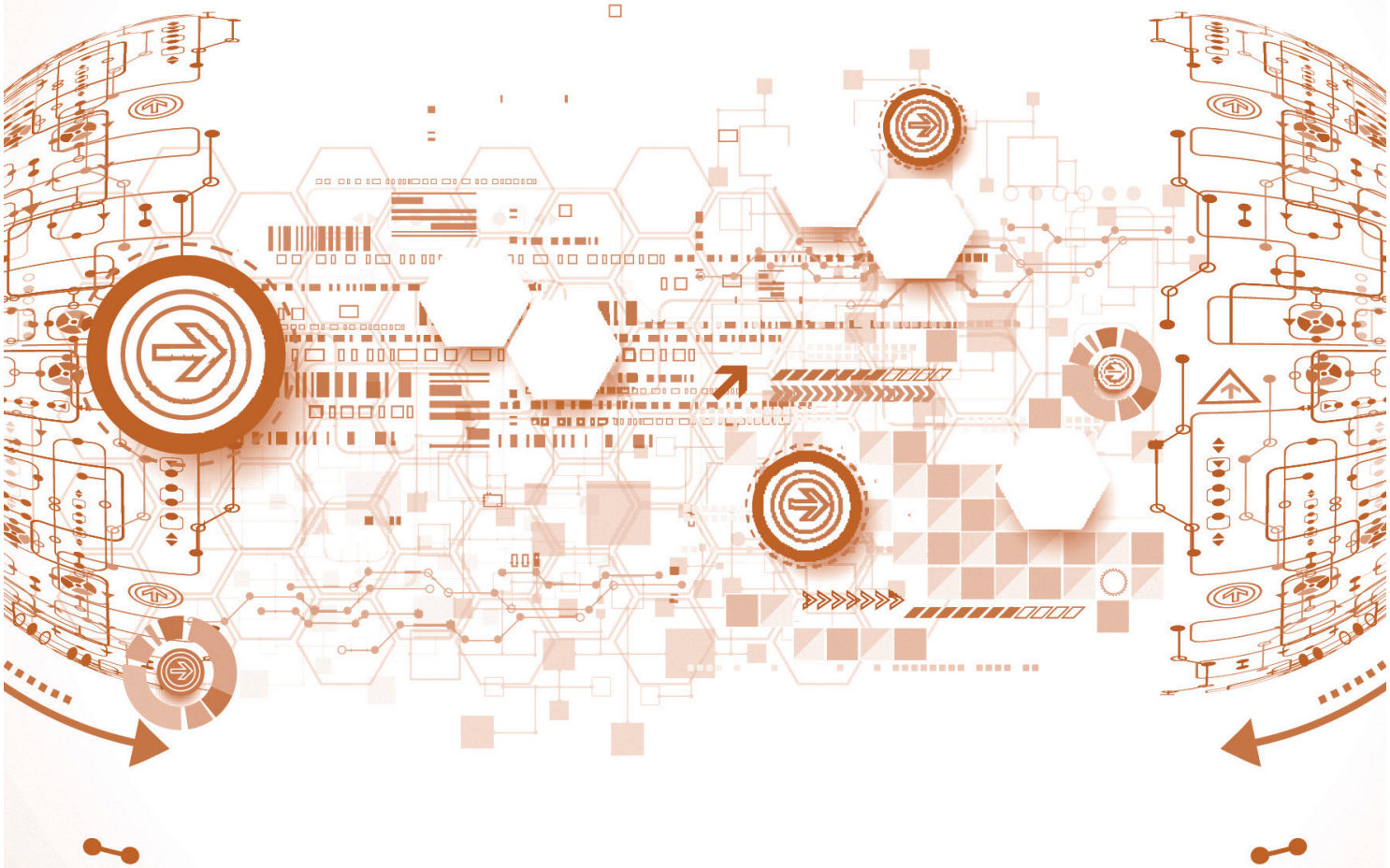
HUNTON& WILLIAMS

Brazil-U.S. Business Council

U.S. CHAMBER OF COMMERCE

CNI
Confederação Nacional da Indústria



EM BUSCA DE SOLUÇÕES: ATRIBUTOS DE AUTORIDADES DE PROTEÇÃO DE DADOS EFICAZES

Brasília
2017

EM BUSCA DE SOLUÇÕES: ATRIBUTOS DE AUTORIDADES DE PROTEÇÃO DE DADOS EFICAZES

HUNTON& WILLIAMS

Brazil-U.S. Business Council

U.S. CHAMBER OF COMMERCE

CNI
Confederação Nacional da Indústria

EM BUSCA DE SOLUÇÕES: ATRIBUTOS DE AUTORIDADES DE PROTEÇÃO DE DADOS EFICAZES

Brasília
2017

CNI
Gerência Executiva de Propriedade Industrial - GEPI

FICHA CATALOGRÁFICA

C748b

Confederação Nacional da Indústria
Em busca de soluções : atributos de autoridades de proteção de dados eficazes / Confederação Nacional da Indústria. – Brasília : CNI, 2017.
52 p. : il.

1. Proteção de Dados. 2. APDS. I. Título.

CDU: 004.02

A U.S. Chamber of Commerce é a maior organização de negócios do mundo e representa o interesse de mais de 3 milhões de empresas de todos os portes, setores e regiões, bem como as câmaras estaduais e locais e as associações de indústria.

Hunton & Williams é um escritório mundial de advocacia com quase 800 advogados atendendo clientes nos Estados Unidos, na Europa e na Ásia. Suas áreas de privacidade global e segurança cibernética lideram o mercado e foram classificadas como umas das melhores práticas mundiais nesses temas.

Reconhecimentos: os autores deste relatório agradecem as seguintes pessoas por suas contribuições: Rosario Mille, do Estudio Millé, Susan Park e Taeuk Kang, da Bae, Kim & Lee LLC, Haim Ravia e Dotan Hammer, da Pearl Cohen Zedek Latzer, Kristin Wilson, da Belly Gully, Luis Burgueño e Roberto Rosas, da Von Wobeser y Sierra S.C.

CNI
Confederação Nacional da Indústria
Setor Bancário Norte
Quadra 1 – Bloco C
Edifício Roberto Simonsen
70040-903 – Brasília – DF
Tel.: (61) 3317- 9000
Fax: (61) 3317- 9994
http://www.portaldaindustria.com.br/cni

Serviço de Atendimento ao Cliente – SAC
Tels.: (61) 3317-9989 / 3317-9992
sac@cni.org.br

SUMÁRIO

APRESENTAÇÃO

A incorporação das novas tecnologias em uma estratégia para o desenvolvimento da indústria brasileira será essencial para a competitividade do país e para melhorar a sua participação nas cadeias globais de valor.

Em alguns países, a Indústria 4.0 já começa a se tornar realidade, inclusive com o apoio dos governos das principais potências econômicas, que a tem colocado no centro de suas estratégias de política industrial.

O desenvolvimento de uma economia digital, baseada em dados, tem desafiado reguladores em todo o mundo. A CNI tem contribuído com o debate sobre a elaboração de uma lei de proteção de dados pessoais no Brasil, que enfrenta um duplo desafio: além de balancear os interesses envolvidos, fazê-lo com agilidade, a fim de evitar que o *gap* de competitividade entre o país e alguns de seus principais competidores aumente.

Como demonstração da sua relevância para a indústria, em 2017, o tema foi elencado entre as propostas da Pauta Mínima da Agenda Legislativa da CNI, documento que reúne os projetos prioritários para o setor produtivo sob análise do Congresso Nacional, elaborado a partir do debate entre as 27 federações estaduais da indústria e mais de 60 associações setoriais.

O imenso volume de informações e a velocidade com que são geradas demandam um novo modelo de gestão e cuidado com os dados. O papel das Autoridades de Proteção de Dados, ou *DPAs*, na sigla em inglês, vem ganhando importância, pois constata-se que, em muitos casos, as estruturas regulatórias existentes podem não ser capazes de lidar com esses novos desafios.

É nesse contexto que a CNI, em parceria com a *U.S. Chamber of Commerce* e com o Conselho Empresarial Brasil-Estados Unidos, traz para o debate brasileiro o relatório "Em busca de soluções: atributos de autoridades de proteção de dados eficazes". Sem sugerir a adoção de um modelo específico, espera-se que o relatório permita um aprofundamento nas discussões sobre esse novo e importante ator na governança dos dados.

1 INTRODUÇÃO

Com um número crescente de competências em todo o mundo, as autoridades de proteção de dados e outras reguladoras de privacidade (coletivamente, "APDs")[1] desempenham um papel fundamental na gestão da proteção de dados e na promoção de uma cultura mais informada e centrada na privacidade. A maneira como as APDs desempenham as suas funções reflete as bases da lei de privacidade de suas jurisdições. Em alguns países, a privacidade é vista como direito humano fundamental. Em outros, é considerada instrumento de proteção dos consumidores. Os princípios fundamentais de um país com respeito à proteção de dados influenciam o papel do regulador e resultam em diferentes práticas, estruturas e valores entre as APDs. Como a convergência de privacidade tem aumentado entre as jurisdições e como o papel das APDs tem evoluído para se adaptar às mudanças no cenário legal, a ideia de uma APD eficaz deve ser colocada para análise e discussão.

1 Este relatório utiliza o termo "APD" para descrever as instituições que executam as leis e regulam as práticas de proteção de dados e privacidade. Conforme analisado nesta publicação, nem todas as instituições que executam as leis e regulam as práticas de proteção de dados e privacidade tratam unicamente dessas questões. A Comissão Federal de Comércio dos Estados Unidos (FTC, na sigla em inglês), por exemplo, é a principal reguladora de privacidade e de práticas de segurança de dados nos Estados Unidos e executa diversas outras leis que protegem os consumidores contra uma ampla gama de práticas danosas, incluindo práticas anticompetitivas, comerciais enganosas e desleais. Para a consistência da nomenclatura, este documento refere-se tanto às reguladoras com foco único quanto às multitemáticas como APDs.

Este relatório destaca os principais atributos das APDs que contribuem para a gestão eficaz da proteção de dados e explora como o nível de eficácia varia de acordo com as diferentes estruturas, funções e os recursos. Entre os atributos mais eficazes de uma APD está a inclinação para tratar os regulados como parceiros e não como adversários. Esse traço manifesta-se no compromisso de promover a educação, a conscientização e a transparência, solicitando feedback e colaborando com os *stakeholders* relevantes (incluindo consumidores, outros reguladores e a comunidade regulada). As APDs eficazes também demonstram ter compreensão e capacidade de se adaptar às evoluções empresariais e tecnológicas.

Enquanto todas as APDs estão encarregadas do dever fundamental de proteger os dados pessoais, suas metodologias, suas práticas e seus escopos de trabalho diferem muito. Neste relatório, pretendemos explorar essas diferenças e destacar semelhanças entre as APDs mais eficazes. Os riscos e os desafios da gestão da proteção de dados têm crescido nos últimos anos com a onipresença e o aumento do valor dos dados na economia global, tornando imprescindível compreender como regular efetivamente a proteção de dados.

2 QUALIDADES DAS APDS EFICAZES

Na realização deste estudo, identificamos várias das principais caraterísticas das APDs que contribuem para a gestão eficaz da proteção de dados. O elo comum entre todas as APDs analisadas é que as verdadeiramente eficazes tratam os regulados como parceiros, e não como adversários. As APDs mais eficazes têm em comum o compromisso de promover a educação e a conscientização, orientando e assistindo de forma consistente a comunidade regulada na tomada de boas decisões.

Elas também buscam o aprimoramento por meio de *feedback* e têm disposição de agir de modo transparente. Além disso, identificamos que as APDs que apresentaram aptidões para colaborar e buscar conhecimentos sobre a evolução dos ambientes de tecnologia e negócios têm maior impacto nas respectivas jurisdições. Esta seção explora essas e outras caraterísticas que consideramos críticas para o sucesso de uma APD.

2.1 AS APDS EFICAZES PROMOVEM EDUCAÇÃO E CONSCIENTIZAÇÃO

Para transmitir efetivamente os valores da proteção de dados, as APDs devem ser educadoras e defensoras da privacidade e, assim, promover a cultura da proteção de dados junto à comunidade regulada. A APD deve disseminar os princípios de responsabilização para educar, envolver e aconselhar a comunidade regulada em conformidade com as leis de proteção de dados. As APDs também devem disponibilizar serviços de informação ao público, sensibilizar e informar os indivíduos sobre seus direitos de privacidade.

As APDs têm um importante papel na educação para as organizações a respeito das práticas de proteção de dados e do esclarecimento sobre as expectativas legais. As necessidades de educação e conscientização são impulsionadas pelo fato de que o descumprimento das normas nem sempre é intencional. Muitas vezes, ele é causado pela falta de conhecimento, compreensão ou conscientização. O Instituto de Investigação em Ciências Sociais (Institute for Research in the Social Sciences), por exemplo, concluiu que a falta de conscientização das organizações sobre os direitos relativos à proteção de dados contribuiu para que indivíduos enfrentassem dificuldades em exercer o seu direito de acesso (GABINETE DE INFORMAÇÕES DO ENCARREGADO, 2015). Da mesma forma, a Agência dos Direitos Fundamentais da União Europeia (European Union Agency for Fundamental Rights) atribui a maioria dos descumprimentos das obrigações de registro nos estados-membros da União Europeia à falta de conscientização e compreensão (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010).

Uma APD com abordagem proativa e orientada para a educação e conscientização a respeito das normas sobre proteção de dados ajuda a maximizar o cumprimento da legislação. As APDs não têm recursos para executar todas as ações e políticas ou fazer cumprir cada direito de privacidade. Para usar eficientemente seus recursos pessoais e financeiros limitados, as APDs devem ter estratégias relacionadas à maximização da capacidade de aplicar as leis de proteção de dados e, ao mesmo tempo, reduzir os casos de descumprimento. Por exemplo, diversas APDs instaram organizações a realizar regularmente Avaliações de Impacto sobre a Privacidade (AIPs) com o propósito de ajudar a identificar e mitigar os riscos à privacidade associados às práticas de tratamento de dados. No Reino Unido (TRILATERAL RESEARCH & CONSULTING, 2013) e na França (CNIL, 2012), as APDs publicaram orientações passo a passo sobre como conduzir as AIPs e como orientar o gerenciamento de riscos à privacidade. As APDs também têm incentivado as organizações a implementar programas de privacidade e contratar responsáveis pela proteção de dados. Com esses mecanismos de autorrevisão, as organizações adotam abordagens

mais ponderadas em relação ao manuseio dos dados e contribuem para reduzir práticas evitáveis que apresentem riscos para a privacidade dos indivíduos[2].

Há muitos exemplos de APDs com campanhas destinadas a promover a conscientização e a compreensão mais profunda sobre as normas de proteção de dados. Comumente, as APDs, em todo o mundo, realizam estudos, publicam relatórios e artigos técnicos sobre proteção de dados. Muitas vezes, esses estudos e relatórios são elaborados em conexão com conferências e iniciativas que disseminam informações para conhecimento público sobre os direitos relativos à proteção de dados. As APDs mais eficazes continuam a inovar ao incentivar as organizações a adotar mecanismos de responsabilização. Por exemplo, em algumas jurisdições, as APDs têm realizado concursos para destacar as melhores práticas em matéria de proteção de dados e têm atribuído prêmios para as organizações que fazem uso de tais práticas. A APD da Eslovênia, por exemplo, seleciona, anualmente, uma organização pública ou privada considerada a mais bem-sucedida na proteção de dados pessoais. As APDs na França e na Espanha concedem prêmios financeiros anuais para organizações que adotam as melhores práticas no âmbito de proteção de dados. (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?a], p. 48-49). No México, a APD realizou a "Competição de Inovações e Boas Práticas na Proteção de Dados Pessoais 2016" para reconhecer e promover as melhores práticas de proteção de dados desenvolvidas pelas iniciativas pública e privada em âmbito nacional e internacional (INAI, 2016a).

Outras APDs realizam eventos formais e informais, voltados à comunidade regulada, para difundir a conscientização sobre a proteção de dados. Por exemplo, a APD da Nova Zelândia realiza a "Semana da Privacidade" com fóruns, palestras e uma exposição de arte destinada a difundir conhecimentos e debater questões sobre privacidade e proteção de dados (PRIVACY WEEK, 2017). Além disso, ocasionalmente, a APD da Nova Zelândia sedia eventos gratuitos, no horário de almoço, em grandes cidades, para discutir os riscos à privacidade associados à tecnologias emergentes. Em Hong Kong e Singapura, as APDs sediam cursos, workshops e conferências que introduzem os participantes em novos tópicos relacionados à privacidade e ajudam a guiá-los no cumprimento de obrigações relativas à privacidade[3]. A APD de Hong Kong também envia exposições itinerantes para comunidades locais onde o público pode explorar e interagir com painéis de telas informativas para aprender mais sobre como proteger a própria privacidade[4].

2 Estudo patrocinado pelo Gabinete do Comissário para a Informação do Reino Unido verificou que a grande maioria das grandes empresas ou empresas intensivas em dados instaladas no Reino Unido voluntariamente empregou profissionais específicos para trabalhar com conformidade na proteção de dados. London Economics, Implicações da proposta da Comissão Europeia para um regulamento geral sobre proteção de dados para os negócios: Final Report to the Information Commissioner's Office (Maio 2013) - 10.

3 Veja: https://www.pcpd.org.hk/english/education_training/organisations/workshops/ workshop.html; https://www.pdpc.gov.sg/news/Events/page/0/year/2016/month/All/personal-data-protection-eminar-2016; https://www.pdpc.gov.sg/news/Events/page/1/year/2015/month/All/personal-data-protection-seminar-2015; and https://www.pdpc.gov.sg/news/Events/page/2/year/2014/month/All/personal-data-protection-seminar-2014.

4 Veja https://www.pcpd.org.hk/english/news_events/events_programmes/roadshow/index. html; https://www.pcpd.org.hk/english/news_events/media_statements/press_20151221a.html; and https://www.pcpd.org.hk/english/news_events/media_statements/ press_20131129.html.

2.2 AS APDS EFICAZES BUSCAM *FEEDBACK*

As APDs que buscam *feedback* na comunidade regulada têm mais condições de compreender e aprimorar suas capacidades de gestão. Em muitas jurisdições, as APDs convocam as diversas partes interessadas para participar de reuniões com representantes das iniciativas pública e privada ou para conduzir pesquisas sobre questões de proteção de dados para ajudar a avaliar a opinião pública e a eficácia de seus regulamentos. Elas também solicitam comentários do público sobre o seu trabalho para ajudar a orientar a formulação de políticas. Por exemplo, na França, antes da adoção de um novo procedimento de registro para as afiliadas francesas de grupos que tinham implementado Regras Vinculativas das Empresas (RVE), a APD francesa contou com mais de 60 empresas multinacionais com RVEs para discutir o procedimento proposto pela APD (CNIL, 2015b).

O Gabinete do Comissário para a Informação do Reino Unido (UK Information Comissioner's Office "ICO") tem focado, particularmente, na solicitação de *feedback* público para informar sua estratégia e formular políticas por meio de uma combinação de estudos e consultas públicas. Por exemplo, em 2014, o órgão publicou uma consulta sobre a seleção de provedores para seu selo de privacidade para oferecer às organizações a oportunidade de opinar acerca dos critérios a serem observados (ICO, [201-?]). O Departamento de Comércio dos EUA (The U.S. Department of Commerce) estabeleceu vários processos colaborativos com representantes da indústria, da sociedade civil e da academia para discutir novas tecnologias relacionadas à privacidade. Esses processos colaborativos costumam resultar em um consenso sobre as melhores práticas de privacidade e os melhores códigos de conduta que influenciam os reguladores federais e estaduais na interpretação das leis.

Além de solicitar *feedback* público, a complexidade das tecnologias, das práticas de negócios e das questões sociais associadas ao tratamento de dados tem levado as DPAs a buscar treinamentos e opiniões de especialistas, como acadêmicos, técnicos, consultores, economistas e organizações de pesquisa. No verão de 2012, como parte da iniciativa para melhorar o foco do país em matéria de proteção de dados, a APD da Sérvia convocou especialistas para conduzirem um seminário para seus funcionários sobre questões de proteção de dados. O órgão reconheceu que, para dar o pontapé em uma forte abordagem de proteção de dados, deve-se concentrar em educar o público e as empresas (HUNTON & WILLIAMS, 2012).

2.3 AS APDS EFICAZES OFERECEM ORIENTAÇÃO E ASSISTÊNCIA

As APDs que oferecem orientação e assistência ajudam a melhorar o cumprimento das normas e a diminuir a incerteza no mercado. O ambiente regulatório em constante evolução demanda que as APDs esclareçam interpretações sobre questões legais peculiares ou obscuras e compartilhem opiniões sobre novas práticas e tecnologias. A assistência das APDs orienta as empresas reguladas. Isso permite que as organizações avaliem e ajustem as suas práticas em conformidade com as normas. As APDs podem fornecer essa orientação quando novas leis são aprovadas ou entram em vigor[5], após os tribunais emitirem importantes pareceres[6], quando áreas problemáticas são identificadas ou com a evolução e surgimento de tecnologias e práticas de negócios[7].

As APDs podem oferecer orientações de diferentes formas. Entre outros instrumentos, as APDs emitem diretrizes, elaboram documentos de posição e respostas às perguntas mais frequentes (FAQs, na sigla em inglês) para transmitir seus pontos de vista sobre determinadas práticas, esclarecer questões jurídicas e o estado da legislação e colocar questões para a comunidade regulada. Isso pode ser destinado a entidades, setores, práticas de negócios ou tecnologias.

Também há maneiras mais informais para transmitir orientações para a comunidade, como discursos, *workshops*, entrevistas e coletivas de imprensa. Além disso, muitas APDs respondem perguntas diretamente para empresas e indivíduos por meio de e-mails, cartas ou atendimentos pessoais.

Além de aconselhar as entidades reguladas, as APDs podem auxiliá-las no cumprimento das normas. Muitas APDs prestam consultoria sob a forma de auditorias voluntárias de proteção de dados ou visitas educativas a pedido das entidades reguladas. Essas avaliações resultam no fornecimen-

5 Por exemplo, menos de um mês antes de uma nova lei entrar em vigor, em janeiro de 2016, para ampliar a obrigação de notificação dos dados do País para todos os controladores de dados, a APD holandesa publicou uma orientação prática para ajudar as organizações a identificar casos em que as violações à segurança de dados devem ser relatadas à APD e aos titulares dos dados. Consideram a Obrigação de Reportar Falhas nos Dados no Ato de Proteção de Dados (PAPD), Políticas de Privacidade para a Aplicação do Artigo 34a do PAPD (8 de Dez. 2015), disponível em https://www.huntonprivacyblog.com/ files/2016/01/beleidsregels_meldplicht_datalekken.pdf. Da mesma forma, em resposta a uma nova obrigação ao abrigo da lei francesa de proteção de dados para obtenção de consentimento prévio antes da colocação ou acesso de cookies na web dos dispositivos dos usuários, a APD francesa liberou um conjunto de perguntas frequentes, ferramentas técnicas e códigos-fonte relevantes que forneceram orientações sobre como obter o consentimento para a utilização de cookies e tecnologias semelhantes, em conformidade com a União Europeia e com os requisitos franceses de proteção de dados. Acesse http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/. A orientação esclareceu quais cookies estão isentos da exigência de consentimento sob a lei de proteção de dados francesa. Seguindo o decreto do Ato de Proteção de Informações Pessoais e o Ato de Rede de TI na Coreia do Sul, o Ministério do Interior e a Comissão de Comunicações da Coreia liberaram manuais práticos para o cumprimento das duas leis.

6 Por exemplo, um mês após o Tribunal de Justiça da União Europeia (CJEU) anular a decisão da Comissão Europeia sobre a adequação da proteção oferecida pelo Safe Harbor, certas APDs publicaram orientações sobre os mecanismos jurídicos para as transferências transnacionais de dados para ajudar legalmente na transferência de dados pessoais para os Estados Unidos. Consulte, por exemplo, a Commission Nationale de l'Informatique et des Libertés, Safe Harbor: What Should Companies Do? (8 de fevereiro de 2016), disponível em http://www.cnil.fr/linstitution/actualite/ article/article/safe-harbor-que-doivent-faire-les-entreprises; e https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

7 Por exemplo, inúmeras APDs emitiram orientações que endereçam compras online, marketing direto, concursos, sorteios e rastreamento de consumidor para aumentar a consciência dos consumidores e comerciantes e para ajudar todas as partes a entender os seus respectivos direitos e obrigações quanto à lei de proteção de dados. Em 2014, a APD israelita sediou uma conferência para as empresas de transporte público sobre questões de privacidade relacionadas a um novo sistema de transporte eletrônico com smartcard, implantado em Israel. Antes da eleição nacional em Israel em 2015, a APD israelita também emitiu orientações aos partidos políticos sobre a salvaguarda da Rotação dos Eleitores.

to de conselhos práticos e recomendações sobre a melhoria das práticas em matéria de proteção de dados. Não há aplicação de penalidades associadas a essa consultoria.

Diante do rápido aumento de coleta de dados pessoais pelas iniciativas pública e privada, as APDs buscam novas maneiras de aumentar a escala do seu atendimento. Muitas APDs publicaram orientações, instrumentos de autoavaliação, modelos de formulários e kits de ferramentas para ajudar as organizações e contribuir para assegurar que as práticas comerciais estejam em conformidade com as leis de proteção de dados. No Reino Unido, por exemplo, o ICO buscou alcançar uma audiência mais ampla e disponibilizou uma ferramenta para auxiliar as organizações a recordar e treinar seus funcionários a respeito de proteção de dados. A ferramenta inclui vídeos de treinamento, módulos de *e-learning*, cartazes promocionais e *checklists* (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 106-107). O ICO também desenvolveu uma ferramenta online de autoavaliação para organizações de pequeno e médio portes aferirem o cumprimento de leis de proteção de dados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 106-107). Do mesmo modo, o Departamento de Saúde e Serviços Humanos dos Estados Unidos (The U.S. Department of Health and Human Services), principal regulador da privacidade de informações de saúde no país, publicou uma ferramenta de avaliação de risco que auxilia as entidades reguladas a avaliar se as suas práticas de segurança de informação estão em conformidade com a lei estadunidense de privacidade das informações de saúde. No México, a APD disponibilizou um centro de treinamento interativo online para empresas, público e governo, em que as pessoas podem participar de cursos relacionados a diferentes aspectos da proteção de dados (INAI, [2016?]). Como parte desses esforços, muitas APDs têm desenvolvido códigos de conduta, programas de certificação e outras estruturas de autogovernança para prover assistência sobre cumprimento das normas para uma audiência mais ampla[8].

Ao fornecer orientação e assistência, as APDs devem estar conscientes de que os seus posicionamentos criam expectativas legítimas na comunidade regulada. A consistência, portanto, é essencial. Também é importante para a APD se conscientizar sobre potenciais efeitos e consequências jurídicas das suas declarações, que podem ser encaradas como posicionamentos oficiais da APD, em especial pelo fato de que a orientação e a assistência, geralmente, não estão sujeitas ao mesmo nível de supervisão jurídica e controle de decisões mais formais. Portanto, as APDs devem tomar cuidado para evitar a imposição de novas obrigações jurídicas sobre entidades reguladas por meio de orientações ou interpretações jurídicas pouco ortodoxas que encontram apoio frágil em normas jurídicas ou jurisprudências. Ao criar mais incerteza jurídica por meio de orientação e assistência, a APD pode gerar mais efeitos negativos do que positivos.

8 Por exemplo, o México tem implementado um sistema de autorregulamentação referido como a encadernação de parâmetros de regulação com a APD autorizando, supervisionando e revogando as entidades certificadoras que implementam o sistema.

2.4 AS APDS EFETIVAS SÃO RAZOÁVEIS

Um atributo chave de uma APD é a sua capacidade de ser razoável e prudente. Afinal, há muito em jogo na fiscalização e no cumprimento dos direitos relativos à proteção de dados. O surgimento de tecnologias inovadoras pode ser sufocado, o comércio desencorajado e o bem-estar social reduzido pela aplicação ineficaz ou ineficiente que produz apenas benefícios escassos. As APDs mais eficazes compreendem que, quando se trata de fazer cumprir as leis de proteção de dados, a velha máxima "quantidade não é qualidade" é verdadeira. As APDs priorizam suas atuações tendo em vista quais empresas e práticas desencadeiam a maioria das reclamações, quais apresentam o maior risco potencial e quais são suscetíveis de resultar em danos mais significativos (ICO, p. 116-117). Por meio dessa estratégia, as APDs podem ter um maior impacto.

Para pôr em prática essa perspectiva e maximizar a eficácia das suas ações de controle, as APDs têm encontrado sucesso ao utilizar uma abordagem baseada no risco para a realização de auditorias e investigações, ações de fiscalização, processos judiciais, imposição de multas e outras sanções. Essa abordagem requer que as APDs avaliem os benefícios das ações, comparando-os com os custos de oportunidade associados. Por meio desse processo, as APDs podem escolher cuidadosamente em quais setores, empresas, atividades e tecnologias deve mirar, com base no cálculo da magnitude potencial e a probabilidade de danos associados às práticas de dados em questão. De fato, essa visão é coerente com diversos ordenamentos jurídicos. A Seção 5 do FTC Act (Federal Trade Comission Act), principal lei utilizada para regular a privacidade nos Estados Unidos, proíbe as práticas desleais de comércio. Para uma prática ser considerada desleal, a FTC deve estabelecer que: (1) o ato ou a prática causa, ou tem a probabilidade de causar, danos substanciais; (2) o dano não é superado por benefícios para os consumidores ou para a concorrência; e (3) o dano não foi razoavelmente evitado pelos próprios consumidores. Portanto, o FTC deve equilibrar tanto os danos quanto os benefícios (FEDERAL TRADE COMISSION, 1980, p. 949, 1070).

Além disso, as APDs mais eficazes não se submetem a uma abordagem única para todos os casos. Elas analisam as peculiaridades de cada situação. Em vez de tratar todas as organizações e violações da mesma forma, as APDs são mais eficazes quando ajustam as suas respostas às circunstâncias pertinentes. Ser flexível significa formular uma estratégia que leva em consideração a conduta, o histórico da organização, as normas do setor e a gravidade da situação. O histórico da organização de cumprimento das normas (ou seja, infrações eventuais ou repetidas) e de cooperação (ou seja, cooperativo ou não cooperativo) deve ser levado em conta nas decisões da APD. Outro fator a ser considerado é a intenção dos infratores, que pode variar desde entidades que desobedeceram, deliberadamente, notórias responsabilidades de proteção de dados até aquelas que tomaram uma decisão razoável em uma situação que envolveu uma legislação instável ou

recente. Essa visão personalizada de fiscalização resulta em APDs de maior impacto ao realizar auditorias, iniciar investigações e fiscalizar. As APDs também levam em conta as peculiaridades para determinar a imposição e a extensão das sanções necessárias (por exemplo, advertências e sanções financeiras).

Ao adotar um tratamento mais flexível, as APDs incentivam a comunidade regulada e diferenciam as organizações de acordo com o comportamento e as circunstâncias. Nesse sentido, elas tendem a premiar as empresas com histórico de cumprimento das leis e que têm demonstrado respeito pelos direitos de privacidade. Ao mesmo tempo, essas APDs reforçam o controle e são menos complacentes com reincidentes. A perspectiva flexível traz vantagens para todos os envolvidos e incentiva o monitoramento e a cooperação dos regulados com as autoridades reguladoras. Em retorno, tem-se uma fiscalização mais leve, que promove, ao mesmo tempo, a autogovernança e a eficiência das APDs na alocação de seus recursos.

A abordagem com base no risco também promove eficiência administrativa. Como indicado acima, para as APDs, faz parte da rotina responder consultas e reclamações a respeito de infrações de direitos de dados pessoais. Elas também desencadeiam investigações ou auditorias por iniciativa própria. Considerando que os recursos são escassos, as APDs priorizam seus objetivos da forma mais eficaz. Na busca de casos de descumprimento das normas, as APDs têm tido necessidade de serem seletivas para serem eficazes ou correm o risco de esgotarem os escassos recursos e obterem menos resultados a partir de suas ações (ICO, p. 117).

Como resultado, é importante para as APDs se concentrarem em questões graves e não triviais. Por exemplo, em 2014, o Reino Unido implementou uma nova estratégia para os esforços do ICO no processamento de reclamações, focada na investigação de infrações graves e reiteradas da legislação de proteção de dados (HUNTON & WILLIAMS, 2013). Assim, o ICO não investiga todas as denúncias que recebe. Em vez disso, ele seleciona as investigações e trabalha para resolver os litígios entre organizações e indivíduos. O ICO observou que

[...] muitas vezes, somos atraídos para disputas individuais entre organizações e seus clientes, em que a legislação que supervisionamos pode ser uma parte periférica da questão controversa. Queremos focar naqueles que agem de forma errada reiteradamente e tomar medidas contra aqueles que cometem infrações sérias contra a legislação (HUNTON & WILLIAMS, 2013).

2.5 AS APDS EFETIVAS SÃO TRANSPARENTES

As APDs devem agir de forma transparente para que possam ser responsáveis pelas diversas partes interessadas, inclusive pela comunidade regulada. É importante que as partes compreendam as decisões da APD e as razões que influenciaram a sua fiscalização ou as suas iniciativas políticas. Sem transparência, é difícil prever como o cumprimento das normas será julgado, compreender as decisões da APD, cumprir tais decisões ou questioná-las. Ações de fiscalização pouco transparentes, teorias jurídicas, objetivos políticos e outras importantes questões regulatórias também dificultam a responsabilização da APD por suas decisões. A transparência ajuda a construir confiança em decisões e ações da APD e impedem que as APDs sejam consideradas arbitrárias e inconsistentes.

As APDs devem se esforçar para serem transparentes de várias maneiras. Primeiro, as APDs devem, desde o início, ter a missão e o alcance de autoridade claramente definidos. Preferencialmente, esses parâmetros de autoridade devem ser estabelecidos em lei. As APDs com missão e alcance de autoridade definidos em lei são menos propensas a regular arbitrariamente as novas tecnologias ou indústrias ou expandir a sua autoridade de forma arbitrária. Segundo, as APDs devem estabelecer mecanismos de avaliação, como relatórios ou auditorias anuais, para que as partes interessadas possam avaliar se elas atuam de forma eficaz, eficiente, razoável e se atingem seus objetivos.

Terceiro, as APDs devem definir e comunicar claramente os objetivos e as prioridades para a interpretação e aplicação da legislação. Definir os objetivos e as prioridades permite às partes interessadas uma melhor ideia do que é esperado delas e indica onde elas devem concentrar seus esforços para aprimorar o cumprimento das normas. Por exemplo, para ajudar a guiar as suas decisões, o Gabinete do Comissário para a Proteção da Privacidade (Office of the Privacy Commissioner - OPC), no Canadá, define as prioridades estratégicas para concentrar recursos nas disputas de privacidade identificadas pela APD como as mais prementes. Estas definições ajudam a identificar as prioridades do OPC nos esforços de conscientização, investigações e auditorias, ações judiciais, orientações ou estudos e projetos de pesquisa (CANADÁ, 2015).

Em quarto lugar, as APDs devem fundamentar as suas decisões com explicações concretas dos fatores que conduziram ao julgamento. Muitas APDs publicam os critérios utilizados para tomar decisões, apresentam razões e explicações para os seus pontos de vista e revelam as provas e bases empíricas sobre a quais se fundamentam. Além disso, as APDs publicam regularmente relatórios de transparência com informações sobre as suas atividades de fiscalização e boletins referentes a decisões e regulamentos adotados recentemente. Em cumprimento ao artigo 28(5) da Diretiva da Proteção de Dados, todas as APDs na União Europeia publicam relatórios anuais sobre o estado

de proteção dos direitos de privacidade em suas jurisdições (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a). No México, o público pode revisar o orçamento anual de despesas da Secretaria do Tesouro, que, entre outros detalhes, fornece informações sobre a alocação de recursos públicos da APD mexicana, objetivos, programas e iniciativas de investimento (MÉXICO, 2016). Além disso, a APD mexicana precisa emitir um relatório anual em que detalha a suas realizações e estatísticas relevantes do ano anterior (INAI, 2016b).

Da mesma forma, o comissário de privacidade da Nova Zelândia deve preparar e publicar um relatório anual após o encerramento de cada ano financeiro (NOVA ZELÂNDIA, 2004ª, s. 150). A APD da Nova Zelândia também é auditada anualmente pelo Auditor Geral (NOVA ZELÂNDIA, 2004b, s. 156). Na Coreia do Sul, as agências governamentais são obrigadas a apresentar para a APD um plano anual de proteção de dados relevante para a sua área, enquanto a APD é obrigada a apresentar à Assembleia Nacional um relatório anual descrevendo o planejamento e a aplicação dos seus programas de proteção de dados (COREIA DO SUL, 2011). Em Israel, a APD é obrigada a publicar relatórios anuais referentes à supervisão e à fiscalização do cumprimento das normas no ano anterior (ISRAEL, 1981). Além disso, a Comissão Pública de Proteção da Privacidade de Israel, organismo independente cujos membros são professores e profissionais de privacidade, emite o seu próprio comentário no relatório anual da APD com recomendações e exigências de ações concretas (ISRAEL, 1981). A APD israelita está sujeita ainda à supervisão parlamentar pelo Comitê de Constituição, Direito e Justiça, que, normalmente, dedica uma das suas sessões para deliberar sobre o Relatório Anual da APD e sobre o comentário público da Comissão (ISRAEL, 1981). As APDs mais ativas fornecem atualizações mais frequentes por meio de blogs, releases de imprensa e boletins. A APD da Itália, por exemplo, distribui informativos mensais com as decisões mais atualizadas e os regulamentos adotados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a).

As APDs eficazes também fornecem informação para que as entidades aprimorem a sua transparência. Como um auditor atuante, a APD francesa oferece avisos antecipados dos seus planos de auditoria e das suas prioridades de cada ano por meio de alerta de seu programa de inspeção anual (CNIL, 2015a). Em 2015, a APD francesa anunciou seus planos para conduzir 550 inspeções em 2015 – 350 inspeções no local e 200 revisões de documento e audiências. A APD advertiu que um quarto das inspeções no local incidiria sobre o monitoramento do circuito fechado de televisão e forneceu uma lista de tecnologias ou operações de processamento de dados em que outras inspeções teriam foco.

2.6 AS APDS EFICAZES SE ESFORÇAM PARA COORDENAR E COOPERAR

As APDs que cooperam e trabalham em conjunto com outros reguladores, dentro e fora dos seus respectivos países, aumentam a sua eficácia e a sua consistência em nível mundial. A coordenação poderá envolver: (1) adoção de ações de fiscalização em conjunto, (2) compartilhamento de informações sobre futuras denúncias e de informações relevantes sobre elas, (3) facilitar a pesquisa conjunta e os programas de educação, (4) estimular a troca de conhecimentos e experiências entre as entidades por meio de programas de formação e intercâmbio pessoal, (5) promoção de uma compreensão das condições econômicas e jurídicas e de teorias que impactam na aplicação da leis de privacidade aplicáveis, e (6) troca de informações sobre os desenvolvimentos relacionados à privacidade em seus respectivos países. A coordenação pode beneficiar as APDs, economizar seus recursos e evitar a duplicação de esforços. A fiscalização redundante, como sobreposição das investigações e auditorias, não só leva ao risco de aplicação inconsistente e um aumento da carga de regulamentação sobre a comunidade como pode resultar no desperdício da utilização de recursos públicos. A coordenação facilita a fiscalização do cumprimento das normas e permite que os reguladores agrupem seus recursos e reduzam o desperdício[9].

Há inúmeros exemplos de iniciativas que promovem a cooperação entre as APDs e aumentam a consistência da aplicação das normas e da regulação. Entre os mais importantes está a Global Privacy Enforcement Network - GPEN, estabelecida em 2007 por iniciativa dos países membros da Organização para a Cooperação e o Desenvolvimento Econômico (Organization for Economic Cooperation and Development). A GPEN é “uma rede de mais de 50 países, projetada para facilitar a cooperação transfronteiriça na aplicação das leis de privacidade” (HERT; PAPAKONSTANTINOU, 2013). Entre outras atividades, a GPEN incentiva o compartilhamento de “melhores práticas na abordagem aos desafios transfronteriços” e o desenvolvimento de “prioridades de cumprimento compartilhadas” (HERT; PAPAKONSTANTINOU, 2013). A GPEN também realiza uma varredura anual de fiscalização de privacidade, em que as APDs participam de forma cooperativa na pesquisa de websites e aplicativos para avaliar suas práticas de privacidade e conformidade com as leis de privacidade (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b). As APDs na região da Ásia e do Pacífico têm em vigor um mecanismo de cooperação similar de proteção da informação dentro do âmbito do fórum para a Cooperação Econômica Ásia-Pacífico (Asia-Pacific Economic Cooperation Forum) (APEC, [201-]).

9 Em algumas jurisdições, múltiplas agências reguladoras executam os direitos de proteção de dados simultaneamente, muitas vezes com regulamentos diferentes. Cada ano, por exemplo, o Estado Federal Alemão e as APDs estaduais realizam uma conferência bienal chamada de Conferência dos Comissários de Proteção de Dados Alemães, uma oportunidade para que as APDs de todo o estado alemão e do Comissário Federal para a Proteção de Dados e a Liberdade de Informação possam compartilhar as suas visões sobre questões atuais de proteção de dados, além de discutir casos relevantes e adotar resoluções destinadas a harmonizar a forma de aplicação das normas em toda a Alemanha. Durante a conferência, as APDs alemãs normalmente adotam várias resoluções relativas à proteção de dados, incluindo, por exemplo, questões de privacidade associadas a veículos conectados, colaboração da APD com as autoridades de concorrência, tecnologia de reconhecimento facial, privacidade dos funcionários, criptografia fim-a-fim e privacidade de dados de saúde.

Muitas APDs também assinam memorandos de entendimento (Memorandum Of Understanding, MOUs) para promover a cooperação e o compartilhamento de informações. Os MOUs não criam obrigações jurídicas de prestação de assistência entre as APDs, mas celebram o interesse das partes em promover cooperação e assistência mútua. Os MOUs normalmente estabelecem os objetivos de cooperação e descrevem os procedimentos para a colaboração nas áreas de fiscalização, educação e pesquisa. Além disso, muitas APDs participam de iniciativas conjuntas de conscientização realizadas anualmente, como o Dia Internacional da Privacidade e da Proteção de Dados (International Data Privacy and Protection Day), Semana da Conscientização sobre a Privacidade da Ásia-Pacífico (Asia-Pacific Privacy Awareness Week), o Dia da Internet Mais Segura (Safer Internet Day) e o Dia da Proteção de Dados da União Europeia (Data Protection Day of the European Union) (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, 2011).

A colaboração da APD é particularmente importante na Europa, onde as APDs dos estados membros compartilham uma estrutura comum de proteção de dados. Na UE, o Grupo de Trabalho Artigo 29 (Article 29 Working Party) ajuda os países a desenvolver uma interpretação comum da Diretiva de Proteção de Dados. O grupo fornece um fórum formal em que as APDs da UE "podem harmonizar a aplicação das suas respectivas legislações", o debate, a aprovação, a aplicação de novos regulamentos e políticas e o trabalho para garantir que os princípios da proteção de dados sejam aplicados de forma contundente no seio dos estados membros (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 47). Tais reuniões cooperativas não têm de ser necessariamente formais para terem um impacto positivo. Por exemplo, a APD portuguesa mantém uma reunião anual informal com a APD espanhola para discutir os principais desenvolvimentos no mundo da proteção de dados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?] a, p. 47). Tanto a realização formal de seminários quanto a informal permitem que as APDs compartilhem as suas experiências e os seus conhecimentos e promovam a consistência das ações (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 114).

Em abril de 2016, após quatro anos de esboços e negociações, o muito aguardado Regulamento Geral sobre Proteção de Dados da UE – PIBR (EU Geral Data Protection Regulation - GDPR) adotou um único conjunto normativo que se aplica a todos os países da UE, em substituição às normas de cada país. Entre outras iniciativas, o PIBR estabelece a política de um Balcão Único para garantir a cooperação e uniformidade entre as APDs da UE em matéria de fiscalização e cumprimento das normas de proteção de dados. O conceito de Balcão Único determina que, sempre que uma empresa está estabelecida em mais de um estado membro da UE, a APD do principal estabelecimento da empresa vai atuar como autoridade principal para o processamento de dados internacional. Essa política altera a abordagem anterior da UE, conforme a Diretiva 95/46/CE, que sujeitava as

empresas às APDs de cada país em que estivessem estabelecidas, o que, muitas vezes, levava a aplicações inconsistentes e imprevisíveis.

O PIBR promoverá a cooperação obrigatória entre as APDs da UE e um mecanismo para garantir a aplicação coerente do novo regime. Especificamente, quando uma APD da UE tomar uma ação ou esboçar uma medida que tem um impacto em toda a UE, o caso deverá ser referido à recém-criada Autoridade Europeia para a Proteção de Dados (a "Administração") (e, por vezes, a Comissão Europeia), que tem o poder de emitir um parecer não vinculativo, que deve ser levado em conta pela APD pertinente, na tentativa de chegar a uma decisão consensual sobre a questão entre APD e "Administração". Isso é feito para ajudar a garantir que o PIBR seja consistentemente aplicado, e que as APDs trabalhem juntas e aprendam umas com as outras para alcançar a decisão correta. Em certas situações, a Comissão Europeia pode exigir que a APD suspenda a proposta de medida por um período para reconciliar as posições divergentes entre a APD e a "Administração". De acordo com a Comissão Europeia, "O mecanismo de consistência preserva o papel das APDs nacionais, assegura a cooperação entre as APDs e a 'Administração' e confere um papel de escudo à Comissão." (EUROPEAN COMISSION, 2013).

2.7 AS APDS EFICAZES ENTENDEM DE NEGÓCIOS E TECNOLOGIAS

Na economia digital de hoje, as APDs mais eficazes possuem conhecimento sobre negócios e tecnologias. No que diz respeito a negócios, elas devem incorporar em seus processos de tomada de decisão e em suas políticas e regulamentos: (1) mudanças nos modelos de negócios, mais e mais dependentes de dados do consumidor para o crescimento econômico, (2) desafios dos ambientes de negócios competitivos que eles regulam e (3) complexidades do mercado global em constante evolução.

Sobre tecnologia, as responsabilidades das APDs são duplas. Em primeiro lugar, elas devem permanecer à frente das tecnologias emergentes e os desafios a elas inerentes para tomar decisões e modificar suas políticas e seus regulamentos. Ao mesmo tempo, elas devem ter cuidado para não tomar decisões ou impor encargos administrativos em relação a possibilidades futuras em vez do estado atual da tecnologia. As APDs também devem estar atentas ao criar políticas tecnológicas neutras que não incentivem excessivamente ou entravem a utilização de determinadas tecnologias. Para se tornarem tecnologicamente mais hábeis, as APDs contratam cada vez mais funcionários com habilidades técnicas, formam parcerias com especialistas externos e convidam organizações e agências para educá-los em tecnologia. Por exemplo, em março de 2015, a FTC criou um escritório dedicado a estudo e pesquisa, que realiza trabalhos sobre privacidade e segurança de informação, veículos conectados, casas inteligentes, transparência algorítmica, métodos

de pagamento emergentes, grandes volumes de dados e internet das coisas (FEDERAL TRADE COMISSION, 2015).

Além disso, as APDs devem utilizar as mais recentes tecnologias para melhorar a sua eficiência, eficácia e transparência. Elas podem publicar postagens em blogs e boletins informativos, seminários na web ou usar plataformas de mídia social para aumentar a conscientização, como páginas de hospedagem de vídeos no YouTube, Twitter e Facebook, que lhes permitam interagir informalmente com a comunidade regulada para aumentar a conscientização sobre as questões da proteção de dados. Em Hong Kong, a APD adota uma abordagem única com a cobrança de uma taxa nominal anual para fazer parte do Data Privacy Officer's Club, uma organização para indivíduos e empresas, na qual é possível ter acesso a boletins eletrônicos informativos com releases de imprensa, materiais de orientação e regulamento recentemente adotados pela APDs (DATA PROTECTION OFFICERS CLUB, [201-?]).

Para a eficácia das APDs, ter uma forte presença online se tornou essencial. As APDs devem manter websites amigáveis e tecnologicamente atualizados, em que os recursos relevantes possam ser encontrados. Uma função de pesquisa altamente eficaz é uma necessidade[10]. As APDs eficazes publicam informações e documentos de orientação sobre direitos e obrigações em matéria de proteção de dados e links para sínteses da legislação, com critérios e decisões da agência em matéria de proteção de dados, de preferência, em vários idiomas[11]. Para aliviar a sobrecarga de regulamentos que pesa sobre as empresas, as APDs devem permitir que as empresas: (1) enviem eletronicamente documentos oficiais, (2) registrem ou notifiquem as APDs sobre o processamento de dados pessoais e (3) solicitem e recebam recomendações e informações. As APDs de Israel, Polônia e Espanha, por exemplo, permitem que as empresas se registrem às suas respectivas APDs online, enquanto os websites da Bélgica e da Irlanda proporcionam que as empresas apresentem notificações de vazamentos de dados online. O website da APD israelita autoriza que a maioria dos formulários e documentos relativos às bases de dados seja enviada por e-mail e permite que os proprietários das bases de dados paguem online as taxas de registro aplicáveis. Alguns sites de APDs também fornecem mecanismos para que os indivíduos possam apresentar reclamações por via eletrônica (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [201-?]). Por exemplo, o ICO atualizou seu site para oferecer um caminho guiado ao usuário, que o auxilia a relatar problemas (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 117-118). O website da APD israelita também consente que os indivíduos enviem reclamações por meio de um formu-

10 Em Israel, o website das APDs tem uma ferramenta de pesquisa online que permite aos usuários encontrar bancos de dados das empresas registradas.

11 As APDs, muitas vezes, tornam seus sites e os correspondentes recursos online disponíveis em múltiplos idiomas, como os originários da França, da Itália, da Letônia, dos Países Baixos e da Suíça. Na Espanha e na Suécia, os websites das APDs e alguns dos seus recursos online estão disponíveis em seis a 10 línguas, respectivamente.

lário *online*. Na Nova Zelândia, os indivíduos podem inserir informações sobre as suas queixas em um formulário online, que gera um e-mail de solicitação para as APDs (PRIVACY COMISSIONER, [201-?]). Na Coreia do Sul, a APD permite ainda a resolução de litígios em matéria de proteção de dados por meio da arbitragem online, e os indivíduos e as empresas poderão solicitar resoluções online dos seus litígios[12].

As APDs também devem utilizar a tecnologia para aumentar a sua própria eficácia e eficiência internas, como a construção de bancos de dados digitais para armazenar, organizar e acessar facilmente informações vitais (por exemplo, gravações de constatações, análise de dados e documentos dos tribunais). Uma utilização mais eficaz da tecnologia para esses fins também permitirá às APDs compartilhar informações relevantes com maior facilidade com outras agências, dentro e fora dos seus países, para promover a cooperação e reduzir redundâncias.

12 THE ELECTRONIC COMMERCE MEDIATION COMMITTEE. Página principal. Disponível <http://www.ecmc.or.kr>. Acesso em: 10 ago. 2017.

3 ATRIBUTOS ORGANIZACIONAIS DAS APDS

Além das práticas e habilidades das APDs, os atributos organizacionais contribuem para o sucesso de uma APD. O financiamento, a autonomia, a responsabilidade e autoridade de uma APD são alguns atributos organizacionais que variam de acordo com o sistema jurídico. Esta seção explora como a estrutura, as funções e os recursos de uma APD podem repercutir na eficácia das APDs.

3.1 FUNÇÕES DE UMA APD

Enquanto todas as APDs estão ocupadas com o dever fundamental de proteger dados pessoais, os métodos, a autoridade legal e o âmbito dos seus trabalhos variam bastante. Dependendo da jurisdição, a APD pode servir como supervisora, investigadora, árbitra, educadora, responsável por elaborar políticas ou todas elas. Para serem eficazes, as APDs devem se esforçar para incorporar as qualidades discutidas na seção II, independentemente das suas funções e dos seus deveres específicos. As subseções a seguir fornecem uma visão geral das diferentes funções das APDs e as competências legais que lhes são concedidas sob os respectivos sistemas de administração.

3.1.1 Supervisão

Em muitas jurisdições, as APDs supervisionam as empresas para cumprir a legislação de proteção de dados de maneira proativa. As APDs utilizam diferentes mecanismos para supervisionar o cumprimento, como auditorias, registros e notificação de regimes concebidos para informar as APDs das práticas de maior risco.

Para manter a APD informada, as regras de alguns países determinam que as organizações notifiquem a APD de certas questões de proteção de dados, como a transferência de dados fora do país, o processamento de dados confidenciais ou a ocorrência de uma violação de dados. Em outras jurisdições, a APD mantém um registro público de todas as operações de tratamento baseado em notificações e registros apresentados. Em outras jurisdições, as APDs servem como vigilante e exigem que as organizações busquem a aprovação antes de se dedicar a certos tipos de atividades de processamento de dados. Nessas jurisdições, a APD pode ser responsável por autorizar o tratamento de dados pessoais sensíveis ou aprovar a transferência de dados pessoais para outros países com base nas restrições legais aplicáveis.

Como vigilantes, as APDs adotam um papel proativo na realização de auditorias e inspeções para controlar e avaliar o cumprimento das normas. Nesse papel, a APD pode analisar o cumprimento das normas sem necessitar de qualquer indicação ou suspeita de violação ou má conduta. Por exemplo, muitas APDs na UE têm autoridade legal para realizar uma auditoria ou examinar os operadores envolvidos no processamento de dados, independentemente de saber se existe razão para acreditar que a ilegalidade ou a má conduta ocorreu ou é suscetível de ocorrer (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 22). A autoridade da APD para examinar o cumprimento legal de forma proativa, sem ser provocada, varia de acordo com a jurisdição. As APDS podem, então, realizar: (1) inspeções no local, onde ela pode visitar as instalações da empresa e acessar tudo o que armazena dados pessoais (por exemplo, servidores, computadores e aplicativos)[13] , (2) revisão de documentos enviados pela entidade sob fiscalização mediante solicitação por escrito, (3) audiências em que a APD pode convocar representantes das organizações a comparecer para serem questionados e para fornecerem todas as informações necessárias à APD e (4) inspeções remotas das APDs sobre um website da organização ou outros serviços por ela prestados *online*.

13 Por exemplo, a Agência de Seguridade e Internet da Coreia (Korea Internet & Security Agency - KISA), uma filial da Coreia Comunicações Comissão, realizam inspeções no local por violações das leis de proteção de dados.

3.1.2 Investigação

Em geral, as APDs são encarregadas de investigar potenciais violações de leis de privacidade e proteção de dados. Por exemplo, o comissário de privacidade argentino está habilitado para investigar qualquer questão em que se considera que a privacidade do indivíduo é passível de ser violada. Na sua função investigadora, as APDs podem iniciar fiscalizações por iniciativa própria baseadas em indícios de descumprimento (como problemas descobertos em auditorias proativas) ou por reclamações de indivíduos, da sociedade civil e dos governos relacionados com as queixas de proteção de dados.

Em Hong Kong, por exemplo, o Comissário de privacidade inicia investigações por conta própria, em alguns casos, baseado em sua avaliação de monitoramento proativo, ao mesmo tempo que responde a um volume significativo de queixas por parte do público em geral[14].

Para ajudar as APDs a efetuar a função de investigação, muitas jurisdições concedem a elas a autoridade para recolher informações por meio de solicitações, demandas de produção de informações e solicitações de acesso (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b). As APDs podem, por exemplo, ter autorização para obter acesso aos dados pessoais tratados pelas entidades, buscar documentos relativos a esse processo e exigir o testemunho relevante (por exemplo, em Hong Kong, Canadá, México e EUA) (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 22). Além disso, algumas APDs estão autorizadas a entrar nas instalações em que o processamento de dados é realizado e confiscar provas e, em determinadas circunstâncias, sem o consentimento do proprietário ou sem autorização prévia do Judiciário (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 22). A Comissão de Proteção de Bases de Dados de Singapura, por exemplo, está autorizada a entrar nas instalações de uma organização sem mandado desde que dê um aviso prévio de dois dias (mas a APD deve obter um mandado de busca para visitas sem aviso prévio ou para confiscar informações) (JAY, 2014). A APD de Israel tem o direito de realizar auditorias e inspeções sem aviso prévio nas instalações onde as bases de dados são mantidas e recolhidas bem como coletar informações e apreender computadores.

3.1.3 Arbitragem

As APDs desempenham um papel importante na aplicação dos direitos relativos à proteção de dados dos indivíduos. Dependendo da jurisdição, a APD pode funcionar como um procurador que objetiva o ressarcimento de danos por violações de privacidade ou como um mediador que concilia

14 Ver Comissão para privacidade de dados pessoais, Ann. Rep. 48-77 (2014-15), disponível em https://www.pcpd.org.hk/misc/annual_reports/ar2014_15/ar2014_15/index.html.

as disputas que envolvem essas violações dentro da estrutura jurídica pertinente. Como esses papéis variam de acordo com a jurisdição, as APDs geralmente recebem uma série de competências legais para exercer suas responsabilidades designadas.

Muitos sistemas jurídicos outorgam às APDs a capacidade de processar alegada violação de privacidade. Essas APDs podem levar as ações antes, independentemente a um tribunal ou a pedido de terceiros.

Elas são responsáveis por apresentar o caso contra o indivíduo ou as organizações suspeitas de violar a lei de proteção de dados. Outras jurisdições outorgam às suas APDs a capacidade de executar as leis de proteção de dados diretamente. Nessa capacidade, as APDs têm poderes quase judiciais que lhe permitem ouvir queixas, decidir os méritos do caso trazido por um requerente (como um fórum alternativo às autoridades judiciais), emitir declarações de não conformidade e resoluções ou impor medidas de correção (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?] a, p. 26). No entanto, as decisões administrativas feitas pela APD podem ser objeto de recurso aos tribunais por meio do sistema judicial[15]. Certas jurisdições limitam a autoridade executória das APDs a um papel mais passivo no que se refere aos pedidos de tribunais ou de autoridades de aplicação da lei. Essas APDs emitem tipicamente decisões não vinculantes e entram em acordo com as partes interessadas, mas estão obrigadas a iniciar uma ação judicial ou apresentar disputas a outros organismos judiciais se nenhum acordo puder ser alcançado. Na Suíça, por exemplo, o Comissário Federal para a Proteção de Dados e Informação não tem poderes para aplicação direta das leis contra organizações privadas ou públicas. Em vez disso, ele pode emitir recomendações não vinculantes à organização e apresentar a questão ao Tribunal Administrativo e ao Supremo Tribunal Federal para uma decisão caso as recomendações sejam rejeitadas ou ignoradas[16].

Da mesma forma, a Comissão de Privacidade Belga pode formular recomendações não vinculantes, mas deve apresentar uma queixa criminal ao Ministério Público Federal de Violações Criminais ou propor uma ação civil perante o Tribunal de Primeira Instância[17] . O Comissário de Privacidade Argentino pode encaminhar as questões que não puderem ser resolvidas ao Diretor de Processos de Direitos Humanos, que, por sua vez, pode remeter a questão para o Tribunal de Revisão dos Direitos Humanos para emitir decisões vinculantes. Em Hong Kong, a APD só pode emitir "avisos de aplicação não vinculantes" após encontrar uma violação da lei da proteção de dados. Essas notificações de aplicação oferecem ao infrator a oportunidade de corrigir a sua conduta, mas os tribunais, em vez da APD, têm o poder de impor sanções em caso de descumprimento das normas[18].

15 Por outro lado, no México, a APD está habilitada pela Constituição Mexicana para a emissão vinculante de decisões finais e de decisões incontestáveis e para impor multas e sanções para as infrações de privacidade.
16 Jay, supra nota 63, em 178.
17 Jay, supra nota 63, em 24.
18 Ver Regulamento de (Privacidade) Dados Pessoais (Personal Data (Privacy) Ordinance), (2012-13) PAC. 486, §§ 50, 50A (H.K.).

Na Coreia do Sul, tanto o Ministério do Interior como a Comissão de Comunicações da Coreia podem emitir pedidos de medidas corretivas e multas administrativas (COREIA DO SUL, 2011).

As APDs têm muitos recursos específicos à sua disposição para lidar com as violações da legislação. Dependendo da jurisdição, a APD pode ter poder para emitir um aviso ou uma reprimenda, celebrar acordo, impor sanções ou ordenar reparação de danos. Determinadas APDs na UE têm a autoridade legal para impor multas administrativas, sujeitas à revisão judicial. Em outras jurisdições, as APDs podem negociar acordos, mas não têm autoridade para multar infratores (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 35), enquanto outras APDs estão habilitadas a ordenar ressarcimentos, inclusive financeiros. No Reino Unido, por exemplo, o Gabinete do Comissário para a Informação pode emitir determinados tipos de multas administrativas, mas não está habilitado a obrigar o infrator a reparar danos[19]. Nos EUA, a Comissão Federal Comercial (FTC) tem a capacidade de firmar acordos com empresas[20]. Vários desses acordos têm obrigado as empresas a implementar programas de segurança e de privacidade abrangentes, contratar peritos independentes para executar avaliações bienais, reparar consumidores, devolver ganhos ilícitos, excluir informações indevidamente obtidas dos consumidores ou oferecer robustos mecanismos de informação e escolha para os consumidores. A APD de Israel pode emitir declarações de descumprimento e multas. Ela também pode suspender ou revogar os registros de banco de dados, medidas essas sujeitas à revisão no Tribunal ISRAEL. Protection of Privacy Law, 5741–1981, section 10a. O Comissário Filipino de Privacidade é autorizado a conceder indenização sobre assuntos que afetem qualquer informação pessoal (Philippines, 2011).

No exercício de suas responsabilidades de aplicação das normas, as APDs também podem ter o poder de intervir em práticas de processamento de dados para evitar ou mitigar o risco de uma violação. Isso inclui competência para: (1) aprovar uma operação de transformação de dados sensíveis antes que seja efetuada, (2) ordenar a descontinuação de uma atividade de processamento de dados ou a modificação, exclusão ou destruição dos dados processados, (3) proibição, bloqueio temporário ou permanente de atividades de processamento de dados[21] e (4) exigir o registro de certos tipos de tratamento de dados e a aplicação de salvaguardas específicas para impedir o processamento ilícito de dados ou o comprometimento dos dados[22] (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 22-24, 77). A grande maioria das APDs da UE tem alguma forma de autoridade, como a competência para emitir um aviso de proibição ou liminares contra o processamento de dados em violação da lei de proteção de dados.

19 Jay, nota supra 63, em 206.
20 Apesar de que a FTC não pode cobrar sanções monetárias civis por violações da Seção 5 da lei da FTC, ela pode emitir multas por violação de determinados estatutos de privacidade, como a Lei de Proteção da Privacidade de Crianças Online (Children's Online Privacy Protection Act) ou a Lei de Informação de Crédito Justo (Fair Credit Reporting Act) e Não Chamar (Do not Call). Além disso, se uma empresa viola uma ordem de liquidação, a FTC pode procurar sanções monetárias civis para a Seção 5 violações.
21 Por exemplo, o comissário de privacidade Filipino pode impor uma interdição temporária ou permanente sobre o processamento de informações pessoais mediante diagnóstico que o processamento será prejudicial para a segurança nacional e o interesse público.
22 Jay, supra nota 63, em 116.

3.1.4 Divulgação

Na maioria das jurisdições, o escopo de trabalho da APD inclui recomendações, aconselhamentos e orientações para a comunidade regulada e para os funcionários do governo. Por exemplo, as APDs regularmente informam aos titulares dos dados sobre os seus direitos, aconselham às entidades sobre as suas obrigações, respondem perguntas sobre as leis de proteção de dados e emitem interpretações sobre o significado das regras existentes. Alguns países dividem funções de consultor. No México, por exemplo, o Ministério da Economia é encarregado de educar as corporações nacionais e internacionais sobre as suas obrigações de proteção de dados segundo a Lei de Proteção de Dados Mexicana e trabalhar em cooperação com as autoridades nacionais da APD para, entre outras atividades, emitir orientações relevantes para o conteúdo e o alcance dos avisos de privacidade[23]. Na Rússia, enquanto o Roskomnadzor é a autoridade federal responsável pela proteção dos dados pessoais dos indivíduos, outra instituição, conhecida como o FSTEK, Serviço Federal de Controle Técnico e de exportação da Rússia, é responsável pelo desenvolvimento de regulamentos técnicos no processamento de dados (por exemplo, requisitos para sistemas de TI utilizados para efetuar o processamento e medidas necessárias para as transferências legítimas de dados)[24]. O FSTEK, muitas vezes, também está envolvido nas inspeções efetuadas pelo Roskomnadzor[25].

3.1.5 Definição de políticas

Muitas APDs atuam como responsáveis pelas políticas públicas, seja desenvolvendo diretamente ou subsidiando com informações os órgãos regulamentadores. Em qualquer caso, as APDs são frequentemente consultadas por uma questão de praticidade[26] (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 26). Dada a sua experiência na lei de proteção de dados e a sua familiaridade com a comunidade regulada, as APDs podem ajudar a iluminar os responsáveis pelas políticas e tornar mais eficaz a legislação de proteção de dados e de resposta às mudanças no ambiente regulatório.

No que diz respeito ao aconselhamento dos responsáveis pelas políticas, em certas jurisdições, o papel de consultor das APDs está bem estabelecido e formalizado pelo estatuto. Em tais jurisdições, o Executivo e o Legislativo são obrigados a consultar a APD antes da promulgação da legislação ou de regulamentos relevantes. Por exemplo, o Artigo 28(2) da Diretiva de Proteção de

23 Jay, nota supra 63, em 116.
24 Jay, nota supra 63, em 132.
25 Jay, nota supra 63, em 132.
26 Na França, Itália, Alemanha, Áustria e Grécia, a consulta à APD é legalmente exigida na elaboração de regulamentos executivos. Jay, nota supra 63, em 28.

Dados da União Europeia estabelece que organismos de supervisão sejam consultados pelos legisladores na elaboração de medidas regulamentares ou administrativas relativas ao tratamento de dados pessoais. Em outras jurisdições, as atividades consultivas das APDs são opcionais e devem ser realizadas em uma base *ad hoc*. A FTC, por exemplo, frequentemente testemunha perante o Congresso dos Estados Unidos sobre privacidade e proteção de dados e sobre questões relativas à proteção do consumidor (FEDERAL TRADE COMISSION, 2014). As APDs também podem aconselhar os poderes Executivo e Legislativo dos países sobre propostas de legislação.

Além de aconselhar os responsáveis pelas políticas, as APDs podem ter poder quase legislativo para promulgar regulamentos, supervisionar o desenvolvimento de códigos de conduta e emitir pareceres vinculantes para a comunidade regulada (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. [20--?]a, p. 8, 83, 44). A APD da França, por exemplo, está habilitada para estabelecer procedimentos e padrões para o processamento de dados pessoais e tem emitido códigos de conduta para o seu cumprimento (FEDERAL TRADE COMISSION, 2014, p. 44). Em Hong Kong, o Comissário para a Proteção da Privacidade é autorizado a aprovar e emitir códigos de conduta que ofereçam orientação prática para dar cumprimento às disposições da lei de proteção de dados. Nos termos da legislação do Reino Unido, o Comissário da Informação tem autoridade para emitir códigos de prática da indústria. Da mesma forma, as APDs da Irlanda têm autoridade para propor e elaborar códigos que, se aprovados pelo legislador, produzem efeitos jurídicos vinculantes[27]. Na Nova Zelândia, as APDs têm o poder de emitir códigos de prática para indústrias específicas, como agências de relatórios de crédito e fornecedores de serviços de telecomunicações. Em Israel, embora as diretrizes emitidas pela APD não sejam juridicamente vinculantes por si só, elas servem efetivamente como princípios orientadores para o exercício dos poderes de aplicação das APDs. Além disso, algumas APDs podem propor reformas legislativas e regulamentares relevantes para a legislação em matéria de proteção de dados para abordar questões emergentes (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 44). Nos EUA, o Departamento de Comércio convocou vários processos de parcerias multilaterais sobre questões de privacidade associadas a novas tecnologias, como sistemas de aeronaves não tripuladas, aplicações móveis e tecnologias de reconhecimento facial. Esses processos reúnem as partes interessadas da indústria, da sociedade civil e do meio acadêmico para desenvolver códigos de conduta voluntários, declarações de direitos, listas das melhores práticas e de outros tipos de orientação relacionados a questões de privacidade e proteção de dados.

27 Lei de Proteção de Dados de 1988 e 2003 (Data Protection Acts of 1988 and 2003) (Acts No. 25/1988, 6/2003) § 13 (Ir.), disponível em https://www.dataprotection.ie/docs/Law-On-Data-Protection/m/795.htm.

3.2 ATRIBUTOS ESTRUTURAIS DE UMA APD

Os atributos estruturais de gestão de uma APD são características importantes a serem consideradas ao avaliar as qualidades de uma APD efetiva. A estrutura de gestão da APD pode ser dividida em quatro elementos chave: (1) a fonte de fundos financeiros da APD, (2) o sistema de nomeação e afastamento de funcionários da APD, (3) a autoridade de tomada de decisões e autonomia da APD e (4) o âmbito jurisdicional e de aplicação da APD.

3.2.1 Fundos financeiros

A fonte e a adequação do financiamento de uma APD podem ter um impacto significativo sobre a autonomia, os incentivos e a eficácia de uma APD. Abaixo, alguns exemplos das diferentes possibilidades de financiamento das APDs.

• Algumas APDs são totalmente financiadas pelos respectivos governos e não são financiadas por meio de suas atividades de fiscalização (por exemplo, taxas de registro ou receitas de sanções). A maioria das APDs dos estados membros da UE é totalmente financiada pelos seus orçamentos governamentais nacionais. Isso inclui, por exemplo, as APDs na Estônia, na França, na Itália e nos Países Baixos (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 20). Fora da Europa, as APDs na Argentina, no México, na Nova Zelândia e na Coreia do Sul, por exemplo, são totalmente financiadas pelos respectivos governos nacionais.

• Outras APDs são financiadas pelos respectivos governos e por meio das suas atividades de fiscalização. Essas podem ser incentivadas a aumentar as suas atividades de aplicação da lei para aumentar seus recursos. Os exemplos incluem Hong Kong, Israel, Luxemburgo e Malta (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 20).

• Outras APDs são financiadas exclusivamente por meio de suas atividades. Um exemplo notável é o Reino Unido, em que as taxas de inscrição são a única fonte de financiamento para a APD do país (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 20). As APDs financiadas exclusivamente por meio de suas atividades podem ter um incentivo ainda maior para aumentar suas ações.

Independentemente da fonte de financiamento, muitas APDs não recebem recursos suficientes para lhes permitir ser tão autônomas e eficazes. Um estudo realizado pelo ICO do Reino Unido realçou a questão: “como os orçamentos públicos permanecem sob pressão, as APDs são suscetíveis a continuar enfrentando a perspectiva de restrições financeiras, o que significa que, no futuro, isso pode ser problemático para que as APDs possam realizar todo o seu trabalho. As pesquisas [tam-

bém] têm indicado em diversas APDs que a falta de pessoal e de recursos financeiros adequados são riscos relevantes para a sua autonomia" (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b , p. 88-89).

O estudo determinou que a falta de recursos "pode representar uma barreira à resposta das APDs aos desafios da proteção de dados que as novas tecnologias trazem" (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b , p. 130). As APDs em países como Áustria, Bulgária, Romênia, Chipre, França, Grécia, Itália, Letônia, Países Baixos, Portugal e Eslováquia têm relatado prejuízos pela falta de financiamento e de pessoal. (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 19, 44-92).

Há algum risco de que fontes e adequação do financiamento podem influenciar indevidamente as decisões e ações de uma APD e, finalmente, inibir a sua capacidade de cumprir os seus objetivos regulamentares. Para reduzir esse risco, as fontes de financiamento e a suficiência do financiamento devem ser transparentes para que o público e a comunidade regulada tenham confiança de que a APD age de forma independente e eficaz. Como medida de controle adicional, os orçamentos das APDs também devem ser sujeitos a revisões periódicas governamentais para garantir que eles são adequados, e que os fundos são utilizados de forma eficaz e eficiente.

3.2.2 Mandato dos funcionários de proteção dos dados

Embora a independência de uma APD do governo nunca possa ser absoluta, para que uma APD seja estruturalmente mais autônoma (e vista pelo público e comunidade regulamentada como tal), os processos de nomeação e afastamento de funcionários da APD devem ser transparentes, justos e imparciais. A autonomia estrutural está "de fato, principalmente assegurada pelo procedimento de nomeação e afastamento dos funcionários." (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 19).

Para serem eficazes, as APDs devem ser vistas como reguladoras confiáveis e que não dependam de influências externas e agendas políticas. O estudo do ICO do Reino Unido constatou que uma grande maioria do público "acreditava que era importante que [as APDs] fossem independentes do governo e dos negócios." (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 84). O mesmo estudo também ressaltou que "a independência de algumas APDs foi questionada pela Comissão Europeia. Há preocupações relacionadas a nomeações políticas dos dirigentes das APDs ou que [são] supervisionados por um ministério de governo específico ou parecem ter limitado a ação contra outras instituições públicas em que tem havido uma violação da proteção de dados." (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b, p. 85). O Tri-

bunal de Justiça da União Europeia também indicou que as APDs devem permanecer livres de influências externas, sejam elas direta ou indiretas do Estado. "O simples risco de influência política por meio do Estado é suficiente para dificultar o desempenho independente das tarefas da APD." (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]b , p. 83-91). A nomeação e os processos de remoção transparentes e justos também ajudam a garantir que as APDs sejam estruturalmente autônomas e confiáveis para as diversas partes interessadas. Abaixo está um resumo das várias formas em que os funcionários da APD são nomeados e removidos do cargo.

- **Opções de nomeação**

Em muitos países da UE (por exemplo, Alemanha, Eslovênia e Grécia), os funcionários da APD são eleitos por assembleias legislativas (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 19). Alguns países fazem mais do que outros para garantir que as nomeações sejam justas e para terem uma APD independente e autônoma. A Grécia, por exemplo, exige um consenso entre a situação e a oposição ao governo antes que um funcionário de uma APD seja nomeado (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 19).

Na outra extremidade do espectro, estão países como Hong Kong, Irlanda, Israel, Luxemburgo, Filipinas, Reino Unido, Lituânia e Estônia. Neles, os funcionários da APD são diretamente nomeados pelos respectivos governos sem dar a oportunidade de que as vozes da oposição da legislatura questionem a nomeação (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 19). Em países como Argentina, Dinamarca e Letônia, as APDs estão conectadas aos respectivos ministérios da justiça (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 8). Nestes casos, muitas vezes, há dúvida da medida em que os funcionários da APD nomeados possam ser autônomos e não estejam comprometidos com os políticos que os colocaram no escritório (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 8).

Alguns países envolvem vários poderes do governo (Executivo, Legislativo e Judiciário) e organizações públicas no processo de designação e nomeação da APD (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a , p. 8). Entre esses países estão Argentina, França, México, Espanha, Portugal e Bélgica. Um exemplo desse processo também pode ser encontrado nos EUA, onde o presidente nomeia um indivíduo para ser um Comissário da FTC, e a nomeação deve ser confirmada pelo Senado antes que o indivíduo tome posse (SOLOVE; HARTZOG, 2014). No México, o poder Legislativo nomeia sete comissários da APD, que podem ser vetados pelo presidente no prazo de dez dias a contar a partir da nomeação[28]. Na Coreia do Sul, há diferentes processos de nomeação

28 Constituição Política dos Estados Unidos Mexicanos (Constitución Política De Los Estados Unidos Mexicanos) [C.P], alterado, Diário Oficial da Federação (Diario Oficial de la Federación) [DO], 5 de Fevereiro de 1917 (MEX), art. 6, Seção A, subseção VII, parágrafos 8, 9 e 10 (2016), disponível em http://www.diputados.gob.mx/LeyesBiblio/ htm/1.htm.

para os diversos reguladores de proteção de dados. A Assembleia Nacional e o Chefe do Supremo Tribunal de Justiça nomeiam os membros da Comissão para a Proteção de Informações Pessoais, que são examinados e nomeados pelo presidente (COREIA DO SUL, 2011, Art. 67). Para a Comissão de Comunicações da Coreia, dois membros são nomeados pelo presidente, e três membros são nomeados mediante recomendação da Assembleia Nacional (destes três últimos, o partido político no poder recomenda um, e o partido da oposição, outros dois)[29]. Na Argentina, a APD é nomeada pelo presidente e apresentada ao Congresso Nacional para aprovação.

Quanto mais entidades desempenharem um papel no processo de seleção da APD, mais provável que a APD tenha a capacidade e o incentivo para agir de forma justa e independente. Quando as APDs são exclusivamente nomeadas por uma entidade governamental ou política, há risco de que elas não sejam tão autônomas como o público e a comunidade regulada esperam.

- **Opções de Remoção**

Os procedimentos de remoção e os limites de prazos justos ajudam a garantir que as APDs continuem independentes e autônomas assim que os nomeados tomam posse. Os funcionários das APDs não devem permanecer no poder uma vez que eles não sejam mais eficazes ou sejam arbitrariamente removidos do poder por motivos políticos. Para ajudar a garantir processos justos, os procedimentos e os motivos para a remoção devem ser estabelecidos em lei.

Nos EUA, por exemplo, os Comissários da FTC servem em períodos escalonados de sete anos e não podem ser removidos do cargo exceto por "ineficiência, negligência do dever ou maleficência no escritório." (SOLOVE; HARTZOG, [201-?], p. 608). Não mais do que três comissários da FTC podem ser membros do mesmo partido político (SOLOVE; HARTZOG, [201-?], p. 608). No México e na Itália, os funcionários da APD também podem servir apenas em um prazo de sete anos. Na Nova Zelândia, o Comissário para a proteção da privacidade pode servir vários mandatos de cinco anos (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a, p. 20). Nas Filipinas, os funcionários da APD podem servir em mandatos de dois a três anos. Em países como Polônia e Eslovênia, os funcionários da APD podem ser removidos somente por motivos de má conduta específicos em conformidade com os mesmos procedimentos utilizados para nomeá-los[30]. Em Israel, os funcionários da APD podem ser removidos em conformidade com os procedimentos gerais de demissão do serviço civil israelita[31]. Em Hong Kong, o comissário de privacidade só

29 Ato relativo à criação e ao funcionamento da Comissão de Comunicações da Coreia (Act on the Establishment and Operation of Korea Communications Commission), Mar. 23, 2013, art. 5 (S. Kor.).

30 Id.

31 A decisão executiva do Governo Israelita número 2464 datado de março 8, 2015; "Rotação e regime de ocupação para altos funcionários" ("Rotation and Tenure Arrangements for Senior Officials"), o Comissário do Serviço Público (Commissioner of Public Service) 1.6 de fevereiro 8, 2016) (em hebraico), disponível em http://www.csc.gov.il/DataBases/CommissionGuidelines/Documents/GuideLine16.pdf.

pode ser demitido das suas funções pelo chefe do Executivo com a aprovação pela resolução do Conselho Legislativo em razão da incapacidade de realizar as funções do escritório ou mau comportamento[32]. Tais práticas de remoção e limites de prazo podem ajudar a reduzir a influência política e a pressão e promover uma APD mais independente. Em países como Irlanda e Nova Zelândia, no entanto, o próprio governo pode diretamente remover os funcionários da APD, que suscitam preocupações sobre se tais funcionários podem ser verdadeiramente independentes, especialmente quando houver monitorização do cumprimento governamental das leis de proteção de dados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?] a., p. 20). Os procedimentos de remoção tendem a ser justos quando eles (1) são claramente codificados em lei e (2) incluem salvaguardas destinadas a evitar a remoção de funcionários da APD por razões arbitrárias ou políticas. Para promover uma APD eficaz, justa e independente, os seus funcionários precisam saber que serão removidos do poder quando não forem mais eficazes ou quando agirem de modo oposto aos interesses da sociedade, e dessa forma, não baseados em caprichos do poder político.

3.3 AUTORIDADE PARA A TOMADA DE DECISÃO E AUTONOMIA

Além do financiamento adequado e dos procedimentos de nomeação e remoção apropriados, a autoridade para a tomada de decisão e autonomia de uma APD são os principais elementos estruturais na análise de sua efetividade. Em algumas jurisdições, os poderes da APD são estabelecidos em lei. Por exemplo, as constituições do México, de Portugal e da Grécia reconhecem explicitamente a existência e as competências das suas APDs, que podem supervisionar a legislação de proteção de dados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?] a., p. 20). Em Malta e na Espanha, as APDs têm distintas personalidades jurídicas ao abrigo da lei. Na Eslovênia, a APD tem o direito de iniciar ações judiciais e questionar a constitucionalidade da legislação perante o tribunal constitucional nacional (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, [20--?]a., p. 20).

Nos EUA, a FTC, considerada a APD federal de fato, tem recebido progressiva autonomia para a tomada de decisão. Ao longo dos anos, por exemplo, o Congresso deu à FTC: (1) o poder de aplicar a Lei de Reporte de Crédito Justo (Fair Credit Reporting Act)(que garante que as agências de informações respeitem a privacidade dos consumidores), (2) poderes de regulamentação e aplicação da Lei de Proteção da Privacidade das Crianças Online (Children's Online Privacy Protection Act) e (3) autoridade, sob a Lei Gramm-Leach-Bliley, para estabelecer regras de salvaguardas para

32 Ver Decreto (Privacidade) de Dados Pessoais (Personal Data (Privacy) Ordinance), (2012-13) Cap. 486, §§ 5(3), 5(4), 5(5) (H.K).

proteger registros e informações de clientes de instituições financeiras (SOLOVE; HATZOG, [201-?], p. 603-604). Nos termos da Seção 5 da lei da FTC, a FTC também tem ampla autoridade para acionar empresas por atos ou práticas desleais ou enganosos. A autoridade de tomada de decisão e autonomia da FTC tem crescido na medida em que o Terceiro Circuito do Tribunal de Apelações confirmou que a FTC pode propor processos judiciais contra empresas por práticas de segurança de dados insuficientes ou enganosas apesar de não ter a obrigação de publicar regras ou regulamentos em relação ao que constituem padrões de segurança razoável[33].

Com grande autoridade e independência, no entanto, surge grande responsabilidade. Quanto mais potente e independente uma APD, mais ela deve ser responsável por suas ações e transparente. Os mecanismos de avaliação, como relatórios anuais e auditorias, podem ser estabelecidos para garantir que as partes interessadas relevantes possam avaliar se as APDs atuam efetivamente, de forma equitativa e eficaz, e se atingem seus objetivos. Para assegurar que as APDs não abusem de sua autoridade e independência e para manter a confiança do público e da comunidade regulada, as APDs devem permitir questionamentos de suas decisões e ações. Isso pode incluir: (1) canais de reclamação e reparação relativos a ações de aplicação e a regulamentos existentes, (2) consultas públicas de políticas e regulamentos e (3) audiências em que as APDs podem ser questionadas sobre decisões importantes que tomaram.

3.4 ÂMBITO JURISDICIONAL

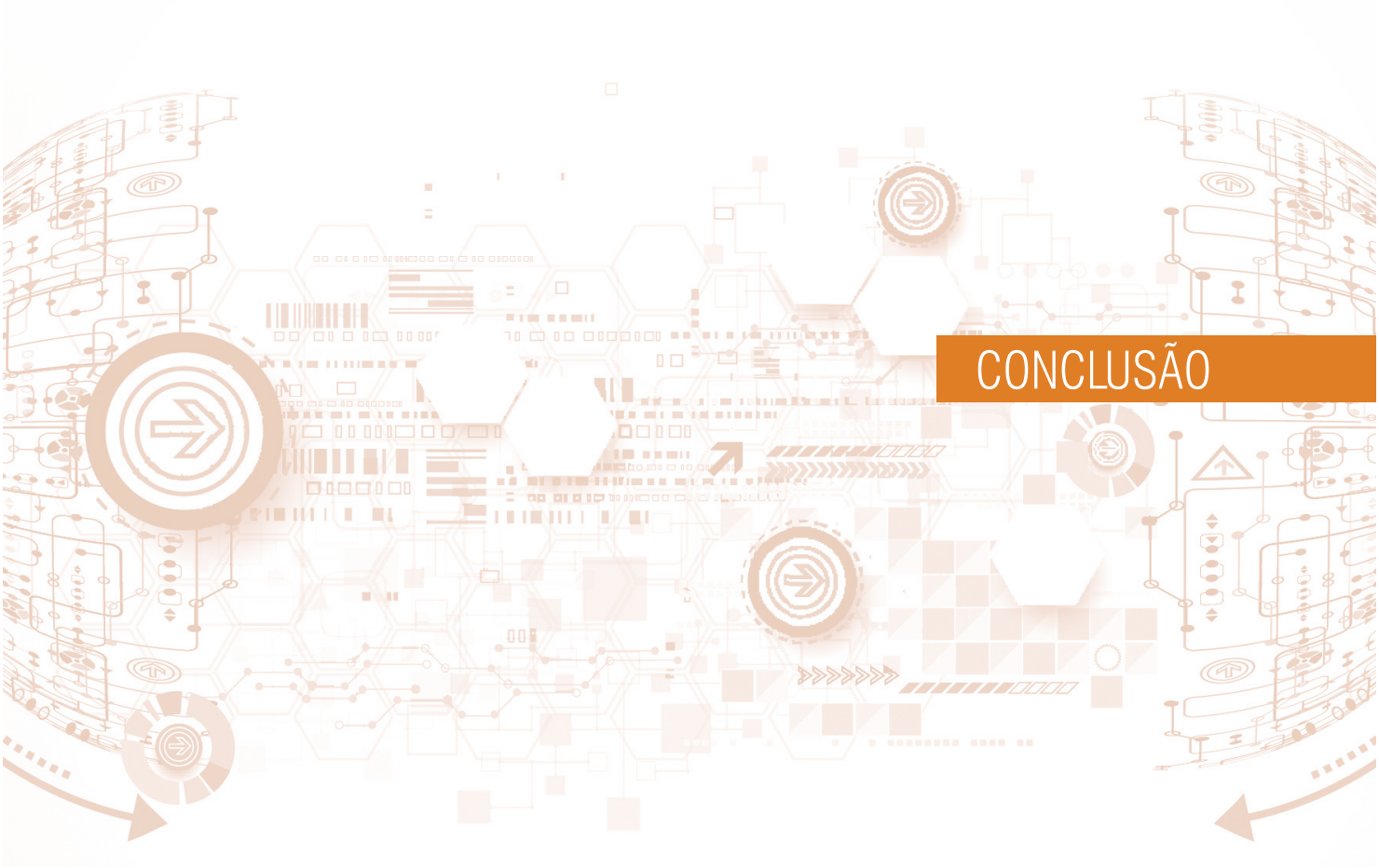
As APDs, em diferentes países, têm variados âmbitos jurisdicionais de poder. Por exemplo, algumas se concentram unicamente na proteção de dados, enquanto outras têm uma vasta gama de responsabilidades, desde o processamento de pedidos de "liberdade de informação" à supervisão de informação ambiental.

Nos EUA, por exemplo, a FTC processa o regulamento de proteção de dados e de aplicação e também protege os consumidores de forma mais geral contra práticas anticoncorrenciais, enganadoras e práticas comerciais desleais. No México, a APD concentra-se em ambas as questões de proteção de dados e as relacionadas ao acesso à informação do público[34]. Em Israel, a APD é parte do Ministério da Justiça e tem a responsabilidade sobre as questões de regime de assinatura eletrônica israelita e de relatórios de crédito[35].

33 FTC v. Wyndham Worldwide Corp, 799 F.3d 236 (3d Cir. 2015).
34 Constituição Política dos Estados Unidos Mexicanos (Constitución Política De Los Estados Unidos Mexicanos) [C.P.], alterado, Diário Oficial da Federação [DO], 5 de Fevereiro de 1917 (MEX), art. 6, seção A, subseção VII, parágrafos 1 e 2, disponível em http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm.
35 Lei de Assinatura Eletrônica israelita (Israeli Electronic Signature Law), 5761-2001, Seção 9 (ISR). (tradução não oficial), Disponível em https://www.law.co.il/media/esig/Israeli_didsig_law_english.pdf.

Algumas APDs concentram-se unicamente na iniciativa pública ou na privada, enquanto outras se dedicam a ambas. Uma pesquisa sobre a realidade em 32 países, conduzida em 2011 pela Associação Internacional de Profissionais de Privacidade, descobriu que "a norma generalizada entre jurisdições é dotar as suas APDs com um amplo âmbito de autoridade, mais de 90% dos entrevistados, ao indicar as suas áreas de foco, incluem os setores público e privado." (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, [201-?], p. 6). O estudo concluiu igualmente que "as responsabilidades da APD variam desde a aplicação das leis, relacionamento com os poderes públicos (por exemplo, com o Legislativo), à mediação, para nomear alguns, com a grande maioria dos entrevistados indicando a responsabilidade pelos setores públicos e privados - das organizações e dos indivíduos." (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, [201-?], p. 6). Alguns países oferecem poderes de proteção de dados para diferentes agências com base nos tipos de empresa ou práticas das agências normalmente reguladas.

Por exemplo, nos EUA, embora os seus poderes de aplicação de proteção de dados às vezes possam se sobrepor, o Departamento de Serviços Humanos e de Saúde, a Comissão Federal de Comunicações, a FTC e a Comissão de Valores Mobiliários e Câmbios têm âmbito jurisdicional sobre os tipos específicos de indústrias ou práticas que normalmente regulam (ou seja, saúde sanitária, comunicações, práticas de comércio desleais ou enganosas e instituições financeiras, respectivamente). Na Alemanha, o Comissário Federal de Proteção de Dados e da Liberdade de Informação tem um departamento especial unicamente responsável pela proteção de dados no setor de telecomunicações e de serviços postais (INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, [201-?], p. 9). Na Coreia do Sul, há quatro entidades com competências relacionadas à proteção de dados: (1) a Comissão de Proteção de Informações Pessoais, (2) o Ministério do Interior, que regula as questões gerais de proteção de dados ao abrigo da Lei de Proteção de Informações Pessoais, (3) a Comissão de Comunicações da Coreia que regula as questões de privacidade relacionadas a provedores de serviço online e (4) a Comissão de Serviços Financeiros, que regula as questões de privacidade relacionadas à indústria de serviços financeiros.



CONCLUSÃO

Em um crescente mercado global dependente de dados, uma gestão eficaz da proteção de dados promove a responsabilização em casos de descumprimento da lei ao mesmo tempo em que estimula o cumprimento das normas pela comunidade. Uma APD equilibrada, que educa e apoia os indivíduos e os negócios, está bem colocada para encontrar o equilíbrio adequado entre promover sólidas práticas de proteção de dados e proporcionar à comunidade regulada ferramentas para que se autogovernem e prosperem na economia digital.

Como o papel da APD evolui com as mudanças dos cenários jurídicos, o debate em torno das características e das qualidades de uma APD eficaz deve considerar os princípios subjacentes de equidade, transparência, colaboração e consistência. Esses princípios servirão de base para uma estrutura de gestão de dados bem-sucedida, independentemente da diversidade de culturas de privacidade de dados em todo o mundo.

REFERÊNCIAS

APEC. **APEC cross-border privacy enforcement arragement (CPEA)**. [201-]. Disponível em: <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>. Acesso em: 10 ago. 2016.

CANADÁ. **As prioridades de privacidade do OPC 2015-2020:** o mapeamento de um curso para maior proteção. 2015. Disponível em: <http://publications.gc.ca/ site/eng/9.801466/publication.html>. Acesso em: 10 set. 2016.

CNIL. **BCR:** la CNIL facilite les formalités liées aux transferts internationaux de données. 2015b. Disponível em: < https://www.cnil.fr/fr/bcr-la-cnil-facilite-les-formalites-liees-aux-transferts-internationaux-de-donnees>. Acesso em: 10 ago. 2017.

CNIL. **Methodology for privacy risk management.** 2012. Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>. Acesso em: 10 set. 2016.

CNIL. **Program des controles.** 2015a. Disponível em: <http://www.cnil.fr/linstitution/actualite/article/article/program-des-controles-2015>. Acesso em: 10 set. 2016.

COREIA DO SUL. **Personal information protection act.** Art. 67. 29 mar. 2011.

DATA PROTECTION OFFICERS CLUB. **About the data protection officers club.** [201-?]. Disponível em: <https://www.pcpd.org.hk/misc/dpoc/about.html>. Acesso em: 10 ago. 2017.

EUROPEAN COMISSION. **The proposed general data protection regulation:** the consistency mechanism explained. 02 jun. 2013. Disponível em: <http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm>. Acesso em: 10 ago. 2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Proteção de dados na união europeia:** o papel das autoridades nacionais de proteção de dados: reforço da arquitetura dos direitos fundamentais na UE II. p. 42-43, 2010.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Supra note,** n. 2, [20--?]b.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Supra note,** n. 3, [20--?]a.

FEDERAL TRADE COMISSION. **BCP'S office of technology research and investigation:** the next generation in consumer protection. 23 mar. 2015. Disponível em: < https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next>. Acesso em: 10 ago. 2017.

FEDERAL TRADE COMISSION. **FTC Policy Statement on Unfairness.** 17 dez. 1980. Disponível em: <http://www.ftc.gov/bcp/policystmt/ ad-unfair.htm>. Acesso em: 01 set. 2016.

FEDERAL TRADE COMISSION. **Privacy and data security update 2015.** 2014. Disponível em: <https://www.ftc.gov/reports/privacy-data-security-update-2015>. Acesso em: 10 ago. 2017.

GABINETE DE INFORMAÇÕES DO ENCARREGADO. **Direitos de proteção de dados:** o que o público quer e o que o público quer de autoridades de proteção de dados. [S.l.: s.n.], 2015.

HERT, Paul; PAPAKONSTANTINOU, Vagelis. **Three scenarios for international governance of data privacy:** towards an international data privacy organization, preferably a UN agency? A journal of law and policy for the information society. V. 9 n. 2, p. 271-324, 2013.

HUNTON & WILLIAMS. **New Approach to Data Protection Concerns.** 2013. Disponível em: <https://www.huntonprivacyblog.com/ files/2014/01/A-new-approach-consultation.pdf>. Acesso em: 10 set. 2016.

HUNTON & WILLIAMS. **Treinamento sobre a proteção de dados pessoais pelo mundo e peritos Europeus.** 9 jul. 2012. Disponível em: <http://www.huntonprivacyblog.com/wp-content/files/2012/07/Serbia- Commissioners_Statement.pdf>. Acesso em: Acesso em: 10 set. 2016.

ICO. **Informações do gabinete do comissário, a estrutura de critérios para um regime de selo de privacidade subscrito ICO.** [201-?]. Disponível em: <https://ico.org.uk/about-the-ico/consultations/privacy-seals-draft-framework-criteria>. Acesso em: 10 set. 2016.

ICO. **Supra note.** n. 2. [201-?].

INAI. **CEVINAI.** [2016?]. Disponível em: <Http://cevifaiprivada.ifai.org.mx/swf/cevinaiv2/cevinai/campus.php>. Acesso em: 14 set. 2016.

INAI. **Inovação e Boas Práticas sobre a Competição de Proteção dos Dados Pessoais.** 2016a. Disponível em: <http:// premioinnovacionpdp.inai.org.mx/Pages/Bienvenida.aspx>. Acesso em: Acesso em: 10 set. 2016.

INAI. **Relatório de Trabalho de 2015. 2016b.** Disponível em: <http://inicio.ifai.org.mx/nuevo/ informará%20de%20Labores%202015%20ok_Med.pdf>. Acesso em: 10 set. 2016.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. **Data protection authorities: 2011 global survey.** 2011. Disponível em: <https://iapp.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf>. Acesso em: 10 ago. 2017.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. **Supra note.** n. 44. [201-?].

ISRAEL. **Protection of Privacy Law**, 5741–1981, section 10a.

JAY, Rosemary P. **Data protection & privacy** 2015. 3. ed. [S.l.:s.n.], 2014.

MÉXICO. Cámara de diputados. **The 2016 annual federation expenses budget.** 2016. Anexo técnico. Disponível em: <http://www.diputados.gob.mx/LeyesBiblio/pdf/PEF_2016.pdf>. Acesso em: 10 set. 2016.

NOVA ZELÂNDIA. **Crown Entities Act 2004, section 150**. 2004a. Disponível em: <http://www.legislation.govt.nz/act/public/2004/0115/latest/DLM329631.html>. Acesso em: 10 set. 2016.

NOVA ZELÂNDIA. **Crown Entities Act 2004, section 156**. 2004b. Disponível em: <http://www.legislation.govt.nz/act/public/2004/0115/latest/DLM329631.html>. Acesso em: 10 set. 2016.

PHILIPPINES. **Republic act n. 10173.** 2011. Disponível em: <http://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/>. Acesso em: 10 ago. 2017.

PRIVACY COMISSIONER. **Privacy week.** 2017. Disponível em: <https://www.privacy.org.nz/forums--and-seminars/privacy-week>. Acesso em: 10 ago. 2017.

PRIVACY COMISSIONER. **Online complaint form.** [201-?]. Disponível em: <https://www.privacy.org.nz/your-rights/complaint-form>. Acesso em: 10 ago. 2017.

SOLOVE, Daniel J.; HARTZOG, Woodrow. **Supra note.** n. 102, [201-?].

SOLOVE, Daniel J.; HARTZOG, Woodrow. **The FTC and the New Common Law of Privacy.** Colum. 114, L. Rev. 583, 608. 2014.

TRILATERAL RESEARCH & CONSULTING. **Privacy impact assessment and risk management.** 2013. Disponível em: <https://ico.org.uk/media/1042196/trilateral-full-report.pdf>. Acesso em: 10 ago. 2017.

HUNTON& WILLIAMS

Brazil - U.S. Business Council

U.S. CHAMBER OF COMMERCE

CNI

Confederação Nacional da Indústria

CNI. A FORÇA DO BRASIL INDÚSTRIA