoais.

Em particular, o Comissário tem poderes para:

a. ordenar ao controlador e ao operador o fornecimento de informações necessárias, dando aviso de informação;
b. realizar investigações e auditorias, dando aviso de avaliação;
c. obter de outra forma acesso a documentos e instalações "poderes de entrada e inspeção";
d. exercer poderes corretivos, inclusive por meio de advertências e repreensões ou dar ordens por meio de aviso de execução, que exige que controladores/operadores tomem ou se abstenham de tomar medidas especificadas "aviso de execução"; e
e. emitir multas administrativas na forma de aviso de multa, que pode ser emitido também no caso de uma autoridade pública não cumprir as disposições do GDPR.

Para manter a independência do Judiciário, o Comissário não está autorizado a exercer suas funções em relação ao tratamento de dados pessoais por indivíduo atuando em capacidade judicial, ou por um tribunal atuando em sua capacidade judicial.

No entanto, a supervisão do poder judicial é assegurada por organismos especializados.[19] Isso reflete a abordagem adotada no Regulamento (UE) 2016/679 (artigo 55, 3).

No que diz respeito à atuação de fiscalização e sanção de autoridades públicas, prevista na terceira parte do DPA 2018, o Comissário tem poderes gerais de investigação, correção, autorização e aconselhamento em relação ao tratamento de dados pessoais a que se aplica essa terceira parte da lei, podendo notificar o agente de tratamento sobre suposta violação, emitir avisos ou repreender agentes de tratamento que tenham infringido a lei, e emitir, por sua própria iniciativa ou a pedido, pareceres ao Parlamento, ao governo ou a outras instituições e órgãos, bem como ao público. Além disso, o Comissário tem poderes para emitir avisos de informação, avisos de avaliação e avisos de execução, bem como poder de acessar documentos e dependências, e de emitir multas administrativas na forma de autos de infração.

De acordo com seus relatórios anuais mais recentes (2018–2019, 2019-2020), o Comissário conduziu uma série de investigações e tomou medidas coercitivas no que diz respeito ao tratamento de dados por autoridades públicas. Por exemplo, o IC conduziu investigação e publicou parecer em outubro de 2019 sobre uso da tecnologia de reconhecimento facial por parte da polícia em locais públicos. Outro exemplo de ação coercitiva nessa área é a multa de £ 325.000 emitida pelo Comissário em maio de 2018 contra o *Crown Prosecution Service* pela perda de DVDs não criptografados contendo gravações de entrevistas policiais. O Comissário de Informação também conduziu investigações sobre tópicos mais amplos, por exemplo, no primeiro semestre de 2020, sobre uso de extração de telefones celulares para fins de policiamento e tratamento de dados das vítimas pela polícia.

Ao final do documento, a Comissão considera que o Reino Unido e o DPA 2018 garantem nível de proteção de dados pessoais transferidos da União Europeia que é essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679. Além disso, a Comissão considera que, no seu conjunto, os mecanismos de fiscalização e as vias de recurso na legislação do Reino Unido permitem que infrações sejam identificadas e punidas na prática e oferecem vias de recurso jurídicas ao titular dos dados para obter acesso aos dados pessoais a ele relacionados, retificação ou exclusão desses dados.

[19] Para os tribunais da Inglaterra e do País de Gales, essa supervisão é fornecida pelo *Judicial Data Protection Panel*. Na Irlanda do Norte, o *Lord Chief Justice* nomeou um juiz do *High Court* como *Data Supervisory Judge*, e, na Escócia, o *Lord President* nomeou um juiz responsável pela supervisão de dados para investigar quaisquer reclamações. Finalmente, na Suprema Corte, um dos juízes é nomeado para exercer a função.

Uruguai

A decisão que reconheceu o Uruguai como país com nível de proteção equivalente ao padrão estabelecido pela União Europeia deu-se em 21 de agosto de 2012, tendo como padrão de análise a Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa ao tema (anterior ao GDPR)[20].

Segundo o entendimento da Comissão, a aplicação de normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de *habeas data*, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento, a fim de exercer o direito de acesso, retificação e supressão, e por um controle independente efetuado pela Unidade Reguladora e de Controle de Dados Pessoais (*Unidad Reguladora y de Control de Datos Personales* – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28 da Diretiva 95/46/CE, e que atua de forma totalmente independente. Além disso, qualquer parte interessada pode recorrer aos tribunais para pedir indenização por danos sofridos em consequência do tratamento ilícito dos seus dados pessoais.

A autoridade uruguaia de proteção de dados apresentou à Comissão explicações e deu garantias sobre o modo como sua legislação é interpretada, tendo assegurado que a lei, em matéria de proteção de dados, é aplicada de acordo com essa interpretação. A autoridade explicou nomeadamente que, nos termos do artigo 332 da Constituição do país, a Lei n. 18.331 é aplicável supletivamente às questões que não são reguladas em leis especiais que criam e regem determinadas bases de dados.

No que se refere ao princípio da transparência, a autoridade comunicou que a obrigação de prestar informações necessárias às pessoas a quem os dados dizem respeito é aplicável em todas as situações. Relativamente ao direito de acesso, a autoridade de proteção de dados especificou que é suficiente que a pessoa em causa prove sua identidade quando apresentar o pedido. Também foi especificado que as exceções relativas ao princípio das transferências internacionais, previstas no artigo 23, n. 1, da Lei n. 18.331, não podem ser interpretadas em âmbito mais vasto que o previsto no artigo 26, n. 1, da Diretiva 95/46/CE.

Desse modo, a Comissão considerou, para efeito do artigo 25, n. 2, da Diretiva 95/46/CE, que a República Oriental do Uruguai assegura nível adequado de proteção dos dados pessoais transferidos a partir da União Europeia.

[20] UNIÃO EUROPEIA. Comissão Europeia. *Commission Implementing Decision of 21 August 2012 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Eastern Republic of Uruguay with Regard to Automated Processing of Personal Data*. 2012. Disponível em: https://eur-lex.europa.eu/eli/dec/2012/484/oj. Acesso: 11 de dezembro de 2021.

Para os fins almejados no presente estudo, deve-se ressaltar que a autoridade uruguaia foi criada pela Lei n. 18.331, de 11 de agosto de 2008, como autoridade central do sistema de proteção de dados pessoais do país. A URCDP não está estruturada de maneira semelhante a uma autarquia em regime especial e não possui, portanto, personalidade jurídica própria. Ela é um órgão público inserido na estrutura da *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento* – Agesic, instituição responsável por capitanear ações para o desenvolvimento tecnológico do Uruguai. A Agesic é uma unidade executora com autonomia técnica, dependente da Presidência da República Oriental do Uruguai.

Israel

Assim como no caso uruguaio, a decisão de adequação de Israel, de 31 de janeiro de 2011, teve como base a Diretiva 95/46/CE do Parlamento Europeu e do Conselho. A decisão reconhece que a aplicação das normas jurídicas relativas à proteção de dados é garantida pela possibilidade de recurso administrativo e judicial e pela supervisão independente exercida pela autoridade de controle, a Autoridade Israelita para os Assuntos Jurídicos, Informação e Tecnologia (ILITA), dotada de poderes de investigação e de intervenção, e que atua com plena independência[21].

Novamente, menciona-se que a autoridade israelita apresentou explicações e forneceu garantias sobre o modo como a legislação é interpretada, tendo assegurado que a lei, em matéria de proteção de dados, é aplicada de acordo com essa interpretação. A decisão da Comissão, portanto, leva em conta essas explicações e garantias. Para efeitos do artigo 25, n. 2, da Diretiva 95/46/CE, considera-se que o Estado de Israel assegura nível adequado de proteção em relação às transferências internacionais automatizadas de dados pessoais a partir da União Europeia ou, quando não são automatizadas, estão sujeitas a tratamento automatizado adicional no Estado de Israel.

É importante destacar que, atualmente, em Israel, a autoridade de proteção de dados é a *Israeli Privacy Protection Authority* – PPA, inserida na estrutura do Ministério da Justiça. Ela deve publicar relatórios anuais sobre as atividades desempenhadas no exercício anterior, os quais são submetidos à análise crítica de órgão colegiado composto por professores, profissionais da área e representantes da sociedade civil (*The Public Council for Privacy Protection*), que encaminhará suas observações a uma comissão do Poder Legislativo, encarregada de supervisionar a matéria (*Constitution and Law Committee*).

[21] UNIÃO EUROPEIA. Comissão Europeia. *Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data*. 2011. Disponível em: https://eur-lex.europa.eu/eli/dec/2011/61(1)/oj. Acesso: 1 de dezembro de 2021.

Recursos nacionais x Recursos disponibilizados às Autoridades de Proteção de Dados

A seguir, realizamos um comparativo entre os recursos nacionais aos Estados aos quais o GDPR se aplica e os recursos disponibilizados às suas respectivas autoridades de proteção de dados. Foram levantados o Produto Interno Bruto (PIB) de cada país[22], seu número de habitantes[23], orçamento das autoridades e seu número de funcionários (relativamente ao ano de 2021, em conformidade com o estudo elaborado pelo EDPB apresentado no tópico 1 deste *white paper*).

País	Itália
Autoridade de Proteção de Dados	Garante per la Protezione dei Dati Personali
PIB	US$ 1,92 trilhão
Recursos financeiros	€ 35.627.273,00
Habitantes	60.341.753
Recursos pessoais	133

País	Espanha
Autoridade de Proteção de Dados	Agencia Española de Protección de Datos
PIB	US$ 1,36 trilhão
Recursos financeiros	€ 15.762.500
Habitantes	46.779.233
Recursos pessoais	189

País	França
Autoridade de Proteção de Dados	Commission Nationale de L'Informatique et des Libertés
PIB	US$ 2,69 trilhões
Recursos financeiros	€ 21.507.000
Habitantes	65.468.526
Recursos pessoais	245

[22] De acordo com as informações contidas no site Trading Economics: https://tradingeconomics.com.
[23] De acordo com as informações contidas no site Worldometer: https://www.worldometers.info.

País	Holanda
Autoridade de Proteção de Dados	Dutch Data Protection Authority
PIB	US$ 925 bilhões
Recursos financeiros	€ 26.274.528
Habitantes	17.186.062
Recursos pessoais	175

País	Irlanda
Autoridade de Proteção de Dados	Data Protection Commission
PIB	US$ 440 bilhões
Recursos financeiros	€ 19.100.000
Habitantes	5.000.001
Recursos pessoais	175

País	Alemanha
Autoridade de Proteção de Dados	Federal Commissioner for Data Protection and Freedom of Information
PIB	US$ 3,96 trilhões
Recursos financeiros	€ 94.793.900
Habitantes	84.145.628
Recursos pessoais	1.083

País	Reino Unido
Autoridade de Proteção de Dados	Information Commissioner's Office
PIB	US$ 2,7 trilhões
Recursos financeiros	€ 7.141.134
Habitantes	10.735.752
Recursos pessoais	112

País	Hungria
Autoridade de Proteção de Dados	Hungarian National Authority for Data Protection and Freedom of Information
PIB	US$ 176,3 bilhões
Recursos financeiros	€ 4.522.744
Habitantes	9.627.286
Recursos pessoais	117

País	Polônia
Autoridade de Proteção de Dados	Personal Data Protection Office (UODO)
PIB	US$ 625 bilhões
Recursos financeiros	€ 8.281.844
Habitantes	37.790.630
Recursos pessoais	271

País	Bélgica
Autoridade de Proteção de Dados	Autorité de Protection des Données (APD)
PIB	US$ 575 bilhões
Recursos financeiros	€ 9.002.200
Habitantes	11.521.238
Recursos pessoais	67

País	Suécia
Autoridade de Proteção de Dados	Swedish Authority for Privacy Protection (IMY)
PIB	US$ 550 bilhões
Recursos financeiros	€ 11.955.000
Habitantes	10.184.260
Recursos pessoais	95

País	Noruega
Autoridade de Proteção de Dados	Norwegian Data Protection Authority (Datatilsynet)
PIB	US$ 444,5 bilhões
Recursos financeiros	€ 7.066.000
Habitantes	5.478.446
Recursos pessoais	62

País	Luxemburgo
Autoridade de Proteção de Dados	Commission Nationale pour la Protection des Données – CNPD
PIB	US$ 68,5 bilhões
Recursos financeiros	€ 7.200.000
Habitantes	639.679
Recursos pessoais	54

País	Dinamarca
Autoridade de Proteção de Dados	Danish Data Protection Agency
PIB	US$ 325 bilhões
Recursos financeiros	€ 5.997.848,31
Habitantes	5.819.683
Recursos pessoais	271

País	Eslováquia
Autoridade de Proteção de Dados	Office for Personal Data Protection of the Slovak Republic
PIB	US$ 104 bilhões
Recursos financeiros	€ 1.744.595
Habitantes	5.463.213
Recursos pessoais	45

País	Áustria
Autoridade de Proteção de Dados	Austrian Data Protection Authority
PIB	US$ 435 bilhões
Recursos financeiros	€ 4.227.000
Habitantes	8.933.346
Recursos pessoais	45

País	Bulgária
Autoridade de Proteção de Dados	Personal Data Protection Commission
PIB	US$ 77,65 bilhões
Recursos financeiros	€ 1.564.285
Habitantes	6.877.774
Recursos pessoais	81

País	Chipre
Autoridade de Proteção de Dados	Office of the Commissioner for Personal Data Protection
PIB	US$ 23,5 bilhões
Recursos financeiros	€ 711.918
Habitantes	1.215.584
Recursos pessoais	18

País	Estônia
Autoridade de Proteção de Dados	Data Protection Inspectorate
PIB	US$ 28 bilhões
Recursos financeiros	€ 850.000
Habitantes	1.327.737
Recursos pessoais	19

País	Finlândia
Autoridade de Proteção de Dados	Office of the Data Protection Ombudsman
PIB	US$ 255 bilhões
Recursos financeiros	€ 3.790.000
Habitantes	5.552.319
Recursos pessoais	53

País	Grécia
Autoridade de Proteção de Dados	Hellenic Data Protection Authority (HDPA)
PIB	US$ 200 bilhões
Recursos financeiros	€ 2.811.111
Habitantes	10.354.278
Recursos pessoais	42

País	Croácia
Autoridade de Proteção de Dados	Croatian Personal Data Protection Agency (AZOP)
PIB	US$ 65,1 bilhões
Recursos financeiros	€ 1.244.015
Habitantes	4.071.065
Recursos pessoais	35

País	Islândia
Autoridade de Proteção de Dados	Icelandic Data Protection Authority
PIB	US$ 23,5 bilhões
Recursos financeiros	€ 1.987.454
Habitantes	344.232
Recursos pessoais	19

País	Lituânia
Autoridade de Proteção de Dados	State Data Protection Inspectorate
PIB	US$ 46,8 bilhões
Recursos financeiros	€ 1.638.000
Habitantes	2.671.054
Recursos pessoais	62

País	Liechtenstein
Autoridade de Proteção de Dados	Data State Inspectorate
PIB	US$ 31 bilhões
Recursos financeiros	€ 1.326.430
Habitantes	1.858.130
Recursos pessoais	32

País	Letônia
Autoridade de Proteção de Dados	Data Protection Office
PIB	US$ 6,1 bilhões
Recursos financeiros	€ 1.143.000
Habitantes	38.276
Recursos pessoais	7

País	Malta
Autoridade de Proteção de Dados	Office of the Information and Data Protection Commissioner
PIB	US$ 14,5 bilhões
Recursos financeiros	€ 620.000
Habitantes	443.127
Recursos pessoais	15

País	Romênia
Autoridade de Proteção de Dados	National Supervisory Authority for Personal Data Processing
PIB	US$ 287,9 bilhões
Recursos financeiros	€ 1.023.563
Habitantes	19.064.310
Recursos pessoais	29

País	Eslovênia
Autoridade de Proteção de Dados	Information Commissioner
PIB	US$ 51 bilhões
Recursos financeiros	€ 2.483.314
Habitantes	2.108.977
Recursos pessoais	49

Autoridade Nacional de Proteção de Dados brasileira (ANPD)

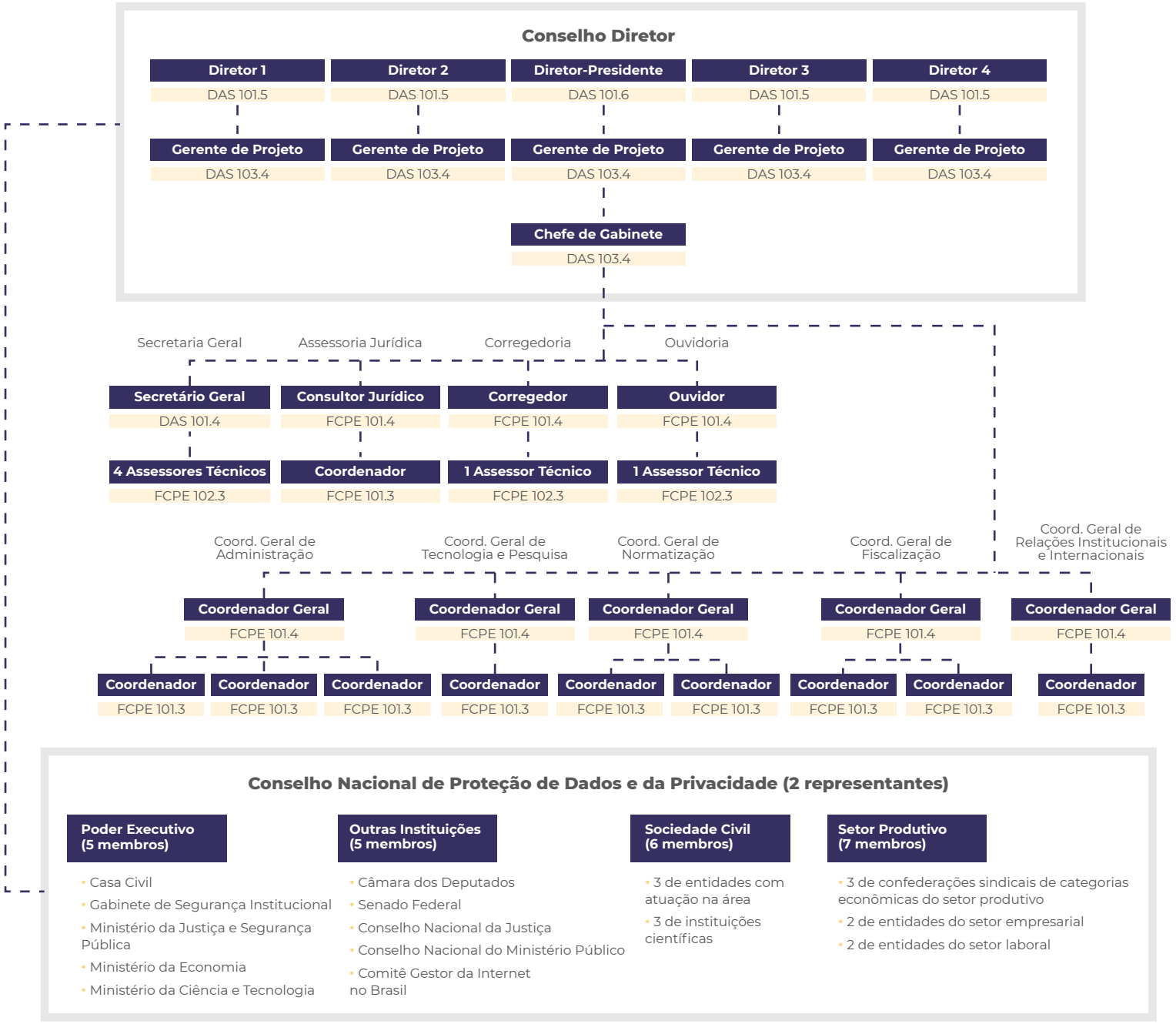
Recursos financeiros e pessoais

O Plano Orçamentário para o ano de 2022 da Autoridade Nacional de Proteção de Dados (ANPD), elaborado pela Coordenação Geral de Administração e aprovado pelo Conselho Diretor, subdivide-se nas seguintes categorias:

i. Estudos e Pesquisas sobre Modernização Tecnológica e Comunicação: relacionados à proteção de dados pessoais e privacidade, nos âmbitos nacional e internacional;
ii. Sistemas de TI exigidos pela LGPD: contratação de serviços ou sistemas relevantes para proteção de dados, privacidade e segurança da informação;
iii. Estudos, pesquisas e produção de indicadores: objetivando ampliar a atuação da ANPD, por meio de cooperações técnicas, convênios e outros instrumentos congêneres;
iv. Fiscalização Regulatória: execução de ações de fiscalização, averiguação e auditoria, adotando desdobramentos pertinentes; e
v. Administração da Unidade: despesas necessárias ao estabelecimento da estrutura física da ANPD (aluguel de sede própria, aquisição de mobiliário e equipamentos), diárias e passagens, realização de eventos institucionais e capacitação dos servidores.

O valor definido pela Presidência da República com destinação à Autoridade foi de R$ 40.520.385,00, com as seguintes destinações: 16% para área de Estudos e Pesquisas, 15% para aquisição de sistemas de TI exigidos pela LGPD, 6% direcionados a estudos, pesquisas e produção de indicadores, 12% para cobrir gastos relacionados à fiscalização regulatória do cumprimento da Lei Geral de Proteção de Dados (foram destinados, portanto, R$ 4.862.446,20 para cumprimento da fiscalização regulatória da autoridade em 2022). Os 51% restantes foram direcionados à administração da unidade.

No que diz respeito à estrutura da ANPD, o seguinte organograma demonstra o número de funcionários e sua organização dentro da Autoridade:



***Fonte:** Autoridade Nacional de Proteção de Dados, 2021.*

Cada um dos cinco diretores da ANPD conta com um gerente de projetos dedicado, exclusivamente, a assessorá-lo, sendo que o Diretor-Presidente conta também com a chefia de gabinete. Além disso, fazem parte da estrutura da ANPD: Secretaria Geral, Assessoria Jurídica, Corregedoria, Ouvidoria, Coordenação de Administração, Coordenação de Tecnologia e Pesquisa, Coordenação de Normatização, Coordenação de Fiscalização e, finalmente, Coordenação de Relações Institucionais e Internacionais. Esses postos são ocupados por servidores investidos em cargo ou função de confiança, com dedicação exclusiva.

Ao realizar a comparação do valor total destinado à ANPD e seu número de funcionários com o valor do PIB nacional e o número de habitantes, respectivamente, temos a seguinte relação:

País	Brasil
Autoridade de Proteção de Dados	Autoridade Nacional de Proteção de Dados
PIB	US$ 1,62 trilhão
Recursos financeiros	R$ 40.520.385 (aprox. € 6.421.910)
Habitantes	214.602.689
Recursos pessoais	59[24]

No comparativo do valor total destinado à ANPD (aproximadamente € 6.421.910) com o orçamento de autoridades dos países mais populosos da União Europeia, **por meio da análise percentual do PIB**[25], temos:

País	Brasil	Alemanha	França	Itália	Espanha
Habitantes	214.602.689	84.145.628	65.468.526	60.341.753	46.779.233
Orçamento	€ 6.421.910	€ 94.793.900	€ 21.507.000	€ 35.627.273	€ 15.762.500

Natureza jurídica

Em 27 de dezembro de 2018, o Poder Executivo brasileiro apresentou a Medida Provisória n. 869/2018, que realizou alguns ajustes na LGPD, mas cujo principal objetivo foi a criação da ANPD, estruturada como órgão público, sem aumento de despesa (art. 55-A). Essa opção levantou receio de que, por estar formalmente vinculada ao Poder Executivo, a ANPD não apresentasse necessária independência para exercer suas funções, o que se acentuou em 18 de junho de 2019, quando, antes mesmo de ser concluída a tramitação legislativa da MP n. 869/2018, sobreveio a Lei n. 13.844/2019, cujos artigos 2º, VI, e 12 inseriram formalmente a ANPD na estrutura da Presidência da República.

Esse formato se consolidou em 8 de julho de 2019, com a conversão da MP n. 869/2018 na Lei n. 13.853/2019, que inseriu na LGPD o art. 55-A, §§ 1º e 2º, prevendo textualmente que essa estrutura é transitória e deverá ser reavaliada após dois anos, para, eventualmente, transformá-la em autarquia especial, contados da "entrada em vigor da estrutura regimental da ANPD". A estrutura regimental foi definida pelo Decreto n. 10.474/2020, cujo art. 6º dispôs que sua entrada em vigor seria a data de publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União, o que somente aconteceu em 6 de novembro de 2020. Consequentemente, a revisão estrutural está prevista para ocorrer até novembro de 2022.

[24] Dos quais 5 são membros do Conselho Diretor e 23 do CNPD. Fonte: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/estrutura-organizacional-1.

[25] Convertido de dólares americanos para euros.

A autoridade reguladora de um sistema de proteção de dados pessoais pode se estruturar de várias formas sem que isso necessariamente comprometa o exercício de suas funções. Tanto que a Convenção 108/1981 do Conselho da Europa exigia que os Estados signatários se comprometessem a adotar uma série de padrões mínimos, sem, contudo, determinar único modelo a ser seguido.

Na União Europeia, viu-se que as autoridades reguladoras de proteção de dados pessoais costumam ser estruturadas para tratar especificamente desse tema, havendo previsão legislativa de várias garantias para seu bom funcionamento. No modelo europeu, somente se considera independente a autoridade que reúna determinados requisitos previamente abordados, previstos no art. 52 do Regulamento 2016/679 (GDPR).

Por estar atualmente estruturada como órgão em vez de autarquia, a ANPD não preenche, em tese, todos esses requisitos. Seu orçamento está atrelado ao da Presidência da República e não há carreira de apoio diferenciada, no sentido de que não há concurso público específico para seleção dos servidores que nela atuam, ao contrário do que ocorre em algumas autarquias, como INSS e Banco Central[26].

A opção por estruturar a ANPD como órgão público foi objeto de intensas críticas, tanto do meio jurídico quanto da imprensa. A primeira crítica é no sentido de que a ANPD não foi estruturada como agência reguladora, tanto que ela não consta do rol do art. 2º da Lei n. 13.848/2019, que elenca algumas das principais agências reguladoras em atividade no país, e a ela não se aplicam as regras estabelecidas na referida lei sobre interação com outras agências reguladoras e órgãos de controle[27].

A segunda crítica, relacionada à primeira, destaca que, caso tivesse sido estruturada como autarquia, a ANPD teria "gestão administrativa e financeira descentralizada", nos termos do Decreto-Lei n. 200/1967, art. 5º, inciso I. Porém, a estruturação como órgão faz com que ela não tenha orçamento próprio, sendo vinculada ao orçamento geral da Presidência da República (visto que as demais fontes de receita previstas no art. 55-L da LGPD tendem a ser de menor monta), o que pode comprometer sua autonomia financeira. Esse aspecto é agravado pelo fato de a ANPD não recolher taxas para remunerar serviços prestados, como análise de regras corporativas vinculantes (*binding corporate rules*) e outros documentos[28].

[26] PARENTONI, Leonardo. Por que confiar na Autoridade Nacional de Proteção de Dados? Revista da Faculdade de Direito da UFMG, ago. 2021.

[27] PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados: Uma visão otimista. Revista do Advogado (AASP), n. 144, nov. 2019, p. 209-219.

[28] Idem.

Em terceiro lugar, a estrutura atual da ANPD dificultaria que ela organizasse quadro próprio de servidores, devidamente especializados – por meio da criação de carreira própria, composta por membros selecionados em concurso público específico no qual se exigisse a demonstração de conhecimentos em matéria de proteção de dados pessoais. Pelo contrário, a inclusão da ANPD como órgão da Presidência da República faz com que sua força de trabalho seja composta por servidores de outras carreiras, já em exercício no serviço público, além dos escolhidos para ocupar funções de confiança[29].

A quarta crítica diz respeito à possível falta de autonomia técnica da ANPD, porque seus diretores poderiam sofrer pressões de ordem política, sobretudo quando a Autoridade Nacional estivesse fiscalizando o próprio Poder Público[30].

Nesse contexto, a Diretoria da Autoridade espera que, neste ano, a ANPD seja transformada em autarquia especial, visto que, atualmente, existe garantia de atuação independente com o Conselho Diretor, sabatina no Senado, autonomia técnica e decisória, mas sem orçamento e corpo de pessoas próprios[31]. As negociações têm sido realizadas juntamente ao Ministério da Economia[32].

Autarquia é uma entidade da Administração Indireta que adquire personalidade jurídica de direito público com a entrada em vigor da lei que a criou, tornando-se, assim, sujeito de direitos e obrigações para desempenhar atividades típicas da Administração Direta, submetida ao controle finalístico ou tutela.

Nos termos do Decreto-Lei n. 200/67, a autarquia é definida como serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receita próprios para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada (art. 5º, I).

Segundo Hely Lopes Meirelles, a autarquia não age por delegação, mas por direito próprio e com autoridade pública, na medida do *jus imperii* que lhe foi outorgado pela lei que a criou.

[29] Idem.

[30] Idem.

[31] LEORATTI, Alexandre. Diretora diz esperar que autoridade de dados seja autarquia já em 2022. Poder 360, 06 ago. 2021. Disponível em: https://www.poder360.com.br/economia/diretora-diz-esperar-que-autoridade-de-dados-seja-autarquia-ja-em-2022. Acesso em: 12 de dezembro de 2021.

[32] PORTAL DA PRIVACIDADE. ANPD envia ao Ministério da Economia proposta para se tornar autarquia, 21 jun. 2021. Disponível em: https://www.portaldaprivacidade.com.br/anpd-envia-ao-ministerio-da-economia-proposta-para-se-autarquia. Acesso em: 12 de dezembro de 2021.

Como pessoa jurídica de Direito Público interno, a autarquia traz, para a consecução de seus fins, uma parcela do poder estatal que lhe deu vida. Sendo um ente autônomo, não há subordinação hierárquica da autarquia para com a entidade estatal à qual pertence, porque, se isso ocorresse, anularia seu caráter autárquico. O que há é mera vinculação à entidade matriz que, por isso, passa a exercer controle legal, expresso no poder de correção finalística do serviço autárquico[33].

São autarquias especiais as agências reguladoras e as associações públicas. Agências reguladoras, como se pretende que a ANPD seja, são autarquias com regras específicas e regime especial, que objetivam basicamente regulamentar serviço público realizado por particular, ou seja, é uma entidade governamental fiscalizando serviços públicos.

Assim, a autarquia sob regime especial se distingue da autarquia comum apenas por lhe conferir a lei maiores privilégios, de modo a ampliar sua autonomia e possibilitar o cumprimento adequado de suas finalidades. No âmbito federal, a autarquia de regime especial mais conhecida é o Banco Central do Brasil (Lei n. 4.595/64) e agora surgem as Agências Reguladoras, criadas para controle e fiscalização dos serviços públicos concedidos, atividades típicas do Estado, mas atuando de forma descentralizada, com autonomia técnica, administrativa e financeira.

Exemplos de Agências Reguladoras Federais incluem ANEEL (Agência Nacional de Energia Elétrica), ANATEL (Agência Nacional de Telecomunicações), ANP (Agência Nacional de Petróleo), ANTAQ (Agência Nacional de Transportes Aquaviários), ANVISA (Agência Nacional de Vigilância Sanitária) e ANTT (Agência Nacional de Transportes Terrestres).

É importante destacar que, embora as críticas à atual estrutura da ANPD e, principalmente, à sua vinculação ao Poder Executivo sejam pertinentes, elas não resultam, necessariamente, na falta de independência do órgão.

Conforme destaca Parentoni[34], em análise sobre o tema, a LGPD atribuiu à ANPD e a seus diretores uma série de garantias que, ao menos em um primeiro momento, parece ser suficiente para conferir necessária independência. Antes da confirmação dos diretores, os nomes indicados pelo Presidente da República devem se submeter à sabatina pelo Senado Federal, por força do art. 55-D, § 2º da LGPD, estando sujeitos ao mesmo tipo de controle aplicável aos ocupantes dos mais altos cargos da República, como os Ministros do Supremo Tribunal Federal.

[33] MEIRELLES, Hely Lopes. Direito administrativo brasileiro. 23. ed. São Paulo: Malheiros, 1998, p. 298.

[34] PARENTONI. Op. Cit. 2021.

O mesmo artigo também exige que os indicados apresentem "reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade". Ainda que esses critérios contenham conceitos jurídicos indeterminados, podem servir de fundamento à negativa do Senado Federal, em casos extremos nos quais o indicado manifestamente não preencha os critérios.

Uma vez empossados, os diretores terão mandato por prazo fixo (LGPD, art. 55-D, §3°) e, durante esse período, não se sujeitam a afastamento preventivo, salvo por decisão fundamentada do próprio Presidente da República, após recomendação de comissão especial, conforme art. 55-E, § 2°. Por sua vez, o afastamento definitivo do cargo somente poderá decorrer de "renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar", instaurado pelo Ministro de Estado Chefe da Casa Civil da Presidência da República (art. 55-E).

Durante o exercício de suas funções, o art. 55-B da LGPD assegura "autonomia técnica e decisória à ANPD" e, muito mais do que simples retórica, esse dispositivo acarreta importante repercussão prática. Caso ele não existisse, haveria possibilidade de decisões tomadas pelo Conselho Diretor da ANPD serem submetidas a reexame de instâncias superiores do Poder Executivo, eventualmente até do próprio Presidente da República, por força do art. 56, § 1° da Lei n° 9.784/1999 (Lei Geral do Processo Administrativo).[35] Contudo, a mencionada redação do art. 55-B da LGPD afasta essa possibilidade, assegurando que decisões do Conselho Diretor da ANPD sejam definitivas na esfera administrativa.

Mesmo após o término do mandato e a efetiva desvinculação da ANPD, os ex-diretores permanecem sujeitos à fiscalização do Poder Público e da sociedade. Isso porque o art. 55-F da LGPD lhes impõe prazo de desincompatibilização de 6 meses, período durante o qual ex-diretores não poderão se envolver em qualquer atividade potencialmente causadora de conflito de interesses, em virtude das informações a que tiveram acesso enquanto integravam a ANPD, nos termos da Lei n° 12.813/2013 (Lei do Conflito de Interesses).

[35] Idem.

Conclusão

Com base no exposto, é possível resumir os elementos que demonstram autonomia e independência de uma autoridade supervisora:

• A existência da Autoridade e sua independência funcional e operacional de instituições públicas e do setor privado estão estabelecidas na legislação. Isso inclui definir características de independência na legislação ou designar explicitamente essa independência.

• Os dirigentes da Autoridade são nomeados por ato oficial e por prazo determinado, de acordo com regras definidas na legislação. Garantias de autonomia e independência aqui incluem:

a. Qualificações e condições de elegibilidade necessárias para serem nomeados;

b. Regras e procedimentos para a nomeação;

c. Prazo;

d. Número de mandatos possíveis;

e. Condições que regem as obrigações do chefe da Autoridade, incluindo abster-se de qualquer ação incompatível com seus deveres e não se envolver em qualquer ocupação incompatível durante e após o mandato;

f. Condições limitadas e fundamentadas para remoção;

g. Requisitos para diversidade de membros, como de diferentes setores ou nomeados de ou por diferentes órgãos (Judiciário, Legislativo, comércio ou associações profissionais).

• A Autoridade é dotada de recursos humanos, técnicos e financeiros, instalações e infraestruturas necessárias ao desempenho eficaz das suas atribuições. As garantias típicas dessa característica incluem:

a. Autoridade tem orçamentos dedicados, separados, anuais ou plurianuais;

b. Financiamento é adequado e estável;

c. Autoridade pode acessar outras fontes de fundos e reembolsos;

d. Autoridade tem controle total sobre como usa seu orçamento; e

e. Autoridade escolhe e tem sua própria equipe, que está sujeita à direção do chefe da Autoridade.

• A Autoridade funciona como órgão autônomo e independente. Os recursos que demonstram essa função incluem:

a. Autoridade pode deliberar livremente sobre quaisquer questões que se enquadrem em sua competência, quer sejam apresentadas pelo Governo, quer sejam tomadas por ela sem encaminhamento a uma autoridade superior;

b. Autoridade tem poder de iniciar investigações;

c. Chefe ou diretores da Autoridade têm poder de se reportar diretamente ao chefe do governo ou legislatura e falar publicamente;

d. Chefe ou diretores da Autoridade permanecem livres de influência externa, direta ou indireta, e não buscam nem aceitam instruções de ninguém;

e. Chefe ou diretores da Autoridade gozam de imunidade contra ações judiciais pessoais por ações realizadas no âmbito de suas funções oficiais;

f. Autoridade decide como conduz seu trabalho, como gasta seu tempo e dinheiro, quais procedimentos usa para investigações e como planeja suas atividades;

g. Autoridade tem acesso às informações necessárias para conduzir seus trabalhos, incluindo convocação de testemunhas, administração de juramentos, obrigando a produção de provas e visitando as instalações relevantes;

h. Autoridade está sujeita a controle financeiro que não afete sua independência; e

i. Funcionários da Autoridade estão sujeitos ao dever de sigilo profissional e às regras que regem os conflitos de interesses ou atividades políticas, incluindo ocupações e benefícios incompatíveis.

• As decisões e as ações da Autoridade são feitas de forma transparente. Isso inclui relatórios regulares ao parlamento, governo e ao público, e oportunidades de participação do público em suas atividades.

Finalmente, é importante destacar que, conforme visto anteriormente, quando da análise pela Comissão Europeia acerca do nível de adequação de um sistema de proteção de dados pessoais, levam-se em conta, entre outros elementos, a existência de mecanismos adequados para fazer valer os direitos dos titulares de dados (como vias de recurso administrativas e judiciais) e, no que tange às autoridades supervisoras, a existência de poderes de investigação, intervenção e sanção.

Entre esses poderes das autoridades supervisoras, inclui-se a existência de meios de investigação também da atuação de entidades públicas em suas atividades de tratamento de dados pessoais, razão pela qual os critérios acima elencados, sobretudo no que dizem respeito à interação com órgãos públicos, são cruciais para o adequado funcionamento da autoridade no desempenho de suas funções.

Com esses requisitos na prática, é possível considerar que a autoridade apresenta autonomia e independência em sua atuação, ainda que não esteja necessariamente estruturada como autoridade formalmente independente do Poder Executivo (conforme observado, por exemplo, na decisão de adequação concedida ao Uruguai).

Mais relevante para autonomia e independência de uma Autoridade de Proteção de Dados do que sua natureza jurídica ou estrutura são os poderes que ela, de fato, detém para exercer suas atribuições – sobretudo para proteger os titulares de dados e para garantir a aplicação das leis de privacidade e proteção de dados no território de sua competência.

Créditos

Sócios

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino
Juliano Maranhão
Ricardo Campos
Henrique Fabretti

Conteúdo jurídico

Giovana Figueiredo Peluso Lopes

Coordenação editorial

Bruno Toranzo

Revisão

Rony Vainzof
Caio César Carvalho Lima
Bruno Toranzo
Yasmin Brandão

Arte e diagramação

Paola Cosentino

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF