# AGENDA PRIORITÁRIA DO FÓRUM – 2024

Pela Política Nacional de Proteção de Dados Pessoais e da Privacidade

O Fórum Empresarial da LGPD, que reúne mais de 100 entidades representativas dos mais diversos setores da economia brasileira, apresenta a sua **Agenda Prioritária para o ano de 2024.**

## 1) POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

A economia e os negócios atuais são inevitavelmente movidos a dados e algoritmos. Ou seja, dados pessoais são muito mais que o novo petróleo, muito mais que um mero insumo. Eles são a mola propulsora para os mais diversos mercados, mesmo nos setores mais tradicionais. É praticamente impossível falar em atividade econômica sem falar também em dados como grandes vetores de condições de mercado e de transações econômicas.

A competitividade das empresas dos mais diversos setores no Brasil é prejudicada por certo grau de insegurança jurídica sobre a regulamentação da proteção de dados pessoais, algo fundamental tendo em vista as mais variadas e necessárias atividades empresariais envolvendo o tratamento desses dados , como para prevenção à fraude, proteção ao crédito, marketing, comércio, e para o treinamento e desenvolvimento da inteligência artificial, incluindo o compartilhamento de dados entre entidades, públicas e privadas, e transferência internacional, por exemplo.

Porém, em que pese:

- A Lei Geral de Proteção de Dados (LGPD) ter sido sancionada em 14/08/2018 e estar em vigor desde 18/09/2020[1];
- A Autoridade Nacional de Proteção de Dados (ANPD) operar desde novembro de 2020;
- A LGPD prever que compete a ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPDPP), assim como ao Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política;

[1] Sanções administrativas desde 01/08/21.

- A Portaria ANPD 25/2022 ter previsto o início do processo regulatório em até 1 ano (fase 2) das Diretrizes para a PNPDPP, visando direcionar a atuação de todos os atores envolvidos no ecossistema de proteção de dados, inclusive a ANPD, considerando as demais políticas públicas publicadas, como a Estratégia Digital, o Plano Nacional de IoT, dentre outras;
- O Planejamento Estratégico da ANPD (2021-2023), aprovado pelo Conselho Diretor em janeiro de 2021, prever em seu mapa estratégico estabelecer ambiente normativo eficaz para a proteção de dados pessoais,

A ANPD publicou, no dia 29 de dezembro de 2023, a primeira revisão da Agenda Regulatória para o Biênio 2023-2024. O seu item 15, que justamente contempla as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, passou da Fase 2 para a Fase 4. Ou seja, o início do seu processo regulatório deve ocorrer somente até dezembro de 2024.

A mudança no item 15, conforme a ANPD, foi necessária para viabilizar a participação dos futuros membros da segunda composição do CNPD, órgão consultivo da ANPD, e que desempenha papel importante na elaboração das diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Ocorre que o Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) está inoperante, aguardando que sejam nomeados seus novos integrantes, conforme lista tríplice já apresentada pela ANPD.

O Fórum defende, com urgência, a criação de um Plano de Nação para Dados no Brasil, por meio da Política Nacional de Proteção de Dados Pessoais e da Privacidade, de forma a gerar segurança jurídica mediante a visão clara da perspectiva brasileira sobre o tema. Para tal finalidade, defendemos:

1) O fortalecimento da ANPD para dar efetividade à sua agenda regulatória de forma mais célere, incluindo por meio da consolidação da sua centralidade nas questões referentes ao tratamento de dados pessoais;
2) A nomeação dos novos integrantes do Conselho Nacional de Proteção de Dados Pessoais e Privacidade;
3) O imediato início dos trabalhos para o estabelecimento das diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

## 2) ATUAÇÃO RESPONSIVA DA ANPD E CAUTELA NA PUBLICIZAÇÃO PRECOCE DE PROCEDIMENTOS DE FISCALIZAÇÃO AINDA EM ANDAMENTO

A premissa da LGPD e do processo de fiscalização consiste na atuação responsiva da ANPD, com a adoção de medidas proporcionais ao risco identificado e à postura dos agentes regulados.

Desse modo, com a regulamentação da dosimetria e o início das sanções administrativas, é fundamental ressaltar os seguintes pontos de atuação da ANPD em seu processo fiscalizatório (conforme Resolução 01/2021 CD/ANPD):

- Exigência de mínima intervenção na imposição de condicionantes administrativas;
- Fiscalização baseada em evidências e riscos regulatórios;
- Estímulo à conciliação direta entre as partes e priorização da resolução do problema;
- Incentivo à responsabilização e prestação de contas;
- Mecanismos de transparência, retroalimentação e autorregulação.

Entretanto, é extremamente preocupante a publicização na mídia de notas técnicas e menções a nomes de empresas envolvidas em procedimentos administrativos ainda em trâmite, sem decisão final irrecorrível pela ANPD.

Sabemos e compreendemos a importância de a ANPD dar transparência e informar a sociedade sobre o seu trabalho realizado e sobre os resultados alcançados na fiscalização e aplicação da LGPD.

Porém, a divulgação precoce de notas técnicas de procedimentos ainda sem conclusão e dos nomes das empresas envolvidas em processos preparatórios ou sancionatórios pode causar danos irreparáveis à reputação das organizações, prejudicando seu funcionamento e afetando negativamente sua relação com clientes (titulares de dados) e parceiros de negócios, especialmente ponderando que já há casos concretos em que empresas foram prejudicadas devido a essa exposição pública ocorrida antes da conclusão do processo.

Importante lembrar que o procedimento preparatório serve para a Coordenação Geral de Fiscalização realizar averiguações preliminares, quando os indícios da prática de infração não forem suficientes para a instauração imediata de processo administrativo sancionador.

Mesmo no caso do procedimento sancionador, ainda não há conclusão de mérito sobre a conduta do agente de tratamento, pois eventual auto

de infração enunciará suposta conduta ilícita imputada ao autuado, com a indicação dos fatos a serem apurados e do dispositivo legal ou regulamentar relacionado à suposta infração.

Nesse sentido, sugerimos que a ANPD pondere a possibilidade de divulgação de informações em formato estatístico ou agregado. Isso permitirá uma visão geral dos avanços e desafios enfrentados na proteção de dados, sem comprometer a reputação de empresas envolvidas em processos em andamento, os quais podem ter diversos desfechos, inclusive a ausência de sanção.

Caso contrário, a publicização precoce pode gerar estigma desnecessário e injusto, comprometendo a confiança no ambiente empresarial.

## 3) AGENDA REGULATÓRIA - CONCLUSÃO DOS TEMAS INICIADOS

Há muitos temas abertos na agenda regulatória da ANPD que carecem de conclusão para trazer maior segurança jurídica ao mercado. São eles:

- Transferência internacional de dados baseada em mecanismos flexíveis que tenham interoperabilidade com sistemas adotados em outras jurisdições, além de selos e certificações;
- Hipóteses legais de tratamento de dados pessoais;
- Relatório de Impacto à Proteção de Dados Pessoais;
- Comunicação de incidentes e especificação do prazo para notificações;
- Regulamento sobre Encarregado de Dados

Reitera-se, nesse ponto, que é essencial o fortalecimento da ANPD para que consiga dar vasão e cumpra os prazos previstos nas agendas regulatórias, de modo a promover segurança jurídica e previsibilidade para os agentes de tratamento e titulares de dados quanto aos diversos temas pendentes de normatização no âmbito da proteção de dados pessoais.

## 4) CÓDIGOS DE CONDUTA SETORIAIS E CORREGULAÇÃO

Seguindo a tradição europeia, o Brasil introduziu a possibilidade de coprodução normativa em proteção de dados. O artigo 50 da LGPD elenca diversos elementos e balizas para o instituto. Em seu §3,

estabelece que regras de boas práticas e de governança poderão ser reconhecidas e divulgadas pela ANPD.

A dinâmica da era digital exige regulações versáteis que proporcionem e fomentem, equilibradamente, segurança jurídica para os agentes econômicos e proteção de direitos e garantias individuais. Especialmente em legislações de proteção de dados pessoais, códigos de conduta setoriais e órgãos privados de monitoramento (estes, embora não previstos pela LGPD, também não foram por ela vedados), que podem ser reconhecidos por autoridades públicas, também representam importantes instrumentos regulatórios, de forma a absorver melhor incertezas e desenvolver parâmetros consolidados de eficácia legal mediante a atuação de organizações especializadas nas práticas do seu respectivo setor.

Nesse sentido, visando propor parâmetros e proporcionar maior segurança jurídica, alguns setores já lançaram ou estão em fase de elaboração dos seus códigos de conduta ou guias de boas práticas:

- Associação Brasileira das Empresas de Softwares (ABES) – publicado.
  Confederação Nacional da Saúde (CNSaúde) – publicado e em fase de atualização com operadoras.
- Confederação Nacional dos Dirigentes Lojistas - em elaboração
- Federação Brasileira de Bancos (Febraban) – publicado.
- Federação das Empresas de Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP). – publicado.
- Sindicato Nacional das Empresas de Telefonia e de Serviço Celular, Móvel e Pessoal (Conexis Brasil) - publicado.
- Zetta – publicado.
- Associação Nacional dos Bureaus de Crédito (ANBC) – não publicado – uso interno.

## 5) EDUCAÇÃO E LETRAMENTO

Apesar dos avanços nos últimos anos, é permanente a necessidade do Brasil em caminhar rumo ao estabelecimento de uma sólida cultura e conscientização de proteção de dados. Para tanto, a conscientização e a orientação da ANPD aos diversos agentes envolvidos acerca de medidas e parâmetros para o tratamento lícito e responsável dos dados pessoais é imprescindível.

Desde início, é preciso que os titulares de dados conheçam seus direitos e sejam orientados a exercê-los diretamente junto aos controladores e, uma vez não atendidos, nos termos da LGPD, busquem meios alternativos de solução de conflitos.

Estimular que o Poder Judiciário seja acionado nos casos de pretensão resistida, e não ser balcão de reclamações para toda e qualquer controvérsia envolvendo dados pessoais, é salutar para todos: titulares de dados, agentes de tratamento e Estado.

Importante atentar-se ao risco de sobrecarga de demandas no Poder Judiciário, ainda mais as de caráter repetitivo, sobre possíveis violações de dados pessoais. Tal risco pode se tornar ainda maior caso venha a ser adotada a teoria do dano moral *in re ipsa* (presumido), o que entendemos não ser o mais adequado.

Portanto, um caminho para que se evite referida judicialização é a transparência e a conscientização perante os titulares de dados sobre como os seus dados pessoais são tratados, esclarecendo e demonstrando que pode ser mais benéfico para a resolução de seus problemas procurar diretamente o controlador dos dados.

Inclusive, a própria LGPD dispõe que vazamentos individuais ou de acessos não autorizados poderão ser objeto de conciliação direta entre controlador e titular e, somente caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata esta previsão.

Interessante haver também mecanismos próprios da ANPD para conciliação direta entre as partes e priorização da resolução do problema, como por exemplo ocorre nas relações de consumidor, via Consumidor.gov.br, do Ministério da Justiça, para a proteção dos direitos dos titulares de dados pessoais quando envolver relação de consumo.

Por fim, nos termos do art. 55-J, VI, da LGPD, ressalta-se a necessidade da contínua promoção do conhecimento das normas e das políticas públicas sobre proteção de dados pessoais por meio de debates com acadêmicos, sociedade civil, setor empresarial, ANPD e o Poder Judiciário sobre o tema, bem como com a veiculação de propagandas educativas, a exemplo do efetuado pela União Europeia, e a promoção e incentivo de educação digital, inclusive nas escolas desde o ensino fundamental.

Estabelecer o diálogo entre estes atores beneficia e ajuda a consolidar a cultura de proteção de dados pessoais no Brasil.

Inclusive, esse deveria ser o eixo central da futura Política Nacional de Proteção de Dados Pessoais.

## 6) SEGURANÇA CIBERNÉTICA

Ameaças cibernéticas representam risco contínuo e crescente para empresas, investidores, clientes e nações. O tema vai muito além da proteção de dados pessoais e segredos de negócios corporativos, pois ataques cibernéticos podem prejudicar as operações de organizações e países. Os incidentes e o modelo de operação dos criminosos são cada vez mais complexos, transnacionais, profissionais, constantes e com potencial lesivo devastador.
Por todos esses motivos, diversos países estão se mobilizando sobre o tema: em dezembro de 2022, o Reino Unido atualizou sua Estratégia Nacional de Cibersegurança; em dezembro de 2022, o Parlamento Europeu publicou uma nova diretiva de cibersegurança para a União Europeia; em março de 2023, os EUA publicaram sua nova Estratégia Nacional de Cibersegurança.

Apenas em 2020 o Brasil apresentou sua Estratégia Nacional de Segurança Cibernética (e-Ciber), mas não alocou responsabilidades para as ações nela propostas.

No dia 26 de dezembro de 2023, o presidente Lula assinou decreto estabelecendo a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

Na medida em que as organizações brasileiras avançam na sua transformação digital, também aceleram o seu comprometimento com a segurança da informação e a segurança cibernética.

Proteger o espaço cibernético e fortalecer as capacidades de respostas contra ameaças cibernéticas requer a continuidade de políticas e ações conjuntas que maximizem os esforços em prol de um espaço cibernético mais seguro e resiliente, e que garanta à sociedade a confiança na interação com o ambiente digital.

Nesse sentido, reconhecemos que o uso intensivo das tecnologias digitais, como soluções de computação em nuvem, IA, dentre outras, são fundamentais para que tal segurança seja proporcionada.

Adicionalmente, é imprescindível o estímulo à cooperação internacional, com intuito de posicionar o Brasil globalmente na discussão com iniciativas voltadas ao intercâmbio de boas práticas internacionais e ao incentivo à cooperação jurídica. A ratificação do Brasil à Convenção de Budapeste Contra Crimes Cibernéticos materializa esse esforço, que pode ser complementado com a adesão à iniciativa internacional Paris *Call*.

Nesse sentido, pretendemos engajar na agenda de defesa cibernética em 2024, com foco em alguns itens que consideramos estratégicos para o país, a saber:

- Implementação de uma Política Nacional de Segurança Cibernética voluntária e colaborativa: defendemos a urgência na execução da Política Nacional de Cibersegurança, que busque a qualificação dos dados públicos, que dialogue com as diferentes esferas da União, que tenha regras definidas colaborativamente com a sociedade, em especial o setor privado, e que sejam entendidas como diretrizes para que se avance a maturidade e a resiliência da economia digital brasileira, permitindo desenvolvimento confiável da nova economia, otimização de recursos públicos através de parcerias público-privadas, visando melhorar os indicadores internacionais para o Brasil;

- Adoção de políticas públicas e incentivos para a qualificação de mão de obra em segurança cibernética: É urgente que tenhamos uma política especial para ampliar e acelerar programas de capacitação, educação e formação em cibersegurança, com propostas voltadas à disseminação na rede pública e privada de ensino, privilegiando o ensino básico, médio e técnico, incorporando-os à grade curricular.. Esse tem sido um grande gargalo para que empresas de todos os setores avancem na implementação de tecnologias e práticas de segurança cibernética;

- Programa nacional de conscientização: É fundamental o estabelecimento de um amplo programa nacional de conscientização da população e das organizações em relação ao espaço cibernético e sobre boas práticas de proteção de dados, privacidade, assim como de resiliência, permitindo acelerar o desenvolvimento de competências nacionais nas áreas de segurança cibernética. Cada vez mais, a educação em torno da proteção de dados e da privacidade se torna um elemento indissociável à educação em segurança, prevenção e mitigação de riscos cibernéticos.

## 7) INTELIGÊNCIA ARTIFICIAL

O Fórum defende a adoção de amplas políticas públicas para a promoção segura e inclusiva da inteligência artificial. Junto às entidades empresariais e à comunidade, trabalhamos o desenvolvimento e o uso responsável da IA de forma ética e transparente, com o compromisso de atenuação de potenciais riscos e vieses. Participamos amplamente do debate regulatório no país e

acreditamos que ainda é necessária uma ampla discussão nacional para amadurecer a posição da sociedade brasileira sobre eventual regulação da IA.

A IA tem caráter instrumental e representa uma grande revolução tecnológica mundial, como uma tecnologia de propósito geral. Também defendemos que temas como alocação de deveres e responsabilidade civil, governança adequada, e outros aspectos regulatórios sejam amplamente cobertos pelas legislações e instituições já vigentes no país para que a futura regulação de IA seja objetiva, complementar e harmônica ao ordenamento jurídico brasileiro, especialmente em relação à LGPD, considerando que muitas aplicações de IA dependem do tratamento de dados pessoais.

Diferentes modelos regulatórios da IA estão em debate em vários países, inclusive em relação a pontos nevrálgicos sobre o tema, como a própria definição da tecnologia em escopo, das estruturas de gestão de risco e o papel da autorregulação.

Atualmente, há dois principais modelos de regulação da IA em discussão no Congresso Nacional. Em uma direção, o texto debatido e aprovado na Câmara dos Deputados tem estrutura contextual, principiológica e evolutiva, que privilegia a regulação setorial, com direitos e obrigações condizentes com os riscos efetivamente verificados no uso da IA. O outro, decorrente do relatório elaborado por uma comissão de juristas do Senado Federal, tem forte inspiração no modelo proposto (e ainda não adotado) pela União Europeia (UE), com estrutura rígida, pré-classificação de risco e sem análise de impacto regulatório para avaliar o potencial de desestímulo à inovação e competividade.

Além disso, o nível de adoção da IA pela sociedade brasileira, em especial pelos diferentes setores produtivos, incluindo o Estado, ainda é muito baixo, e diante disso é preciso que esses atores passem a ter amplo conhecimento da tecnologia e dos potenciais riscos de uma proposta legislativa. Os riscos de médio e de longo prazo para a inovação e a competitividade brasileira postos por uma legislação prematura são muito maiores do que os eventuais benefícios de curto prazo.

Encorajamos o Brasil a seguir acompanhando de perto e contribuindo com frutíferas iniciativas globais para melhores práticas para a IA, como as lideradas pelo G7, pela OCDE e pela ISO.

É muito importante que o país não fique parado e busque um alinhamento internacional às melhores práticas de governança de IA pelas organizações, assim como para mitigações de risco.

## 8) SOBERANIA DIGITAL COMPETITIVA

A popularização da IA em 2023 evidenciou a relevância da transformação digital para o desenvolvimento econômico e social brasileiro, assim como para a competitividade das nossas organizações no mercado global. Face a esse cenário, defendemos que o país tenha uma efetiva estratégia para a promoção da soberania digital competitiva:

- Que permita às organizações brasileiras terem acesso às novas tecnologias produzidas no país ou no exterior: a inovação hoje em dia ocorre em uma velocidade estrondosa, em especial no que tange à das novas tecnologias digitais. É importante que as nossas empresas tenham acesso livre e facilitado às mais inovadoras e disruptivas tecnologias que estão sendo desenvolvidas e ofertadas a partir de outras jurisdições. Nesse sentido, medidas unilaterais que restrinjam o armazenamento ou o processamento de dados no exterior por organizações locais vão na contramão e prejudicam a competitividade das nossas organizações.

- Que possibilite a integração às cadeias globais de valor cada vez mais digitalizadas por meio da busca ativa por convergência regulatória com mercados estratégicos: com o progressivo avanço da economia digital global abrem-se grandes oportunidades para empresas locais, novas ou tradicionais. Integrar-se nessas novas cadeias globais de valor, seja ofertando um novo serviço digital ou integrando serviços digitais a um produto, passa a ser uma oportunidade para nossas organizações se desenvolverem e manterem competitivas no mercado global. É relevante, para tanto, que tenhamos políticas públicas ativas para a convergência regulatória com mercados estratégicos. Entre elas, lembramos:

    - Da relevância da regulamentação e convergência das bases legais para transferência internacional de dados;
    - Da necessidade de ambiciosos compromissos para a construção de capítulos sobre comércio eletrônico nos acordos comerciais;
    - Da busca por convergência regulatória com legislações em torno de segurança cibernética, computação em nuvem e inteligência artificial.

- Que facilite o acesso e reduza o custo de processamento de dados para atividades de pesquisa e desenvolvimento de modelos computacionais por empresas locais: é sabido que o

desenvolvimento e a calibragem de modelos computacionais sofisticados, em especial os de IA generativa ou os modelos fundacionais, dependem de altíssima capacidade de processamento de dados. Defendemos que o governo brasileiro tenha um plano para a ampliação do parque de centro de processamento de dados no país, assim como tenha políticas públicas para a redução do custo do processamento de dados para atividades de pesquisa e desenvolvimento por organizações locais;

- Que tenha política públicas de estímulo ao desenvolvimento de modelos computacionais em língua portuguesa brasileira, assim como a partir de bases de dados ligadas a setores nos quais o Brasil é competitivo ou demanda uma atenção especial: biodiversidade, extração mineral e vegetal, agropecuária, saúde pública, educação, logística e transportes, entre outros.

**Sobre o Fórum Empresarial LGPD**

O Fórum foi criado por um amplo grupo de entidades empresariais, que se reúnem desde 2020, para ações de promoção de segurança jurídica na aplicação da LGPD e de avanço da cultura da proteção de dados e da privacidade no país. Em outubro de 2021, esse grupo decidiu criar o Fórum a partir de uma política de governança estabelecida, sendo uma coalizão empresarial multissetorial, apartidária e sem personalidade jurídica própria formada por entidades, associações e confederações empresariais.

Desde o início, o Fórum LGPD foi protagonista de importantes iniciativas e políticas públicas para o aprimoramento da segurança jurídica e da cultura da privacidade no Brasil, entre elas, a criação da ANPD, a elevação de proteção de dados pessoais a um direito constitucional e atividade exclusiva da União e a independência da ANPD. O Fórum também tem sido um ativo ator nos temas de regulamentação da LGPD, assim como na promoção de eventos e documentos orientadores para aprimorar a segurança jurídica e a cultura da privacidade no Brasil.

Para mais informações, consultar:
https://abessoftware.com.br/forumLGPD/.

FÓRUM EMPRESARIAL LGPD

**Entidades signatárias, em ordem alfabética:**

ABES - Associação Brasileira das Empresas de Software

ABRACLOUD - Associação de Hosting do Brasil

ABRAMGE - Associação Brasileira de Planos de Saúde

ABRANET - Associação Brasileira de Internet

ABRAPP - Associação Brasileira das Entidades Fechadas de Previdência Complementar

ABIMAQ/SINDIMAQ - Associação Brasileira da Indústria de Máquinas / Sindicato Nacional da Indústria de Máquinas

ABINEE - Associação Brasileira da Indústria Elétrica e Eletrônica

ANBI - Associação Nacional de Bureaus de Informação

ANBC - Associação Nacional dos Bureaus de Crédito

ANUP - Associação Nacional das Universidades Particulares

CNDL - Confederação Nacional de Dirigentes Lojistas

Conexis Brasil Digital

FecomercioSP - Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo

IBDEE - Instituto Brasileiro de Direito e Ética Empresarial

ICOLAB - Instituto de Colaboração em Blockchain

MBC - Movimento Brasil Competitivo

MID - Movimento Inovação Digital

SINOG - Associação Brasileira de Planos Odontológicos

Zetta

FÓRUM EMPRESARIAL LGPD

São Paulo, 20 de fevereiro de 2024.

**Atenciosamente,**

Secretário-executivo: Rony Vainzof - FecomercioSP
Secretário-executivo adjunto: Andrei Gutierrez - ABES
Diretor de articulação: Thômaz Corte Real – ABES
Diretora de articulação: Mariana Castro – ABES
Secretariado: FecomercioSP e ABES