Documento integrante do Projeto Conjunto "Implementação e Regulamentação Efetiva da Nova Lei de Proteção de Dados brasileira"

O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD)

Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP)

17 Abril 2020

Este é um de uma série de Short Papers produzidos como parte do projeto conjunto especial "Implementação e Regulamentação Efetiva da nova Lei Geral de Proteção de Dados Pessoais (LGPD)", organizado pelo CIPL e CEDIS-JDP. Este projeto objetiva facilitar o compartilhamento de informações sobre a LGPD; informar e avançar a implementação e interpretação construtiva, dotada de perspectiva visionária e consistente da LGPD; possibilitar o compartilhamento de experiências e melhores práticas da indústria; e promover estratégias regulatórias efetivas no que concerne à LGPD.

Sumário

O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD)

I. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o estabelecimento de uma autoridade de proteção de dados para o Brasil – a Autoridade Nacional de Proteção de Dados (ANPD). A LGPD confere à ANPD responsabilidades importantes no que tange a sua interpretação, aplicação e execução de sanções por descumprimento. Em razão disto, a ANPD será de importância central para a efetividade e o sucesso desta lei.

Dada a curta linha de tempo até a data efetiva da LGPD e a urgência das prioridades imediatas da LGPD, é importante que a ANPD seja estabelecida e se torne operacional o mais rápido que possível. Independente da data de entrada em vigor da LGPD, a ANPD deve ser estabelecida imediatamente como uma questão de urgência, dado o seu número de ações necessárias antes de que a LGPD se torne efetiva e aplicável.

A LGPD inclui muitas disposições que requerem interpretação, orientação e ações adicionais pela ANPD, antes de que organizações possam efetivamente implementá-las. Tais responsabilidades exigem que a ANPD seja composta por indivíduos com expertise na área de proteção de dados, além das áreas de tecnologia da informação e ciência de dados. Isso também requer que a ANPD tenha estrutura, recursos, orçamento e autonomia institucional adequados para poder operacionalizar e levar a cabo as responsabilidades daí decorrentes. Ter tal expertise e estrutura operacional vai possibilitar à ANPD tanto cumprir o mandato da LGPD quanto alcançar expectativas e necessidades razoáveis dos brasileiros e das organizações regulamentadas pela LGPD.

Este artigo discutirá brevemente as seguintes questões: (a) por que uma autoridade de proteção de dados é essencial para o sucesso da LGPD e da economia digital no Brasil; (b) as responsabilidades e tarefas específicas da ANPD conforme a LGPD; (c) o quadro de funcionários e os recursos necessários para a ANPD, incluindo a formação profissional necessária e os perfis que devem estar representados entre os membros e sua equipe; e (d) considerações e princípios para uma supervisão e regulação efetivas e engajamento construtivo com as organizações reguladas pela LGPD.

II. CONDIÇÕES PARA A EFETIVIDADE DA ANPD E QUAIS DEVEM SER SUAS PRIORIDADES

A. POR QUE É IMPORTANTE TER UMA ANPD FORTE, TÉCNICA E EFETIVA

Todas as autoridades internacionais de proteção de dados compartilham responsabilidades que são inerentes à sua posição regulatória. Tais responsabilidades são relacionadas a proteger os indivíduos; garantir que o desenvolvimento econômico, digital e social do Brasil esteja alinhado com os princípios de privacidade e proteção aos dados pessoais; e assegurar a efetividade da LGPD. Elas ilustram a importância do estabelecimento imediato de uma ANPD forte e eficaz.

- **Garantir condições adequadas para a transformação digital da economia e da sociedade brasileiras**. A proteção de dados pessoais implica gerar confiança na sociedade digital e garantir o desenvolvimento econômico e tecnológico, a inovação e a livre iniciativa (ver Artigo 2 da LGPD). A ANPD

Um relatório de 2017 da Câmara de Comércio dos Estados Unidos mostrou que um ambiente regulatório favorável à cooperação internacional no âmbito de serviços de comunicações e tecnologia da informação no Brasil adicionaria US$1,19 bilhão em receitas governamentais, US$25,44 bilhões em contribuições ao PIB, US$5,31 bilhões em aumento de investimentos e 78.420 empregos a longo prazo no Brasil.

será uma peça fundamental nessa transformação digital, posto que terá conhecimento técnico sobre proteção de dados, tecnologia da informação e ciência de dados.

- **Conduzir de modo consistente a interpretação e o cumprimento da LGPD e de leis relacionadas.** A consistência resulta em segurança jurídica para indivíduos e organizações, e confiança na economia digital. Os brasileiros devem ser possibilitados a esperar o mesmo nível de proteção de dados pessoais e os mesmos direitos independentemente de onde estiverem localizados e de com quem interagirem. As atividades comerciais precisam de consistência e segurança jurídica para que possam operar de forma efetiva, e empresas estrangeiras esperam tal consistência para poderem investir no Brasil.
- **Fornecer as diretrizes sobre proteção de dados necessárias para organizações implementarem a LGPD.** A LGDP é uma lei baseada em princípios e, por isso, oferece flexibilidade para as organizações por ela reguladas implementarem muitas de suas disposições conforme apropriado a seus negócios e aos riscos de suas atividades de tratamento de dados pessoais. Contudo, certas disposições requerem esclarecimentos adicionais pela ANPD – veja a Seção B abaixo. É importante que a ANPD priorize o desenvolvimento de diretrizes para orientar tais organizações, em particular pequenas e médias empresas e startups, na implementação de medidas apropriadas de proteção de dados pessoais.
- **Educar os indivíduos e as organizações a respeito da proteção de dados pessoais**. A LGPD é a primeira lei geral de proteção de dados no Brasil e, como tal, traz novos direitos aos indivíduos e requisitos de conformidade para organizações públicas e privadas. À medida em que o Brasil se encaminha para uma sociedade e economia digitais, os brasileiros devem ser instruídos sobre seus direitos de proteção de dados. Eles devem ter um entendimento básico de como podem controlar seus dados pessoais, e devem ser capazes de confiar no ecossistema de proteção de dados. Por sua vez, as organizações devem ser conscientizadas de suas obrigações e responsabilidades para com os indivíduos. Elas devem tomar medidas protetivas adequadas e assumir as responsabilidades para poder gerar tal confiança nos meios digitais. A ANPD tem um papel-chave na educação de indivíduos e de organizações e deve atuar de forma colaborativa e construtiva com eles.
- **Assegurar segurança jurídica tanto para indivíduos quanto para organizações.** A ANPD deve ter responsabilidade primária pela interpretação e cumprimento da LGPD – veja a Seção B abaixo. Paralelamente, a ANPD deve interagir com outros reguladores (p. ex., reguladores de consumo ou concorrência e promotorias públicas) quando houver conflitos de competência. É necessário que a ANPD assegure uma abordagem consistente e centralizada à interpretação e à execução da LGPD. Isso não só facilitará o acesso de indivíduos à ANPD (por exemplo por meio do envio de reclamações e perguntas), como evitará que tais indivíduos busquem auxílio a reguladores diversos sobre a mesma questão. Por sua vez, tal abordagem consistente e centralizada fornecerá às organizações seguranã jurídica e significará que elas poderão usufruir de um único interlocutor para todas as questões de regulação e cumprimento de proteção de dados. Por fim, essa abordagem evitará que diversos reguladores executem as disposições da LGPD de forma descentralizada.
- **Servir como o principal especialista do Brasil em práticas emergentes para políticas de proteção de dados e em liderança de ideias (*thought-leadership*).** A ANPD deve liderar e informar o debate nacional sobre proteção de dados. Para fazer isso efetivamente, ela deve não apenas ser especialista na lei que regula, mas também nas tecnologias e organizações reguladas. Para isso, deve engajar-se construtivamente com organizações dos setores público e privado, assim como com outras autoridades reguladoras – veja a Seção D abaixo.

- **Possibilitar a colaboração bilateral efetiva com autoridades internacionais de proteção de dados**. A maioria das formas modernas de tratamento de dados pessoais inclui transferências internacionais de tais dados. Em decorrência, muitas supostas violações à proteção de dados terão dimensões e implicações internacionais. Isto vai requerer que a ANPD atue colaborativamente com autoridades de proteção de dados de países estrangeiros.
- **Ser o principal ponto de contato e representante do Brasil em fóruns e organizações internacionais**. As autoridades de proteção de dados em todo o mundo estão atualmente trabalhando juntas através inúmeros órgãos de cooperação e conferências, e utilizando mecanismos de colaboração. A ANPD deve participar destes fóruns para garantir que o Brasil tenha voz nas discussões internacionais sobre proteção de dados, e no desenvolvimento de políticas de proteção de dados globais. O Artigo 55-J-IX, especificamente, dá à ANPD o dever de "promover a cooperação com autoridades de proteção de dados de outros países, de natureza internacional ou transnacional."
- **Avançar a harmonização da proteção de dados a nível global.** É importante possibilitar e preservar diferenças regionais e nacionais no que tange à privacidade e à proteção de dados pessoais. Contudo, a vasta maioria dos princípios de proteção de dados pode e deve ser harmonizada entre diferentes regimes globais de privacidade. A ANPD deve identificar em que pontos a LGPD se alinha com regimes globais de privacidade reconhecidos (tais como o Regulamento Geral sobre a Proteção de Dados – RGPD ou GDPR da UE[1]) e em que pontos difere deles. Isso vai melhorar o nível geral de proteção de dados para brasileiros e possibilitar que organizações brasileiras façam negócios em escala global.

Fóruns onde autoridades de proteção de dados de todo o mundo trabalham juntas incluem o Working Party on Security and Privacy in the Digital Economy (SPDE - Grupo de Trabalho em Segurança e Privacidade na Economia Digital) da OECD, o Global Privacy Assembly (GPA - Assembleia Global de Privacidade, anteriormente conhecida como International Conference of Data Protection and Privacy Commissioners - Conferência Internacional dos Comissários para a Proteção dos Dados e Privacidade (ICDPPC)), o Ibero-American Data Protection Network (RIPD - Rede Ibero-Americana de Proteção de Dados), a Global Privacy Enforcement Network (GPEN - Rede Global para a Proteção da Privacidade) e a Cross-border Privacy Enforcement Arrangement (CPEA - Arranjo Transfronteiriço para a Garantia da Privacidade) da APEC (Cooperação Econômica Ásia-Pacífico).

B. PRIORIZANDO AS RESPONSABILIDADES E ATIVIDADES DA ANPD DE ACORDO COM A LGPD

A LGPD estabelece um papel significativo para a ANPD. A ANPD deve garantir que dados pessoais sejam protegidos de acordo com as regras da LGPD (Artigo 55-J-I) através da emissão de opiniões técnicas e diretrizes (Artigo 55-J-XX), educação (Artigo 55-J-VI), execução de sanções por descumprimento (Artigo 55-J-IV), recebimento e tratamento de reclamações e perguntas (Artigo 55-J-V), cooperação internacional (Artigo 55-J-IX) e edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade (Artigo 55-J-XIII).

Para permitir esse papel, a LGDP também oferece à ANPD um amplo espectro de deveres e tarefas específicos que são cruciais para a efetividade da LGPD. A ANPD deve ser estabelecida o mais rápido que possível, de modo que possa começar a executar essas tarefas e, particularmente, desenvolver as diretrizes necessárias à organizações para que sejam capazes de entrar em conformidade com a LGPD. Na ausência dessa

[1] Regulamentação (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas naturais com respeito ao tratamento de dados pessoais e sobre a livre movimentação de tais dados e a revogação da Diretriz 95/46/EC (General Data Protection Regulation – Regulamento Geral sobre a Proteção de Dados), disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1567000484507&uri=CELEX:32016R0679>.

orientação e dos necessários esclarecimentos por parte da ANPD, as organizações não serão capazes de implementar completa e efetivamente a lei.

As seguintes disposições da LGPD contêm as obrigações mais urgentes da ANPD:

1. Preparar a Política Nacional de Proteção de Dados Pessoais e da Privacidade

O Artigo 55-J-III requer que a ANPD elabore diretrizes para a Política Nacional para Proteção de Dados e Privacidade (Política Nacional).

A Política Nacional será o instrumento através do qual a ANPD definirá suas estratégias e prioridades, e definirá como vai operar da forma mais efetiva – veja a Seção D. Ao elaborar esse documento, a ANPD deve levar em consideração o limitado tempo entre seu estabelecimento e a data de entrada em vigor da LGPD, ajustando seu plano de implementação a esse aspecto. Esse plano deve focar-se nas ações imediatas que a ANPD deve realizar para agir de forma mais efetiva no sentido de proteger os brasileiros e a economia do Brasil – assim como delineado nos pontos a seguir desta Seção B.

Trabalhar nesse plano estratégico deve ser uma alta prioridade para a ANPD, já que isso a ajudará a realizar o resto de seus deveres. Esta Política Nacional deve ser submetida à consulta pública, para assegurar que múltiplos *stakeholders* ofereçam suas contribuições.

2. Reconhecer boas práticas e exemplos de ponta em programas de govenança de dados

O Artigo 50 estabelece que controladores e operadores[2] podem desenvolver boas práticas relacionadas à governança de atividades de tratamento de dados. O Artigo 50, parágrafo 2, estabelece que tais boas práticas poderiam ser operacionalizadas na forma de programas de governança de privacidade, e delineia uma série de elementos para estes programas relacionados à responsabilização organizacional.[3] O Artigo 50, parágrafo 3, estabelece que a ANPD pode reconhecer e promover tais boas práticas. De fato, desenvolver boas práticas e governança de dados pode ajudar as organizações a cumprirem com o Artigo 6-X da LGPD, o qual estabelece que as atividades de tratamento de dados devem seguir os requisitos de responsabilização e prestação de contas (*accountability*).

O princípio da *accountability* é globalmente reconhecido como alicerce para uma efetiva regulamentação da proteção de dados pessoais e da privacidade. Ele permite que as organizações sejam capazes de efetivamente proteger dados pessoais e de demonstrar para varios *stakeholders* que medidas de proteção foram tomadas apropriadamente. Ter um programa de privacidade em funcionamento é o fundamento para a conformidade com todas as obrigações de privacidade aplicáveis estabelecidas por lei e regulamentação. Os elementos fundamentais específicos de programas de privacidade baseados em *accountability* (tais como avaliação de risco, monitoramento e cumprimento) asseguram permanente conformidade com as regras de privacidade

---

[2] "Operadores" é o termo usado na LGPD equivalente a "processadores de dados" na RGPD. Conforme o Artigo 5, VII, da LGPD, operadores são "pessoas naturais ou jurídicas, de natureza pública ou privada, que processam dados em nome do controlador".

[3] O CIPL tem trabalhado amplamente na responsabilização organizacional e publicou uma série de artigos descrevendo os elementos da responsabilização e como as organizações podem operacionalizar a responsabilização. Veja os seguintes documentos oficiais do CIPL: The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 de julho de 2018, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf>; e Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>.

e proteção de dados, e permitem com que tais programas permaneçam atuais mesmo em vista de mudanças tecnológicas e de negócios.

A LGPD explicitamente incorpora o princípio de *accountability* e incentiva as organizações a estabelecerem programas de privacidade para operacionalizá-lo. A ANPD deveria, como uma de suas principais prioridades, exercitar seu mandato para promover e reconhecer tais programas. Isso será particularmente útil para pequenas e médias empresas, e outras empresas brasileiras que ainda não possuem práticas maduras de proteção de dados, experiência ou os recursos necessários para entrar em conformidade com a LGPD sem exemplos de melhores práticas e disponibilização de ferramentas.

Esse trabalho não precisa começar do zero. Por exemplo, o *Accountability Framework*[4] do CIPL tem sido amplamente usado por organizações globais para conformidade com leis de privacidade em múltiplas jurisdições. Há também outras estruturas globais que fornecem modelos de boas práticas e estruturas de governança que podem vir a ser desenvolvidos no Brasil, tais como os ISO Standards, a Cooperação Econômica Ásia-Pacífico (APEC), o Sistema de Regras de Privacidade Transfronteiriças (CBPR) e *binding corporate rules* (BCR). Na verdade, organizações do setor privado no Brasil já estão trabalhando com empresas e consultorias jurídicas em *frameworks* de conformidade com a LGPD que precisarão ser revisados e reconhecidos pela ANPD.

3. Estabelecer regras, procedimentos e diretrizes para organizações conforme requerido pela LGPD

Outra importante prioridade da ANPD deve ser fornecer diretrizes sobre diversos tópicos quando solicitado e permitido pela LGPD. As organizações brasileiras precisam de clareza e de orientação para verificar se seus processos internos estão de acordo com a LGPD, para implementar a LGPD e fornecer adequadamente proteção de dados para os indivíduos.

3.1 Regras sobre compartilhamento de dados

A portabilidade de dados é um facilitador da economia digital. De acordo com o Information Commissioners' Office do Reino Unido (UK ICO), o conceito de compartilhamento de dados se refere ao compartilhamento entre organizações que são *controllers* (ao invés de entre *controllers* e *processors*, já que os últimos atuam sob as instruções dos *controllers*). O compartilhamento de dados inclui dar acesso aos dados a terceiros, por qualquer meio, independende de sua localização. Pode ocorrer de forma rotineira e programada, ou de forma pontual.[5]

A LGPD determina regras específicas e limitações no compartilhamento de dados que requerem elaboração adicional por parte da ANPD. Sem orientações sobre compartilhamento de dados, as organizações podem optar por não investir recursos em certas práticas de compartilhamento que são comuns e/ou necessárias. Isso pode ocasionar a paralização de tratamentos de dados considerados urgentes ou necessários para propósitos de interesse público.[6] As organizações, tanto públicas quanto privadas, ficarão receosas de que a ANPD possa proibir tais práticas de compartilhamento de dados e tomar medidas coercivas contra elas.

---

[4] O Accountability Framework (Estrutura de Responsabilidade) do CIPL pode ser encontrado em artigos mencionados na nota de pé de página número 3. Ele é composto de sete elementos de responsabilização: liderança e supervisão; avaliação de risco; políticas e procedimentos; transparência; treinamento e conscientização; monitoramento e verificação; e resposta e aplicação da lei.

[5] UK ICO Data Sharing Code of Practice – Proposta de código para consulta. Disponível em <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/>.

[6] Podemos tomar como exemplo a orientação dada pelo UK ICO sobre Proteção de Dados e Coronavírus, a qual pretende fornecer às organizações, particularmente aquelas do setor da saúde, a segurança de que elas podem prosseguir com medidas de contenção do vírus que exijam o tratamento de dados pessoais. Disponível em <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/>, 12 de março de 2020.

(i) Compartilhamento de dados pessoais sensíveis entre controladores

O Artigo 11, parágrafo 3, dá à ANPD autoridade para regulamentar ou proibir o compartilhamento de dados pessoais sensíveis "para propósito de vantagem econômica", depois que consultar entidades públicas relevantes.

É particularmente importante que a ANPD forneca diretrizes relacionadas com o compartilhamento de dados pessoais sensíveis. Tais diretrizes devem abordar, por exemplo:

- O significado de "para propósito de vantagem econômica" e se o compartilhamento de dados pessoais seria permitido para fins de interesse público;
- Se o compartilhamento de dados seria permitido quando os indivíduos fornecem consentimento informado;
- O compartilhamento de dados pessoais sensíveis nos casos em que os indivíduos não podem fornecer consentimento, ou quando é substancialmente difícil obter consentimento, em particular quando não há ameaça direta ou risco de prejuízo aos indivíduos (p.ex., crises no setor de saúde);
- O compartilhamento de dados pessoais sensíveis por pequenas e médias empresas e startups, incluindo formas relacionadas de abordagem de risco (p. ex., farmácias locais);
- Casos de compartilhamento de dados através de *application program interfaces* (APIs); e
- Casos de compartilhamento de dados sensíveis em aplicativos de inteligência artificial onde esses dados são necessários para garantir um tratamento de dados justo e evitar discriminação e viés algorítmico.

(ii) Compartilhamento de dados entre organizações públicas e privadas

O Artigo 26, parágrafo 1, estabelece que é vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto se isso recair em uma das circunstâncias ali descritas (p. ex. quando os dados estão publicamente disponíveis ou quando são necessários para a execução de um contrato). O Artigo 27 determina que tal compartilhamento de dados pode ocorrer apenas com o consentimento do titular dos dados, exceto quando: (i) a lei determina que o consentimento não é necessário; (ii) as organizações públicas forneceram informações ao público conforme o Artigo 23-I; e (iii) é permitido como uma das exceções previstas no Artigo 26, parágrafo 1. O Artigo 27, em seu parágrafo único, também dispõe que organizações do setor público deverão notificar a ANPD quando compartilharem dados com organizações privadas, e que a ANPD pode estabelecer regulações adicionais sobre como essas informações devem ser fornecidas. Finalmente, o Artigo 30 dispõe que a ANPD pode publicar regras complementares sobre compartilhamento de dados de organizações públicas para organizações privadas.

O compartilhamento de dados entre organizações públicas e privadas é uma prática comum em qualquer economia, mas deve ser acompanhado por medidas de responsabilização e garantias de todas as partes envolvidas no esquema de compartilhamento. Assim, a orientação da ANPD sobre esse assunto também é de vital importância.

Esse compartilhamento de dados é necessário, por exemplo, durante o processo de *on-boarding* de novos fornecedores de serviços de pagamento, como os bancos, que precisam obter informações fiscais da Receita Federal. Tal compartilhamento também é necessário no contexto de aquisições comerciais em que as organizações devem obter certas informações de autoridades federais e estatais, as quais, em muitos casos, inclui dados pessoais sobre os indivíduos envolvidos na operação. O compartilhamento de dados de organizações públicas a organizações privadas é relevante também para fins de interesse público quando a indústria carece de informações que poderiam ser usadas para desenvolver produtos e serviços que impulsionariam melhorias no setor público (como o setor da saúde).

Finalmente, a atual pandemia do COVID-19 reforçou a necessidade de compartilhamento de dados entre os setores público e privado para poder rastrear, modelar, prever e combater a disseminação do vírus. Muitas autoridades de proteção de dados em diversos países publicaram informações, diretrizes e documentos para auxiliar os *stakeholders* nacionais e internacionais a lidar com a crise.[7]

A ANPD deve esclarecer, o quanto antes:

- As circunstâncias em que as organizações do setor público podem compartilhar dados pessoais com organizações do setor privado;
- O papel do consentimento e contratos nesse compartilhamento de dados, e as circunstâncias nas quais o consentimento não é necessário ou em que obter consentimento constitui uma tarefa onerosa;
- Se todas as atividades de compartilhamento de dados requerem que organizações do setor público notifiquem a ANPD, ou se essa notificação deve ser fornecida com base no nível de risco envolvido no compartilhamento de dados; e
- O tipo de medidas de *accountability* necessárias para promover confiança no compartilhamento de dados.

3.2 Regras sobre o direito à portabilidade de dados

O Artigo 18-V da LGPD dá à ANPD autoridade para publicar regulamentações sobre como organizações devem implementar o direito à portabilidade de dados.

Assim como o compartilhamento de dados, a portabilidade de dados também é um facilitador da economia digital. Ela permite que indivíduos possam mover seus dados pessoais de um serviço a outro, em vez de estarem "presos" a um provedor de serviços específico. Se bem regulamentado, esse direito pode agir como um facilitador da confiança digital, da concorrência e do crescimento econômico, em especial para pequenas e médias empresas.

O direito à portabilidade de dados não é um direito novo nas leis e regulamentações brasileiras. O setor bancário já trabalha com portabilidade de dados no contexto de portabilidade de crédito entre instituições financeiras e no contexto de *open banking*. Os usuários de serviços de telecomunicações também se beneficiam de regras de portabilidade. Além disso, a indústria tecnológica está trabalhando internacionalmente para possibilitar o exercício desse direito no âmbito da proteção de dados pessoais.[8]

A ANPD deve trabalhar com múltiplos *stakeholders*, incluindo setores da indústria e outros reguladores brasileiros, para compreender e maximizar os benefícios e as oportunidades da portabilidade de dados para indivíduos e para as organizações. A regulamentação da ANPD sobre portabilidade de dados tem o potencial de impulsionar a padronização de regras de interoperabilidade relacionadas a dados pessoais. Isso resultará em ganhos de eficiência para a economia digital brasileira, serviços melhores e mais diversificados para os consumidores, e a consolidação do direito à portabilidade.

3.3 Diretrizes sobre informações a serem fornecidas aos indivíduos em relação às atividades de tratamento de dados pessoais

O Artigo 55-J-X exige que a ANPD disponha sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial. Esta é uma peça-chave para o princípio de transparência da LGPD contemplado no Artigo 6, VI e para o direito dos titulares de dados pessoais de obter

[7] Ver, por exemplo, Global Privacy Assembly's Data Protection and Coronavirus (COVID-19) Resources, o qual compilou orientações e informações de autoridades de proteção de dados proteção de dados <https://globalprivacyassembly.org/covid19/>.

[8] Veja, por exemplo, o Data Transfer Project, disponível em <https://datatransferproject.dev/>.

informações claras, adequadas e abrangentes sobre o tratamento de dados de acordo com o Artigo 9 da LGPD.

Para que indivíduos sejam capazes de exercer seus direitos conforme a LGPD, e tenham controle sobre seus dados pessoais, eles primeiro precisam compreender como as organizações estão coletando e usando esses dados. Contudo, o nível de entendimento e informação fornecido vai depender de diversas circunstâncias, tais como o contexto das operações de tratamento de dados (p. ex., aparelhos com Internet das Coisas comparado a aplicativos de celular), a faixa etária dos indivíduos (p. ex., crianças, adultos ou idosos), a complexidade das atividades de tratamento (p. ex. dados processados por folhas de pagamento comparado com informações analíticas), etc.

Internacionalmente, a organizações do setor privado vêm desenvolvendo boas práticas com relação a informar os indivíduos a respeito do tratamento de dados. Isso inclui, entre outras: usar uma *layered approach* para o fornecimento de informações; usar recursos, tais como vídeos e ilustrações no lugar de apenas informações baseadas em texto; e oferecer informações em diferentes estágios da transação entre usuário e organização. O fornecimento de informações aos indivíduos, portanto, deixou de ser uma mera notificação legalista de privacidade, e tornou-se uma prática de transparência centrada no usuário e no *design* de produtos e serviços.

A ANPD deve priorizar a publicação de diretrizes sobre como as organizações devem buscar fornecer aos indivíduos informações contextuais, efetivas e práticas de tal forma que não crie uma fatiga devido ao excesso de notificações.

3.4 Regras sobre os prazos e os meios de responder às solicitações de direitos dos titulares de dados

O Artigo 18 da LGPD estabelece os direitos do titular de dados pessoais. O parágrafo 5 estabelece que os prazos e meios para que as organizações respondam a solicitações relativas ao exercício desses direitos serão regulamentados adicionalmente (sem menção expressa à ANPD).

Além disso, o Artigo 18, I e II da LGDP dispõe que os indivíduos têm o direito de obter confirmação sobre a existência de atividades de tratamento de dados por parte de controladores, assim como o direito de ter acesso a seus dados pessoais. O Artigo 19 dispõe que estes devem ser fornecidos em formato simplificado e imediatamente, ou de modo abrangente, dentro de 15 dias. Adicionalmente, o Artigo 19, parágrafo 3, autoriza a ANPD a publicar regulamentações adicionais sobre o acesso em circunstâncias específicas.

O exercício de direitos de proteção de dados permite que os indivíduos tenham o controle de seus dados pessoais. Devido à complexidade das operações de tratamento de dados, as organizações precisam de tempo para responder às solicitações individuais. Isso pode incluir a verificação do indivíduo que realiza a solicitação; analisar e esclarecer a solicitação quando necessário; localizar os dados em vários sistemas, bases de dados e servidores; responder aos indivíduos em um formato inteligível; excluir dados/limitar o tratamento quando necessário; e outras operações. A maioria das organizações precisará adaptar processos existentes e levar fatores em consideração, tais como questões de interoperabilidade entre diferentes sistemas.

A ANPD é a autoridade mais bem posicionada para publicar regras sobre os prazos e os meios para que as organizações respondam a solicitações relacionadas aos seus direitos como titulares de dados, e deve fazê-lo com prioridade. A LGPD não dispõe sobre os prazos da maioria dos direitos, e apenas define um curto prazo de 15 dias para o direito de acesso. A ANPD deve engajar-se com organizações de diversos tamanhos e setores para que a ajudem a compreender a complexidade de suas operações de tratamento de forma a determinar prazos mais adequados e realistas, assim como os meios para responder às solicitações. Ela também deve considerar seguir padrões internacionais; por exemplo, o RGPD determina um prazo de um mês para responder às solicitações de direitos de titulares de dados, extensível para mais dois meses, dependendo da complexidade e do número de solicitações.[9]

[9] Artigo 12(3) do RGPD.

3.5 Regras sobre o papel e os deveres do encarregado pelo tratamento de dados pessoais

O Artigo 41 da LGPD dispõe que os controladores devem nomear um indivíduo ou entidade para ser responsável pelo tratamento de dados pessoais. Esse indivíduo, definido pela LGPD como "encarregado", é frequentemente chamado no cenário internacional de *Data Protection Officer* (DPO). O parágrafo 2 lista as atividades do encarregado e o Parágrafo 3 estabelece que a ANPD pode publicar regras complementares com relação à definição e às tarefas dos encarregados. Isso inclui em que situações as organizações estariam dispensadas de apontar um encarregado devido a sua natureza e tamanho, assim como o tamanho de suas operações de tratamento de dados.

A função do encarregado é um componente essencial do princípio da *accountability*. Ela/ele desempenha um papel crucial em capacitar as organizações para garantir e demonstrar tanto a conformidade com a privacidade de dados, quanto a efetiva proteção da privacidade dos indivíduos.[10]

Há algumas áreas que podem apresentar desafios para as organizações, ou exigir esclarecimentos, interpretação e orientação para garantir uma implementação efetiva do papel do encarregado. Os desafios incluem: se organizações múltiplas dentro de um único grupo corporativo podem indicar um único encarregado; se as organizações podem ter mais de um encarregado; se o papel do encarregado pode ser terceirizado; e outros. Ao publicar regras sobre o papel do encarregado, a ANPD deve incentivar uma interpretação flexível das exigências do encarregado e baseada em resultados, a fim de possibilitar que encarregados possam atuar nos mais diversos tipos de organizações, incluindo organizações multinacionais, pequenas e médias empresas, startups, ONGs e organizações públicas.

3.6 Regras e procedimentos sobre relatórios de impacto e o conceito de tratamento de "alto risco"

Uma das tarefas da ANPD sob o Artigo 55-J-XIII é publicar regras e procedimentos relativos à proteção de dados e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais quando o tratamento de dados pode resultar em alto risco aos princípios da proteção de dados delineados na LGPD. Além disso, o Artigo 38 dispõe que a ANPD pode exigir que os controladores preparem as relatórios de impacto. O Artigo 10, Parágrafo 3 ainda especifica que a ANPD pode exigir relatórios de impacto quando os controladores processarem dados pessoais com base em seus legítimos interesses.

A LGPD também aborda a noção de risco em várias outras disposições, incluindo: (i) O Artigo 44-II, que estabelece que o tratamento de dados será considerado "irregular" quando ilegal ou quando não atingir as expectativas razoáveis de titulares de dados com relação à segurança de seus dados pessoais, levando em consideração os riscos que são razoavelmente esperados do tratamento de dados; (ii) o Artigo 48, que determina que controladores devem comunicar à ANPD e aos titulares de dados sobre a ocorrência de violações de dados que possam resultar em riscos ou danos relevantes aos titulares dos dados; (iii) o Artigo 50, parágrafo 1, dispõe que os controladores terão que levar em conta os riscos e benefícios das atividades de tratamento quando desenvolverem boas práticas em relação à governança de tais atividades; (iv) e o Artigo 50, parágrafo 2, I-d, delineia avaliações de risco como um dos elementos possíveis de programas de governança de dados.

Conforme visto acima, muitas disposições da LGPD referem-se especificamente aos conceitos de tratamento de "risco", "alto risco" e avaliações de risco (incluindo relatórios de impacto). Assim, a LGPD efetivamente incorpora uma abordagem baseada em risco da proteção de dados, exigindo que organizações empreendam um exercício de ponderação (*balancing exercise*) entre riscos e benefícios para indivíduos resultantes de atividades de tratamento de dados, tanto ao estabelecer seu programa de privacidade quanto ao implementar certas disposições da LGPD. A LGPD, contudo, não define o termo "alto risco", nem a noção de

[10] Artigo do CIPL DPO - Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf>.

uma abordagem baseada em risco. A LGPD exige que a ANPD publique regras sobre relatórios de impacto e exige que as organizações realizem essas avaliações.

Antes que a ANPD exija que avaliações de risco sejam realizadas, ela deve consultar a indústria e fornecer diretrizes sobre a noção do risco e os elementos a serem ponderados como parte de tais avaliações.[11] Além disso, as regras e os procedimentos a serem publicados pela ANPD devem orientar sobre diferentes metodologias para as avaliações de risco requeridas pelos diversos dispositivos da LGPD conforme visto acima, e ao mesmo tempo devem dar flexibilidade para que organizações decidam a respeito da metodologia que é a mais apropriada às suas atividades de tratamento de dados e aos seus negócios. A ANPD também deve abordar os prazos para que as organizações executem relatórios de impacto quando solicitadas pela ANPD. Ela deve considerar que, dada a natureza da exigência, além da natureza e complexidade das operações de tratamento sendo avaliadas, as organizações podem precisar de períodos mais longos, tais como 30 a 60 dias, para executar relatórios de impacto mediante solicitação.

3.7 Regras relacionadas aos prazos para notificação à ANPD de incidentes de segurança que possam acarretar riscos aos titulares de dados

O Artigo 48 determina que os controladores devem notificar a ANPD e os titulares dos dados, dentro de um prazo razoável, sobre incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais. O parágrafo 1 dá autoridade à ANPD para definir o que constitui um "prazo razoável".

Assim como no que se refere aos prazos para atender a solicitações de direitos individuais, como mencionado acima, as organizações precisam ter segurança jurídica para implementar essa exigência a LGPD. A ANPD deve definir, assim que possível, o que constitui um "prazo razoável" para notificação de incidentes de segurança. Por exemplo, 10 dias úteis constituiriam um prazo razoável, pois permitiria que as organizações analisassem o incidente ligado à segurança e trabalhassem para implementar medidas que minimizem seu impacto sobre os indivíduos, em vez de concentrar seus esforços em prol das exigências de notificação.

A ANPD também deve oferecer clareza sobre o que constituiria "risco ou dano relevante aos titulares de dados", e como organizações podem avaliar tais riscos e danos relevantes no contexto de uma violação de dados — ver acima as regras e os procedimentos sobre avaliações de risco e o conceito de tratamento de "alto risco". É importante que tanto as organizações quanto a ANPD limitem a notificação de incidentes a apenas o que é absolutamente necessário, a fim de evitar que a ANPD e os indivíduos fiquem sobrecarregados por notificações menores e triviais. A notificação excessiva pode levar a danos de reputação desnecessários a organizações e pode aumentar desnecessariamente a carga de trabalho da ANPD. Não se deve considerar necessário que as organizações notifiquem a ANPD e os titulares de dados sobre incidentes insignificantes. Por exemplo, algumas diretrizes internacionais fornecem exemplos de incidentes que estão e que não estão sujeitos às exigências de notificação.[12]

---

[11] O CIPL escreveu extensivamente sobre a noção de abordagem baseada em risco: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR , disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>; A Risk-based Approach to Privacy: Improving Effectiveness in Practice, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf>; Protecting Privacy in a World of Big Data, The Role of Risk Management, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf>; The Role of Risk Management in Data Protection, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf>.

[12] Ver Diretriz 29 do Grupo de Trabalho sobre notificação relativa à violação de dados pessoais sob a Regulamentação 2016/679, adotada em 3 de outubro de 2017 e endossada pelo Comitê Europeu para a Proteção de Dados durante sua

3.8 Regras, diretrizes e procedimentos simplificados e especiais para as pequenas e médias empresas

O Artigo 55-J-XVIII dispõe que a ANPD deve publicar regras, diretrizes e procedimentos simplificados, incluindo prazos, para auxiliar pequenas e médias empresas e startups na implementação da LGPD.

Cumprir com a LGPD será particularmente desafiador para as pequenas e médias empresas em razão de seus limitados recursos, orçamento, maturidade em relação às regras de tratamento de dados pessoais, e experiência com conformidade co tais regras. A ANPD não deve apenas oferecer orientação, mas também ferramentas simplificadas que possam empoderar as pequenas e médias empresas a avaliar os riscos de suas atividades de tratamento de dados e implementar exigências específicas da LGPD para mitigar tais riscos. A ANPD deve considerar exemplos de orientação e ferramentas simplificadas para pequenas e médias empresas fornecidas por DPAs ao redor do mundo, tais como o UK ICO,[13] o Data Protection Commissioner irlandês[14] ou a Data Protection Agency da Espanha,[15] entre outros. Ela deve considerar também estabelecer *helplines* específicas para responder aos questionamentos das pequenas e médias empresas e apoiar seus esforços de conformidade com a LGPD.[16]

3.9 Normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da LGPD

O Artigo 63 dispõe que a ANPD emitirá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da LGPD, levando em consideração a complexidade do tratamento de dados envolvidos e a natureza dos dados.

A LGPD, no entanto, não define o termo "banco de dados". Em teoria, todas as organizações que mantêm e processam dados pessoais usam banco de dados de algum modo e o termo poderia ser interpretado de forma a significar quaisquer sistemas de TI que tratam dados pessoais. A ANPD deve esclarecer o propósito desta exigência da LGPD. Ela também deve esclarecer sob quais circunstâncias as organizações ficariam sujeitas a ela, assim como quais obrigações da LGPD elas conseguiriam cumprir de forma progressiva, e como.

4. Esclarecendo as disposições da LGPD

O Artigo 55-J, XIII dispõe que a ANPD tem a tarefa geral de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade.

Como mencionado anteriormente, a ANPD tem responsabilidade fundamental pela interpretação da LGPD. Isso inclui a interpretação das disposições da LGPD que exigem esclarecimento adicional para que as organizações as implementem com segurança jurídica.

As disposições que exigem esclarecimento incluem (entre outras):

- Quais organizações ficariam sujeitas ao escopo da LGPD de acordo com o Artigo 3 nas complexas circunstâncias de tratamento de dados, tais como se a lei se aplicaria a um controlador localizado fora do Brasil unicamente devido ao fato de que usa operadores que estejam localizados no Brasil, embora tal controlador não tenha coletado dados pessoais no território brasileiro, nem tenha oferecido serviços diretamente a indivíduos brasileiros;

---

primeira Reunião Plenária. Disponível em <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

[13] ICO SME data protection hub, disponível em <https://ico.org.uk/for-organisations/business/>.

[14] Irish DPC Guidance for SMEs, disponível em <https://www.dataprotection.ie/en/guidance-landing/guidance-smes>.

[15] Ferramenta AEPD para PMEs "Facilita RGPD", disponível em: <https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd>.

[16] Veja, por exemplo, a linha de atendimento da ICO, disponível em <https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/>.

- Como as organizações podem "considerar a finalidade, a boa-fé e o interesse público" ao processar dados pessoais cujo acesso é público, conforme o Artigo 7, parágrafo 3 da LGPD, e em que consistem os "dados pessoais cujo acesso é público";
- Quem é responsável por fornecer informações a indivíduos sobre atividades de tratamento de dados e sob quais circunstâncias, conforme exigido pelo Artigo 9 da LGPD;
- Em que consistem informações de "conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca", as quais invalidariam o consentimento de acordo com o Artigo 9, parágrafo 1 da LGPD;
- Como regras relacionadas à governança e boa prática adotadas de acordo com o Artigo 50 podem estabelecer as obrigações para cada parte envolvida nas atividades de tratamento de dados pessoais, em particular levando-se em consideração que a LGPD não exige expressamente que elas participem de *data processing agreements* ou medidas contratuais relacionadas; e
- Como as organizações devem cumprir as disposições da LGPD relativas ao tratamento de dados pessoais de crianças, inclusive fornecer informações a crianças de acordo com o Artigo 14, parágrafo 6 da LGPD; abordar questões relativas à verificação de identidade; abordar questões relativas a crianças vulneráveis que não conseguem obter consentimento parental, mas ainda assim têm o direito de se beneficiarem do acesso à internet etc.; e outros.

5. Incentivar a adoção de padrões técnicos da indústria e estabelecer padrões técnicos para as organizações

Padrões técnicos são uma ferramenta importante e flexível para capacitar a implementação de requisitos legais no campo da proteção de dados e segurança de dados. A ANPD deve incentivar mais amplamente a criação de padrões e também a consideração e adoção de padrões internacionais já estabelecidos.

5.1 Padrões técnicos da indústria para direitos de titulares de dados

Os Artigos 51 e 55-J-VIII dão à ANPD a obrigação de "estimular" estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis.

Apesar de a LGPD prever que tais padrões técnicos serão desenvolvidos pela indústria, a LGPD sugere um papel proativo para a ANPD na facilitação do desenvolvimento de tais padrões técnicos. Esse papel exige reconhecimento e familiaridade da complexidade da economia digital, dos diversos tipos de atividades empresariais e da natureza das consequentes diversas atividades de tratamento. A ANPD também deve engajar-se ativamente com a indústria e outros *stakeholders* relevantes sobre essa questão.

5.2 Padrões técnicos e organizacionais relativos à segurança de dados

O Artigo 46 da LGPD dispõe que controladores e operadores devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O parágrafo 1 dispõe à ANPD autoridade para articular os padrões técnicos mínimos para essas medidas de segurança, em particular a respeito da proteção de dados sensíveis.

Organizações, particularmente pequenas e médias empresas, precisam ter clareza sobre o que seja o mínimo esperado delas nos vários cenários de tratamento de dados, de modo que possam adequadamente proteger dados levando em consideração os riscos de suas atividades de tratamento. Ao conduzir seus deveres com respeito à segurança de dados, a ANPD deve levar em conta que medidas de proteção de segurança apropriadas vão variar conforme a natureza do negócio e das atividades de tratamento envolvidas, assim

como os tipos de dados pessoais tratados. Ela deve também conceber padrões que sejam flexíveis, adaptáveis e *future-proof*, e que não sejam limitados ao *state of the art* da segurança de dados.

Finalmente, a ANPD também deve ser guiada por padrões internacionais de segurança de dados, tais como os PCI – *Payment Card Industry standards*[17] e os diferentes padrões da ISO sobre privacidade e segurança de dados,[18] uma vez que eles já são comumente usados ao redor do mundo e são conhecidos por muitas empresas brasileiras que têm operações globais.

5.3 Padrões e técnicas de anonimização

O Artigo 12 da LGPD dispõe que dados anonimizados não serão considerados dados pessoais sob a LGPD, exceto quando o processo de anonimização for revertido ou puder ser revertido por meios razoáveis. Portanto, o tratamento de dados anonimizados cai fora do escopo desta lei. O parágrafo 3 do Artigo 12 dá à ANPD autoridade para publicar padrões e técnicas de anonimização, e realizar verificações acerca de sua segurança, após consultar o Conselho Nacional de Proteção de Dados Pessoais.

A anonimização de dados deve ser incentivada e habilitada, já que é peça chave para a inovação e a economia digital brasileira. Ela permite não somente que o tratamento de dados em geral respeite regras de proteção de dados, mas também permite que as organizações continuem a processar e extrair valor dos dados em contextos fora dos propósitos originais para os quais os dados foram coletados. A ANPD deve fornecer padrões e técnicas para a anonimização assim que possível, além de publicar orientação sobre o que constituem "meios razoáveis" para reversão da anonimização de dados. Finalmente, a ANPD deve buscar inspiração e incentivar a convergência com boas práticas e orientações sobre anonimização emitidas internacionalmente por autoridades de proteção de dados, academia e organizações da indústria.[19]

6. Possibilitar transferências internacionais de dados pessoais

O Artigo 33-I dispõe que transferências internacionais de dados pessoais serão permitidas a países ou órgãos internacionais que disponham de um nível de proteção de dados que seja equivalente à proteção oferecida pela LGPD. Alternativamente, o Artigo 33-II também permite que transferências internacionais de dados sejam realizadas quando as organizações implementarem algum dos mecanismos de transferência internacional de dados ali previstos. Esses mecanismos incluem: cláusulas-padrão contratuais, cláusulas contratuais que são específicas para determinada transferência, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos.

A ANPD é responsável por determinar quando um terceiro país ou órgão internacional tem um nível adequado de proteção de dados conforme o Artigo 34. De modo semelhante, a ANPD é responsável por definir o conteúdo dos mecanismos protetores mencionados acima conforme o Artigo 35.

Transferências internacionais de dados são um componente-chave de atividades de tratamento de dados pessoais, em particular para empresas brasileiras que operam na economia digital global — seja conduzindo negócios com empresas globais ou expandindo seus negócios para além das fronteiras brasileiras. Ter mecanismos apropriados de transferência de dados disponíveis é particularmente relevante para as

[17] PCI Security Standards, disponível em <https://www.pcisecuritystandards.org/pci_security/>.

[18] Ver, por exemplo, ISO/IEC 27001, Information Security Management, disponível em <https://www.iso.org/isoiec-27001-information-security.html>; and ISO/IEC 27701: 2019, Security techniques – Extension to ISO/IEC 27001 and ISO 27002 for privacy information management – Requirements and guidelines, available at <https://www.iso.org/standard/71670.html>.

[19] Ver, por exemplo, "Anonymisation: Managing Data Protection Risk Code of Practice," disponível em <https://ico.org.uk/media/1061/anonymisation-code.pdf>; and the Irish DPC's guidance on "Anonymisation and Pseudonymisation," <https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation>.

pequenas e médias empresas, cujo crescimento pode frequentemente depender da criação de parcerias com empresas internacionais.

O texto da LGPD, da forma como está escrito, poderia ser interpretado de forma a vedar transferências internacionais até que a ANPD publique uma lista de países adequados ou defina o conteúdo de mecanismos de transferência. Portanto, a ANPD deve esclarecer, assim que possível, que as organizações ainda podem aplicar os mecanismos do Artigo 33 da LGPD para permitir transferências internacionais de dados pessoais (como, por exemplo, cláusulas contratuais específicas), ao mesmo tempo em que a ANPD trabalha no conteúdo dos mecanismos de transferência e avalia a adequação de países terceiros.

Além disso, ao definir o conteúdo dos mecanismos de transferência e realizar avaliações de adequação, a ANPD deve considerar exemplos internacionais e engajar-se com órgãos internacionais que já passaram por essa experiência (como, por exemplo, a Comissão Europeia e a APEC). Em particular, a ANPD deve reconhecer esquemas internacionais de certificação de privacidade como capacitadores de transferências internacionais, uma vez que eles exigem que as organizações certificadas implementem uma série de medidas de proteção de dados de alto padrão. Exemplos de tais esquemas de certificação incluem certificações fornecidas por:

- International Organization for Standardization (ISO);
- APEC-CBPR System;
- APEC Privacy Recognition for Processors (PRP);
- EU-US Privacy Shield;
- Binding Corporate Rules (BCR); and
- National Institute of Standards and Technology (NIST).

7. Conscientização sobre proteção de dados e educação de indivíduos e organizações

Uma das tarefas da ANPD sob o Artigo 55-J-VI é promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança. Uma tarefa relacionada sob o Artigo 55-J-VII é que a ANPD deve promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade.

Para que a LGPD seja uma lei efetiva, todos os *stakeholders* envolvidos devem estar cientes de seus direitos e obrigações sob esta lei. Os indivíduos devem estar cientes de seus direitos de proteção aos dados pessoais e como exercê-los, e as organizações devem ter conhecimento de suas obrigações. A conscientização é, assim, uma das tarefas mais importantes da ANPD. A ANPD deve desenvolver uma estratégia de educação, comunicação e conscientização, acompanhada de um plano de ação de curto prazo (como, por exemplo, de dois anos). Par fazer isso, ela deve identificar e engajar-se com *stakeholders*-chave, que poderiam trabalhar como parceiros para elaborar tal plano (instituições acadêmicas, ONGs, especialistas privados, plataformas de mídia e tecnologia, por exemplo).

8. Preparação para fiscalização regulatória

8.1 Estabelecer um procedimento administrativo de execução de sanções administrativas

O Artigo 53 exige que a ANPD definirá, por meio de regulamento próprio sobre sanções administrativas a infrações à LGPD, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. O Artigo 52, parágrafo 4, dispõe sobre o cálculo de multas.

As obrigações da ANPD relacionadas ao esclarecimento e à interpretação da LGPD, emissão de orientações relativas à sua implementação e instrução de *stakeholders* são responsabilidades-chave iniciais para qualquer autoridade de proteção de dados recentemente estabelecida. Isso é particularmente relevante no contexto

de um país que não tem histórico de um arcabouço jurídico para proteção de dados. Contudo, nenhuma autoridade de proteção de dados pode ser efetiva sem procedimentos apropriados para fazer cumprir a lei que foi encarregada de executar.

A ANPD deve, portanto, desenvolver e ser transparente em relação a seus procedimentos e prioridades de execução da LGPD, inclusive no que tange a como ela calculará multas. Estas devem levar em consideração a gravidade da atividade infratora, seus riscos para os indivíduos, assim como medidas de mitigação tomadas pelas organizações no contexto de seus esforços de implementação do princípio de *accountability* e de seus programas de governança de dados. A ANPD deve também levar em consideração que, no curto e médio prazo, as organizações estão trabalhando para atingir a conformidade com a LGPD em um cenário incerto, já que muitas provisões da LGPD ainda estão abertas à regulamentação e esclarecimento adicionais pela ANPD.

Além disso, ao executar a LGPD, a ANPD deve sempre levar em consideração e seguir os princípios e critérios da Constituição Brasileira e da Lei n. 9.784, de 29 de janeiro de 1999. Eles incluem, entre outros, os princípios da legalidade, propósito, motivação, razoabilidade, moralidade, direito à ampla defesa e segurança jurídica.

Finalmente, a transparência é um princípio importante para a ANPD — ele deve ser implementado não apenas na fase de planejamento e comunicação dos procedimentos de execução da LGPD, mas também na própria fase de execução de sanções administrativas por descumprimento da LGPD. A transparência resulta em um cenário de confiança entre todos os *stakeholders* envolvidos, inclusive indivíduos e organizações reguladas.

8.2 Implementar mecanismos para receber petições e reclamações dos titulares de dados

O Artigo 55-J-V exige que a ANPD aprecie petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação. O Artigo 55-J-XXIV também exige que a ANPD implemente mecanismos para registrar reclamações de titulares de dados, e o Parágrafo 6 observa que reclamações podem ser analisadas e resolvidas de maneira agregada e padronizada.

Lidar com reclamações é uma das obrigações-chave de qualquer autoridade de proteção de dados, e é capacitadora da compensação de indivíduos e da sua retomada de controle sobre seus dados pessoais. A ANPD é uma autoridade reguladora tanto para as organizações quanto para os indivíduos. Como tal, ela deve estar disponível para responder às suas preocupações, consultas e reclamações.

Portanto, a ANPD deve estabelecer procedimentos para permitir que ela receba, analise e responda a petições e reclamações de indivíduos. Ela deve levar em consideração o grande número de brasileiros classificados como titulares de dados sob a LGPD e que potencialmente poderiam apresentar petições e reclamações. Conequentemente, a ANPD deve explorar ferramentas tecnológicas disponíveis para otimizar este processo (p. ex., ferramentas de verificação de identidade, *ticketing systems*, etc.). Ela eeve estar pronta para se posicionar ou adaptar seus processos onde houver picos de reclamações (p. ex., após um grande vazamento de dados por uma companhia de tecnologia que tenha chamado atenção da mídia). Finalmente, ela deve também consultar outros reguladores brasileiros e aprender com suas experiências em lidar com o público.

Para assegurar a eficiência e evitar ficar "paralisada" devido a grandes números de reclamações, a ANPD deve educar os indivíduos e lembrá-los de que eles devem inicialmente direcionar suas reclamações às organizações relevantes. As organizações têm um dever de desenvolver procedimentos para lidar com reclamações e quaisquer outras questões apresentadas pelos titulares de dados. Apenas aquelas reclamações que não forem inicialmente resolvidas por uma organização devem ser canalizadas para a ANPD.

C. COMPOSIÇÃO, FUNCIONÁRIOS E OUTROS RECURSOS DA ANPD

A ANPD deve estar adequadamente dotada de recursos (tanto financeiros quanto em termos de funcionários disponíveis), e possuir o conhecimento técnico e a especialização necessários para desempenhar efetivamente seus deveres e executar a LGPD. Isso significa ter um número suficiente de advogados, profissionais da segurança da informação, tecnologistas, economistas e outros profissionais com especialidade técnica relevante, levando em consideração as características e o tamanho do Brasil.

Em comparação, desde a implementação da RGPD, o UK ICO aumentou sua força de trabalho em 40% para 700 funcionários, e tem a meta de chegar a 825 funcionários em tempo integral em 2021.[20] A população do Reino Unido é de 66,5 milhões de pessoais, enquanto que a do Brasil é de 211 milhões, três vezes maior, o que dá uma indicação sobre quantos funcionários a ANPD poderia precisar para cumprir seus deveres sob a LGPD. De forma similar, o *Data Protection Commissioner* (DPC) irlandês aumentou sua equipe de cerca de 110 funcionários no final de 2018, para 140 funcionários no final de 2019.[21] No total, 21 países da UE aumentaram os orçamentos de suas autoridades de proteção de dados em 2019, sendo que 17 deles afirmaram que precisariam de um aumento de, no mínimo, 30% a 50% no orçamento.[22]

O Brasil pode não estar apto a imediatamente alcançar o mesmo nível de dotação orçamentária e de funcionários que essas jurisdições, uma vez que a LGPD estabeleceu a ANPD sem aumento do orçamento. Contudo, uma combinação de realocação razoável de recursos, indicação de quadros técnicos e equipe qualificada e experiente, assim como a priorização estratégica de tarefas, permitirão que a ANPD alcance efetividade razoável dentro do tempo existente e das suas restrições orçamentárias.

D. CONSIDERAÇÕES FINAIS SOBRE REGULAÇÃO EFETIVA

Uma regulação efetiva depende de estratégias que possibilitem o melhor uso possível de recursos disponíveis. Isso inclui a priorização e concentração de atividades regulatórias que prometem os melhores resultados para indivíduos e sociedade.

Conforme delineado acima, a ANPD deve priorizar suas atividades relacionadas à regulação responsiva, a qual busca fomentar abordagens de fiscalização regulatórias que sejam adaptadas às realidades sociais e econômicas contemporâneas. Uma pesquisa do CIPL demonstrou que a regulação responsiva é mais eficaz do que a punição (que, por sua vez, também têm um papel importante a desempenhar).[23] A regulação responsiva também resulta na promoção tanto da do direito à privacidade quanto do uso benéfico de dados pessoais e inovação.[24]

A regulação responsiva baseia-se no engajamento construtivo com organizações reguladas ao fornecer-lhes informações, aconselhamento e suporte. Isso também significa fomentar uma cultura de diálogo aberto entre os reguladores, organizações reguladas e outros *stakeholders* relevantes (tal como especialistas

---

[20] Relatório anual do ICO 2018-19, disponível em <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>.

[21] Relatório Anual do DPC 2019, disponível em <https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf>.

[22] Primeira supervisão sobre a implementação da RGPD e os papéis e recursos das autoridades supervisoras nacionais, Comitê Europeu para a Proteção de Dados, 26 de fevereiro de 2019, página 7. Disponível em <https://www.dataprotection.ro/servlet/ViewDocument?id=1633>.

[23] Relatório do CIPL sobre Regulação para buscar Resultados: Strategies and Priorities for Leadership and Engagement, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf>.

[24] Relatório do CIPL sobre incentivos à *accountability*: How Data Protection Authorities and Law Makers Can Encourage Accountability, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>.

acadêmicos e privados), além de aprender com as experiências deles sobre o tratamento de dados pessoais responsável e em conformidade com as leis vigentes. Escutar e aprender com esses *stakeholders* vai equipar a ANPD e permiti-la desenvolver suas diretrizes, normas e regulamentos de maneira informada, realista e efetiva.

Em outras palavras:

- Um sistema regulatório será mais efetivo onde for mais consistente e der suporte a comportamentos que são amplamente vistos como justos, proporcionais e éticos;
- As organizações devem ser responsáveis por evidenciar seu comprometimento com comportamentos que atraiam a confiança dos reguladores, assim como de sua própria gestão e equipe, clientes, fornecedores, investidores e outros *stakeholders*;
- O aprendizado é fundamental e é incentivado por um engajamento aberto e construtivo entre autoridades reguladoras e organizações reguladas, mas é desencorajado pela ênfase na culpa e na punição;
- Sistemas regulatórios precisam ser baseados em diálogo e cooperação mútuos que sejam explicitamente direcionados para maximizar conformidade com leis vigentes, prosperidade e inovação.
- Quando organizações violam as regras, uma resposta proporcional se faz necessária, e penalidades mais severas devem ser reservadas para infrações deliberadas, reiteradas ou intencionais.

III. CONCLUSÃO

Nunca será demais destacar a importância e a urgência de se estabelecer uma ANPD efetiva. Para que as organizações implementem as exigências da LGPD efetivamente, é essencial que a ANPD seja estabelecida sem demora e que comece a cumprir suas responsabilidades o quanto antes. Dados os desafios relativos a recursos e tempo que ela enfrentará com de entrada em vigor da LGPD, a ANPD deveria elaborar uma estratégia baseada em resultados que priorizasse suas obrigações imediatas e de curto prazo, em particular oferecendo diretrizes e editando normas e regulamentação quando necessário. Também deve estabelecer uma abordagem de fiscalização regulatória de longo prazo que seja consistente com as abordagens regulatórias modernas.

Em caso de dúvidas sobre este artigo, ou informações adicionais, entre em contato com Giovanna Carloni, gcarloni@huntonAK.com; Matthew Starr, mstarr@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Laura Schertel Mendes, lsm@lauraschertel.com.br; e Danilo Doneda, danilo@doneda.net.

Apêndice – Mapeamento das Tarefas da ANPD sob a LGPD

Nota: manteve-se o texto original da LGPD quando possível.

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
Atividades relativas a diretrizes, recomendações, autorregulação da indústria		
55-J, I	Zelar pela proteção dos dados pessoais, nos termos da legislação	
55-J, II	Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei	
55-J, VIII	Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis	A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais (Art. 51)
55-J, X	Dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial	A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento (Art. 23, parágrafo 1)
55-J, XIII	Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei	A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais (Art. 4, parágrafo 3) A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (Art. 11, parágrafo 3) A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais (Art. 12, parágrafo 3)

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
		O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (Art. 13, parágrafo 3) O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (Art. 18, V) A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência (Art. 40) Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento (Art. 19, parágrafo 3) A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos (Art. 19, parágrafo 4) A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei (Art. 46, parágrafo 1) A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
		entidade ou o volume de operações de tratamento de dados (Art. 41, parágrafo 3) A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 (Art. 62) A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados (Art. 63) A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação [compartilhamento de dados de entidades públicas para organizações privadas] (Art. 27, parágrafo único) A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais (Art. 30)
55-J, XVIII	Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei	
55-J, XIX	Garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso)	
55-J, XX	Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos	

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
Atividades estratégicas		
55-J, III	Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade	
Atividades de fiscalização		
55-J, IV	Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso	A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (Art. 10, parágrafo 3) O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: determinação da autoridade nacional, quando houver violação ao disposto nesta Lei (Art. 15, IV) Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional [referentes a transferências de dados pessoais de entidades públicas para privadas] (Art. 26, parágrafo 2) A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei (Art. 27) O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Art. 48) Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
		ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei (Art. 50, parágrafo 2, II) A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (Art. 38) O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Art. 48) A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. (Art. 48, parágrafo 2) Estabelecer um procedimento administrativo de cumprimento, incluindo como calcular multas (Art. 52, parágrafos 1 e 4; Art. 53)
55-J, V	Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação	
55-J, XI	Solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei	A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei (Art. 29) Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação (Art. 31) A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público (Art. 32)

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
55-J, XVI	Realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público	Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (Art. 20, parágrafo 2)
55-J, XVII	Celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942	
Atividades educacionais		
55-J, VI	Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança	
55-J, VII	Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade	
Atividades relacionadas à coordenação e cooperação nacional e internacional		
55-J, IX	Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional	
55-J, XIV	Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento	Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório (Art. 55-J, parágrafo 2)
55-J, XXI	Comunicar às autoridades competentes as infrações penais das quais tiver conhecimento	
55-J, XXII	Comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal	
55-J, XXIII	Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação	A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados,

Artigo	Obrigações básicas da ANPD sob Art. 55-J	Atividades relacionadas descritas em outras disposições da LGPD
		conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei (Art. 55-J, parágrafo 3) A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD (Art. 55-J, parágrafo 4)
Atividades administrativas		
55-J, XII	Elaborar relatórios de gestão anuais acerca de suas atividades	
55-J, XXIV	Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei	
55-J, XV	Arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas	

Atividades adicionais da ANPD relacionadas a transferências internacionais de dados pessoais

- Autorizar transferências internacionais de dados pessoais submetidos à aprovação da ANPD (Art. 33, V e Art. 35, parágrafo 2)
- Avaliar o nível de adequação de entidades internacionais e terceiros países (Art. 33, I e Art. 34), inclusive quando exigido por organizações públicas ou controladores (Art. 33, parágrafo único).
- Determinar o conteúdo de cláusulas específicas e cláusulas contratuais padrão para transferências internacionais de dados pessoais, assim como BCRs (Regras Corporativas Vinculativas), selos, certificações e códigos de conduta (Art. 35)
- Designar órgãos responsáveis pelas certificações no contexto da transferência internacional de dados (Art. 35, parágrafo 3) e revisar suas atividades (Art. 35, parágrafo 4)
- Gerenciar notificações relativas a mudanças em mecanismos para salvaguardar transferências internacionais de dados (Art. 36)