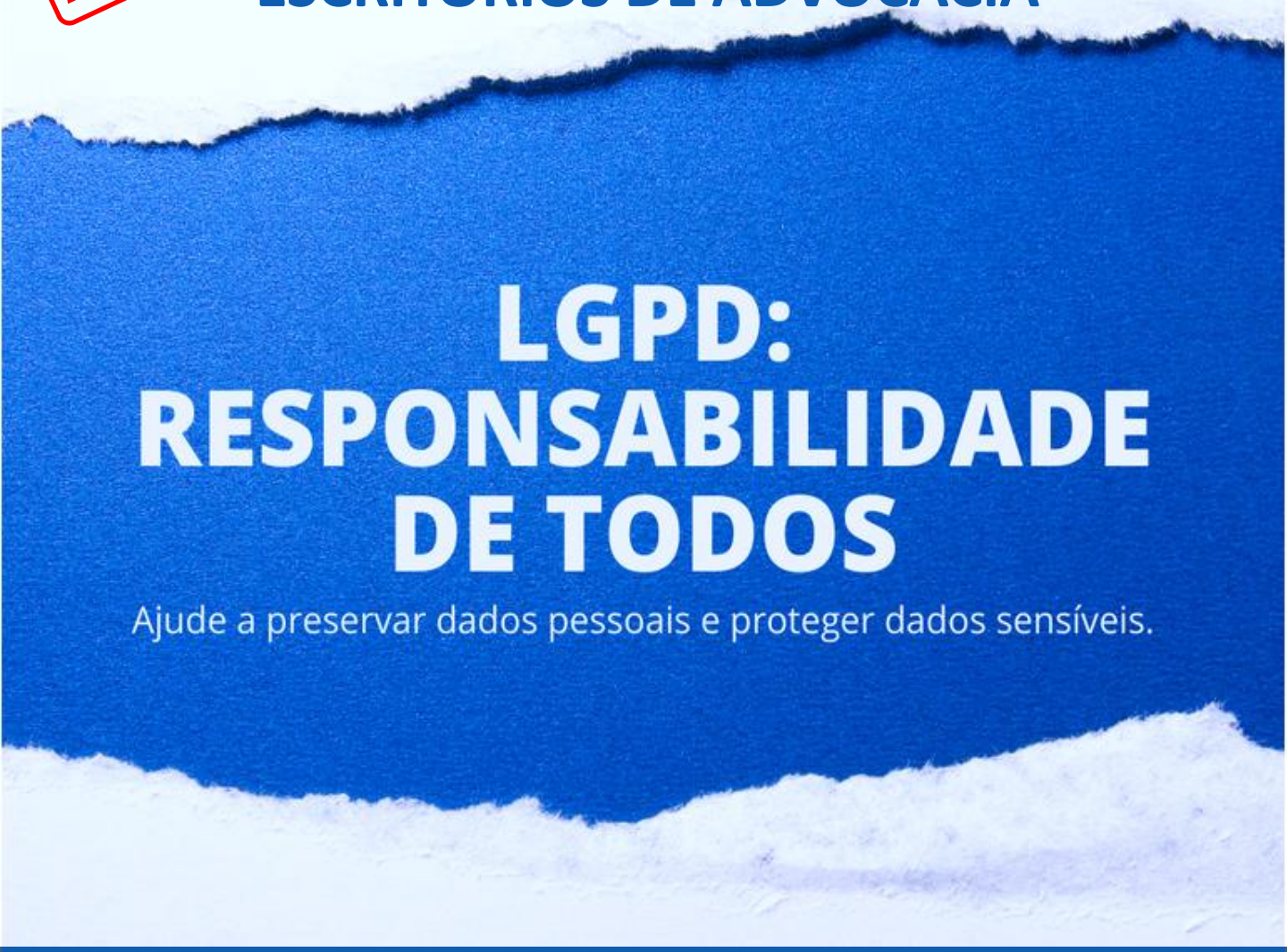
OAB SÃO PAULO
Subseção Campinas

2ª EDIÇÃO

Guia LGPD Aplicada aos ESCRITÓRIOS DE ADVOCACIA



COMISSÃO DE DIREITO À PRIVACIDADE
E PROTEÇÃO DE DADOS PESSOAIS
OAB CAMPINAS

2024

Dados Internacionais de Catalogação na Publicação (CIP)

Guia LGPD aplicada aos escritórios de advocacia 2024 [livro eletrônico]: LGPD responsabilidade de todos: Comissão de Direito à Privacidade e Proteção de Dados Pessoais / coordenação geral Valéria Reani Rodrigues Garcia, Manuel David Rodrigues Masseno. -- 2. ed. - Campinas, SP : Ordem dos Advogados do Brasil. 3ª. Subseção Campinas, 2024.

Presidência OAB. 3ª. Subseção Campinas: Luciana Freitas
Formato: PDF
ISBN: 978-65-984342-0-5

1. Proteção de dados pessoais - Brasil. 2. Brasil. Lei geral de proteção de dados Pessoais (2018). I. Garcia, Valéria Reani Rodrigues. II. Masseno, Manuel David Rodrigues. II. Título.

CDD- 341.27

Sueli Costa - Bibliotecária - CRB-8/5213

(SC Assessoria Editorial, SP, Brasil)

Índices para catálogo sistemático:

1. Lei geral de proteção de dados pessoais 341.27

Diretores da Revista Guia 2ª Edição OAB Campinas

Valéria Reani Rodrigues Garcia – Presidente da Comissão de Direito à Privacidade e Proteção de Dados Pessoais (CDPPDP)
Orestes Bacchetti Júnior – Vice- Presidente da Comissão de Direito à Privacidade e Proteção de Dados Pessoais
Aline Andrietta – 1ª Secretária da Comissão de Direito à Privacidade e Proteção de Dados Pessoais
Spencer A. C. de Almeida – 2º Secretário da Comissão de Direito à Privacidade e Proteção de Dados Pessoais

Coordenação Geral
Valéria Reani Rodrigues Garcia

Comissão Técnica Científica e Revisão
Valéria Reani Rodrigues Garcia
Manuel David Rodrigues Masseno - Membro Consultor Internacional da Comissão de Direito à Privacidade e Proteção de Dados Pessoais

Suporte referência e levantamento sistemático dos Atos da ANPD
Anna Carolina de Medeiros Silva e Gabriela Marangoni - Membros Efetivos da Comissão de Direito à Privacidade e Proteção de Dados Pessoais

Autores da Comissão de Direito à Privacidade e Proteção de Dados Pessoais

Adriana Senna Pessoto Garibe
Aline Andrietta
Ana Cristina da Costa Elias Olivari
Ana Paula Silva de Oliveira
Anna Carolina de Medeiros Silva
Beatriz de Andrade Junque
Beatriz Pistarini de Souza
Camilla Jimene
Carlos Alberto Casanova Campos
Cecília Rezende de Freitas
Gabriela Marangoni
Henrique Fabretti
Isadora Coimbra Diniz
Marcelo Vieira de Menezes
Marcelo Pereira Fujita
Marcela Fuga Antunes Cardoso
Maria Laura Zoéga
Mirian Barreta Palla
Nathália Guerra de Sousa
Orestes Bacchetti Junior
Raquel Helena Rinaldi Maciel
Renata Lima de Mattos Rocha
Renata Proximo da Silva
Rodrigo Carvalho e Silva Canguçu de Almeida
Roseli Gomes Martins
Sérgio Antônio Pohlmann
Sylvio Sobreira Vieira
Valéria Reani Rodrigues Garcia

Autora Convidada
Angelina Teixeira

Editoração
Miriam Bizarro

Suporte Editorial
Valéria Reani Rodrigues Garcia
Gabriela Marangoni

Sobre os Autores do Guia da 1ª e 2ª EDIÇÃO Guia LGPD Aplicada aos ESCRITÓRIOS DE ADVOCACIA 2024

Adriana Senna Pessoto Garibe - Advogada coordenadora da área de Direito Digital do Lemos Advocacia para Negócios; Bacharel em Direito pela PUC-Campinas; Pós-graduanda em Direito Digital e Proteção de Dados pelo EBRADI; com certificação EXIN PDPF e Certificação EXIN PDPP.

Aline Andrietta - Advogada especializada em direito condominial, proteção de dados (LGPD) e consultoria empresarial, com foco no Terceiro Setor; assessora juridicamente OSC's, focando em conformidade legal e desenvolvimento sustentável.

Ana Cristina da Costa Elias Olivari – Advogada, Especialista em Direito Empresarial e *Compliance* Trabalhista pela EMD; Especialista em Direito e Processo do Trabalho pela PUC-Campinas, Diplomada *en Derecho Digital* pela Universidade Anáhuac (México).

Anna Carolina de Medeiros Silva – Advogada; Especialista em Direito Digital, *Compliance*, Proteção de Dados, em Processo Civil e em Direito de Família e Sucessões; com certificação EXIX como *Data Protection Officer*.

Angelina Teixeira – Advogada, em Portugal; Licenciada [Graduada] em Direito e Pós-Graduada em Direito da Contratação Pública Prática pela Universidade Católica Portuguesa (Porto); Especialista em Direito do Ordenamento, do Urbanismo e do Ambiente pela Faculdade de Direito da Universidade de Coimbra; Mestre em Direito Administrativo pela Faculdade de Direito da Universidade do Porto; Doutoranda em Ciências Jurídico-Públicas na Universidade do Minho; Formadora acreditada pelo Instituto do Emprego e Formação Profissional, de Portugal.

Beatriz de Andrade Junque - Advogada; Bacharel em Direito pela PUC-Campinas; Especialista em Direito Digital e *Compliance* pelo IBMEC - São Paulo; Presidente da Comissão de Direito Digital da OAB Indaiatuba; Cofundadora do Grupo de Estudos de Direito Digital (GEDD) da PUC- Campinas.

Beatriz Pistarini de Souzas– Advogada; Bacharel em Direito pela PUC-Campinas; Especialista em Direito Digital e *Compliance* pelo IBMEC-São Paulo; Cofundadora do Grupo de Estudos de Direito Digital (GEDD) da PUC-Campinas.

Camilla do Vale Jimene – Advogada; Professora especializada em Direito Digital na LEC/EPD/MACKENZIE e PECE-USP; Reconhecida pelo *ranking* Análise Advocacia Mulher, por quatro anos consecutivos (2021, 2022, 2023 e 2024), como a advogada mais admirada do país na especialidade de Digital.

Carlos Alberto Casanova Campos – Advogado; Especialista em Direito Digital e *Compliance* pela EPD, em Direito Civil e Direito Processual Civil e em Direito Empresarial pela PUC-Campinas.

Cecília Rezende de Freitas – Advogada especialista em Privacidade e Proteção de Dados Pessoais; Especialista em Direito Contratual pela PUC/COGEAE e em Direito Societário pela FGV-GVLAW;

Gabriela Marangoni – Advogada; Bacharel pela PUC-Campinas; Especialista em Direito Contratual, *Compliance* e em Privacidade e Proteção de Dados Pessoais.

Henrique Fabretti Moraes– Advogado; Sócio do Opice Blum Advogados; Líder das práticas de proteção de dados e inteligência artificial; reconhecido como FIP; Certificado pelo IAPP em CIPM, CIPP/E, CIPT e CDPO/BR, no qual também é membro do *Research Advisory Board*.

Isadora Coimbra Diniz - Advogada especialista da área de *Compliance* da Finocchio & Ustra, Sociedade de Advogados; reconhecida nas especialidades de *Compliance* e nos setores económicos, automotivo e autopeças, química e petroquímica.

Marcela Fuga Antunes Cardoso – Advogada; Pós-Graduada em Direito Digital e *Compliance* pela Faculdade IBMEC/São Paulo, em Direito Processual Civil pela EPD; Gestora de Privacidade pela TI EXAMES; Cursando MBA em Gestão do Direito nas Empresas pela FUNDACE/USP.

Marcelo Fujita - Bacharel em Direito; Pós-graduado em Direito Constitucional Aplicado – Faculdade de Ciências Aplicada; Escola de Extensão da UNICAMP; Tecnólogo em Redes de Computadores.

Marcelo Vieira de Menezes – Bacharel em Processamento de Dados pela UNIT – Universidade Tiradentes; MBA em *Cybersecurity* e *Cybercrimes* e em Gestão e Governança de Tecnologia da Informação pela Anhanguera.

Manuel David Masseno- Professor Adjunto do Instituto Politécnico de Beja, em Portugal, no qual é Encarregado da Proteção de Dados e pertence à Coordenação do Laboratório UbiNET - Segurança Informática e Cibercrime.

Mírian Barreta Palla - Advogada; Graduada em Direito pela UNESP; Especializada em Direito Marítimo e Portuário pela UNISANTOS e em Direito Civil e Processo Civil pela UNIARARAS; mestranda na área de Meio Ambiente pela Faculdade de Tecnologia da UNICAMP.

Nathália Guerra de Sousa - Advogada especialista em Privacidade e Proteção de Dados Pessoais; Especialista em Direito Médico e em Direito Digital e *Compliance*; Certificada CDPO/BR e CIPM pela IAPP; Sócia da Sanatti Consultoria.

Orestes Bacchetti Junior – Advogado; Bacharel em Direito pela Universidade São Francisco - USF; Pós-graduado em Direito Empresarial; Especializado em Direito Imobiliário.

Renata Lima de Mattos Rocha – Advogada especialista em Proteção de Dados; Especialista em Direito Empresarial pela FGV; certificada como *DPO* pela PUC-Campinas; *Compliance Officer* pela LEC.

Renata Proximo da Silva - Advogada especializada em direito do trabalho relações do trabalho, *compliance* e privacidade e proteção de dados.

Rodrigo Canguçu de Almeida – Advogado; Especialista em Direito Empresarial pela EPD e Especialista em Direito Digital e Proteção de Dados pela EBD.

Raquel Elena Rinaldi Maciel – Advogada; Diretora Executiva da **govDADOS**, Ceo e *founder* da EXPERIENCE DATA; especialista em Direito Digital pela Universidade de Genebra e Doutora em Direito pela UERJ; consultora em proteção de dados e privacidade.

Roseli Gomes Martins **–** Advogada, na área de atuação de Direito do Trabalho**;** Diretora da Associação dos Advogados Trabalhistas de Santos**;** Presidente da Comissão de Direito Digital, Privacidade e Proteção de Dados da OAB/Praia Grande.

Sergio Antonio Pohlmann - Cientista da Computação; CISSP, CCSP, CSSLP, SSCP, CGRC, CCISO; Consultor e Instrutor de Segurança da Informação, autor de livros de Tecnologia e LGPD.

Sylvio Sobreira Vieira - CEO da SVX *Corporate*; Especialista em governança; gerenciamento privacidade e proteção de dados; especialização pela *University of Pennsylvania* em *Privacy Law and Data Protection*; Membro Executivo da Academia Europeia da Alta Gestão e da IAPP; gestor de processos de Inovação, Transformação Digital, Governança e Conformidade.

Valéria Reani Rodrigues Garcia - Advogada sênior; Escritora; Professora; **Mestre LLM Proteção de Dados - LGPD e GDPR NA** Fundação Ministério Público em parceria com Universidade De Direito Lisboa-2023; *Lead Implementer for Data Privacy Protection* pela ABNT ISO/IEC 27701 Certificada em Direito Europeu de Dados Pessoais e Certificada em Governança de Dados e Inteligência Artificial pela Universidade de Sorbonne, Paris em parceria com a CNIL - Agência Francesa de Proteção de dados, em 2024; Certificada *ECOMPLY* Gestão de dados; Certificada na Escola de Governança Internet EGI do Comitê Gestor Da Internet CGI e nic.br 2023; mãe e avó.

MENSAGEM DA DIRETORIA

O ordenamento jurídico brasileiro referente à proteção de dados pessoais é regido pela Lei Federal nº 13.709, de 14 de agosto de 2018, conhecida como **Lei Geral de Dados Pessoais** (**LGPD**). Essa legislação representa um marco significativo na regulamentação abrangente produzida, embora também suscite incertezas em relação à sua aplicação.

A **LGPD** impacta a operação de todas as empresas, independentemente do porte - sejam elas pequenas, médias ou grandes - que lidam com informações pessoais. Isso inclui também os escritórios de advocacia, desde os empreendimentos individuais até os grandes escritórios que atuam em diversas regiões do país. Com o objetivo de preservar e proteger a prática da advocacia, a **OAB Campinas** busca orientar os profissionais do Direito à luz da nova legislação.

Portanto, é essencial estabelecer e aprimorar de forma contínua uma cultura de integridade e proteção dos direitos dos titulares de dados pessoais sob a responsabilidade dos advogados. Isso requer uma reflexão de toda a classe e dos escritórios de advocacia, desde as instâncias superiores e o planejamento estratégico, passando pelas soluções tecnológicas empregadas, até as atividades mais cotidianas que envolvem o comportamento de cada membro da equipe do escritório.

Diante desse panorama e reconhecendo a relevância da implementação e evolução contínua de uma cultura de integridade e proteção dos direitos dos titulares de dados pessoais sob a guarda dos advogados, a **OAB Campinas** lança a **2ª Edição do Guia informativo**. Este material reafirma o compromisso da instituição com todos os advogados e advogadas, não apenas de Campinas, mas também de outras regiões, visando disseminar o conhecimento e abordar todos os aspectos relacionados à cultura da privacidade, a fim de desempenhar seu papel de segurança jurídica em prol da advocacia.

Para elaborar a 2ª Edição, a **OAB Campinas** contou com o trabalho realizado pela **CDPPDP - Comissão de Direito à Privacidade e Proteção de Dados Pessoais**. O objetivo desta Edição é, sobretudo, atualizar e trazer material novo, para atender às prioridades a serem adotadas nos escritórios de advocacia no que diz respeito à proteção de dados pessoais. Espera-se que a sua consulta seja útil e esclarecedora no contexto das mudanças e desafios enfrentados pelo setor de serviços jurídicos em relação à implementação das conformidades previstas na **LGPD.**

Desejamos a todos uma excelente leitura!

Luciana Freitas
Presidente da OAB Campinas

APRESENTAÇÃO

Com o advento da **LGPD**, a transparência, como um princípio básico, tornou-se ainda mais premente para as organizações que lidam com os dados pessoais dos seus clientes, fornecedores e colaboradores. Nesta Nova Era Tecnológica, o que parecia ser trivial deve agora ser encarado com um especial cuidado, também e até sobretudo pela Advocacia. Afinal, a percepção dos dados pessoais como um ativo de valor intangível e de seu adequado tratamento como um Direito Fundamental ganhou dimensão e forma, mais ainda com sua constitucionalização explícita.

A Advocacia, mais do que qualquer outra área de atuação humana, precisa saber utilizar os dados pessoais coletados de forma planejada e segura, tomando as decisões corretas a partir de dados extraídos de forma legal e, ainda mais, demonstrando ética e transparência no relacionamento com os clientes. Para o que tem de se manter atenta e acompanhar as mudanças que têm ocorrido no Direito e na Sociedade em geral.

Por esse motivo, essa ***2ª Edição do Guia da LGPD aplicada aos Escritórios de Advocacia*** é mais do que uma entrega da **CDPPDP - Comissão de Direito à Privacidade e Proteção de Dados Pessoais da OAB Campinas**. Como é patente, para todos os minimamente interessados nestas matérias no Brasil inteiro, a nossa Comissão vem promovendo uma série de palestras e debates com renomados especialistas em matéria de Privacidade e Proteção de Dados, inclusive internacionais, no sentido de subsidiar e apoiar no desenvolvimento de ações para a proteção de dados pessoais, esclarecer os principais aspectos teóricos e práticos da matéria e suas aplicações para todos os operadores de Direito, sobretudo para os escritórios de Advocacia. Assim, este trabalho pretende proporcionar, antes de mais às Advogadas e aos Advogados, condições estruturais de conscientização, sensibilização e aplicação, uma vez que se o tema diz respeito à interpretação da Lei, requer também uma perspectiva multidisciplinar que nos habilite a atuar na sociedade em evolução tecnológica e conectada do Século XXI.

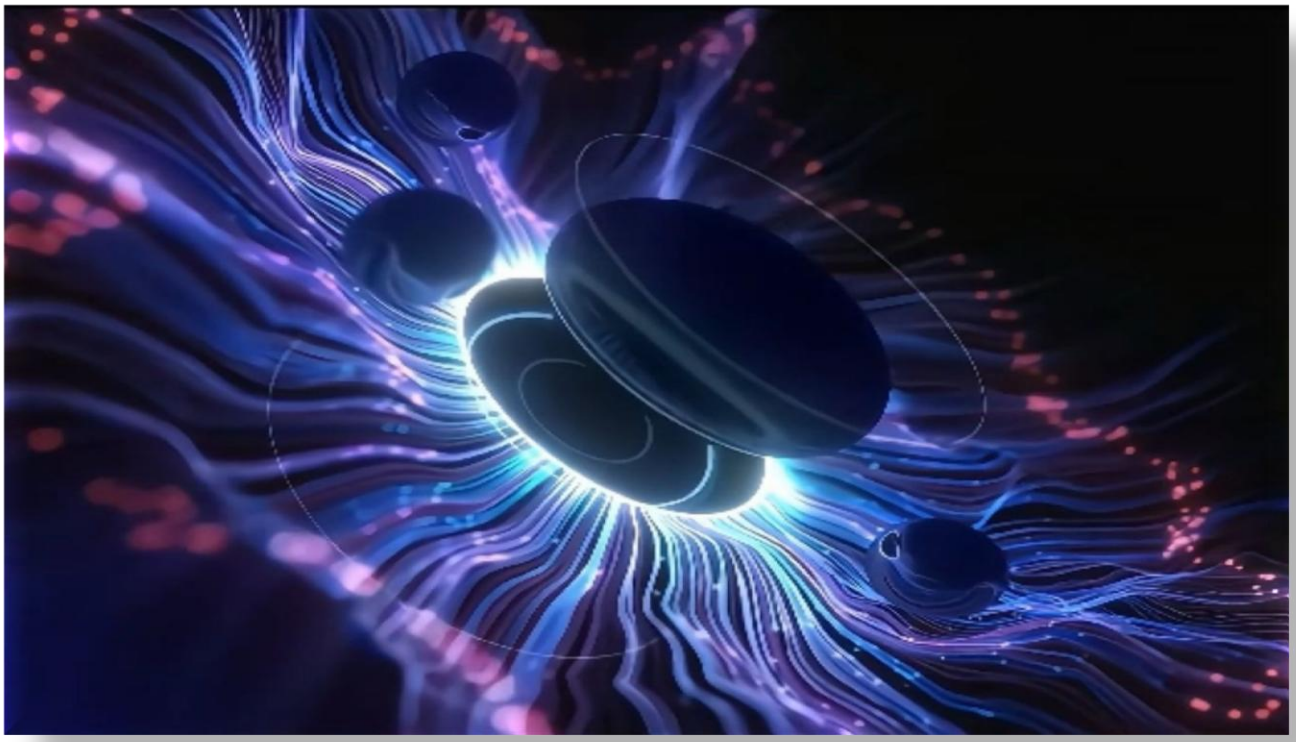
Especificamente, este ***Guia em sua 2ª Edição*** é um esforço no sentido de acompanhar a evolução acelerada dos tempos. Assim, para além da atualização dos textos constantes da primeira 1ª Edição , **analisa criticamente os diversos documentos produzidos pela ANPD - Autoridade Nacional de Proteção de Dados nos últimos dois anos** e traz um complemento no apêndice, tendo por objeto a experiência paralela da Advocacia, na União .Europeia precisamente em Portugal.

Mantendo os métodos inicialmente, este trabalho foi reescrito e escrito por múltiplas mãos, desde diferentes perspectivas, e estando cientes que as várias matérias se cruzam e complementam, o que até nos permite compreender melhor o quanto elas estão interligadas. Com o objetivo de reforçar a consistência dos resultados e ter uma perspectiva externa, a Presidência da Comissão contou com o contributo reforçado de seu Membro Consultor da União Europeia - Professor *Manuel David Masseno*, o qual passou a constar como coorganizador da Edição.

Estamos cientes que os resultados não estão perfeitos, nem esta empreitada nunca ficará terminada. Mas, cumprimos nosso dever de contribuir para a superação dos desafios resultantes da Cultura de Privacidade e Proteção de Dados Pessoais, sensibilizando os gestores de escritórios de Advocacia, assim como cada Advogada e Advogado, quanto à necessidade de efetivarem a adequação permanente à *Lei Geral de Proteção de Dados Pessoais*, incluindo as regulamentações e orientações da ANPD, e as outras Fontes pertinentes, agora ainda mais interpretadas e aplicadas em conformidade com a *Constituição Federal*.

BOA LEITURA!

Valéria Reani Rodrigues Garcia
Presidente da Comissão de Direito à Privacidade e Proteção de Dados Pessoais



PREFÁCIOS

Por Eduardo Tomasevicius Filho

Honra-me a OAB São Paulo, por meio da **Subseção de Campinas**, por iniciativa da sua **Comissão de Direito à Privacidade e Proteção a Dados Pessoais**, pelo convite feito para prefaciar este ***Guia*** sobre a aplicação da **Lei Geral de Proteção de Dados** aos escritórios de advocacia, o qual está na segunda edição. Tive a oportunidade de ler este material, elaborado com esmero pelos colegas advogados membros da comissão, por conta da linguagem acessível, com recursos visuais e riqueza de informações, em que se descrevem os passos a serem dados sobre o modo pelo qual a advocacia deve harmonizar a prática profissional com o tratamento de dados pessoais dos clientes sobretudo aos apontamentos comentados referentes as atividades da nossa Autoridade Nacional de Proteção de dados Pessoais - ANPD.

A importância de um guia como este reside, inicialmente, na autorreflexão que nós, advogados, devemos fazer em relação à nossa própria atividade. Somos procurados e contratados por quem deseja fazer a adequação da sua empresa à **LGPD**. Prestamos consultorias, realizamos treinamentos, e até mesmo podemos atuar como encarregados pelo tratamento de dados pessoais, cabendo, inclusive, a percepção de honorários por essa atividade, conforme se previu na mais recente tabela de honorários lançada pela nossa Seccional. Como a ementa da **LGPD** indica, trata-se de uma lei geral, que precisa ser seguida por todos os profissionais, inclusive os advogados. Nesse sentido, devemos dar exemplos positivos para a sociedade. Portanto, um guia como este é imprescindível para que os colegas que ainda não se adequaram à **LGPD**, recebam auxílio da classe na reorganização do fluxo de dados pessoais dos clientes em seus escritórios.

Ademais, considero relevante que nós, advogados, pensemos sobre o tratamento de dados não apenas de um aspecto formal, de demonstração do cumprimento da **LGPD**, mas que prestemos atenção na quantidade de dados pessoais que coletamos, e se estes são realmente necessários para a finalidade de defesa em juízo, por exemplo. Ou, ainda, cabe observar de que maneira nós, advogados, junto com nossos colaboradores, armazenamos, arquivamos, compartilhamos e descartamos dados pessoais. Não deixa de ser um exercício de eficiência a realização da atividade apenas com os dados relevantes, sem deixar de lado a excelência na prestação de serviços e o respeito ao juramento que todos nós fizemos de defender a justiça e o Estado Democrático de Direito, quando fomos admitidos à OAB.

Eu, que sou advogado especializado na área e fui convidado para o exercício do cargo de *DPO* da Universidade da qual sou professor de direito civil e, nos últimos anos, de direito digital, vejo no cotidiano as dificuldades de criação de uma cultura de tratamento de dados pessoais, ao lidar com um público heterogêneo, formado por alunos e professores de 202 cursos, com milhares de servidores que atuam na administração, bem como com o público externo, que nos procura em razão de nossas atividades de extensão. Por isso, **eu valorizo e aplaudo todas as iniciativas feitas para que a LGPD não seja uma lei que se cumpre por receio de sanções, mas que seja uma lei que proporcionou uma nova mentalidade de garantia a este novo direito fundamental constitucionalmente protegido em nosso país**.

Meus parabéns à OAB Campinas por esta obra e muito sucesso aos colegas advogados na aplicação da **LGPD** em seus escritórios!

De São Paulo a Campinas em 2 de outubro de 2024

Eduardo Tomasevicius Filho
Professor Associado da Faculdade de Direito da USP
Encarregado-Geral pelo Tratamento de Dados Pessoais (DPO) da USP
Advogado inscrito na OAB São Paulo, Subseção Lapa

Por Alexandre Atheniense

É com grande satisfação que aceitei o convite para prefaciar esta nova edição da obra dedicada à proteção de dados pessoais, uma iniciativa louvável da **Comissão de Direito à Privacidade e Proteção a Dados Pessoais** da OAB de Campinas.

Desde sua primeira edição em 2020, este livro tem se consolidado como uma referência indispensável para profissionais e estudiosos da área, oferecendo uma análise aprofundada e prática sobre a implementação de projetos de conformidade com a **Lei Geral de Proteção de Dados** (**LGPD**).

A Comissão de Direito à Privacidade e Proteção de Dados Pessoais da OAB de Campinas merece reconhecimento por seu incansável trabalho de pesquisa e atualização, refletido nesta edição revisada e ampliada.

Em um cenário jurídico em constante evolução, a OAB Campinas, através da Comissão, tem se destacado por sua capacidade de adaptar e integrar as mais recentes diretrizes e interpretações legais, garantindo que esta obra permaneça na vanguarda do conhecimento sobre proteção de dados na esfera Nacional e até como exemplo internacional.

Este livro se diferencia, por sua abordagem prática e acessível, oferecendo orientações claras e detalhadas para a implementação de projetos de conformidade com a **LGPD**, além de comentar, de forma inédita, toda a regulamentação necessária à **LGPD**, que vem fazendo a Autoridade Nacional de Proteção de dados Pessoais através de Resoluções, Notas Técnicas, entres outros Atos Normativos.

Os leitores encontrarão aqui não apenas uma análise teórica das normas legais, mas também exemplos concretos e estratégias eficazes para enfrentar os desafios do dia a dia na proteção de dados pessoais.

A obra aborda desde os princípios fundamentais da **LGPD**, atualizações regulatórias e até questões específicas, como o tratamento de dados de crianças e adolescentes, sempre com um olhar atento às melhores práticas de mercado.

A atualização contínua deste trabalho reflete o compromisso da Comissão com a excelência e a relevância, assegurando que advogados, empresas e demais interessados tenham acesso às informações mais atuais e precisas.

Este esforço é particularmente importante em um momento em que a proteção de dados se torna cada vez mais central para a prática jurídica e para a sociedade como um todo. Assim, esta edição reafirma seu papel como a obra mais qualificada sobre os aspectos práticos da conformidade com **a LGPD,** servindo como um guia essencial para aqueles que buscam implementar e manter políticas eficazes de proteção de dados.

A Comissão de Direito à Privacidade e Proteção de Dados da OAB de Campinas, ao oferecer esta contribuição valiosa, não apenas fortalece a cultura de proteção de dados no Brasil, mas **também inspira outras instituições a seguirem seu exemplo de dedicação e inovação**.

Convido os leitores a explorarem as páginas que se seguem com a certeza de que encontrarão um recurso inestimável para suas práticas profissionais e acadêmicas.
Que esta obra continue a iluminar o caminho para uma gestão responsável e ética dos dados pessoais, contribuindo para a construção de um ambiente digital mais seguro e respeitoso.

Parabéns à OAB Campinas e a Comissão!

De Belo Horizonte a Campinas em 2 de outubro de 2024

Alexandre Atheniense

Sócio de Alexandre Atheniense Advogados em BH, escritório especializado em Direito Digital. Coordenador da Comissão de Direito Digital do CESA - Centro de Estudos das Sociedades de Advogados

Por Alexandra Krastins

É com grande honra que escrevo este prefácio para a Segunda Edição do ***Guia LGPD Aplicada aos Escritórios de Advocacia***. O contexto jurídico atual no Brasil vem sendo profundamente impactado pela Lei Geral de Proteção de Dados Pessoais, e a importância da privacidade e da proteção de dados nunca foi tão clara. Esta obra oferece aos advogados uma ferramenta essencial para adaptar suas práticas à realidade legislativa e tecnológica que agora permeia todas as interações com clientes, colaboradores e parceiros.

A LGPD não apenas regula o tratamento de dados pessoais, mas também impulsiona uma mudança cultural no meio jurídico, exigindo que os escritórios de advocacia implementem políticas de segurança e transparência no tratamento de dados. Os desafios são muitos, mas, como demonstra este guia, as soluções estão ao alcance daqueles que buscam se adequar com diligência e profissionalismo.

Esta Edição, atualizada e ampliada, reflete os avanços e as mudanças mais recentes promovidas pela Autoridade Nacional de Proteção de Dados (ANPD), proporcionando aos escritórios de advocacia uma visão clara e prática sobre como conduzir o tratamento de dados de forma ética e segura. Os diversos autores e especialistas que contribuíram para esta obra são referências em suas áreas, garantindo a profundidade e a precisão necessárias para tratar de um tema tão complexo.

Através deste guia, espero que os advogados e demais operadores do Direito possam aprimorar suas práticas, garantindo que o sigilo profissional e a proteção de dados caminhem lado a lado. Que este livro inspire reflexões e ações concretas, de modo que o Direito continue sendo um pilar fundamental na defesa da liberdade e da privacidade de cada indivíduo.

Desejo a todos uma leitura proveitosa e transformadora.
De São Paulo a Campinas, 07 de outubro de 2024.

Alexandra Krastins
Advogada especialista em Direito Digital.
EX Gerente de Projetos da Autoridade Nacional de Proteção de Dados (ANPD).

Por Longinus Timochenco

A proteção dos dados pessoais não é apenas uma questão de conformidade com a lei, mas um reflexo do respeito à privacidade e aos direitos fundamentais dos indivíduos. Em tempos de crescente transformação digital, a Lei Geral de Proteção de Dados Pessoais emerge como um alicerce crucial para regulamentar o tratamento de informações sensíveis, estabelecendo novas responsabilidades para diversos setores, incluindo a advocacia.

Os escritórios de advocacia, mais do que nunca, são guardiões de um vasto fluxo de dados pessoais e profissionais de seus clientes. A **LGPD**, em sua essência, exige que a advocacia adote um papel proativo na gestão dessas informações, assegurando não só a conformidade com as normativas legais, mas também o compromisso ético com a integridade e segurança dos dados.

Esta 2ª edição do ***Guia LGPD Aplicada aos Escritórios de Advocacia***, elaborada pela Comissão de Direito à Privacidade e Proteção de Dados Pessoais da OAB Campinas, reafirma o compromisso da instituição em oferecer uma base sólida de orientação para advogados(as) de todo o Brasil. Com a colaboração de renomados especialistas e a atualização constante das diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), este guia não apenas aborda as principais questões legais e operacionais da **LGPD**, mas também oferece insights práticos para a implementação de uma cultura robusta de proteção de dados.

Esperamos que esta publicação sirva como uma ferramenta valiosa para o desenvolvimento de boas práticas, auxiliando os escritórios a navegarem pelos desafios impostos pela era da privacidade digital. Que esta leitura inspire uma mudança contínua e estratégica na forma como os dados são tratados no âmbito jurídico, garantindo maior segurança e confiança para os operadores do Direito e seus clientes.

Boa leitura!
De São Paulo para Campinas, em 7 de outubro de 2024.

Longinus Timochenco
Ciso Global Advisor

Por Fabrício da Mota Alves

É com grande satisfação que recebi o convite para prefaciar a 2ª Edição do ***Guia LGPD Aplicada aos Escritórios de Advocacia***, elaborado pela Comissão de Direito à Privacidade e Proteção de Dados Pessoais da Subseção de Campinas do Conselho Seccional de São Paula da Ordem dos Advogados do Brasil.

Este ***Guia*** representa um esforço coletivo para fornecer orientações práticas e atualizadas sobre a implementação da Lei Geral de Proteção de Dados Pessoais no contexto específico das atividades e dos escritórios de advocacia. Desde a publicação da primeira edição, o cenário regulatório e as melhores práticas em proteção de dados evoluíram significativamente, tornando necessária esta atualização. A Autoridade Nacional de Proteção de Dados (ANDP) tem buscado exercer suas atribuições e competências legais em acelerado ritmo regulatório, interpretando e complementando o arcabouço normativo da **LGPD** através da edição de Guias Orientativos e normas regulamentares, mas não se limitando a isso: também através de suas atividades fiscalizatória e repressiva.

Dessa maneira, o sistema brasileiro de proteção de dados pessoais ganha robustez a cada dia, exigindo a atuação suplementar da sociedade e, mais especificamente, de setores organizados. É nesse sentido que **aclamo o presente *Guia*, um documento orientativo dedicado à prática da advocacia. Trata-se da materialização de uma visão contributiva e cidadã, típica da função constitucional da Ordem, que agrega e soma, convidando a advocacia a aderir a uma nova era de respeito e proteção do cidadão**.

Nesta nova edição, busca-se não apenas atualizar o conteúdo existente, mas também expandir o escopo das orientações, incorporando as mais recentes regulamentações da Autoridade Nacional de Proteção de Dados (ANPD) e as experiências práticas acumuladas pelos profissionais do direito nos últimos anos.

O ***Guia*** aborda temas cruciais como o mapeamento de dados, a implementação de políticas de segurança da informação, a gestão de consentimento, o tratamento de dados sensíveis, e as melhores práticas para lidar com incidentes de segurança. Além disso, fornece orientações específicas sobre como adaptar os contratos, procedimentos internos e a cultura organizacional dos escritórios de advocacia às exigências da **LGPD**.

Espero que este guia seja uma ferramenta valiosa para advogados, gestores de escritórios e profissionais do direito em geral, auxiliando-os a navegar pelos desafios e oportunidades trazidos pela era da proteção de dados. A conformidade com a **LGPD** não é apenas uma obrigação legal, mas também uma oportunidade de fortalecer a confiança dos clientes e diferenciar-se no mercado.

Registro, na pessoa de sua Presidente, Valéria Reani, sincero agradecimento a todos os membros da Comissão e colaboradores externos que contribuíram com seu tempo, conhecimento e experiência para a elaboração deste material. Que este guia sirva como um farol, iluminando o caminho para uma advocacia mais ética, segura e alinhada com os princípios fundamentais à proteção de dados e à privacidade.

De Brasília para Campinas, em 7 de outubro de 2024.

Fabrício da Mota Alves
Advogado e Conselheiro Consultivo da Anatel
Ex- Conselheiro Consultivo da ANPD

Por Alexandre Sousa Pinheiro

A aplicação de um instrumento legal sobre proteção de dados a escritórios de advogados obriga a identificar quais os novos aspetos que devem transitar para a sua organização e para o desenvolvimento da atividade dos causídicos, bem como dos colaboradores que exerçam funções nos escritórios.

O ***Guia*** opta por um conceito alargado de colaboradores no escritório de Advogados: "Advogados empregados, Advogados associados, sócios, diretores, CEO, estagiários, auxiliares da limpeza, os Recursos Humanos, os setores administrativo, financeiro e de T.I, bem como a equipe de Marketing."

Atendendo a que, por natureza, os advogados têm acesso e consultam informações pessoais de clientes e consulentes, não surpreende que quer leis quer códigos aprovados pela OAB, previamente à Lei Geral de Proteção de Dados, revelem preocupações e definam regimes jurídicos sobre temas como por exemplo o sigilo profissional. Tal tem como propósito não só garantir uma relação de confiança advogado-cliente/consulente, mas, também, assegurar a proteção da vida privada destes últimos.

A segunda edição do *Guia*, que ora prefaciamos, **apresenta-se muito completa incluindo regras de natureza jurídica de cumprimento necessário pelos escritórios de advogados, assim como regras técnicas e metodológicas fundamentais para obviar a falhas de *compliance***.

O ***Guia*** parte do pressuposto de que o escritório de advogados deve ser interpretado como uma empresa no que respeita à definição das políticas internas e de relação com organizações externas para que se garanta o cumprimento de normativos e de Resoluções e Normas Técnicas aprovadas pela ANPD.

Assim, o resultado de peças processuais, contratos ou consultas jurídicas que se produzam para clientes ou consulentes na área da proteção de dados deve ser igualmente respeitado pelo Escritório.

A interpretação do escritório como estrutura organizativa conduz a conclusões que levam ao cumprimento necessário de regras de segurança, que se desenvolvam quer na conservação de informação pessoal – com o estabelecimento de períodos de retenção de dados, quando não exista definição legal – quer na utilização de plataformas de comunicação cada vez mais utilizadas. Aqui, adverte-se para a adequada escolha e configuração da plataforma; para a definição e atualização de aplicativos; para a escolha e utilização de antivírus atualizados e sejam criados mecanismos que impeçam a inserção de *malware*.

No plano da proteção da informação, o Guia explicita, com segurança, a diferença entre dados pessoal e processo de anonimização – que se concluído de forma adequada elimina a natureza pessoal de uma informação – não olvidando eliminação de dados pessoais prevista no artigo 16.º da **LGPD.**

O complexo de direitos que a lei define é aplicado no quotidiano de um Escritório de Advogados, o que inclui, por exemplo, o direito de cliente/consulente ser informado sobre os tratamentos que sobre os seus dados se efetuem.

O Guia refere, também, de forma completa as exigências normativas para garantir a transferência internacional de dados pessoais, estabelecendo pertinentes comparações com o RGPD/GDPR. Frisam-se as vantagens de aprovação de códigos de conduta para a garantir processos adequado de implementação do **LGPD**.

Este Guia fornece os meios necessários para definir e atualizar os processos de adotar os meios adequados para o cumprimento da legislação sobre proteção de dados pessoais.

De Portugal, para Campinas em 6 de outubro de 2024.

Alexandre Sousa Pinheiro
Doutor em Direito pela Universidade de Lisboa, com Tese sobre Proteção de Dados; Professor da Universidade Europeia, de Lisboa; Membro da Comissão de Acesso a Documentos Administrativo e ex-Membro da Comissão Nacional de Proteção de Dados, ambas de Portugal; Consultor e Encarregado da Proteção de Dados em prestação de serviços.

Por Luciane Cardoso Barzotto

A segunda edição do **Guia LGPD Aplicada aos Escritórios de Advocacia,** de iniciativa da **Comissão de Direito a Privacidade e Proteção de dados Pessoais da OAB Campinas**, é um trabalho robusto que visa fornecer orientações atualizadas para a conformidade dos escritórios de advocacia em relação à **Lei Geral de Proteção de Dados.** Ele destaca a importância crescente da privacidade e do tratamento ético de dados pessoais, tanto no contexto jurídico quanto na sociedade em geral. Esta edição foi coordenada por especialistas em direito digital e proteção de dados, consolidando uma base sólida para a aplicação das normas em escritórios de diferentes tamanhos e estruturas.

O ***Guia*** é organizado de forma a abordar todos os aspectos da **LGPD**, desde os conceitos fundamentais até as práticas cotidianas necessárias para garantir o cumprimento da lei. Ele começa destacando que a **LGPD** impacta diretamente os escritórios de advocacia, uma vez que todos os advogados, de pequenos a grandes escritórios, lidam com dados pessoais sensíveis. O material traz orientações práticas sobre o dever de confidencialidade, políticas de retenção de dados, bases legais para o tratamento e compartilhamento de informações e medidas de segurança a serem adotadas para proteger os direitos dos titulares de dados.

O ***Guia*** é extremamente elogiável por sua profundidade e por oferecer um verdadeiro "*roadmap*" para a implementação de conformidade à **LGPD** nos escritórios de advocacia. Ele não só apresenta as obrigações legais, como também sugere boas práticas e políticas internas que visam fomentar uma cultura de privacidade, incentivando uma mudança de mentalidade entre advogados e seus colaboradores. O conteúdo é enriquecido por uma análise crítica dos documentos mais recentes produzidos pela ANPD, garantindo que os profissionais estejam sempre atualizados com as normativas e diretrizes mais recentes.

É uma obra essencial e louvável, que demonstra o compromisso da OAB Campinas e da Comissão de Direito à Privacidade e Proteção de Dados Pessoais em apoiar o desenvolvimento de uma advocacia ética e moderna. Combinando teoria e prática, **o *Guia* cumpre seu papel de oferecer um suporte claro e acessível para advogados que desejam estar em conformidade com as exigências legais, promovendo um ambiente seguro para o tratamento de dados pessoais e garantindo a confiança dos clientes**.

De RS, para Campinas em 3 de outubro de 2024

Luciane Cardoso Barzotto
Desembargadora do TRT 4ª Região RS

Por Ana Paula Canto de Lima

Com grande honra e satisfação recebi o convite para fazer o prefácio para a OAB São Paulo, Subseção de Campinas. Em especial, pelo tema que me é tão caro, proteção de dados pessoais, **o Guia não apenas orienta, mas convoca os escritórios de advocacia a se adequarem à Lei Geral de Proteção de Dados Pessoais, visto que é indispensável para toda classe**.

A 1ª Edição do ***Guia*** foi um sucesso e a 2ª Edição foi consequência do excelente trabalho de todos que se envolveram no projeto. O guia foi organizado com maestria pela Comissão de Direito à Privacidade e Proteção a Dados Pessoais, com coordenação de dois profissionais muito atuantes que parabenizo pela continuidade do projeto, a Advogada Valéria Reani, a quem agradeço o convite, e o Prof. Manuel Masseno.

O ***Guia LGPD Aplicado aos Escritórios de Advocacia*** é uma ferramenta essencial para os advogados que entendem o valor envolvido na proteção dos dados pessoais de clientes, colaboradores, fornecedores, terceirizados, entre outros, afinal dados são ativos valiosos na nossa sociedade informacional.

É fato que tanto o escritório, quanto o advogado autônomo tratam dados pessoais, portanto precisam observar os cuidados necessários ao armazenar e compartilhar esses dados, ao definir a base legal para cada tratamento, ao realizar o descarte, além de providenciar treinamento adequado, documentos e políticas capazes de orientar e alinhar o time para evitar surpresas desagradáveis. E todos esses temas estão no guia.

O ***Guia*** é providencial, considerando que, como operadores do Direito, devemos primeiro adequar o nosso próprio escritório antes de nos colocarmos à disposição para adequar outras empresas. E para isso, é fundamental compreender a **LGPD** e a partir dessa compreensão, reestruturar operações, processos e procedimentos de maneira adequada.

Nesse sentido, o ***Guia*** contribui enormemente, disponibilizando aos colegas advogados informações e conhecimentos necessários para a adequação de suas atividades à **LGPD**. Por outro lado, a conduta e a postura do advogado devem refletir o seu compromisso com a legislação, começando na sua casa, ou seja, no seu escritório.

O advogado deve atuar como um farol para a sociedade quando se trata de cumprimento de exigências legais, é preciso dar o exemplo, assim os demais colegas serão inspirados a fazerem o mesmo, bem como as pessoas físicas e jurídicas que têm vínculo com o escritório.

A ANPD – Autoridade Nacional de Proteção de Dados, muito citada ao longo do guia, produziu resoluções, enunciados e outros documentos – alguns deles estão no guia – visando proporcionar o direcionamento necessário à interpretação da **LGPD**.

O ***Guia*** explora as mudanças trazidas pela lei que impactaram diretamente nos escritórios de advocacia, destacando aspectos como a revisão de contratos de honorários, como usar adequadamente ferramentas de comunicação, como aplicativos de mensagens, videoconferências e e-mails corporativos, e até os cuidados em reuniões virtuais. Além disso, são fornecidas orientações sobre como fortalecer a segurança da informação, e como elaborar um plano de resposta a incidentes.

Oferece orientações sobre a criação e implementação de uma política de privacidade para escritórios de advocacia, além de outros documentos. Aborda ainda a relevância das boas práticas que devem ser adotadas no cotidiano dos escritórios.

Que todo o empenho voltado para fomentar a proteção de dados pessoais no Brasil possibilite à sociedade a mudança de cultura tão esperada, e que os direitos constitucionais à privacidade e à proteção de dados façam parte da vida de cada cidadão.

Convido a todos os colegas a lerem atentamente as orientações compartilhadas no ***Guia***, ressalto que, ao cumprir as obrigações legais, o escritório terá um diferencial competitivo, demonstrando credibilidade e fortalecendo a confiança dos seus clientes. Por fim, deixo registrado meus parabéns aos organizadores, aos coautores e a todos que participaram da construção de um guia tão relevante para a comunidade jurídica.

De Recife a Campinas, em 12 de outubro de 2024.

Ana Paula Canto de Lima
Advogada, fundadora do escritório Canto de Lima Advocacia; Mestre; LLM em Proteção de Dados (RGPD/LGPD); Professora de pós-graduações em diversos estados sobre proteção de dados, Autora de obras jurídicas indicadas nas bibliografias selecionadas pelo STJ; Conselheira no CNPD; Conselheira na OAB/PE; Membro do ONCiber; Presidente da Comissão Nacional de Crimes Cibernéticos da ABCCRIM; Membro da Comissão de Proteção de Dados CFOAB.

SUMÁRIO

1. Qual o caminho para adequação à LGPD em escritórios de Advocacia?

Por Valéria Reani Rodrigues Garcia

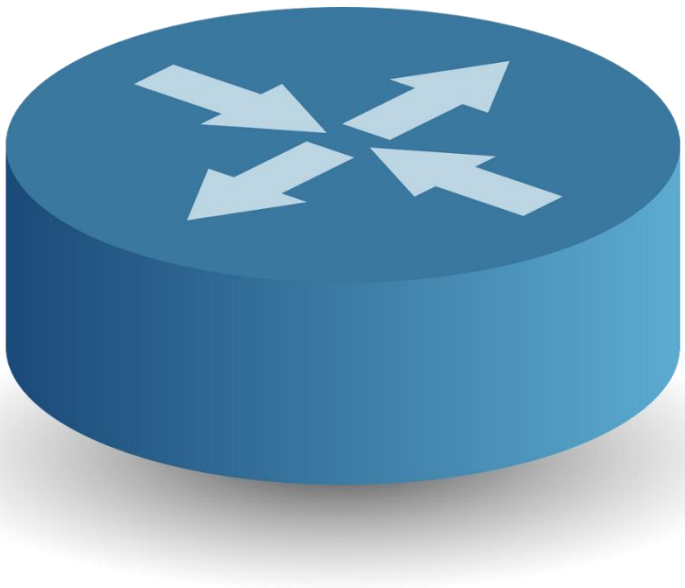
Antes de tudo o mais, a definição de uma metodologia de adequação é, sem dúvida, o caminho para dar início a um projeto de adequação à **LGPD** aplicada ao escritório de Advocacia.

Essa avaliação depende diretamente das necessidades, da estrutura do escritório, da maturidade organizacional em relação aos temas de privacidade e da proteção de dados pessoais, tendo em conta o tempo necessário, assim como o disponível.

Para começar, é necessário ter em mente que não existe um modelo pronto ou um selo que ateste a conformidade completa as regras de proteção de dados.

As iniciativas de adequação devem ser encaradas como processos constantes, em melhoria contínua, durante por toda a vida da organização. Como todos constatamos, a cada dia, novos serviços e produtos são desenvolvidos, processos internos são alterados, novas pessoas são contratadas e novas práticas são adotadas.

Por isso mesmo, a própria **LGPD** determina que as organizações devem ser capazes de demonstrar que adotaram todas as medidas cabíveis, dentro de critérios objetivos de tempo, custo e tecnologia disponível para estarem o mais próximo possível da conformidade, sua responsabilidade proativa (*accountability*).



2. Dever de confidencialidade dos escritórios

Por Ana Cristina da Costa Elias Olivari

Como preconiza o ***Código de Ética e Disciplina da OAB***, "O sigilo profissional é de ordem pública, independendo de qualquer solicitação feita por seu cliente". O que significa reconhecer que a atividade da Advocacia sempre esteve envolvida com o cuidado e dever de sigilo profissional, tanto em defesa de cada cliente quanto àquele exercido pelo Advogado, ou pela Advogada, em defesa de suas prerrogativas, no exercício das atividades. Se não bastasse, tem como dever a defesa de direitos humanos e garantias fundamentais. Tudo isso vem expressamente disciplinado pela ***Constituição Federal***, pelo ***Código de Ética e Disciplina da OAB*** e pelo ***Código Penal***, entre outros normativos.

Temos, por exemplo, o dever de resguardar o segredo profissional e informações privilegiadas recebidas em função do exercício da Advocacia; o dever de guardar sigilo mesmo em depoimento judicial ou a obrigação de anunciar serviços de maneira ponderada e discreta.

Outrossim, o dever de confidencialidade trazido pela **LGPD** traz consigo uma outra amplitude, a de proteção de direitos fundamentais de liberdade e privacidade do titular dos dados pessoais, dados estes recebidos pelo Advogado para mera formalização de consulta ou, mesmo, para o exercício de qualquer direito de seu cliente. Tal dimensão não se confunde com o sigilo profissional tradicionalmente previsto em nossas regras profissionais, pois vai além da guarda de elementos fáticos e físicos inserindo-se na esfera do indivíduo e no modo como são tratados os dados pessoais recebidos para o desenvolvimento dos nossos trabalhos.

A profissão do Advogado não está imune aos rigores da **LGPD**, uma vez que o cuidado com os dados pessoais se inicia desde o momento do contato inicial com o seu titular, seja cliente ou meramente consulente, a partir do cuidado com as informações colhidas, na guarda de diálogos e documentos.

O que torna imprescindível a formalização de termos de confidencialidade e contratos de prestação de serviços que captem, inequivocamente, o consentimento e/ou ciência da pessoa titular quanto à forma do tratamento dos seus dados, guarda, compartilhamento e descarte entre outras circunstâncias de relevo à situação concreta.

Este cuidado passa também pela estruturação das atividades e meios de comunicação ou divulgação dos serviços, adequando-se canais como o uso de mensagens instantâneas e eletrônicas às melhores práticas de segurança e privacidade; políticas de privacidade e de boas práticas internas, como também pela observância de práticas adequadas de guarda física e digital dos documentos confiados e o uso de *softwares* de **gestão de escritórios de Advocacia** ou mesmo o compartilhamento de dados com terceiros que apoiam os serviços jurídicos (contadores; assistentes técnicos, etc).

Por isso, o treinamento e conscientização no que concerne à privacidade e proteção de dados, de toda a equipe de trabalho, sobretudo ao novo texto legal, é imprescindível, fundamental e incorpora uma mudança de cultura e posicionamento em nosso negócio. A adoção de uma política de segurança da informação, de mapeamento dos riscos inerentes a atividade e de gestão de crise igualmente devem estar na ordem do dia do gestor.

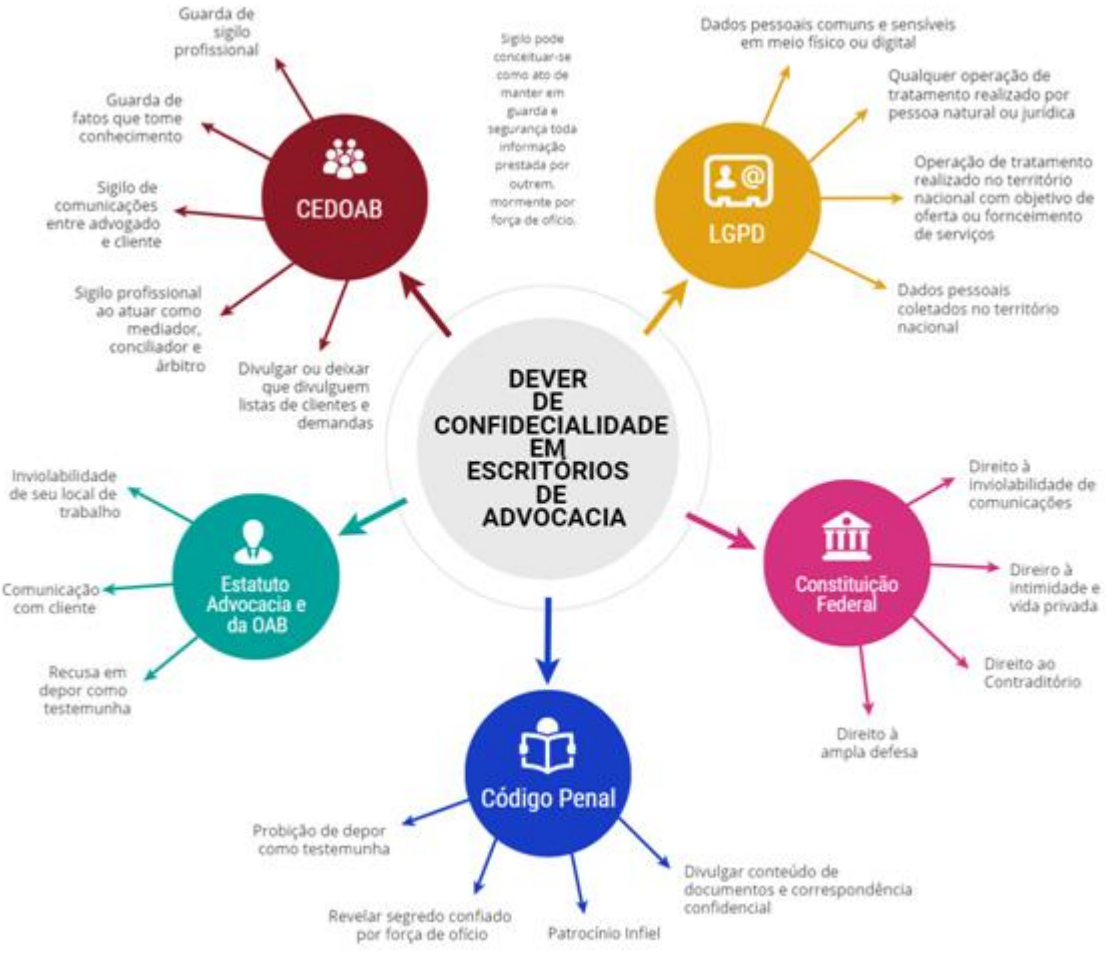


Imagem elaborada pela autora Ana Cristina da Costa Elias Olivari

3. Começando a adequação efetivamente

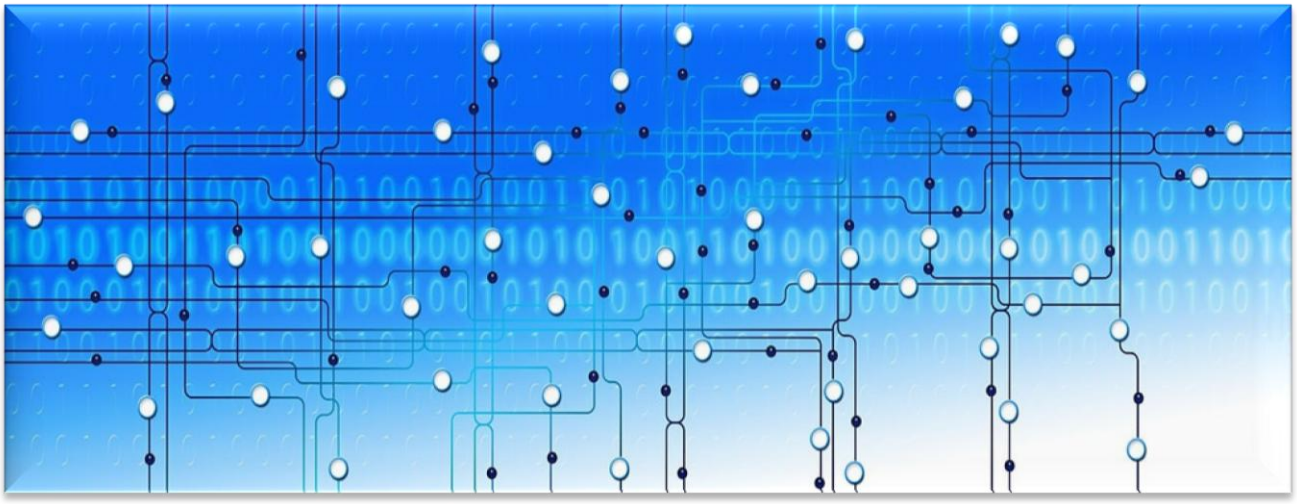
Por Mírian Barreta Palla

3.1. Aspectos gerais da LGPD

Embora o ordenamento jurídico pátrio tenha agasalhado a proteção de dados e da privacidade em diversos diplomas, como a ***Constituição Federal*** (Art. 5º, X e LXXII), o ***Código Civil*** (Art. 21), o **Código de Defesa do Consumidor** (Art. 23) **e** a Lei nº 12.965/2014 (***Marco Civil da Internet***), era imprescindível a regulamentação, através de lei própria, do tratamento de dados pessoais.

À luz da normatização em outros países, a exemplo do expoente ***Regulamento Geral sobre Proteção de Dados da União Europeia*** – adotado em abril de 2016, mas implementado em maio de 2018 –, a Lei brasileira tem como fundamentos, em linhas gerais, garantir proteção da privacidade e autodeterminação informativa dos titulares dos dados, bem como possibilitar transparência no tratamento, redução de riscos, desenvolvimento econômico/ tecnológico, bem como responsabilização dos agentes por tratamento em desconformidade e por incidentes de segurança.

Assim, a **LGPD** exige a realização de adequações nos mais variados aspectos e setores da sociedade, inclusive nos escritórios de advocacia, o que implica uma mudança de mentalidade e, mais que isso, a elaboração e efetivo cumprimento de procedimentos no tratamento de dados pessoais, boas práticas e *compliance*.



3.2. Pois bem, mas o que são os dados pessoais?

A **LGPD** traz um conceito bem abrangente para **dado pessoal**, definindo-o como uma "informação relacionada a pessoa natural identificada ou identificável" (**Art. 5º**,I).

Exemplos de atributos para identificar pessoa Natural de acordo com a Tabela 2 ISO NBR 27701/ 19 e 29100/2020:

Tabela 2 - ABNT NBR ISO/IEC 29100:2020
Exemplos

- Idade ou necessidades especiais de pessoas naturais vulneráveis
- Alegações de conduta criminosa
- Qualquer informação coletada durante serviços de saúde
- Conta bancária ou número de cartão de crédito
- Identificador biométrico
- Extratos de cartão de crédito
- Condenações criminais ou delitos cometidos
- Relatórios de investigação criminal
- Número do cliente
- Data de nascimento
- Informação de diagnóstico de saúde
- Deficiências
- Contas médicas
- Salários dos empregados e arquivos dos recursos humanos
- Perfil financeiro
- Gênero
- Posição no GPS
- Trajetória no GPS
- Localização fornecida por sistemas de telecomunicação
- Endereço residencial
- Endereço IP
- Histórico médico
- Nome
- Identificadores nacionais (por exemplo, número do passaporte)
- Endereço de e-mail pessoal
- Número de identificação pessoal (PIN) ou senha
- Interesses pessoais derivados do rastreamento do uso de *websites*
- Perfil pessoal ou comportamental
- Número do telefone pessoal
- Fotografia ou vídeo identificado a uma pessoa natural
- Preferências de produtos ou serviços
- Origem étnica ou racial
- Crenças religiosas ou filosóficas
- Orientação sexual
- Filiação sindical
- Contas de serviços públicos

Tabela trazida por Valéria Reani Rodrigues Garcia.

***Fonte**: Tabela 2 - ABNT NBR ISO/IEC 29100 – Técnicas de Segurança – Estrutura de Privacidade*

Ante a existência de dados passíveis de ensejar a discriminação da pessoa, a lei garante especial proteção e tratamento aos denominados dados **sensíveis**, relativos à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (**Art. 5º**, II).

Através do processo de **pseudonimização**, descrito no **Art. 13**, §4º, é possível dissociar o dado do indivíduo; contudo, pelo uso de informações adicionais mantidas separadamente pelo controlador (por exemplo, um código verificador), pode-se restabelecer a identificação. Já o **dado anonimizado** não é considerado "pessoal", pois a utilização de técnicas disponíveis no momento do tratamento, em processo irreversível, impede que seu titular seja identificado de forma direta ou indireta (**Art. 5º**, III e XI).

Além da definição de "dados", por se tratar de uma lei conceitual, a LGPD traz outras caracterizações fundamentais inseridas em seu próprio texto, a fim de facilitar a compreensão e a interpretação pelos destinatários da norma:

3.3. Quanto aos sujeitos (art. 5º):

- **titular** (inciso V): *pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*;

- **controlador** (inciso VI): *pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*;

- **operador** (inciso VII): *pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador*;

- **encarregado** (inc VIII): *pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados*;

- **agentes de tratamento** (inc. IX): *o controlador e o operador*;

- **autoridade nacional** (inc. XIX): *órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional* .

3.4 Quanto a conceitos fundamentais (Art. 5º)

• **tratamento (inciso** X): *toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*;

• **banco de dados** (inciso IV): *conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico*;

• **consentimento** (inciso XII): *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;*

• **transferência internacional de dados** (inc. XV): *transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;*

• **uso compartilhado de dados** (inciso XVI): *comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;*

• **relatório de impacto à proteção de dados pessoais** (inciso XVII): *documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

• **bloqueio** (inciso XIII): *suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;*

• **eliminação** (inciso XIV): *exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.*

Conforme disposto no **Art. 3º**, a Lei é **aplicável** a operações de tratamento realizadas por pessoa natural ou pessoa jurídica de direito público ou privado, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I *- a operação de tratamento seja realizada no território nacional;*

II *- a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou*

III *- os dados pessoais objeto do tratamento tenham sido coletados no território nacional.*

Por outro lado, o **Art. 4º** prevê que a lei **não se aplica** ao tratamento de dados pessoais:

I *- realizado por pessoa natural para fins exclusivamente particulares e não econômicos;*

II *- realizado para fins exclusivamente:*
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III *- realizado para fins exclusivos de:*
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

IV *- provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.*

3.5. Quanto aos princípios da LGPD

Como visto, é notório que a **LGDP** anseia por reflexão e criticidade dos agentes, de maneira que devem guardar a boa fé e observar os princípios nela enunciados nas atividades de tratamento de dados.

São 10 (dez) os princípios previstos nos incisos do Art. 6º da lei:

finalidade: propósitos legítimos, específicos, explícitos e informados ao titular;

adequação: compatibilidade do tratamento com as finalidades informadas ao titular;

necessidade: limitação do tratamento ao mínimo necessário, utilizando-se apenas de dados pessoais essenciais a suas finalidades;

livre acesso: consulta facilitada e gratuita, pelos titulares, sobre a forma, a duração do tratamento e a integralidade de seus dados pessoais;

qualidade dos dados: exatidão, clareza, relevância e direito à atualização dos dados;

transparência: informações claras, precisas e facilmente acessíveis aos titulares, observados os segredos comercial e industrial;

segurança: utilização de medidas técnicas e administrativas para proteger os dados pessoais;

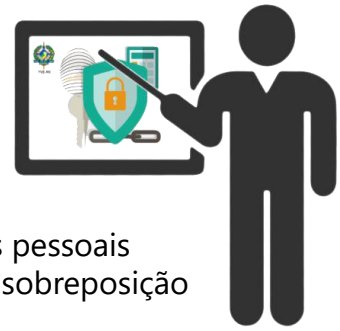
prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

responsabilização e prestação de contas: demonstração, pelos agentes de tratamento, da adoção de medidas eficazes e capazes de comprovar o cumprimento da lei.

4. Bases Legais para o enquadramento

Por Gabriela Marangoni



Tecnicamente falando, base legal é o fundamento do tratamento de dados, uma justificativa capaz de legitimar e autorizar o tratamento de dados pessoais.

A **LGPD** elenca 10 situações em que o tratamento de dados pessoais é possível, legítimo e justificável. E, aqui, destaca-se que não há sobreposição das bases legais, ou seja, não há hierarquia entre elas.

Para definir qual será a base legal a ser utilizada no caso concreto, é necessário avaliar **a origem do dado**, **a categoria e a finalidade.**

As bases legais previstas na LGPD, Art. 7º, são:

a) Consentimento: o tratamento de dados decorre da permissão expressa do titular de dados para que ocorra um determinado tratamento e com a finalidade previamente estabelecida e informada. Conforme artigo 8º da Lei supracitada, para que o consentimento seja válido, ele deve ser livre, específico, inequívoco e expresso.

b) Obrigação legal ou regulatório: o tratamento de dados deriva de uma lei ou instrumento fundamentado em lei. E neste caso, é importante destacar que não é apenas lei, incluindo também portarias, instruções normativas e regulamentos específicos.

c) Políticas públicas: o tratamento de dados deriva da finalidade do desenvolvimento de políticas públicas, ou seja, para solucionar problemas e demandas da sociedade. Esta base legal é destinada aos órgãos da administração pública direta ou indireta.

d) Pesquisa: o tratamento de dados deriva da finalidade de realizar pesquisas, desde que realizada por órgão de pesquisa.

Conforme seu **Art. 10º**, a Lei conceitua como órgãos de pesquisa aqueles órgãos da administração pública direta ou indireta ou que realiza pesquisa sem fins lucrativos, sendo que essa precisa ser constituída no Brasil e possuir no objeto social a realização de pesquisas com caráter científico, histórico, tecnológico ou estatístico.

e) Execução de contrato: o tratamento de dados deriva do cumprimento de uma obrigação prevista em contrato, em que o titular ou a pedido do titular, faça parte da relação contratual.

f) Exercício regular do direito em processo: o tratamento de dados deriva do exercício do direito de acesso à justiça.

g) Proteção da vida: o tratamento de dados deriva do risco iminente a vida do titular ou de um terceiro. É importante destacar que o risco deve ser concreto.

h) Tutela da saúde: o tratamento de dados deriva da prestação de serviços essenciais à saúde. É importante destacar que nesta base legal há restrição, uma vez que se refere aos profissionais da área da saúde ou entidades sanitárias.

i) Legítimo interesse: o tratamento de dados deriva do interesse do controlador ou do terceiro, desde que não ultrapasse os direitos e liberdades fundamentais do titular de dados.

j) Proteção ao crédito: o tratamento de dados decorre da proteção a concessão do crédito.

Ainda, a **LGPD**, no **Art. 11**, dispõe um rol diferenciado para tratamento de **dados pessoais sensíveis:**

Consentimento: o tratamento de dados decorre da permissão expressa do titular de dados para que ocorra um determinado tratamento e com a finalidade previamente estabelecida e informada. Conforme artigo 8ª da legislação supracitada, para que o consentimento seja válido, ele deve ser livre, específico, inequívoco e expresso.

Obrigação legal: o tratamento de dados deriva de uma lei ou instrumento fundamento em lei. E neste caso, é importante destacar que não é apenas lei, incluindo também portarias, instruções normativas e regulamentos específicos.

Realização de pesquisa,: garantida a anonimização dos dados pessoais sensíveis.

Políticas públicas: o tratamento de dados derivada da finalidade do desenvolvimento de políticas públicas, ou seja, para solucionar problemas e demandas da sociedade. Esta base legal é destinada aos órgãos da administração pública direta ou indireta.

Exercício regular do direito em processo: o tratamento de dados deriva do exercício do direito de acesso à justiça.

Proteção da vida: o tratamento de dados deriva do risco iminente a vida do titular ou de um terceiro. E importante destacar que o risco deve ser concreto.

Tutela da saúde: o tratamento de dados deriva da prestação de serviços essenciais à saúde. É importante destacar que nesta base legal há restrição, uma vez que se refere aos profissionais da área da saúde ou entidades sanitárias.

Garantia da prevenção à fraude e à segurança do titular: o tratamento de dados decorre da prevenção à fraude nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Neste caso, resguarda-se os direitos mencionados no artigo 9º da LGPD e no caso de prevalecer o direito de liberdade fundamental do titular que exija proteção aos dados pessoais.

Desta forma, a indicação da base legal será necessária para realizar o mapeamento do fluxo dos dados, relacionando a origem e a finalidade do dado.

5. Direitos dos titulares (clientes, colaboradores, terceirizados e fornecedores do Escritório de Advocacia)

Por Rodrigo Carvalho e Silva Canguçu de Almeida e Valéria Reani Rodrigues Garcia

5.1. Quem é o titular de dados pessoais?

O titular dos dados pessoais é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". O dado pessoal, por sua vez, é definido como "informação relacionada a pessoa natural identificada ou identificável" (**Art. 5º**, I); por exemplo, o Advogado ou a Advogada, a atendente da recepção do escritório de Advocacia, o cliente do escritório, os fornecedores ou outros terceirizados.

Importa esclarecer que o espólio e o *"de cujos"* não são titulares de dados pessoais. A pessoa jurídica não é titular de dados pessoais, mas seus sócios, funcionários e colaboradores são.

Uma vez esclarecido quem são os titulares de dados pessoais, passamos a indicar quais são seus direitos.

5.2. Mas, quais são os direitos dos cidadãos com a entrada em vigor da LGPD?

Todo cidadão brasileiro é titular de seus dados e tem assegurado os direitos fundamentais de liberdade, intimidade e privacidade. Portanto, o titular pode, via de regra, determinar quais de seus dados poderão ser tratados, como serão tratados, e para quais finalidades serão tratados. As exceções deste direito serão objeto de estudo em outro tópico, mas geralmente dizem respeito a determinação legal, preservação da vida, saúde e segurança pública.

Vale lembrar que os direitos dos titulares decorrem dos princípios estabelecidos no **Art. 6º** da **LGPD**, notadamente, o tratamento deve ter propósitos legítimos, específicos, explícitos e informados.

O tratamento deve ser adequado e compatível com as finalidades informadas previamente ao titular. Exemplo: facilidade na consulta de forma gratuita a respeito da duração do tratamento, bem como sobre quais dados são tratados. Direito à exatidão, clareza, relevância e atualização dos dados tratados.

Reiteramos que um dos principais direitos do titular é o de condicionar o tratamento dos dados ao consentimento prévio, expresso, inequívoco e informado, salvo se existir um outro fundamento de legitimidade.

A **LGPD** prevê, nos **Arts. 18 e 20**, uma ampla gama de direitos dos titulares de dados, dentre os quais podem ser destacados os seguintes:

i) acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva;

ii) confirmação da existência de tratamento;

iii) acesso aos dados;

iv) correção de dados incompletos, inexatos ou desatualizados;

v) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;

vi) 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;

vii) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Art. 16;

viii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

ix) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

x) revogação do consentimento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado;

xi) peticionamento em relação aos seus dados contra o controlador, perante a ANPD e perante os organismos de defesa do consumidor;

xii) oposição a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei;

xiii) solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade;

xiv) fornecimento, mediante solicitação, de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Acerca do consentimento, o titular pode exigir sua nulidade e sua revogação. Possui também direito ao acesso facilitado ao tratamento de seus dados e as informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade do tratamento, forma e duração. Sugerimos que seja inserido no contrato de prestação de serviços do advogado ou mesmo na procuração, um parágrafo tratando deste tema.

Contextualizando para o dia a dia de um escritório de Advocacia, o cliente pode, por exemplo, solicitar que seja informado com quem o escritório compartilhou seus dados. Dessa forma, o Advogado terá que informar, por exemplo, que foi compartilhado com o Tribunal de Justiça de São Paulo ou o Tribunal Regional do Trabalho, ou com a empresa responsável pelo *software* que ele utiliza para a gestão de seus casos e processos e, igualmente , com a empresa responsável pela nuvem onde ele armazena os documentos *(Dropbox, Onedrive, iCloud,* etc.) e até mesmo com o Advogado/escritório correspondente contratado para um determinado ato jurídico especifico.

Um exemplo de portabilidade de dados, muito comum para os Advogados, ocorre quando o cliente solicita que seja substabelecido os poderes por ele conferidos para seu novo Advogado que assumirá seus processos. No entanto, vale destacar que a portabilidade de dados ainda depende de definições que serão trazidas pela ANPD, especialmente diante da possível adoção de procedimentos simplificados e diferenciados para pequenas e médias empresas.

A anonimização de um dado é o processo no qual a informação pertencente a uma pessoa deixa de ser capaz de identificá-la ou torná-la identificável, e, portanto, deixa de ser considerado dado pessoal por força de lei.

No entanto, vale destacar que, não basta apenas substituir o nome de uma pessoa por um número ou pelas iniciais do nome. Caso as informações anonimizadas estejam atreladas a outro dado que possa identificar o titular a "anonimização" é falha.

Vale lembrar que os titulares têm direito à segurança de seus dados e também o direito à adequada prevenção de danos, portanto, além de todos os direitos indicados acima, ao tratarmos dados de clientes, colaboradores, terceiro, e, inclusive, da parte contrária, é necessário a observância da **segurança da informação**. Por isso mesmo, os escritórios de Advocacia devem assegurar que as informações estejam protegidas contra vazamentos e, caso ocorra algum incidente, medidas de prevenção devem ser adotadas para minimizar eventual dano ao titular.

Importante consignar que os **direitos do titular de dados** não podem confrontar regras estipuladas em outras leis que obrigam a manutenção de determinadas informações. Por exemplo: o Advogado pode recusar-se a excluir os dados de um cliente, colaborador ou parte contrária, caso exista uma lei estipulando prazo para armazenamento como ocorre com as obrigações trabalhistas, fiscais e previdenciárias inclusive o E-social, que dispensa o consentimento do titular para a guarda desses documentos.

Para encerrar, é importante destacar que o Advogado/ escritório deve adotar cautelas para **certificar que é o próprio titular de dados** que está solicitando informações sobre os dados requisitados. A título de exemplo, é possível pedir que o titular de dados preencha formulário próprio e apresente comprovante para, só então, os dados sejam apresentados. Entretanto deve-se evitar procedimentos complexos e demasiadamente burocráticos.

6. Período de retenção

Por Roseli Gomes Martins

Com a vigência da **LGPD** surgiram procedimentos necessários e também relativos à utilização de boas práticas no tratamento de dados pessoais no dia-a-dia das organizações.

Não seria de outra forma para os escritórios de Advocacia, que lidam diariamente com dados de seus clientes, colaboradores e fornecedores.

Por isso mesmo, é imprescindível cumprir os requisitos da LGPD, adequando-se com as ferramentas corretas, gerenciando as informações de clientes, colaboradores, fornecedores, etc, nos seus canais digitais e em conformidade com a legislação, mormente o **Art. 16** e seus incisos, embora a Lei autorize o tratamento de dados para o exercício regular de direito (**Art. 7.º**, V), sempre que houver legítimo interesse (**Art. 7º**, IX).

No que tange ao **período de retenção e guarda de dados e documentos**, os escritórios de Advocacia devem observar as disposições contidas nas legislações especiais atinentes à área em que atuam. A **LGPD** visa limitar essa retenção e armazenamento de dados, que não devem ser prolongados, sem motivação e finalidade determinada (artigo 15). Vale dizer que o período de retenção e armazenamento de dados deve respeitar o consentimento do titular dos dados e a concretização da finalidade da coleta, que devem estar previstos no contrato de maneira clara e objetiva.

Como exemplos, temos: estipular prazo para **o armazenamento** dos dados coletados; informar ao titular do dado acerca do **prazo de retenção** e requerer seu consentimento; ou **descartar corretamente os dados** após o período de utilização dos mesmos.

Para tanto, se faz necessário um projeto de gestão documental, envolvendo período em que cada informação deve ser armazenada, visando atender a **validade jurídico-fiscal** e aquela de uso interno do escritório.

Primordialmente, os dados de clientes devem ser retidos e armazenados durante todo o curso do processo até a efetiva prestação de contas com aqueles e a devolução dos documentos (se originais) ou sua eliminação (se digitais, endereços eletrônicos, vídeos e áudios).

Todavia, alguns documentos que se originaram no curso do processo (petições, intimações e comunicados enviados aos clientes, prestação de contas, recibos) devem ser guardados por prazos mais longos, visando eventual dúvida do cliente apresentada futuramente perante o órgão de classe dos Advogados, principalmente no que concerne à efetiva prestação de serviço contratada e prestação de contas.

Em relação a fornecedores e prestadores de serviços, a retenção de documentos (notas fiscais, recibos, garantias) devem ser armazenados de acordo com os Artigos 205 e 206 do ***Código Civil***, combinado com o ***Código de Defesa do Consumidor***.

Na área **Trabalhista**, os documentos inerentes a colaboradores e prestadores de serviços devem ser retidos e armazenados (dois) anos a contar da extinção do contrato de trabalho, observados os 5 (cinco) últimos anos de contratação (informações cedidas ao Ministério da Economia, INSS, Caixa Econômica Federal, CAGED, RAIS, e-Social), à exceção dos depósitos do FGTS (30 anos) e recolhimento de contribuições previdenciárias (10 anos).

Na área **Tributária**, em até 5 (cinco) anos, contados da constituição do débito (Art. 173, I do ***Código Tributário Nacional***), o que se aplica à Declaração de Imposto de Renda, ao IPTU ou ao IPVA.

No **Direito Penal**, deve ser calculado com base nas penas para os crimes. Por exemplo, para um crime com pena acima de 2 anos e inferior a 4 anos, a prescrição ocorre em 8 anos.

No **Direito Civil** temos o disposto nos Artigos 205 e 206 do ***Código Civil***, observada a natureza do objeto da ação.

No **Direito Previdenciário**, está prevista a guarda pelo prazo de 10 (dez) anos. O que se aplica à folha de pagamento, ao recibo e ficha de salário-família, aos atestados médicos relativos a afastamentos e incapacidade ou à guia de recolhimento de contribuição previdenciária.

Por fim, a retenção de dados também findará quando houver a revogação do consentimento ou de oposição.

6.1. Política de retenção de dados

Além dos resultados do mapeamento, é recomendado que o escritório elabore uma política de retenção quanto ao período necessário para manutenção de dados.

Abaixo uma tabela ilustrativa para dados pessoais em escritórios de Advocacia, com os respectivos prazos, considerados: clientes no contencioso; clientes consultivos; clientes de *Marketing*, Advogados, fornecedores e colaboradores.

Dados pessoais	Período de retenção	Termo a quo	Fundamento jurídico
Clientes - contencioso	05 anos	Conclusão dos serviços, cessação do contrato ou do mandato	Art. 206, §5°, II, CC com interrupção da prescrição (art. 202, I, CC c/c art. 240, §1°, CPC)
Clientes - consultivo	05 anos	Conclusão dos serviços; cessação dos contrato ou do mandato	Art. 206 §5°, II, CC
Clientes - marketing	01 ano	Opt-out (que deve constar em todas as comunicações)	Art. 6°, III da LGPD
Advogados	10 anos	Extinção do vínculo contratual	Art. 205, CC (prazo geral)
Fornecedores	10 anos (parcerias); 05 anos (consumo)	Extinção do vínculo contratual	Art. 205, CC (prazo geral); Art. 27, CDC (prazo específico de relação de consumo)
Colaboradores (CLT)	05 anos (a prescrição ocorre em 02 anos, mas exige a guarda dos últimos 05 anos, caso seja possível modelar dessa forma)	Extinção do contrato de trabalho	Art. 11, CLT

Tabela elaborada por Alexandre Atheniense

7. Compartilhamento de dados com terceiros

Por Valéria Reani Rodrigues Garcia e Carlos Alberto Casanova Campos

Segundo a **LGPD**, o uso compartilhado pode ser entendido como as situações em que os dados pessoais são comunicados, difundidos, transferidos interconectados ou internacionalmente.

Para qualquer setor de atividade, inclusive para os escritórios de Advocacia, os terceiros, muitas vezes, representam riscos do ponto de vista da proteção de dados. Por isso, devem os escritórios de Advocacia, compreender claramente que, as organizações com as quais compartilham dados pessoais, irão consequentemente realizar tratamento de dados pessoais em nome dos escritórios, e, portanto, serão operadores, além de compreender que os escritórios desenvolvem suas funções como controladores nesse contexto. Adicionalmente, devem gerenciar o relacionamento com terceiros para assegurar que os dados pessoais estejam protegidos em todo o ecossistema ao qual são submetidos.

Como afirmação de boa-fé, convém aos escritórios controladores escolher apenas operadores que adotem medidas apropriadas de proteção e segurança de dados e que estejam dispostos a cooperar em questões relacionadas à proteção de dados.

7.1. Transferência internacional de dados nos escritórios de Advocacia

Em geral, o tema é disciplinado pelos **Arts. 33 a 36** da **LGPD**. A transferência internacional de dados pessoais apenas é permitida nos casos previstos no **Art. 33**.

Tal disposição aplica-se igualmente aos escritórios de Advocacia que tenham outros escritórios correspondentes no exterior.

Além dos casos expressamente autorizados pela ANPD, caberá a ela definir os países ou organismos internacionais com nível de proteção de dados pessoais em conformidade à **LGPD** considerando:

i) as normas gerais e setoriais da legislação em vigor;
ii) a natureza dos dados;
iii) a observância dos princípios e direitos dos titulares;
iv) a adoção de medidas de segurança previstas em regulamento;
v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.

Outras circunstâncias específicas relativas à transferência:

i) o conteúdo de cláusulas-padrão contratuais;
ii) as normas corporativas globais;
iii) os selos, certificados e códigos de conduta aplicáveis.

Assim sendo , algumas regras do artigo 33 devem ser observadas desde já, de modo que a Lei autorize a transferência internacional de dados e que os escritórios de Advocacia devem ter atenção nos seguintes casos:

a) quando o **controlador** oferece e comprova garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD, na forma de cláusulas contratuais específicas para determinada transferência;
b) quando a transferência for necessária para a **cooperação jurídica internacional** entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
c) quando a transferência for necessária para a **proteção da vida** ou da incolumidade física do titular ou de terceiro; ou
d) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o **caráter internacional da operação**, distinguindo claramente essa de outras finalidades.

Entretanto, vale ressaltar que, boa parte dessas hipóteses, ainda dependem de regulamentação pela ANPD e que no cenário de 2024 já podemos citar que foi publicada a Resolução CD/ANPD nº 19, de 23 de agosto de 2024, que aprova o "Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais".

Como bem comenta Felipe Palhares, em seu Perfil público do *LinkedIn*, na mesma data da publicação, o que de fato precisamos saber sobre o Regulamento da ANPD de transferências internacionais de dados.
Para tanto, Palhares assevera que:

— "Se o mecanismo usado para garantir a legalidade das transferências internacionais é a estruturação de cláusulas contratuais, elas provavelmente precisarão ser as SCCs(1). aprovadas pela ANPD, que devem ser incorporadas no prazo máximo de 12 meses.

— Cláusulas contratuais específicas, embora previstas pela legislação, foram tornadas num mecanismo residual, que somente pode ser utilizado quando o controlador comprovar que as cláusulas-padrão não podem ser utilizadas por razões excepcionais.

— É hora de atualizar (de novo) o seu Aviso de Privacidade para incluir informações mais granulares sobre transferências internacionais, incluindo os países de destino dos dados transferidos.

— Ao que tudo indica, as cláusulas-padrão precisarão ser firmadas em português (ou ao menos em formato bi colunado). Será fácil explicar isso aos importadores. Pois eh! Mas não é bem assim!

— Vejamos, como já virou costume, o Regulamento europeu impõe obrigações adicionais aos agentes de tratamento não previstas na LGPD, como a criação de um direito do titular de solicitar cópia das cláusulas-padrão, específicas ou das normas corporativas globais."

1. As SCCs são cláusulas-tipo (também chamadas de "contratos modelo") pré-aprovadas pela Comissão Europeia com o objetivo de assegurar que a transferência internacional de dados pessoais entre uma entidade dentro da União Europeia e outra entidade fora da zona econômica tenha as ***garantias adequadas*** *de que o tratamento de dados terá ao menos o* ***mesmo nível de proteção previsto pela GDPR*** *(General Data Protection Regulation) e que* ***os direitos dos titulares de dados previstos nesta regulação serão respeitados****. Disponível em https://blconsultoriadigital.com.br/sccs-standard-contractual-clauses/#:~:text=As%20SCCs%20são%20cláusulas%2Dtipo,de%20que%20o%20tratamento%20de*

Já em seu comentário a Resolução em seu perfil publico em rede social do *Linkedlin*, Viviane Nóbrega Maldonado, destaca de forma breve porém muito conclusiva que em síntese, haverá, por regra, apenas 3 hipóteses:

"*1. Nada precisará ser feito pelo agente de tratamento se a transferência for realizada para um país que proporcione grau de proteção de dados adequado. E quem decide isso? A ANPD, que fará uma avaliação e criará uma lista desses países adequados (esse é o exato modelo da União Europeia). Nesse caso, o agente de tratamento consulta a lista e, se encontrar o país, ele simplesmente realiza a transferência.*
2. Se o país não estiver na lista (ou seja, não for considerado adequado), o agente de tratamento deverá adotar as cláusulas-padrão contratuais caso o importador seja uma empresa dele desvinculada, assim entendida uma outra entidade.
3. Por fim, se a transferência dos dados a um país não adequado ocorrer dentro do mesmo grupo empresarial ou conglomerado (por exemplo, entre matriz e filial), devem ser adotadas as normas corporativas globais."

Ainda bem complementa Mandonado, que para documento citado acima, no que concerne a hipótese 1, não há exigência; a hipótese 2, interessante adotar o modelo constante da Resolução sem mudar uma vírgula (à exceção do que deve ser customizado) e finalmente na hipótese 3, convém submeter as normas corporativas globais à aprovação da ANPD.

Finalmente, no mais, e em seu todo, a ANPD ressalta nessa Resolução nº 19 a necessidade de medidas de transparência, conforme ao **Art. 31**.

2. Ressaltamos que o conteúdo acima que cita os comentários de Felipe Palhares e Viviane Nóbrega Mandonado, encontram-se em seus respectivos perfis, de forma publica, o que carece de necessidade de autorização, mas que por precaução, a Comissão a pediu de cada um para citação de seus valiosos comentários, ocasião em que ambos, além de autorizar, também sentiram-se honrados.

8. O que muda no dia a dia do escritório de Advocacia?

Por Ana Paula Silva de Oliveira e Valéria Reani Rodrigues Garcia

8.1. Relação do Escritório e seus colaboradores

Quando falamos de colaboradores no escritório de Advocacia estamos incluindo: Advogados empregados, Advogados associados, sócios, diretores, CEO, estagiários, auxiliares da limpeza, os Recursos Humanos, os setores administrativo, financeiro e de T.I, bem como a equipe de Marketing.

Para melhorar essa relação, é importante que o escritório de Advocacia realize algumas ações a nível de conscientização.

Abaixo citamos algumas ações que podem facilitar a implementação na prática:

i) criar um **Comitê de Proteção de Dados**;

ii) realizar **reuniões periódicas** onde os participantes possam interagir, assim como grupos de debates;

iii) efetivar **treinamentos** com interação dos colaboradores;

iv) promover eventos como **seminários e conferências**, para compartilhar o conhecimento;

v) elaborar **políticas internas**;

vi) criar um **canal interno para dúvidas**;

vii) participar de **feiras e café de conhecimentos**.

Abaixo disponibilizamos um **roteiro de conscientização inicial** e algumas ferramentas que podem ser utilizados com todos os colaboradores:

1. Contextualização: Debates sobre a importância da privacidade, tecnologia e Advocacia 4.0.

2. Entendendo a LGPD: Debate sobre os principais pontos da Lei.

3. Posicionamento: Demonstre como o escritório está posicionado no mercado porque ele deve se adequar a LGPD.

4. Entrevista com os colaborares: Entenda como funciona o fluxo de dados com cada profissional e cada setor do escritório.

5. Matriz *SWOT*: Faça um questionário dinâmico com os colaboradores utilizando ferramenta *SWOT* (forças, fraquezas, oportunidades e ameaças),

6. *Brainstorming*: Realização de debates internos para compartilhar ideias.

7. *Overview*: Repasse aos colaboradores o que será feito e como será feito no processo de implementação, sendo relevante, também demonstrar o papel de cada um no processo de adequação.

8.2. Relação do escritório e seus clientes

Além de comunicar todos os colaboradores sobre o processo de implementação, vai ser necessário que os clientes também estejam cientes da adequação da **LGPD** no seu escritório.

Dessa forma, convém elaborar um "Aviso de Comunicação" a todos clientes informando a importância da adequação do escritório de Advocacia à nova Lei, que pode ser encaminhada pelo principal meio de comunicação com os colaboradores e clientes, seja por *e-mail, WhatsApp* ou até mesmo por um comunicado fixado no site institucional.

Além de comunicar o projeto de adequação à **LGPD,** é importante que todo o escritório conheça também os direitos dos titulares que podem ser solicitados, a qualquer momento, pelos seus clientes pessoas físicas.

Especificamente, o escritório de Advocacia atenderá a requisição do titular dos dados e providenciará o solicitado de duas formas:

1º modelo: Formato simplificado e entregue de imediato.

2º modelo: mediante declaração clara e completa com descrição da origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

8.3. A revisão de contratos de honorários

A revisão do contrato de honorários vai ser essencial nesse momento de implementação da **LGPD**, conforme sugestão abaixo:

nos **novos contratos:** inserir cláusulas de proteção de dados específicas e de acordo com o mapeamento de dados do seu escritório.

nos **contratos vigentes:** fazer um termo aditivo de contrato ou termo de consentimento (se for o caso).

O primeiro passo para elaborar essas cláusulas no contrato em adequação é verificar como funciona o fluxo de dados no seu escritório, quais tipos de dados são coletados, onde são armazenados, com quem é compartilhado e como são descartados.

Abaixo destacamos as principais cláusulas que vão ser necessárias no contrato de honorários:

a) cláusula **conceitual** LGPD;

b) cláusula do tipo de **dados pessoais e dados pessoais sensíveis**;

c) cláusula sobre a **atuação do escritório** como controlador;

d) cláusula específica de **tratamento de dados**;

e) cláusula de **compartilhamento**;

f) cláusula de **transferência de dados**;

g) cláusula de **armazenamento**;

h) cláusula de **direito dos titulares**;

i) cláusula de incidente de **segurança**;

j) cláusula de canal de **comunicação e DPO** / Encarregado da proteção de dados

8.4. Novidades para os Advogados

Você sabia que, pela primeira vez, tabela de honorários de 2024, inclui privacidade, proteção de dados e IA?

Ao divulgar a nova **Tabela de Honorários Advocatícios**, a OAB-SP trouxe uma novidade ao incluir de, forma pioneira, itens específicos para atividades relacionadas à Privacidade e à Proteção de Dados Pessoais.

Entendemos que essa inclusão representa **um avanço significativo para os advogados que atuam nessas áreas emergentes** e de extrema relevância no contexto atual, como o avolumar dos aconselhamentos, assim como dos processos, em matéria de Privacidade e Proteção de Dados, inclusive relacionados com a Inteligência Artificial, na seccional paulista da OAB, em especial na subseção de Campinas.

Especificamente, a inclusão encontra-se no item 31, conforme demonstra a imagem da tabela abaixo:

31	ATIVIDADES EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS	VALOR SUGERIDO	
	ATIVIDADES CONSULTIVAS / EXTRAJUDICIAIS		

Para acesso à Tabela: https://www.oabsp.org.br/upload/1885288261.pdf

8.5. Os cuidados com a utilização de aplicativos de troca de mensagens e comunicação em áudio e vídeo, *e-mails* corporativos e SMS

Na Advocacia, a troca de documentos oficiais entre colegas de trabalho bem como entre clientes se tornou rotina, devido à capacidade de visualização célere no compartilhamento de documentos e informações, via celular ou *notebook*, pois as informações e conteúdo são instantâneos ao receptador.

No entanto, é necessário ter alguns cuidados, que chamamos a atenção:

Política interna de Proteção de dados: Elaboração de termos de uso ou uma política de proteção de dados, a exemplo das regras de uso interno da internet e ferramentas tecnológicas**,** para colaboradores e clientes estejam cientes das normas utilização das ferramentas e de como devem ser realizado o tratamento de dados pessoais;

Meio de comunicação padrão: A depender do porte do escritório, é interessante o escritório disponibilizar aos seus colaboradores o acesso a meios de comunicação próprios como a intranet, celular corporativo, plataformas especificas ou e-mails com garantia de criptografia de ponta a ponta;

Grupos em aplicativos de mensagens do escritório: é necessário ter cuidado com os dados pessoais dos participantes, especificamente, nome e telefone, devem ser guardados com sigilo, sendo vedado o compartilhamento com terceiros;

Política de *Backup*: Adotar políticas de cópia de segurança relativamente a todas as mensagens trocadas, sejam escritas, por áudio ou vídeo.

Política de descarte de dados: Excluir documentos/informações daquilo que não é mais necessário, para evitar o vazamento.

8.6. Cuidados a serem observados em reuniões virtuais

Com relação a reuniões *online*, elas ocorrem atualmente em diversas plataformas como por exemplo: *Microsoft Teams, Google Meets, Zoom, Whatsapp, Cisco Webex, Skype* e outras. No entanto é necessário estar atento a segurança e utilização de todas essas plataformas a fim de evitar qualquer incidente de segurança. Dessa forma é importante criar um **guia orientativo** de uso de segurança e sistemas de conferências e reuniões online.

Abaixo listamos alguns cuidados pessoais e técnicos de atenção para todos os Advogados:

8.6.1 - Cuidados Pessoais:

i) crie políticas internas e manuais sobre a utilização de plataforma para reuniões;
ii) realize teste a plataforma antes do horário;
iii) somente grave a reunião depois que todos concordarem com a gravação, resguardando a privacidade e o sigilo da informação. (Algumas plataformas emitem uma notificação quando a gravação é iniciada);
iv) verifique o material que eventualmente vai ser compartilhado evitando o compartilhamento de informações confidenciais do seu escritório;
v) monitorize os participantes e controlar suas permissões e mensagens durante a reunião.

8.6.2 - Cuidados Técnicos:

i) faça a configuração da plataforma antes da reunião iniciar.
ii) configure o som e vídeo realizando testes antes de iniciar.
iii) configure as permissões concedidas (na hipótese de aplicativos).
iv) atualize os aplicativos / *software* e o *browser***.**
v) mantenha sempre o antivírus atualizado.
vi) crie controle de acesso para anfitrião e convidados como por exemplo senhas e *links* específicos para acesso.
vii) tenha um especial cuidado com *links* compartilhados no *chat* fora de contexto, uma vez que podem ter sido inseridas por *malwares*.

Com tudo isso, é importante destacar que o principal foco aqui é o treinamento dos Advogados e demais colaboradores que vão utilizar as ferramentas e realizar a reunião de forma *online*.

8.7. A relação do escritório e o poder público, sobretudo o Judiciário, cadastro de documento sigilosos em processo públicos

Com a vigência da **LGPD**, os tribunais brasileiros estão criando critérios padronizados para adequação à **LGPD**. Dessa forma foi criada a resolução 363/2021, aprovada pelo Conselho Nacional de Justiça (CNJ)(1). Assim, o Judiciário caminha no sentido de cada vez mais se adequar à proteção de dados.

Nesse viés, é importante destacar a relação de todo Advogado e profissional do escritório jurídico com relação a utilização de protocolos e cadastros nos sites dos tribunais.

Por sua vez, o ***Código de Processo Civil*** informa que os atos processuais serão públicos com ressalva dos seguintes:

i) interesse público ou social;

ii) em hipótese de casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes;

iii) dados protegidos pelo Direito Constitucional à intimidade;

iv) em caso de arbitragem, por cumprimento de carta arbitral.

Dessa forma e salvo exceções, os atos processuais ocorrem de forma pública, mas com a vigência da LGPD isso muda?

A resposta para essa pergunta vai depender muito da análise do objeto do processo, sendo necessário que o profissional verifique se o protocolo realizado de modo público pode prejudicar e violar a proteção dos direitos fundamentais de liberdade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural previsto na **LGPD**.

É importante ressaltar que ao solicitar o sigilo no protocolo de peças processuais que não estão no disposto do artigo vai ser necessário fundamentar tal pedido.

Fonte: *CNJ, disponível em: https://www.cnj.jus.br/lgpd-norma-define-criterios-minimos-para-adequacao-pelos-tribunais/*

8.8. Substabelecimento de poderes para Advogados correspondentes

As atividades da Advocacia muitas vezes e na maior parte é terceirizada para outros Advogados realizarem os atos processuais. Nesse caso, estamos falando dos correspondentes jurídicos. Assim, é fundamental a elaboração de termos de consentimento para o Advogado correspondente do escritório de Advocacia.

Nos termos da **LGPD**, os Advogados correspondentes poderão ser considerados como operadores quando atuarem no apoio e sob direção do escritório controlador. Pelo que é importante que o Advogado correspondente siga as diretrizes do escritório controlador, sem atender finalidades próprias.

Ressalta aqui o **Art. 42** da **LGPD**, o qual determina a responsabilidade solidária do controlador e operador por eventuais danos causados ao titular de dados. Consequentemente, o escritório e Advogado correspondente precisam estar alinhados quanto a proteção de dados do titular de dados.

8.9. A relação do escritório de Advocacia e o site corporativo (termos de privacidade, uso de *cookies*), indicação de encarregado, cadastro de *newsletter* e formulários

Os sites dos escritórios de Advocacia são muito afetados pela **LGPD**, pois possuem mecanismos que devem ser adaptados ao contexto da norma. Nesse primeiro momento, vai ser necessário:

i) atualizar a **política de privacidade**, sendo indispensável que o sítio eletrônico apresente um ponto específico com a **apresentação do termo de privacidade** e uso de dados do usuário, não esquecendo da autorização do titular dos dados para o recolhimento das informações **armazenadas;**
ii) atualizar os **termos de uso de site**, que devem ficar em evidência;
iii) atualizar **política de *cookies*,** uma vez que cada visitante deverá ter conhecimento, de forma clara, que seus dados estão sendo armazenados e para qual finalidade e tempo de tratamento.

Convém ter atenção e refletir acerca da necessidade e finalidade com Cadastro de *newsletter* e formulários, a exemplo de "**fale conosco**" ou "**trabalhe conosco**", devem ser adaptados para que sejam **transparentes** e tratem somente os dados que forem estritamente necessários.

8.10. Onde estão armazenados os dados de clientes, colaboradores e fornecedores?

Nesse momento, é necessário mapear onde ficam os arquivos de dados de clientes, colaboradores e fornecedores.

Podem ocorrer os seguintes cenários de armazenamento:

Ambiente Físico

Ambiente Digital/ Online

Físico + Digital/ Online

O armazenamento de dados é uma das fases do ciclo de vida de dados, precisando ser gerenciado pelo escritório. Esse armazenamento é o período que o dado estará armazenado no escritório de acordo com o dispositivo legal setorial específica para cumprir sua finalidade.

Assim, o armazenamento deverá ser realizado até que a finalidade da coleta seja alcançada e enquanto forem necessários para a finalidade, regular execução do contrato ou cumprimento de obrigações decorrentes de lei. Essa regra também vale para documentos físicos, pois o arquivamento desse material algumas vezes é realizado de forma negligente, sendo reaproveitados como rascunhos.

Para tanto, convém criar um controle de acesso para o armazenamento de alguns dados, considerados em todos os ambientes de armazenamento, desde o computador até o arquivo local.

8.11. O descarte de documentos e dados pessoais. Onde, quando e como fazer

O descarte deve ser realizado por meio de uma política correta, levando em consideração algumas **leis específicas** que obrigam a retenção de alguns documentos por um período de tempo específico.

A **disposição legal** de eliminação de dados é prevista no **Art. 16** da **LGPD**, a qual determina que, após o término do tratamento, os dados pessoais serão eliminados.

Vale ressaltar que a eliminação dos dados pode acontecer por solicitação do titular ao escritório de Advocacia, portanto é necessário verificar como as ações de descarte de dados pessoais podem ser realizadas.

8.11.1. Quanto às ações necessárias para realizar o descarte:

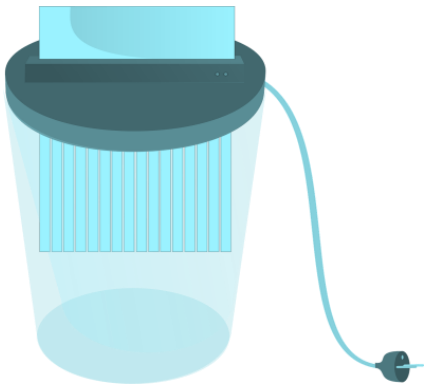
i) verifique os **prazos de retenção obrigatória** na legislação vigente como em normas e resoluções do conselho de classe **profissional;**

ii) elabore uma **política de retenção e descarte** do escritório, vez que este documento comprova que o titular foi informado sobre a política de retenção e descarte da empresa;

iii) evidencie, todos os **registros de descartes** que estão sendo realizados em uma planilha para comprovar em futura auditoria.

Descarte digitais: é necessário estabelecer boas práticas em segurança da informação para que os dados que foram eliminados e, realmente, não estejam acessíveis.

Descarte físico: poderá ser realizado através de máquinas desmagnetizadoras, trituração ou incineração de papéis.



9. O que é um Código de Conduta e sua importância

Por Beatriz de Andrade Junque e Beatriz Pistarini de Souza

Atualmente, um dos maiores desafios diante da legislação de Proteção de Dados, sob o viés econômico e político, é justamente sua implementação.

Como se trata de um marco significativo para a consolidação dos direitos e garantias fundamentais do indivíduo, titular de dados, com intensas mudanças em todos os setores da sociedade, inclusive dentro dos escritórios de Advocacia, se faz necessária a elaboração de um **Código de Conduta**. Neste se estabelecem os princípios éticos e descreve **normas de conduta** que orientam as relações internas e externas de todos os integrantes da organização, com temas abordados que delimitam condutas apropriadas e não apropriadas desde conflitos de interesses, corrupção, assédio, incluindo a confidencialidade de informações, fator essencial para proteger os dados mais importantes da empresa.

O Código de Conduta é uma excelente ferramenta que deve ser utilizada no processo de implementação da **LGPD**, independente do ramo que se encontra em processo de adequação, que visa orientar e disciplinar a conduta de um determinado grupo de pessoas. A própria **LGPD** prevê a possibilidade da criação de códigos de conduta pelo setor privado, nos termos de sua seção II, dedicada às boas práticas e à governança, em seu **Art. 50**, caput:

> "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, **poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos**, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais." *(grifo nosso)*

Consequentemente, os códigos de conduta serão um norteador essencial para previsão de **regras de boas práticas e de governança**, no qual poderão ser estabelecidas condições de organização, regime de funcionamento, procedimentos, obrigações específicas, ações educativas, mitigação de risco e dentre outros pontos essenciais no que tange ao tratamento de dados pessoais.

Concluindo, um Código de Conduta é um ótimo instrumento para garantir os direitos previstos da referida legislação, possibilitando debates dentre as principais especificidades do ambiente corporativo a ser regulado, além de incentivar a inovação com responsabilidade e consolidar a confiança dos titulares de dados, que para o presente guia serão os clientes ou colaboradores, terceirizados e fornecedores de um escritório de Advocacia.

10. É necessária uma política interna do uso da internet e das ferramentas tecnológicas?

Por Beatriz de Andrade Junque e Beatriz Pistarini de Souza

Ao utilizarmos ferramentas tecnológicas, temos consciência de regras implícitas, ou seja, a mantença da moral, dos bons costumes e do decoro com os demais usuários.

Porém, ao abordarmos sobre uma relação de prestação de serviço, em específico um escritório de Advocacia, temos a consciência de que cada um apresenta dinâmica e regras próprias. Portanto, é de suma importância que todos os colaboradores tenham ciência das regras, e que estejam de fácil acesso para consulta.

Conforme mencionado no tópico anterior, a **LGPD**, em sua seção II: "Das Boas Práticas e Governança", no seu **Art. 50**, estabelece a possibilidade de formulação de regras de boas práticas.

Já o § 1º, do mesmo dispositivo, determina acerca do que deve ser levado em consideração para elaborar as regras de boas práticas, sendo os seguintes pontos:

"Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular."

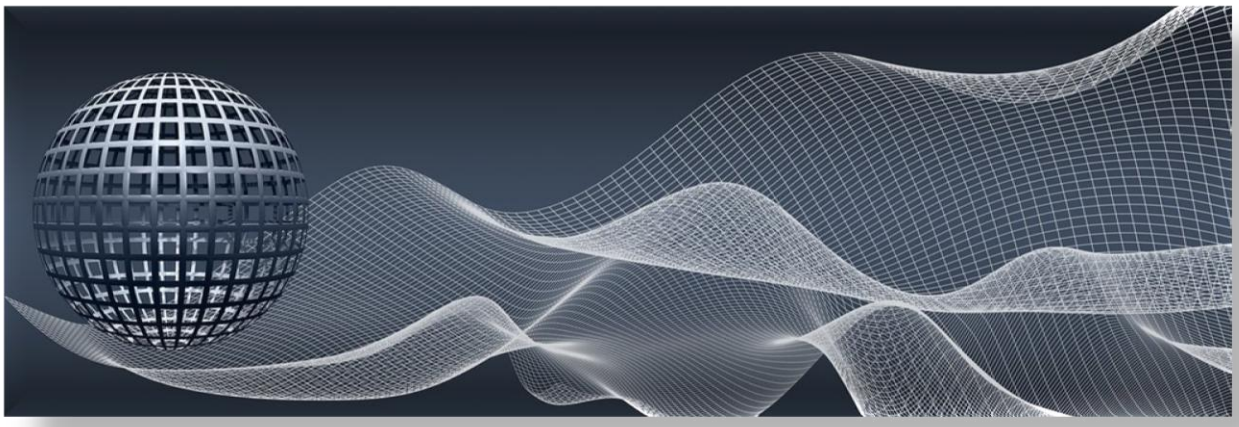
Estipula também outro requisito em seu § 3º, que consiste na necessidade de publicação e atualização periódica, assim como, a possibilidade de reconhecimento e divulgação pela autoridade nacional:

"As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional."

Analisa que a **LGPD** não obriga quanto a criação de uma política interna do uso da internet e das ferramentas tecnológicas, mas orienta quanto à possibilidade de sua criação, abordando acerca do que deve ser levado em conta para sua elaboração, necessidade de atualização periódica e publicação. Portanto, não há estipulação quanto ao que deve conter em seu conteúdo, como será realizado o seu monitoramento, ou penalidades pelo descumprimento.

Muitas vezes, a utilização da internet e de outras **ferramentas tecnológicas** gera uma sensação de anonimato e não incidência de penalidades ao usuário, o que pode levá-lo a ter uma conduta no mundo virtual diversa da que teria no mundo real. Consequentemente, é necessário estabelecer e informar quanto às regras de boas práticas e utilização de meios eletrônicos, mesmo que de certa forma parece ser irrelevante, pois, em determinadas situações o óbvio precisa ser dito e regulamentado.

À vista disso, ao decidir estabelecer uma **política interna do uso da Internet** e das ferramentas tecnológicas, é preciso transcrever a realidade do escritório de Advocacia, determinando o que é permitido e proibido pelo mesmo, a quem é direcionado e a quem se aplica a respectiva política, o que deve ser feito quando identificado um problema e a quem contatar.



Por isso mesmo, é necessário também abordar acerca de mecanismos de identificação do usuário, versando sobre sua necessidade e responsabilidade, ciência quanto à **proteção de dados pessoais**, regulamentar o uso de internet, acesso a rede, meios permitidos de comunicação, como e-mail, redes sociais, aplicativos de envio de mensagem, utilização de computadores, recursos tecnológicos e dispositivos móveis, deixando sempre muito claro as permissões do colaborador em como deve ser o seu comportamento e o que deve estar ciente.

Ao implantar a respectiva política interna, o escritório de Advocacia deverá ter a preocupação de mantê-la atualizada e dar conhecimento a todos os colaboradores.

É também relevante que, ao ocorrer qualquer violação a presente norma, com o colaborador apresentando o devido conhecimento sobre a mesma, há possibilidade de incidência de penalidade, uma vez que o mesmo não pode alegar o desconhecimento.

É de suma importância providenciar ciência a todos os colaboradores, inclusive a alta administração e seguir os **Princípios da LGPD**, elencados em seu **Art. 6º**, já enunciados acima.

Por fim, a **LGPD** não obriga quanto a criação de política interna do uso da internet e das outras ferramentas tecnológicas, porém, para um bom funcionamento e diligência quanto problemas futuros a elaboração desta regulamentação, vislumbrando a realidade em que será inserida, para trazer maior proteção ao escritório de Advocacia e seus colaboradores, que com a sua implementação terão conhecimento das boas práticas de seu ambiente de trabalho, proibições, e medidas que devem ser tomadas ao identificar um problema e a quem contatar.

11. O *roadmap* de adequação

Por Sylvio Sobreira Vieira

11.1. O mapeamento e registro das atividades de tratamento e sua finalidade

A **LGPD** cita como obrigatório ao Controlador e ao Operador manter os registros das atividades de tratamento de dados pessoais. Sendo assim, podemos interpretar o registro identificado como evidência de cada tipo de tratamento, ou, efetivamente o funcionamento do ciclo de vida do dado pessoal, o entendimento, a análise e modelagem de um tratamento, o que chamamos de "mapeamento".

Iniciando um programa de adequação e ***compliance***, será necessário identificar quais macro padrões, ecossistema regulatório, mercado de atuação, produtos ou serviços prestados implicam como fatores críticos de sucesso. O mapeamento será crucial para o sucesso de um programa de *compliance* e proteção de dados, dessa forma, organize um programa de projetos ou um projeto em si para iniciar os trabalhos, identifique todas as áreas da companhia, no caso o escritório de Advocacia.

Este é o trabalho inicial para o escritório de Advocacia (todos os departamentos tratam dados pessoais), selecione responsáveis (*privacy leaders or privacy champions*), estes serão olhos, braços e pernas do programa de *compliance* para o escritório.

A identificação das atividades de tratamento de dados no escritório de Advocacia, pode ser feita de diversas formas, entre as mais comuns estão as entrevistas, análises, evidências, preenchimento de planilhas ou até mesmo *softwares* de *Data Discovery* (onde, conceitualmente, uma ferramenta consegue identificar os **pontos de tratamento de dados**, de acordo com o comportamento do titular nos sistemas, banco de dados e infraestruturas de uma empresa).

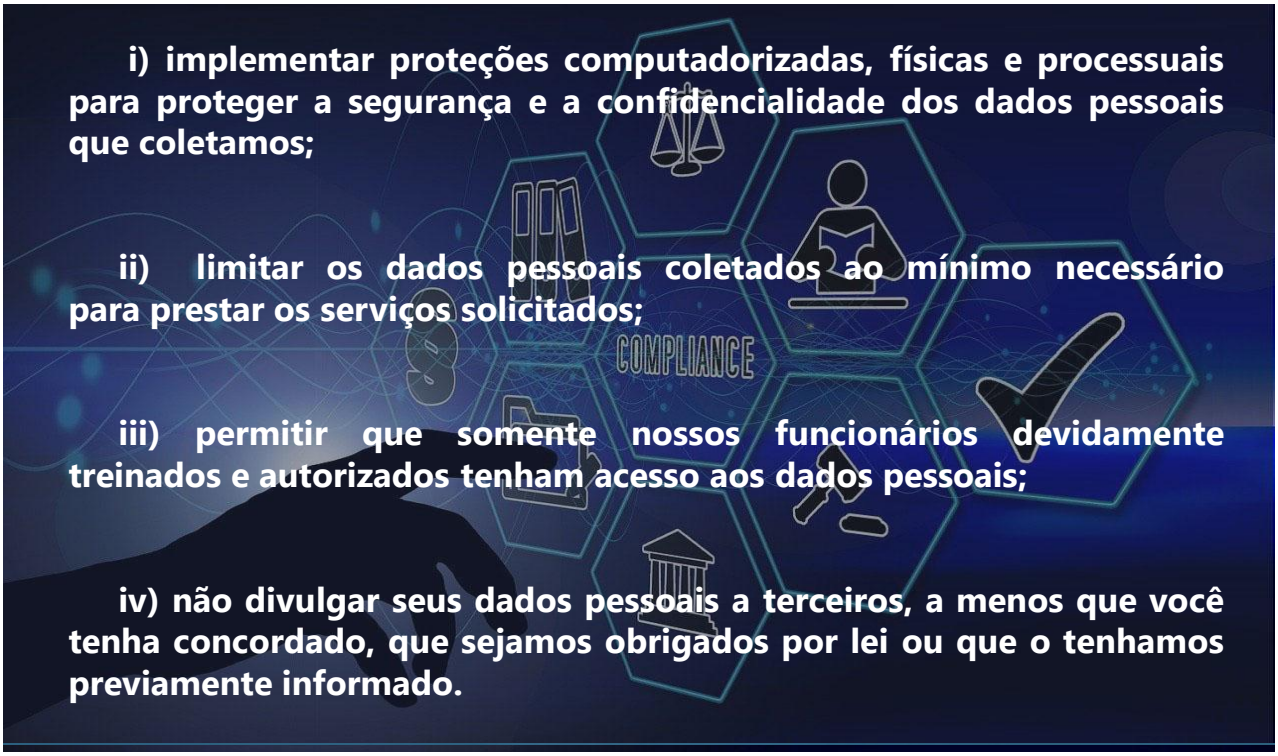
Convém escolher o modelo de mapeamento que mais que mais se ajuste à necessidade e realidade. Porém, é crucial que seja efetivo e tenha capacidade de fornecer total visibilidade sobre as atividades de tratamento do escritório, além de questionar a real necessidade e finalidade de cada tratamento em **conformidade com a LGPD.**

Cada atividade mapeada, deverá respeitar um propósito legítimo, isto é , hipóteses para legitimar o tratamento de dados, previstas nos **Arts. 7º** e **11º** da Lei, onde haverá clareza explicita das informações e propósitos no tratamento, ser específico em respeitar os limites comunicados e conter todas as informações necessárias para que o titular tenha segurança e confiabilidade no programa de proteção de dados pessoais.

11.2. A importância da estrutura de governança em privacidade

Estabelecer um programa ou sistema de **gestão em governança** em privacidade, é um desafio para toda e qualquer organização. Aqui trataremos sobre temas alinhados desde objetivos estratégicos de negócios focados em escritório de Advocacia, até execuções operacionais do dia a dia. Importantíssimo, o escritório desenvolver uma missão, sua visão e estratégia perante a privacidade e proteção de dados. Tendo esta definição, deverá ser desenvolvido e comunicado uma estratégia de trabalho ou *framework* de adequação.

Respeitamos sua privacidade, conforme estratégia de trabalho abaixo:



i) implementar proteções computadorizadas, físicas e processuais para proteger a segurança e a confidencialidade dos dados pessoais que coletamos;

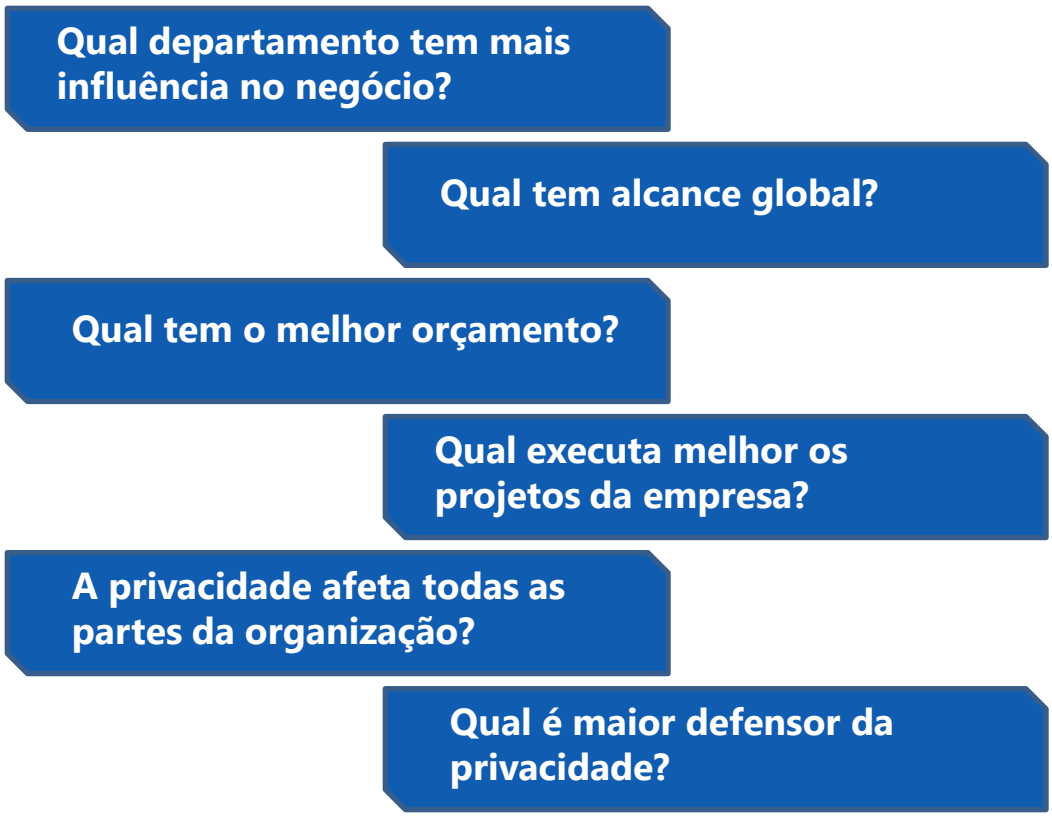
ii) limitar os dados pessoais coletados ao mínimo necessário para prestar os serviços solicitados;

iii) permitir que somente nossos funcionários devidamente treinados e autorizados tenham acesso aos dados pessoais;

iv) não divulgar seus dados pessoais a terceiros, a menos que você tenha concordado, que sejamos obrigados por lei ou que o tenhamos previamente informado.

Inicialmente, na prática, teremos que ter a **identificação dos tratamentos de dados pessoais** (“mapeamento” tratado no item anterior), elucidação das finalidades, alocação de bases legais que irão legitimar os tratamentos e criações de planos de ações que visam assegurar uma maior segurança, prevenção e conformidade as atividades de tratamento de dados pessoais, chegará o momento de encararmos a implantação destes planos de ações.

Ao estabelecer a privacidade dentro de uma organização, convém que sejam respondidas as seguintes questões:



O próximo passo, será selecionar um **Encarregado Dados** que tenha as devidas habilidades, experiências e que não existam conflitos de interesses setoriais no escritório, ou seja, ele é independente e responderá ao mais alto nível do escritório.

Um recurso que será extremamente necessário e ativo durante todo programa de *compliance* será a **conscientização dos titulares**, sejam eles funcionários, fornecedores ou clientes, sendo assim, um plano de treinamento e comunicação será requerido.

Por último cabe ao programa de governança, avaliar e estabelecer a real necessidade de possíveis **aquisições sistêmicas**, as particularidades e considerações, devem ser levadas a rigor para que qualquer insucesso não traga descrédito a estrutura de governança em privacidade.

12. Política de segurança da informação e de privacidade

Por Marcelo Vieira de Menezes

Atualmente, a área de **Tecnologia da Informação (TI)** é a responsável pela guarda dos dados e informações sobre qualquer negócio, seja ele, privado ou público. As bases de dados armazenam várias dessas informações e ainda são consumidos por diversas aplicações diariamente. Com isso, temos uma necessidade de avaliação constante de como a segurança está aplicada para garantir a privacidade dos dados.

A política de **segurança da informação e de privacidade** são diferentes, pois possuem abordagens distintas para alcançar seus próprios objetivos.

Em síntese, a política de segurança da informação tem como responsabilidade proteger o negócio contra riscos e incidentes como vazamento de dados, ataques cibernéticos e indisponibilidade, já a gestão de privacidade busca atuar sobre como a informação é coletada, distribuída e utilizada dentro de uma organização.

12.1. O que é Política de Segurança da Informação (PSI)?

Política de Segurança da Informação consiste em um conjunto de políticas emitidas por uma organização para garantir que todos os usuários de tecnologia da informação, no domínio da organização ou de suas redes, conheçam as regras e diretrizes relacionadas à segurança das informações armazenadas digitalmente em qualquer ponto da rede ou dentro dos limites de autoridade da organização. A mesma deve provir de orientações da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A **PSI** deve, em toda sua estrutura, conter declarações relativas a definição de segurança da informação, seus objetivos e princípios para a orientação de todas as atividades relacionadas à segurança da informação, à atribuição de responsabilidades, gerais e específicas, onde faz-se o gerenciamento da segurança da informação definindo os papéis e ter processos para o tratamento dos desvios e exceções.

A falta de medidas de segurança de dados apropriadas aumenta o risco de incidentes de segurança e de vazamento de dados.

Os vazamentos de dados podem ter um impacto significativo na organização a partir de várias perspectivas:

Perspectiva regulatória: a ANPD pode emitir multas e o controlador pode ser considerado responsável;

Perspectiva judicial: os indivíduos podem ajuizar ações judiciais contra os controladores e operadores, e também algumas instituições públicas podem ajuizar ações civis coletivas contra tais agentes de tratamento; e

Perspectiva reputacional: os vazamentos de dados atraem cada vez mais atenção da mídia.

Por fim, o **PSI** deve ser divulgada para todos os funcionários da empresa e partes externas relevantes de forma que seja entendida, acessível e relevante aos usuários pertinentes.

13. Conscientização, treinamento, e educação corporativa

Por Marcelo Vieira de Menezes

Um dos principais pontos na jornada de adequação do escritório de Advocacia à **LGPD** é a **conscientização dos seus colaboradores**. Sendo sempre o elo mais fraco para a segurança da informação, conscientizar as equipes nas melhores práticas de proteção, privacidade e segurança das informações é em muitas vezes o que evita um problema maior para as corporações em relação a vazamento de dados.

A conscientização deve estar intrinsecamente ligada aos **processos de adequação à LGPD** e deve ter uma periodicidade constante, ao ponto de tornar-se cultural. Para tanto, é importante a participação e o apoio do corpo diretivo da empresa, com isso pode-se garantir um apoio com suporte financeiro e estratégico para o programa de conscientização e treinamentos.

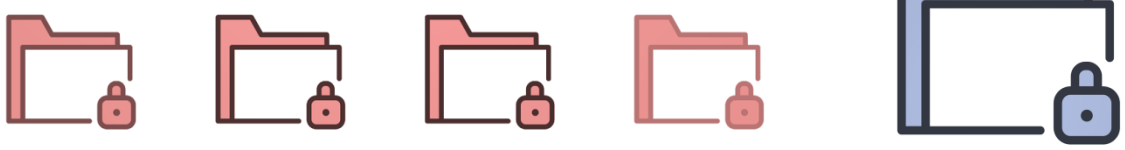
A conscientização deve ser iniciada juntamente com os primeiros levantamentos para a adequação. Nesse momento podemos iniciar a criação de uma cultura de privacidade, envolvendo o maior número possível de colaboradores nos desdobramentos das ações a serem executadas desde a primeira reunião realizada.

Como resultado, convém expor todas as diretrizes da **LGPD** e seus Como resultado, convém expor todas as diretrizes da **LGPD** e seus impactos no dia a dia das atividades do escritório de Advocacia, demonstrando a importância da adequação. À medida em que o projeto avança o nível de maturidade em privacidade crescerá em profundidade e horizontalidade de conhecimento.

A conscientização já anteriormente explorada é fator fundamental para o sucesso da adequação de qualquer organização sobretudo de escritório de Advocacia.

Lembrando que um programa de conscientização acaba se transformando em um processo de **cultura de privacidade e proteção de dados pessoais**, que devemos sempre estar atualizando, pois, novos serviços e processos surgem, e com isso novos tratamentos de dados.

A atualização é constante e este é um fator primordial para o sucesso da adequação do seu escritório de Advocacia.



14. Vazamento de dados: os riscos e cuidados para escritórios de Advocacia

Por Maria Laura Zoéga e Marcela Fuga Antunes Cardoso

Ao contrário do que muitos pensam, os escritórios de Advocacia funcionam como verdadeiras empresas, contando com diversos departamentos, procedimentos, colaboradores e fornecedores, seja para entregar um trabalho de excelência, seja para manter suas atividades em dia.

Por menor que seja a estrutura, ela invariavelmente envolve rotinas importantes e complexas, que são facilitadas com a utilização de tecnologias clássicas (como *e-mails, notebooks, smartphones* e impressoras), ou mais avançadas (como os *softwares* de gestão e automação de processos), tudo visando a dinamizar o exercício da profissão.

Em decorrência disso, o número de dados pessoais que transitam nos escritórios de Advocacia é enorme, envolvendo os próprios processos e a troca diária de *e-mails* e documentos necessários ao desenvolvimento das atividades.

Por essa razão, tais estruturas têm sido cada vez mais alvos de ataques que propiciam o vazamento de informações, dentre elas, dados pessoais.

Nesse sentido, torna-se cada vez importante que os escritórios de Advocacia se preocupem em estar ***compliance* com a LGPD**.

Na realidade, de nada adianta que o escritório conte com uma equipe de T.I. bem estruturada, se os envolvidos em toda a estrutura não têm consciência alguma sobre a importância da proteção de dados e deixam de cumprir práticas relativas a esse tema. Nesse caso, basta, por exemplo, dar um simples *click* em um *link* malicioso, recebido no *e-mail* corporativo, para que a base de dados dos clientes seja inteira vazada.

Bem por isso é que, como visto no capítulo sobre o *Roadmap* de implementação da **LGPD** deste ***Guia*****,** um dos passos iniciais e mais importantes a serem observados é o de conscientização de todos os membros do escritório, o que vai desde a alta direção, até os Advogados associados, estagiários, recepcionistas, copeiros e faxineiros, como já foi explicitado acima.

Aliás, muitos acreditam que a palavra "vazamento" está apenas relacionada apenas a incidentes ocorridos no mundo virtual, quando, na verdade, estes incidentes podem ocorrer tanto no meio virtual, quanto no meio físico. Bem por isso é que a **LGPD** protege os dados pessoais dos titulares tratados em ambos os meios:

"Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Art. 1º)

Um clássico exemplo de vazamento de dados pessoais em meio físico é a perda de um *pen drive* contendo dados de processos sigiloso que conta com dados de saúde. Ou, ainda, a fixação de um *post-it* com informações pessoais de *login* e senha na tela do *notebook* corporativo, dando permissão a qualquer um que sente na mesa para acessar aquele dispositivo.

Assim, para evitar esse tipo de incidente, é perfeitamente possível que os escritórios de Advocacia tomem medidas simples e que independem do tamanho ou complexidade da estrutura, para mitigar ou mesmo eliminar os riscos de vazamento de dados pessoais, como:

i) incentivar comportamentos zelosos a todos os integrantes do escritório para com os dados pessoais que circulam na estrutura, por meio da realização de palestras e realização de simulações de ações do dia a dia do escritório;

ii) implementar uma rotina de discussão de casos ou veiculação de notícias dentre a equipe, colocando o tema "proteção de dados pessoais" em destaque;

iii) evitar anotações em blocos de notas digitais sem senha ou a colagem de *post-its* na tela dos computadores/*notebooks* ou nas mesas de trabalho, contendo informações de *login* e senha de acesso a sistemas e e-*mails* (Política de Mesa Limpa);

iv) eleger uma equipe/membro especializada(o) para cuidar das cópias extraídas de processos físicos, que ficará responsável pela realização do *download* seguro das imagens junto ao sistema do escritório; isso evitará que as imagens/arquivos sejam baixadas em dispositivos pessoais ou pastas não seguras.

v) ao realizar o ajuizamento de ações judiciais, atribuir sigilo à petição inicial e aos documentos que contenha qualificação completa das partes (dados pessoais e dados pessoais sensíveis);

vi) evitar o compartilhamento e a divulgação de PIN e senha de certificados digitais dos Advogados;

vii) bloquear telas de dispositivos em caso de ausência;

viii) implementar uma Política *BYOD* [2] (Traga Seu Próprio Dispositivo) que regulamente a utilização de dispositivos móveis para evitar o acesso indiscriminado ou indevido ao ambiente lógico;

ix) criptografar arquivos e planilhas que contenham qualquer tipo de dado pessoal, sobretudo quando enviadas por e-mail;

x) restringir o acesso a pastas do servidor a cada departamento, quando salvos em equipamentos eletrônicos;

xi) controlar o acesso de colaboradores a salas de arquivos e utilizar chaves e cadeados em armários, quando em caso de arquivos físicos contendo dados pessoais;

xii) trocar periodicamente senhas de acesso a sistemas, e utilizar senhas fortes;

xiii) restringir o acesso de terceiros a pastas ou documentos compartilhados via nuvem (como *Dropbox, Google Drive, One Drive, iCloud*, entre outras). Com isso, arquivos remetidos a terceiros via nuvem não ficarão disponibilizados por tempo e finalidade ilimitados;

2 Bring Your Own Device (BYOD), em inglês, ou, 'Traga Seu Próprio Dispositivo', é a possibilidade de uso de dispositivo móvel particular no ambiente de trabalho, sendo configurado aquele para que seja possível acessar o ambiente lógico da empresa.

xiv) instituir uma Política de Acesso Remoto, principalmente para utilização de Rede Privada Virtual (VPN)(3), às vistas de garantir a proteção e privacidade das informações e dados pessoais que irão trafegar;

xv) prezar pelo sigilo(4) de reuniões e conversas telefônicas em ambientes seguros que evitem o vazamento das informações tratadas entre o escritório e o cliente/terceiro;

xvi) informar parceiros e terceiros com quem o escritório atua sobre as políticas e padrões de segurança adotados, a fim de que se comprometam a segui-los com o mesmo rigor, estabelecendo inclusive contratualmente as responsabilidades que serão atribuídas em caso de descumprimento;

xvii) utilizar de antivírus e outras ferramentas de segurança que evitem ataques, sempre de acordo com as tecnologias mais atualizadas.

3 VPN (Virtual Private Network/'Rede Privada Virtual') é uma rede que tem seu tráfego protegido por um "túnel" criptográfico. Tal serviço tem como objetivo a privacidade e a proteção dos dados que trafegam por ele. É oferecido na internet por diversos provedores que, estando em países que o permitem, não registram a origem da conexão, dificultando investigações e o rastreio da origem das conexões.

4 O dever de sigilo profissional e de eticidade está amparado por disposições previstas no Código de Ética da OAB7.

Apesar de numerosas, as medidas são perfeitamente exequíveis por qualquer escritório de Advocacia, seja ele grande ou pequeno, e evitará a ocorrência de incidentes, sendo importante lembrar que os escritórios têm o dever de resguardar a segurança das informações e a proteção dos dados pessoais que tratam com o mesmo rigor que as empresas comuns.

15. Política de Privacidade específica para escritórios de Advocacia

Por Renata Proximo da Silva e Anna Carolina

Primeiramente, antes de adentrarmos ao tema **Política de Privacidade** e sua importância, cabe apontarmos a importância da governança digital.

A governança digital é um fator estratégico para gerar conhecimento e inovação por meio de tecnologias que proporcionam melhorias para Advogados, Sociedades de Advogados e demais ramos de atividades, trazendo agilidade, transparência e autonomia na realização das tarefas diárias. É baseada em **4 pilares**: **Proteção de Dados Pessoais, Segurança da Informação, Reputação Digital** e ***Compliance***.

15.1. Mas, o que é Política de Privacidade?

A Política de Privacidade nada mais é do que um documento que apresenta todas as regras aplicáveis para o tratamento de dados pessoais realizada pelo seu escritório de Advocacia, sejam esses dados relacionados aos colaboradores internos e/ou parceiros, sejam os relacionados aos clientes e/ou dos clientes dos seus clientes, e assim por diante.

É nessa política que restará demonstrado quais os dados serão coletados pelo seu escritório, com quem serão compartilhados, como serão utilizados, por quanto tempo ficarão retidos, quais as bases legais serão utilizadas para fundamentar esse tratamento e qual a forma que eles serão descartados após findo o contrato de prestação de serviços, além de estabelecer todos os requisitos necessários para a construção de um programa de privacidade e proteção de dados pessoais em conformidade com a Lei.

É nela, também, que restará demonstrado o compromisso do seu escritório junto ao tratamento de dados pessoais de todas as pessoas envolvidas com ele, focando sempre no mais alto nível de cuidado, confidencialidade e conformidade com a legislação.

Assim, a estratégia de privacidade e governança necessita de uma Política de Proteção e Privacidade de Dados definida, implementada, divulgada, executada e monitorada, trazendo ao contexto, exemplos relevantes, como as Políticas Corporativas de Proteção de Dados, de uso de site e demais canais, de *cookies* e de segurança da informação.

Portanto, temos que a **Política de Privacidade** é um dos documentos mais importantes para a aplicação do projeto de implantação junto ao seu escritório de Advocacia, visto sua obrigatoriedade perante a lei, conforme ao **Art. 52**, §1º, inciso IX, e a definição das regras quanto ao tratamento de dados pessoais que serão utilizadas em sua sociedade.

Sendo que estes devem esclarecer ao seu cliente como o seu escritório trata os dados pessoais ao longo do ciclo de vida, levando a conscientização à essa mudança de cultura.

15.2. A aplicação de Política de Privacidade em escritórios de Advocacia

Sendo a Política de Privacidade o documento formal que dispõe sobre quais dados dos titulares será coletado e tratado pelo controlador, de forma detalhada, sendo uma ferramenta eficaz para obtenção de consentimento válido, deve ser considerado primordial para qualquer escritório de Advocacia.

As atividades desenvolvidas pelo escritório de Advocacia devem assegurar a conformidade às recentes obrigações legais, quanto ao tratamento de dados pessoais, deixando de ser meramente uma boa prática, sujeitando o escritório a penalidades e inclusive resguardando sua reputação.

Com a vigência da **LGPD,** os escritórios de Advocacia estão sujeitos a novas obrigações no que diz respeito a manipulação de dados pessoais, ou seja, a partir do momento que os escritórios de Advocacia realizam operação de tratamento de dados pessoais de seus clientes e colaboradores, deve-se observar o previsto na Lei.

É importante que a **Política de Privacidade** deixe claro a finalidade do tratamento de dados pessoais dos clientes, garantindo seu sigilo.

Efetivamente, o **Art. 7º** da **LGPD** prevê a dispensa de consentimento nas seguintes hipóteses:

> "[...] **V.** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> **VI.** para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 *(Lei de Arbitragem)*."

A Política de Privacidade deve garantir que todos os envolvidos no negócio, desde o sócio, Advogado, estagiário, correspondente, até demais colaboradores, estejam comprometidos com a **proteção dos dados compartilhados e tratados.**

Assim os escritórios de Advocacia devem estabelecer ou revisar a Política de Privacidade, incluindo diretrizes que promovam a proteção dos **direitos dos titulares dos dados pessoais**, onde fique claro os motivos, finalidade, legitimidade e quais dados estão sendo coletados, e por quanto tempo serão mantidos os arquivos.

Isso porque, toda vez que o Advogado ou o escritório de Advocacia atuar como controlador, é importante evidenciar em seus contratos a **finalidade do tratamento**, respeitando os termos da **LGPD** e sua Política de Privacidade de Dados Pessoais, e claro, o procedimento para os titulares exercerem seus direitos.

15.3. Convém destacar alguns tópicos importantes para a Política de Privacidade dos escritórios:

i) a observância do **sigilo** das informações recebidas, no exercício da profissão;

ii) o dever de **confidencialidade** quanto aos dados e informações de seus clientes e clientes em potencial;

iii) o dever de confidencialidade quanto aos **documentos arquivados** referentes aos negócios de seus clientes, parceiros, terceiros etc.;

iv) a observância de todos os colaboradores aderirem à política de confidencialidade, desde sua contratação, além das **regras de boas práticas**, governança de proteção de dados;

v) o **treinamento** constante de sua equipe para evitar comentários a respeito dos casos tratados pelo escritório;

vi) a observância do sigilo profissional nas **redes sociais e meios de comunicação**;

vii) a abstenção de coletar dados e informações desnecessários ao caso, principalmente no que diz respeito a **dados sensíveis**;

viii) a garantia da **segurança da informação** por meio de controles de acesso;

ix) exigir de seus fornecedores a **adequação à LGPD**;

x) estabelecer um **prazo para eliminação de dados** e seus procedimentos legais.

15.4. Política de governança de dados

A expressão ***Governance*** não surgiu com a **LGPD**, mas sim voltada às atividades do Estado e suas políticas de gestão pública. Sendo a capacidade governativa avaliada não apenas pelos resultados das políticas governamentais, mas também a forma pela qual o governo exerce o seu poder.

Com o passar do tempo, verificou-se a necessidade de aplicação das práticas do governo serem também aplicadas no âmbito corporativo. O movimento de governança corporativa ganhou forças em meados da década de 80 nos Estados Unidos, alastrando-se pelo mundo, e chegando ao Brasil na última década, com a sanção da ***Lei Anticorrupção*** (Lei nº 12.846, de 1º de agosto de 2013).

Reconhecidas as atividades operacionais de um escritório de Advocacia, podemos entender a necessidade da normatização pela sociedade de Advogados, principalmente para assegurar a conformidade às obrigações legais trazidas pela **LGPD**.

A **LGPD** estabelece, em seu artigo 50, o conteúdo mínimo de um **Programa de Governança de Privacidade**.

A Governança, no âmbito da Advocacia, deve ser vista como um conjunto de práticas internas, padrões definidos por sócios, objetivando controles efetivos, segurança cibernética, proteção de dados e riscos reputacionais.

As **medidas de Governança** devem objetivar: **a) desenvolvimento de normas** internas; **b) sistema de gerenciamento de processos e gestão de pessoas**, ou seja, meios e processos para produzir resultados eficazes e mitigar riscos.

É sempre bom lembrar que a adoção de boas práticas de governança de privacidade é fator considerado na aplicação de sanções. E isso se deve ao fato da capacidade de seu escritório criar uma cultura de proteção à privacidade e definir preceitos internos.

Observe-se que as medidas implementadas devem ser comprovadas, ou seja, todos os treinamentos e procedimentos devem ser documentados (evidenciados) para futura apresentação às autoridades.

Os procedimentos administrativos devem ser aprimorados, como, por exemplo, o início e encerramento de um projeto, a definição de níveis e papéis de controle no escritório.

As etapas essenciais para o exercício da Governança:

i. identificar as partes

ii. mapear as lacunas existentes nos normas anteriores;

iii. avaliar os riscos jurídicos envolvidos, as medidas corretivas e o grau de complexidade para efetivação;

iv. implantar as medidas corretivas necessárias;

v. criar, ou revisar, processos internos;

vi. treinar e formalizar as normas internas perante a equipe.

16. A Resposta a Incidentes de Segurança

Por Isadora Coimbra Diniz

a) O que é Resposta a Incidentes de Segurança

A **LGPD** não traz uma definição específica do que são Incidentes de Segurança, no entanto, em abril de 2024 a Autoridade Nacional de Proteção de Dados publicou a Resolução CD/ANPD nº 15 , de 24 de abril de 2024, define um Incidente de Segurança como "qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais".

Isso significa que estão englobados na definição de incidente de segurança o acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais, bem como a impossibilidade de acesso a determinados dados ou mesmo a perda da capacidade de se assegurar que determinado dado ou informação foram produzidos, expedidos, modificados ou destruídos por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Conforme estudo publicado pelo jornal *Folha de São Paulo*, em julho de 2019, as principais causas de vazamentos de dados pessoais, a mais conhecida entre as hipóteses de Incidentes de Segurança, correspondem a ataques criminosos (51%), falha em sistemas (25%) e erro humano (24%), de modo que é possível inferir que os riscos de um Incidente podem ser reduzidos em até 49% através da contratação de sistemas de segurança compatíveis com o volume e a criticidade dos dados pessoais tratados e treinamentos constantes ao pessoal responsável por executar o tratamento de referidos dados.

A Resposta a Incidentes de Segurança, por sua vez, é a forma como o escritório irá endereçar o eventual Incidente, ou seja, a forma como irá agir para mitigar os riscos decorrentes de um evento adverso confirmado envolvendo dados pessoais, que deve ser formalizada através de um plano de ação.

Portanto, a Resposta a Incidentes de Segurança é o processo que descreve como o escritório irá agir caso ocorra um Incidente de Segurança envolvendo os dados pessoais tratados e tem por objetivo orientar os envolvidos sobre como agir no caso de sua confirmação, reduzindo o tempo de ação, visando minimizar os riscos decorrentes do Incidente e diminuir os custos de recuperação.

Vale destacar que o **Plano de Reposta a Incidentes de Segurança**, ou Política de Incidentes, **e seu constante monitoramento, são parte essencial e obrigatória de um Programa de Privacidade**.

b) Como elaborar uma Política de Incidentes para o escritório

Uma Política de Incidentes de Segurança deverá conter, no mínimo, os elementos indicados abaixo:

i. A definição de Incidente de Segurança;
ii. A descrição dos procedimentos a serem executados na hipótese de suspeita ou confirmação de Incidente Segurança;
iii. A indicação das pessoas a serem acionadas no caso de suspeita ou confirmação de um Incidente de Segurança e as respectivas ações e responsabilidades (“Comitê de Crise”);
iv. As ferramentas, tecnologias e recursos a serem utilizados em caso de confirmação de um Incidente de Segurança;
v. O tempo de resposta esperado ao Incidente;
vi. Os critérios para análise da criticidade do Incidente e eventual necessidade de comunicação à ANPD e titulares sobre o ocorrido;
vii. Os procedimentos internos para registro e monitoramento do Incidente; e
viii. O gerenciamento dos terceiros que podem ser parte do Incidente.

É recomendado que a elaboração da Política de Incidentes seja realizada de forma multidisciplinar, contando com o apoio dos times internos e/ou consultorias especializadas em Tecnologia da Informação, *Marketing*, Recursos Humanos e, como não poderia faltar, Jurídico.

c) Comunicação de Incidentes de Segurança

O **Art. 48** da **LGPD** determina que o controlador deverá comunicar à ANPD e aos titulares a ocorrência de Incidente de Segurança que possa acarretar risco ou dano relevante aos titulares.

Desta forma, entende-se que nem todo Incidente de Segurança precisa ser comunicado, devendo ser analisado, no caso concreto, a possibilidade que de os titulares cujos dados pessoais foram afetados tenham sua segurança, seus direitos e/ou liberdades fundamentais ameaçados em razão do Incidente.

A Resolução CD/ANPD nº 15 trouxe os critérios a serem analisados para a verificação da necessidade de comunicação, conforme indicado abaixo.

Inicialmente, deve ser verificado se o Incidente de Segurança envolve, pelo menos, uma das Categorias de Dados Pessoais mencionadas no artigo 5º da referida Resolução:

i. **Dados Pessoais Sensíveis;**
ii. **Dados de crianças, de adolescentes ou de idosos;**
iii. **Dados financeiros;**
iv. **Dados de autenticação em sistemas;**
v. **Dados Protegidos por Sigilo Legal, Judicial ou profissional**
vi. **Dados em Larga Escala.**

Em seguida, deve ser avaliado se o comprometimento destes dados pessoais pode afetar significativamente interesses e direitos dos titulares dos dados – por exemplo: se é capaz impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade, entre outros, conforme complementa o § 1º do mesmo artigo.

Através da análise destes critérios, será possível verificar se o Incidente de Segurança deve ser ou não comunicado à ANPD e aos titulares.

Ainda, deve ser considerado pelo Comitê de Crise a necessidade de notificar terceiros sobre o Incidente de Segurança – por exemplo: polícia, seguradoras, bancos ou companhias de crédito.

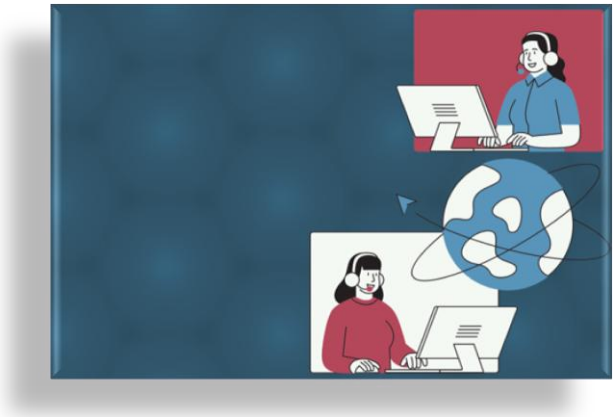
Esta comunicação é apropriada quando há suspeita ou ocorrência de atividade ilegal envolvendo o Incidente de Segurança.

Da mesma forma, o Comitê de Crise deve considerar se o Incidente é capaz de trazer um dano reputacional para o escritório e se é necessária a publicação de aviso para a imprensa e como lidar com possíveis questionamentos de clientes e da mídia.

d) Como comunicar um Incidente de Segurança à ANPD

As comunicações de Incidentes de Segurança à ANPD devem ser realizadas pelo controlador dos dados pessoais, através do link disponibilizado no site da Autoridade: <https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletrônico>.

O prazo para referida comunicação é de 3 dias úteis contados da data do conhecimento do Incidente, ressalvada a existência de prazo para comunicação previsto em legislação específica.



A comunicação será realizada através de formulário eletrônico disponibilizado pela própria ANPD, o qual solicitará as **informações sobre o Incidente** indicadas abaixo:

i. a descrição da natureza e da categoria de dados pessoais afetados;

ii. o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

iii. as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

iv. os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

v. os motivos da demora, no caso de a comunicação não ter sido realizada no prazo de três dias úteis;

vi. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

vii. a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

viii. os dados do encarregado ou de quem represente o controlador;

ix. a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

x. a identificação do operador, quando aplicável;

xi. a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la;

xii. o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais **poderão ser complementadas**, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação, sendo importante que o escritório seja capaz de mapear todas essas informações para o caso de eventual necessidade de comunicação.

Vale destacar que caberá ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, por exemplo, informações cuja divulgação possa representar violação de segredo comercial ou industrial.

e) Como comunicar um Incidente de Segurança aos Titulares

A Resolução CD/ANPD nº 15 trouxe também informações a respeito de como deve ser realizada a comunicação aos titulares, lembrando que esta comunicação deve ser realizada nos casos em que o incidente puder apresentar riscos relevantes aos envolvidos, conforme análise a ser realizada com base nos critérios já indicados neste artigo.

A comunicação aos titulares deverá ser realizada com o uso de linguagem simples e de fácil entendimento e, sempre que possível, de forma direta e individualizada, pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

Caso não seja possível a comunicação direta e individualizada, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

A comunicação aos titulares deverá conter as seguintes informações:

i. a descrição da natureza e da categoria de dados pessoais afetados;

ii. as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

iii. os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

iv. os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;

v. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

vi. a data do conhecimento do incidente de segurança;

vii. o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

f) Registro de Segurança

Por fim, a Resolução CD/ANPD nº 15 inovou ao trazer a obrigação de que, independentemente de comunicação à ANPD e aos titulares, todo Incidente de Segurança deverá ser registrado pelo controlador. O registro do incidente deverá conter, no mínimo, as seguintes informações:

i. a data de conhecimento do incidente;

ii. a descrição geral das circunstâncias em que o incidente ocorreu;

iii. a natureza e a categoria de dados afetados;

iv. o número de Titulares afetados;

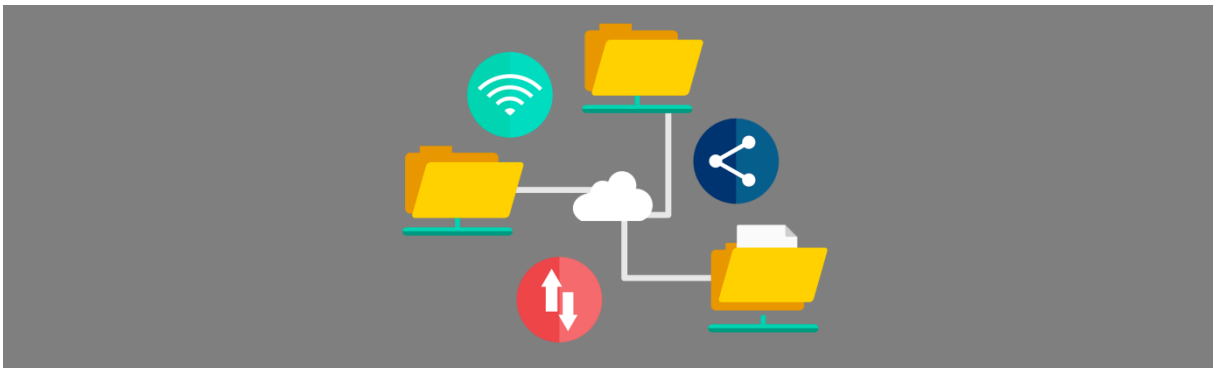
v. a avaliação do risco e os possíveis danos aos titulares;

vi. as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

vii. a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

viii. os motivos da ausência de comunicação, quando for o caso.

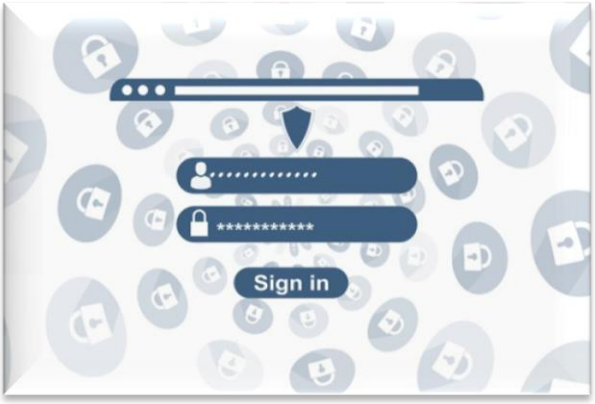
O escritório deverá manter os registros de todos os incidentes de segurança ocorridos, independentemente da classificação do incidente e da realização de comunicação à ANPD, titulares ou outros, pelo prazo mínimo de 5 anos.



17. Orientações de boas práticas

Por Marcelo Fujita e Rodrigo Carvalho e Silva

17.1. Compartilhamento de *login*, senhas, *tokens* e certificados digitais



No que tange a "Boa Prática", a própria **LGPD** norteia os agentes de tratamento com diretrizes a serem observadas e aplicadas em seu Capítulo VII, Da segurança e boas práticas, sendo necessário a realização do mapeamento de risco como escopo para a tomada de decisões de cada escritório.

Preleciona a norma em seu **Art. 46** o dever impositivo aos agentes de tratamento na adoção de "*medidas de segurança, técnicas e administrativas aptas a proteger dados pessoais*", *e.g*, contra acesso de pessoas não autorizadas, dentre outras circunstâncias, sejam elas acidentais ou por dolo, que possam resultar na modificação, exclusão, cópia (...) de dados pessoais.

Diante desse cenário exemplificativo, o **Art. 50** da **LGPD** "**Das Boas Práticas e Governança**" dispõe diversos comandos a serem observados como medidas necessárias pelos agentes de tratamento na formulação de "regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

A "Segurança da informação é tarefa de todos" e "o ser humano é o elo mais fraco da segurança da informação", são frases contextuais inerentes e bem conhecidas no ambiente de tratamento de dados, exigindo do controlador a adoção de uma política de segurança da informação composto com orientações e regras a serem cumpridas por todos, sendo indispensável à aplicabilidade de treinamentos contínuos e atualizados para que a cultura de proteção de dados se integre no ambiente do escritório.

Soluções simples como "folhetos ilustrados; boletins por e-mails, palestras" podem ser adotadas como meio de **treinamento contínuo** para manutenção e atualização da política de segurança da informação, código de conduta, política de privacidade, conforme expresso o §3º do **Art. 50** da **LGPD**, que enfatiza o verbo "dever" quanto à manutenção da publicidade e atualização das regras de boa prática e governança.

Para a atualização das regras de boa prática e governança é imprescindível o monitoramento de futuras publicações da ANPD, tendo em vista sua competência em estabelecer normas técnicas a setores específicos.

Na seção de publicações do site da ANPD, está disponível o **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais**, e cartilhas do Comitê Gestor da Internet no Brasil (CGI.br) <*https://cartilha.cert.br/fasciculos/*>, fascículo Proteção de Dados e fascículo Vazamento de Dados, que podem ser explorados como material auxiliar no programa de proteção de dados.

De forma simples e didática de como aplicar a **LGPD** na rotina de processos existente em um escritório de Advocacia, tenha em mente o encaminhamento de e-mails disponibilizam as opções "Para: *cc: e cco*:", é de bom tom entendê-las e fazer uso consciente e responsável:

Para: enviar *e-mail* para apenas uma pessoa, tendo em vista que o endereço do titular estará visível no recebimento;

cc: com cópia, pode ser útil para meio corporativo na hipótese em que um colaborador cumpra determinada tarefa e ao enviá-la copie para seu superior;

cco: com cópia oculta, é a opção adequada para envio de mensagem em massa, pois cada destinatário visualizará apenas o seu endereço de e-mail. Lembre-se, o endereço de *e-mail* é um dado pessoal e você não é o titular desse dado.

17.2. Exemplo de outras boas práticas para proteção de dados no escritório de Advocacia

Use uma conexão VPN – Conexão VPN estabelece uma conexão segura entre você e a Internet e principalmente contra-ataques externos. Todo o tráfego de dados é roteado por um túnel virtual criptografado. Isso disfarça seu endereço IP quando você usa a internet, tornando sua localização invisível para todos.

Criação de *backups* dos dados armazenados, principalmente em nuvem;

Ativar a criptografia nos discos e mídias externas, como *pendrives*;

Criação de senhas fortes, que contenham a combinação de caracteres especiais, letras maiúsculas, minúsculas e números, evitando utilizar dados pessoais ou palavras comuns;

Habilitando a verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;

Instalar somente aplicativos de fontes e lojas oficiais;

Atualizar sempre o sistema operacional e os aplicativos;

Apagar os dados armazenados **antes de se desfazer/descarte dos equipamentos e das mídias;**

Desconfiar de *links* recebidos por aplicativos de mensagens;

Limitar a divulgação ou fornecimento de dados pessoais na internet, inclusive para redes sociais, ou para empresas, aos casos estritamente necessários;

Certificado Digital: Certificado Digital é uma espécie de identidade eletrônica de uma pessoa ou empresa. Ele funciona como uma carteira de identificação e permite que documentos sejam assinados eletronicamente e à distância, também é possível acessar serviços diversos, especialmente em sites governamentais. Portanto alguns cuidados são essenciais como, por exemplo, criar uma senha forte para evitar que terceiros tenham acesso ao seu certificado e acesse informações utilizando seus dados e não compartilhar o uso do certificado. Em caso de perda de um certificado digital é necessário revogá-lo imediatamente, entre em contato com a autoridade certificadora.

Fotos digitais de processos e documentos: Após tirar cópias digitais de processos judiciais ou extrajudiciais, bem como de documentos pessoais é importante tomar cuidado com a forma como essas fotos serão armazenadas. Ao utilizar um celular cuidado para que essas informações não sejam armazenadas em local de fácil acesso, alguns serviços de armazenamento em nuvem já permitem salvar o documento diretamente neles, sempre que possível escolha essa opção. Se não for possível, após transferir as imagens para um local seguro, lembre-se de excluir do dispositivo.

Advogado correspondente: O Advogado correspondente contratado para prestar serviços deve adotar os mesmos cuidados que qualquer outro colaborador do escritório, da mesma forma é importante solicitar que o correspondente adote medidas de segurança e sigilo pois o contratante poderá ser responsabilizado por qualquer incidente de segurança.

Mensageiros instantâneos: Apesar de ser muito exigido atualmente pelos clientes, o envio de documentos com dados pessoais e dados pessoais sensíveis deve ser evitado, mesmo quando utilizamos um aplicativo que informa utilizar criptografia de ponta a ponta. Como se sabe, não existem garantias de que o documento enviado ou as informações compartilhadas são de fato seguras ou que não sejam armazenadas (ainda que temporariamente) em locais com alto risco de incidentes. Não é incomum uma pessoa enviar, por engano, um documento ou informação para terceiro que não era o destinatário, essa situação, por si só, já caracteriza um incidente de segurança.

Redes Sociais: Cada vez mais advogados e escritórios postam fotos de documentos ou processos em suas redes sociais como forma de gerar conteúdo. Além de questões éticas que devem ser analisadas, há também elementos que podem caracterizar incidente de segurança de dados. Evite postar fotos de documentos de clientes em redes sociais, mesmo se o processo judicial ou administrativo for público.

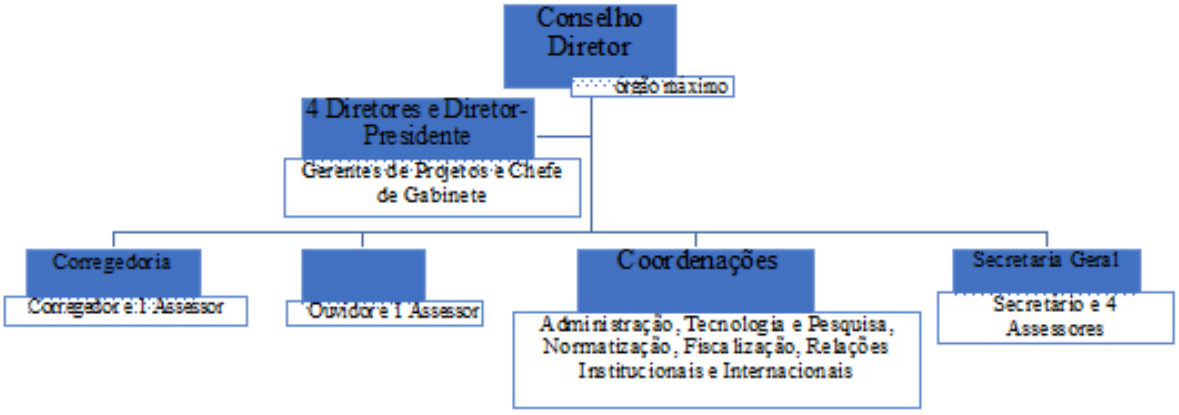
18. Atuação da ANPD – Autoridade Nacional de Proteção de Dados

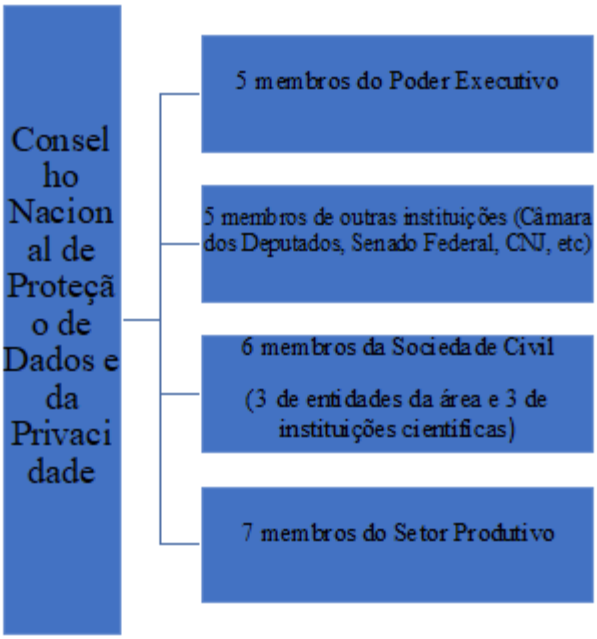
Por Adriana Senna Pessoto Garibe

ANPD Autoridade Nacional de Proteção de Dados

A **Autoridade Nacional de Proteção de Dados**, criada pela Medida Provisória nº 869/18, convertida na Lei nº 13.853/2019, que alterou a Lei Geral de Proteção de Dados, iniciou efetivamente suas atividades com a nomeação de seu primeiro Diretor-Presidente, em 05 de novembro de 2020. O Decreto nº 1.0474, de 26 de agosto de 2020, por sua vez, trouxe a regulamentação da ANPD, estabelecendo sua estrutura regimental e organizacional, incluindo natureza, finalidade e competências.

A ANPD é composta pelo Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto na **LGPD**. O Conselho Diretor é composto por cinco membros: um presidente e quatro diretores, que são nomeados pelo Presidente da República, com aprovação do Senado Federal. O cargo é em comissão e tem mandato de quatro anos. O Conselho Nacional de Proteção de Dados Pessoais é composto por 23 representantes designados pelo Presidente da República, conforme organograma abaixo, possuindo mandato de 2 anos. Por tratar-se de serviço público relevante, não são remunerados.





A **ANPD** é um órgão da administração pública federal, com autonomia técnica e decisória, que em 13 de junho de 2022, por meio da a Medida Provisória nº 1.124, de 13 de junho de 2022, convertida na Lei nº 14.460, de 25 de outubro de 2022, **foi transformada em autarquia de natureza especial**. Tornando-se uma autarquia a ANPD torna-se além de um ente autônomo, um ente sem subordinação hierárquica, semelhante às demais autarquias de regime especial já existentes no Brasil, como é o caso do Banco Central.

Além de outras atribuições determinadas na lei, o órgão é responsável por criar políticas públicas de proteção de dados pessoais e fiscalizar o cumprimento da lei, penalizando administrativamente em caso de descumprimento da legislação.

Cabe lembrar que o Projeto de Lei nº 1.179/2020, posteriormente convertido na Lei nº 14.010/2020, postergou o início da vigência dos artigos relacionados às sanções administrativas da **LGPD**. Assim, as penalidades administrativas previstas em Lei passaram a ser passíveis de aplicação tão somente em 1º de agosto de 2021. São elas: advertência; multa pecuniária (de até 2% do faturamento até o limite de R$ 50 milhões por infração); multa diária, possibilidade de publicização da infração, bloqueio dos dados pessoais envolvidos, suspensão parcial, por até 06 (seis) meses, do banco de dados envolvidos, proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Com relação as penalidades administrativas de competência da ANPD, foi publicado, no dia 27 de fevereiro de 2022, o **Regulamento de Dosimetria e Aplicação de Sanções Administrativas**. A dosimetria é o método que orienta a agência a decidir pela sanção mais adequada para cada caso concreto, além de possibilitar o cálculo do valor da multa quando esta for aplicável. Desta forma, o regulamento pretende garantir a proporcionalidade entre a sanção e a gravidade da conduta do agente, bem como o direito dos infratores ao devido processo legal e ao contraditório.

O valor arrecadado com as multas será destinado ao fundo de defesa de direitos difusos para reparação de eventuais danos causados, por exemplo, ao meio ambiente, ao consumidor, entre outros. Evidentemente, as ações devem levar em conta a gravidade e natureza das infrações, a boa-fé do infrator, a vantagem auferida, a condição econômica, eventual reincidência, o grau do dano, a adoção ou não de mecanismos para minimizar o dano, bem como a adoção de políticas de boas práticas de governança. Por isso, é tão importante que as empresas sejam devidamente adequadas à legislação aplicável.

Para as organizações de médio e grande porte, as consequências do descumprimento da **LGPD** podem ser significativas, pois impactam de forma financeira com aplicação de elevadas multas e comprometem sua imagem perante o mercado através da publicidade do dano. Além das multas previstas na legislação, as empresas podem enfrentar sanções judiciais e perda de credibilidade perante os seus clientes. Por isso, é fundamental que as empresas invistam em políticas e medidas de proteção de dados pessoais para garantir a conformidade com a **LGPD**. Isso inclui a implementação de medidas de segurança, a realização de treinamentos para os colaboradores e a adoção de boas práticas de governança de dados.

Importante destacar que, antes da aplicação de qualquer sanção, haverá a comunicação aos agentes de tratamento e a possibilidade de ampla defesa e apresentação de razões que visem justificar ou mesmo minimizar os eventuais danos causados. Assim, serão levados em consideração pela ANPD: a gravidade e a natureza das infrações; a boa-fé e a cooperação do infrator; a vantagem obtida com a infração; as condições econômicas do infrator; a reincidência e gravidade do dano causado; a adoção de mecanismos e procedimentos internos de proteção de dados; a adoção de políticas de boas práticas e governança; a adoção de medidas corretivas eficazes e a proporção entre a gravidade da infração e a intensidade da penalidade a ser imposta.

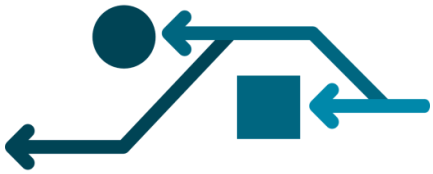
Por fim, existem pelo menos 30 artigos relevantes da **LGPD** que demandam a regulamentação que virá da ANPD, como por exemplo: a definição de cláusula contratual padrão, visando fluxo de dados entre empresas; padrões e regras de portabilidade de dados; prazos para cumprimento dos direitos dos titulares dos dados, dentre outros. Ademais, a Autoridade mitigará o risco de judicialização em massa, pois dentre a suas competências, está a de apreciar petições dos titulares de dados feitas contra o controlador, que não tenham sido satisfatoriamente respondidas.

O que se percebe diante da atuação da ANPD até o momento é que a sua principal função é servir de elo entre sociedade e governo, permitindo que os titulares de dados enviem dúvidas, sugestões e denúncias relacionadas à **LGPD** para eventual apuração. Desempenha também uma importante função de orientadora e de apoiadora dos órgãos de governo e empresas privadas, em relação ao processo de tratamento dos dados pessoais, objetivando a orientação preventiva e trazendo para a sociedade os princípios relacionados à cultura da proteção de dados pessoais, já tão difundidos na Europa.

Fontes :
BRASIL. ***Lei Geral de Proteção de Dados (LGPD)****. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm, Acesso em: 30 de agosto de 2021.*
Maldonado, Viviane Nóbrega (coordenação). ***LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação****. São Paulo-/SP. Editora Thomson Reuters Brasil, 2019.*
BRASIL. Autoridade Nacional de Proteção de Dados. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021. Acesso em: 30 de agosto de 2021.

19. Considerações Finais

Por Carlos Alberto Casanova Campos



A **LGPD** mudou o cenário regulatório brasileiro de proteção de dados e de conformidade, e estabeleceu várias novas exigências que organizações públicas e privadas precisarão implementar. Para muitas organizações, esta é a primeira vez que elas terão que lidar com uma lei abrangente de proteção de dados pessoais, e há muitos requisitos em aberto na **LGPD** que ainda precisam ser melhor especificados, particularmente pela ANPD.

O **Art. 3º da Lei Geral de Proteção de Dados** não deixa dúvidas da extensão dos seus efeitos aos escritórios de Advocacia.

É praticamente impossível afastar o tratamento de dados pessoais das rotinas jurídicas. A elaboração de minutas contratuais, pareces jurídicos, *due diligences* e as petições judiciais ou administrativas dependem do uso de dados pessoais.

Sem contar que os escritórios também possuem colaboradores, prestadores de serviços terceirizados, parceiros comerciais, cujos dados pessoais também devem ser tratados em conformidade com a **LGPD**.

Ainda, a realização das operações acima sem a observância da **LGPD** poderá acarretar aplicação das **penalidades previstas** no **Art. 52**, tais como advertência, multas, bloqueio dos bancos de dados, publicização das infrações aos Advogados / Sociedades de Advogados.

Importante ressaltar que o Plenário do Senado Federal aprovou Proposta de Emenda Constitucional (PEC 17/2019) e, após sua aprovação em processo legislativo, tornou-se a Emenda Constitucional 115/2022, que acrescentou o inciso LXXIX, do artigo 5º, e inciso XXX, do artigo 22, ambos da Constituição Federal de 1988 e, para tanto, incluiu a proteção de dados pessoais, inclusive nos meios digitais, como direitos fundamentais do cidadão, e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Por fim, tendo em vista que a grande maioria dos serviços jurídicos depende do uso de dados pessoais compartilhados pelo cliente, é certo que será cada vez mais exigido dos escritórios de Advocacia a comprovação de conformidade com a **LGPD**.

20. Glossário

Por Orestes Bacchetti Junior

- ABNT NBR ISO/IEC
Associação Brasileira de Normas Técnicas (**ABNT**); NBR – Norma Traduzida para o Português -Brasileira; A Comissão Eletrotécnica Internacional (em inglês: *International Electrotechnical Commission*, **IEC**) é uma organização internacional de padronização de tecnologias elétricas, eletrônicas e relacionadas. Alguns dos seus padrões são desenvolvidos juntamente com a Organização Internacional para Padronização (**ISO**), em Inglês **ISO** é uma sigla para "*International Organization for Standardization*", que significa Organização Internacional de Normalização. Trata-se de uma respeitada organização mundial, com sede em Genebra, que cuida mundialmente de padrões de normatização de procedimentos.

- Anonimização
Utilização de meios técnicos utilizados no tratamento do dado, retirando a possibilidade de associação, direta ou indireta, a um indivíduo.

- ANPD - Autoridade Nacional
A Autoridade Nacional de Proteção de Dados é um órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018. Com a a Medida Provisória nº 1.124, de 13 de junho de 2022, convertida na Lei nº 14.460, de 25 de outubro de 2022, alterou a Lei nº 13.709, de 14 de agosto de 2018 e transformou a Autoridade em autarquia de natureza especial. Já em 23 de janeiro de 2023, foi publicado o Decreto nº 11.401 de 23 de janeiro de 2023, passando a vincular a ANPD ao Ministério da Justiça e Segurança Pública.

- Banco de Dados
Conjunto estruturado de dados pessoais, em suporte eletrônico ou físico, estabelecido em um ou em vários locais.

- Bloqueio
Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

- Browser
É um termo recorrente na Internet e serve como sinônimo, em inglês, para "navegador de Internet". O termo define apps como *Google Chrome, Safari, Opera, Firefox e Edge* que, em comum, permitem que o usuário acesse sites de Internet e também interaja com essas páginas de diversas formas

- CAGED
É a sigla para Cadastro Geral de Empregados e Desempregados (CAGED), é o dispositivo legal utilizado pelo Ministério do Trabalho e Emprego para acompanhar a situação da mão de obra formal no Brasil, a fim de levantar dados de geração de emprego e desemprego no país

- Cláusula padrão
São cláusulas típicas que estão contidas no acordo contratual e que se destinam a tutelar aspectos comuns aos contratos em geral, com especial relevância para as transferências internacionais de dados pessoais.

- Click
Usado atualmente na informática para indicar o ato de pressionar o botão do mouse e aceder a um site, página, link, bem como de apertar um botão de *like* ou de subscrição

- Compliance
É o conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa, bem como evitar, detectar e tratar quaisquer desvios ou inconformidades que possam ocorrer.

- Consentimento
Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- Controlador
Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- Cookie
São pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador.

- Criptografia
Conjunto de princípios e técnicas empregadas para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; criptologia.

- Dado Anonimizado
Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos quando do tratamento.

Dado Pessoal
Informação relacionada à pessoa natural identificada ou identificável.

- Dado Pessoal de Criança e de Adolescente
Dado da criança até 12 anos de idade incompletos e adolescente entre 12 e 18 anos de idade (Estatuto da Criança e do Adolescente - ECA).

- Dado Pessoal Sensível
Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- Divulgação de PIN O que é PIN
Esse código é o PIN, que quer dizer *Personal Identification Number* ou Número de Identificação Pessoal. Isto quer dizer que o PIN é um número que identifica o chip de celular e que protege os dados e informações

- Download
E o mesmo que baixar um arquivo.

- Dropbox
É um serviço de hospedagem de arquivos em nuvem que pode ser usado de forma gratuita, desde que respeitado o limite de 2 GB de conteúdo. Assim, o usuário poderá guardar com segurança suas fotos, documentos, vídeos, e outros formatos, liberando espaço no PC ou *smartphone*.

- Eliminação
Exclusão de dado ou de conjunto de dados armazenados, independentemente do procedimento empregado.

- Encarregado
Pessoa natural, jurídica, comitê ou grupo de trabalho, indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

- e-Social
É uma plataforma online do governo que unificou a entrega de 15 obrigações da área trabalhista para empresas, outras pessoas jurídicas e também para pessoas físicas.

- Framework
É um termo inglês que, em sua tradução direta, significa estrutura. De maneira geral, essa estrutura é feita para resolver um problema.

- Garantia da Segurança da Informação e de Dados
Capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, observando a Política Nacional de Segurança da Informação (PNSI).

- Governança
Consiste em políticas, processos e uma estrutura organizacional para apoiar o gerenciamento de dados corporativos. A governança de dados é essencial para a estratégia geral de uma organização para a gerenciamento de dados.

- Interoperabilidade
Capacidade de sistemas e organizações operarem entre si.

- iCloud
Armazena em segurança suas fotos, vídeos, documentos, músicas, aplicativos e mais, e os mantêm atualizados em todos os dispositivos *iOS*, nos dispositivos *iPadOS,* na *Apple TV* e em *iCloud.com*.

- Link
No âmbito da informática, a palavra link pode significar hiperligação, ou seja, uma palavra, texto ou imagem que quando é clicada pelo usuário, o encaminha para outra página na internet, que pode conter outros textos ou imagens.

- Malwares
É um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas

- Matriz SWOT
Um método de planejamento estratégico que engloba a análise de cenários para tomada de decisões, observando 4 fatores. São eles, em inglês: *Strengths, Weaknesses, Opportunities* e *Threats*. Em português: forças, oportunidades, fraquezas e ameaças.

- Mensageiros instantâneos
É uma aplicação que permite o envio e o recebimento de mensagens de texto em tempo real.

- Notebooks
É um computador pessoal que pode ser transportado com facilidade. Muitos deles estão desenvolvidos para executar softwares e arquivos pesados assim como um desktop.

- *Onedrive*
É um serviço de armazenamento na nuvem da Microsoft que oferece a opção de guardar até 7 GB de arquivos grátis na rede. Ou seja, o usuário pode salvar e acessar seus documentos, fotos, músicas e vídeos a qualquer hora e em qualquer lugar com conexão à Internet, dispensando o uso de pendrives e HD externos.

- Operador
Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- Órgão de Pesquisa
Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

- *Overview*
É uma breve descrição com uma visão geral de um assunto ou tema, sem muitos detalhes.

- *Pen Drive*
Tecnicamente o *pendrive* é um dispositivo portátil de armazenamento com memória flash, acessível através da porta USB

- Pseudonimização
Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

- Política de *Backup*
É um documento que engloba as normas e regras para guiar todo o ciclo do gerenciamento de dados corporativos – desde a concepção até o descarte, escolha do tipo ou estratégia a ser empregada.

- RAIS
Instituída pelo Decreto nº 76.900, de 23/12/75, a RAIS tem por objetivo: o suprimento às necessidades de controle da atividade trabalhista no País, o provimento de dados para a elaboração de estatísticas do trabalho, a disponibilização de informações do mercado de trabalho às entidades governamentais.

- Relatório de Impacto à Proteção de Dados Pessoais
Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- Retenção de dados
A retenção de dados é o armazenamento contínuo de dados de uma organização conforme as definições do negócio.

- Roadmap
É uma espécie de mapa, uma poderosa ferramenta visual e descritiva que apontará como será o produto ou projeto.

- SMS
Conhecido como "torpedo", é uma sigla que significa *Short Message Service*, em inglês ou Serviço de Mensagens Curtas em português.

- Smartphone
Em tradução literal, significa "telefone inteligente". Atualmente, eles contam com inúmeros recursos, ao contrário dos celulares antigos, que só serviam para realizar e receber chamadas e SMS.

- Software
Conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico.

- T.I.- Tecnologia Informação
É um conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

- Titular
Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- Transferência Internacional de Dados
Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

- Tratamento -Toda operação realizada com dados pessoais; como as que se referem a:

- Acesso: Possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados armazenamento - ação ou resultado de manter ou conservar em repositório um dado

- Arquivamento: Ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência

- Avaliação: Ato ou efeito de calcular valor sobre um ou mais dados classificados - maneira de ordenar os dados conforme algum critério estabelecido

- Coleta: Recolhimento de dados com finalidade específica comunicação - transmitir informações pertinentes a políticas de ação sobre os dados

- Controle: Ação ou poder de regular, determinar ou monitorar as ações sobre o dado

- Difusão: Ato ou efeito de divulgação, propagação, multiplicação dos dados, distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido

- Eliminação: Ato ou efeito de excluir ou destruir dado do repositório extração - ato de copiar ou retirar dados do repositório em que se encontrava modificação - ato ou efeito de alteração do dado

- Processamento: Ato ou efeito de processar dados

- Produção: Criação de bens e de serviços a partir do tratamento de dados

- Recepção: Ato de receber os dados ao final da transmissão

- Reprodução: Cópia de dado preexistente obtido por meio de qualquer processo

-Transferência: Mudança de dados de uma área de armazenamento para outra, ou para terceiro

- Transmissão: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc

- Utilização: Ato ou efeito do aproveitamento dos dados

- Upload

O termo *upload se* refere ao ato de "subir" arquivos presentes no seu computador ou celular para um servidor online, ao contrário do download, que é o ato de baixar algo para o seu dispositivo. Se você já postou uma foto no *Facebook ou Instagram*, ou já enviou algum arquivo anexado a um e-mail, você já fez um *upload*. Resumindo, significa enviar um arquivo.

- Uso Compartilhado de Dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

- VPN

Virtual Private Network (Rede Privada Virtual) trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores através de uma rede pública, como a Internet.

21. Temas em Ordem Tipológica e Cronológica de Atuação da ANPD

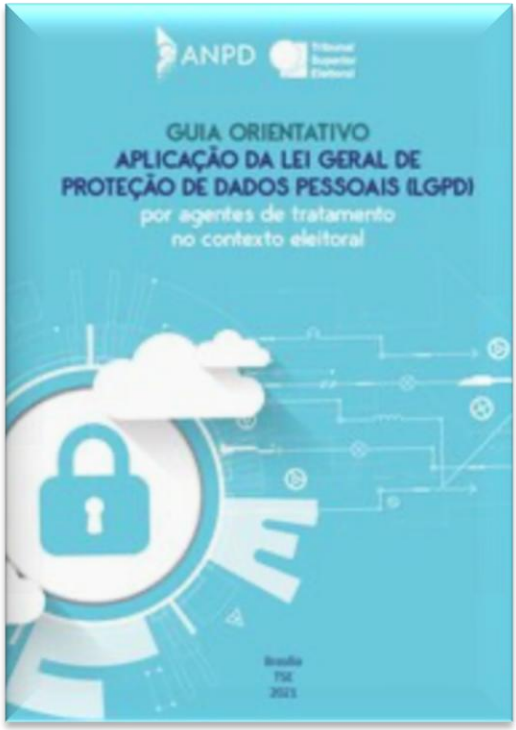
Por Valéria Reani Rodrigues Garcia

21.1 Publicações da ANPD

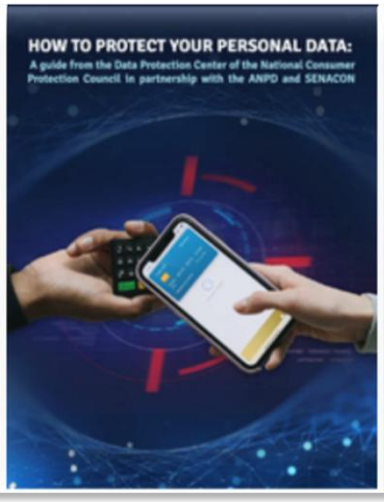
A **Autoridade Nacional de Proteção de Dados**, além dos atos regulamentadores que edita, busca também orientar os agentes sobre o tema de proteção de dados pessoais. Esta Seção é um repositório de normativos, publicações, guias orientativos e documentos técnicos emitidos pela Autoridade.

O objetivo dessas publicações feitas pela ANPD é registrar a memória institucional sobre os temas e servir de referência para titulares de dados pessoais, agentes de tratamento e sociedade em geral.

Clique nas imagens ou acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes



Clique nas imagens ou acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes



Clique nas imagens ou acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

Clique nas imagens ou acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

Clique nas imagens ou acesse: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

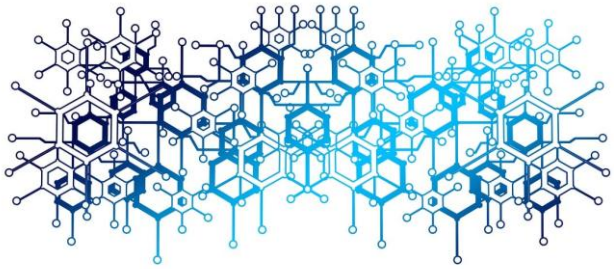
21.2 Outras Publicações

Consulta à Sociedade - *Sandbox* Regulatório de Inteligência Artificial e Proteção de Dados no Brasil.
Relatório de Monitoramento - Relatório de Ciclo de Monitoramento (RCM) da Coordenação-Geral de Fiscalização (CGF) - 1° Semestre de 2023.
Relatório de Monitoramento - Relatório de Ciclo de Monitoramento (RCM) da Coordenação-Geral de Fiscalização (CGF) - Exercício de 2022.
Artigo "Meus dados vazaram, e agora?" - Considerações e orientações da ANPD a respeito do assunto. Publicado em 2021.
Formulário Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP): versão excel; versão pdf.

22. Resoluções

22.1 Resolução CD/ANPD nº 2, De 27 de Janeiro de 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte (alterada pela RESOLUÇÃO CD/ANPD Nº 15, DE 24 DE ABRIL DE 2024).

Por Renata Lima de Mattos Rocha



Desenvolvimento

A **ANPD** publicou Resolução CD/ANPD Nº 2, em 27 de janeiro de 2024 objetivando flexibilizar a aplicação da Lei nº 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte.

De forma clara e objetiva, a Resolução defini os agentes de pequeno porte como:
- **Microempresas**;
- **Empresas de Pequeno Porte**;
- **Startups**;
- **Pessoas Jurídicas de direito privado,** inclusive sem fins lucrativos;
- **Pessoas naturais e entes privados despersonalizados** que realizam tratamento de dados pessoais.

Priorizando a proteção do titular, a Autoridade bem ressalta que, mesmo tratando-se de agentes de pequeno porte, as empresas que realizam tratamento de dados pessoais de alto risco, conforme disposto no Art. 4º da presente Resolução, não se beneficiaram desta Regulamentação.

Outra novidade trazida na aludida Resolução é quanto à forma simplificada de comunicação com o titular de dados prevista nos **Arts. 9** e **18** da **LGPD**, que se dará por meio impresso, eletrônico ou qualquer outro meio que assegure o acesso facilitado das informações pelos titulares dos dados.

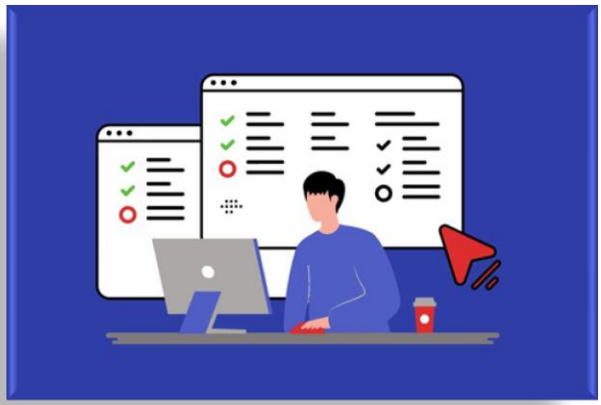
O **Art. 37** da **LGPD** também foi objeto de adequação na presente Resolução, permitindo aos agentes de pequeno porte cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais de uma forma sintetizada, seguindo modelo a ser emitido pela própria ANPD.

Por fim, dois pontos carecem de especial atenção na presente Resolução: restou determinado pela ANPD que os agentes de pequeno porte não precisam nomear um encarregado pelo tratamento dos dados pessoais, conforme exigência constante no **Art. 41** da **LGPD** e que possuem prazo em dobro para atendimento das solicitações previstas nos **Arts. 18**, §§ 3º e 5º, e **19**, inclusive fornecerem declarações simplificadas quanto do atendimento.

Apesar de todas as simplificações apresentadas no texto, o Regulamento bem enfatiza a importância desses agentes adotarem boas práticas de governança e segurança, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento, através políticas simplificadas, porém coesa com as práticas implementadas pelo agente.

Ressaltamos, por fim, que a presente Resolução não significa menor segurança ao titular dos dados, visto que ela é enfática ao esclarecer que dados sensíveis, de alto risco ou complexidade não se enquadram na presente Resolução.

Com isso, pretendeu a ANPD garantir que todas os agentes de tratamento, independente do porte, se adequem à legislação, respeitando a natureza jurídica, porte e limitações de cada um desses agentes, prática esta fundamental para estabelecer uma cultura sólida de proteção de dados pessoais no país.



Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022*

22.1 RESOLUÇÃO CD/ANPD Nº 3, DE 25 DE JANEIRO DE 2023 - Institui o Comitê de Governança Digital da Autoridade Nacional de Proteção de Dados.

Por Renata Próximo da Silva

Desenvolvimento

A **ANPD**, por meio de seu Conselho Diretor, publicou dia 26/01 a Resolução nº 3/2023, que instituiu o Comitê de Governança Digital da Autoridade Nacional de Proteção de Dados.

O Comitê é um órgão de caráter permanente com a finalidade de deliberar sobre assuntos relativos à implementação de ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação no ambiente da Autoridade.

As ações do CGD/ANPD devem estar em consonância com a Estratégia de Governo Digital da administração pública federal e alinhadas ao Planejamento Estratégico da ANPD.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-3-de-25-de-janeiro-de-2023-460124477*

22.3 RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023 - Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

Por Valéria Reani Rodrigues Garcia

Desenvolvimento

A **ANPD** publicou o, tão aguardado, Regulamento de Dosimetria e Aplicação de Sanções Administrativas, através da Resolução CD/ANPD nº 4/2023. Este Regulamento trouxe um norte para que os agentes de tratamento entendessem como as sanções seriam calculadas, possibilitando uma análise mais detalhada de seus processos, com uma avaliação voltada para o risco de serem objeto de sanções de acordo com métricas indicadas pela Autoridade. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, no uso das atribuições que lhe foram conferidas pelo art. 55-J, IV, e § 2º da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), pelo art. 2º, IV, e art. 29 do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, e previstas no Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 1, de 8 de março de 2021.

Segue em anexo a decisão de dosimetria:

ANEXO - REGULAMENTO DE DOSIMETRIA E APLICAÇÃO DE SANÇÕES ADMINISTRATIVAS

A Autoridade Nacional de Proteção de Dados, através deste Regulamento tem por objetivo estabelecer parâmetros e critérios para aplicação das correspondentes sanções administrativas.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf*

22.4 RESOLUÇÃO CD/ANPD Nº 5, DE 13 DE MARÇO DE 2023 - Aprova a Agenda de Avaliação de Resultado Regulatório para o período 2023-2026.

Por Gabriela Marangoni

Desenvolvimento

A Resolução CD/ANPD Nº 05, de 13 de março de 2023, estabelece e aprova a Agenda de Avaliação de Resultado Regulatório para o período 2023-2026, pelo Conselho Diretor da **ANPD**, no âmbito de suas atribuições e no exercício de seus poderes.

Considerando que a Agenda de Avaliação de Resultado Regulatório (ARR) é um instrumento de planejamento e que visa conferir maior previsibilidade e transparência para a atividade regulatória, o Conselho Diretor aprova a seguinte agenda:

AGENDA DE AVALIAÇÃO DE RESULTADO REGULATÓRIO 2023-2026

Ato normativo submetido à ARR	Justificativas	Cronograma
Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados	Com base nos seguintes incisos do §3º do art. 13 do Decreto nº 10.411, de 30 de junho de 2020: - Ampla repercussão na economia ou no País (inciso I); - Impacto significativo em organizações ou grupos específicos (inciso III); e - Tratamento de matéria relevante para a agenda estratégica do órgão (inciso IV).	Definição de indicadores de monitoramento: maio/2023. Conclusão da ARR: dezembro/2026.
Regulamento de Dosimetria e Aplicação de Sanções Administrativas	Com base nos seguintes incisos do §3º do art. 13 do Decreto nº 10.411, de 30 de junho de 2020: - Ampla repercussão na economia ou no País (inciso I); - Impacto significativo em organizações ou grupos específicos (inciso III); e - Tratamento de matéria relevante para a agenda estratégica do órgão (inciso IV).	Conclusão da ARR: dezembro/2026.

Fonte: *ANPD, disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-5-de-13-de-marco-de-2023-469722336*

22.5 RESOLUÇÃO CD/ANPD Nº 6, DE 3 DE ABRIL DE 2023 - Institui o Programa de Gestão e Desempenho no âmbito da Autoridade Nacional de Proteção de Dados; e revoga a Portaria ANPD/PR Nº 19, de 26 de novembro de 2021.

Por Gabriela Marangoni

Desenvolvimento

Para reforçar as práticas de governança de dados, a ANPD instituiu o Programa de Gestão e Desempenho da Autoridade Nacional de Proteção de Dados - PGD/ANPD que possui como resultados e benefícios:

I - promover a cultura orientada a resultados;
II - promover a produtividade e a qualidade das entregas;
III - contribuir para a otimização dos recursos;
IV - melhorar a qualidade de vida e o bem-estar dos servidores;
V - contribuir para a atração, retenção e desenvolvimento de servidores;
VI - contribuir para a motivação e o comprometimento dos servidores;
VII - estimular o desenvolvimento do trabalho criativo, da inovação e da cultura de governo digital.

Além disso, estabelece que poderão ser adotadas, no PGD/ANPD, a modalidade de trabalho presencial ou teletrabalho. Em caso de teletrabalho, pode ser em regime integral ou parcial.

No mais, estabelece que o PGD/ANPD poderá incluir todos os servidores, empregados públicos e contratados temporários em exercício nas unidades da ANPD, com registro do participante e aprovação da chefia imediata no Sistema do PGD/ANPD, cabendo à Coordenação-Geral de Administração coordenar o processo de atualização da tabela de atividades, bem como caberá aos titulares das unidades apresentar, sempre que necessário, à Coordenação-Geral de Administração, proposta de otimização do espaço físico no âmbito de suas unidades.

Reitera-se que a Coordenação-Geral de Administração da ANPD poderá expedir instruções complementares sobre os procedimentos necessários ao cumprimento desta Resolução e que em casos de omissão, serão decididos pelo Diretor-Presidente, com suporte técnico da Coordenação-Geral de Administração.

Por fim, estabelece a revogação da Portaria ANPD/PR nº 19, de 26 de novembro de 2021.

Fonte: *ANPD, disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-6-de-3-de-abril-de-2023-475189920*

22.6 RESOLUÇÃO CD/ANPD Nº 7, DE 17 DE AGOSTO DE 2023 - Aprova a Política de Comunicação Social da Autoridade Nacional de Proteção de Dados.

Por Carlos Alberto Casanova Campos

Desenvolvimento

A **ANPD** publicou, no dia 17 de agosto de 2023, sua Resolução nº 07/2023, que aprovou a Política de Comunicação Social da Autoridade Nacional de Proteção de Dados.

O normativo tem como objetivos orientar as ações de comunicação da ANPD, contribuir para o cumprimento da missão institucional do órgão, direcionar as ações estratégicas da comunicação institucional, promover o fortalecimento da imagem institucional, elaborar um plano de implementação desta Política para criar e manter fluxos de comunicação que facilitem a interação da ANPD com seus diversos públicos.

O Normativo também ressalta as diretrizes da Política de Comunicação Social da ANPD destacando a promoção quanto ao respeito à Constituição Federal e às leis, em especial a **LGPD**; a oferta de amplo conhecimento à sociedade sobre a atuação da Autoridade; difundir informações que contribuam para o entendimento das ações administrativas, regulatórias e sancionatórias da Autoridade; a garantia quanto ao alinhamento, coerência e solidez nos discursos institucionais; a divulgação de forma clara, simples, didática, acessível e alinhadas aos Objetivos Estratégicos da Autoridade os regulamentos, notas técnicas, guias, informativos e notícias, bem como os serviços, campanhas, projetos e iniciativas institucionais; também assegura que as publicações nos canais oficiais atendam aos interesses públicos e institucionais; promove o incentivo a inovação de conteúdos, formatos e linguagens que estejam alinhadas com a missão institucional e com os avanços tecnológicos e sociais; desenvolve formas de auxiliar no fomento de um clima organizacional favorável ao desenvolvimento institucional, bem como orientar e apoiar diretores, coordenadores, servidores, colaboradores e prestadores de serviços nas demandas de Comunicação Social.

Ainda no contexto deste normativo, tratou de operacionalizar as condutas acima descritas, a partir de um Plano de Comunicação Social, aprovado pelo Conselho Diretor da ANPD, que contemplará, no mínimo, cronograma de execução das medidas, seus responsáveis e instrumentos de monitoramento.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-7-de-17-de-agosto-de-2023-503878944 acesso em 24/05/2024*

22.7 RESOLUÇÃO CD/ANPD Nº 8, DE 5 DE SETEMBRO DE 2023 - Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD).

Por Orestes Bacchetti Junior

Desenvolvimento

Por esta Resolução, a **ANPD** instituiu sua Política de Governança de Processos.

O normativo tem os objetivos de mitigar ou reverter prejuízos gerados por incidentes; de assegurar a responsabilização e a prestação de contas; de promover a adoção de boas práticas de governança, prevenção e segurança; e de fortalecer a cultura de proteção de dados pessoais no País.

ANEXO
POLÍTICA DE GOVERNANÇA DE PROCESSOS DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD

Em Anexo a esta Resolução, vem a Política de Governança de Processos da Autoridade, instrumento que estabelece os princípios, as diretrizes, os objetivos, os instrumentos, a estrutura e as responsabilidades relativos à Governança de Processos no âmbito das unidades organizacionais da ANPD.

Fonte: *ANPD, disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-8-de-5-de-setembro-de-2023-508638337*

22.8 RESOLUÇÃO CD/ANPD Nº 9, DE 24 DE OUTUBRO DE 2023 -

Aprova o Aviso de Privacidade do sítio eletrônico da Autoridade Nacional de Proteção de Dados.

Por Carlos Alberto Casanova Campos

Desenvolvimento

A **ANPD** publicou o Aviso de Privacidade do seu sítio eletrônico, na forma do Anexo desta Resolução.

O Aviso de Privacidade do qual trata o caput tem a finalidade de esclarecer e informar aos titulares que acessam o sítio eletrônico da ANPD como seus dados pessoais são tratados, especialmente no que se refere às operações de coleta, uso, armazenamento e compartilhamento.

O Aviso de Privacidade de que trata o caput será divulgado no sítio eletrônico da ANPD.

Para auxiliar na elaboração do Aviso de Privacidade, também conhecida como Política de Privacidade, nos *websites* de forma pública aos titulares de dados.

A ANPD inseriu na Resolução um anexo bastante esclarecedor dos principais itens que devem estar na Política para conhecimento dos titulares de dados.
Segue em o anexo para consulta:

ANEXO
AVISO DE PRIVACIDADE DO SÍTIO ELETRÔNICO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A Autoridade, através deste Regulamento, tem por objetivo estabelecer parâmetros e critérios para aplicação na elaboração da declaração, e esclarecer os pontos principais que devem constar no respectivo documento

Fonte *ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/RESOLUOCD_ANPDN9DE24DEOUTUBRODE2023RESOLUOCD_ANPDN9DE24DEOUTUBRODE2023DOUImprensaNacional.pdf*

22.9 RESOLUÇÃO CD/ANPD Nº 10, DE 5 DE DEZEMBRO DE 2023 -

Aprova o Mapa de Temas Prioritários para o biênio 2024-2025 e dispõe sobre a periodicidade do Ciclo de Monitoramento. O ANEXO II desta Resolução é a Nota Técnica nº 19/2023/FIS/CGF/ANPD.

Por Cecília Rezende de Freitas

Desenvolvimento

A Resolução tem como principais objetivos definir e priorizar temas de atuação da **ANPD**, bem como estabelecer um ciclo bianual de monitoramento das atividades de fiscalização.

Para tanto, estabelece um Mapa de Temas Prioritários que deverá guiar a elaboração de documentos de governança e as prioridades das áreas técnicas da ANPD, em detrimento de outras atividades de fiscalização a respeito de matérias não elencadas no referido mapa.

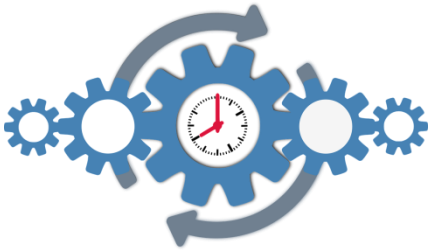
Neste sentido, estão elencados como temas prioritários para o biênio 2024-2025, os direitos dos titulares, incluindo como objetivos, ações de fiscalização preventiva e orientativa em setores como o Poder Público, plataformas digitais, setor financeiro e telecomunicações, com colaboração potencial de Bacen, Anatel e Senacon; a proteção de dados de crianças e adolescentes no ambiente digital, incluindo a fiscalização do tratamento de dados em plataformas digitais e proposta de salvaguardas; o uso da IA para reconhecimento facial e tratamento de dados pessoais, incluindo como objetivo a identificação de riscos e fiscalização de sistemas de reconhecimento facial, especialmente em áreas públicas; e, a raspagem e agregadores de dados, incluindo a fiscalização de operações de tratamento de dados por raspagem e proposição de medidas de adequação à **LGPD**.

O Relatório de Ciclo de Monitoramento 2024-2025 considerará as informações coletadas entre o 2º semestre de 2023 e o 1º semestre de 2025, sendo que o Mapa de Temas Prioritários para o biênio 2026-2027 e o Relatório de Ciclo de Monitoramento do biênio 2024-2025 deverão ser submetidos ao Conselho Diretor até 30 de novembro de 2025 e apreciados até o final do mencionado ano.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528*

22.10 RESOLUÇÃO CD/ANPD N° 11, DE 27 DE DEZEMBRO DE 2023 -

Altera a Agenda Regulatória para o biênio 2023-2024.



Por Cecília Rezende de Freitas

Desenvolvimento

A Resolução tem como principais objetivos alterar a Agenda Regulatória da **ANPD** para o biênio 2023-2024, bem como estabelecer novas prioridades e fases de regulamentação conforme as necessidades emergentes.
Para tanto, estabelece para a primeira fase, iniciativas incluindo a regulamentação e/ou orientação e esclarecimentos, conforme o caso, acerca dos seguintes itens: Dosimetria e

Aplicação de Sanções Administrativas; Direitos dos titulares de dados pessoais, Comunicação de incidentes e especificação do prazo de notificação; Transferência Internacional de Dados Pessoais; Relatório de Impacto à Proteção de Dados Pessoais; Encarregado de proteção de dados pessoais; Hipóteses legais de tratamento de dados pessoais; Definição de alto risco e larga escala; Dados Pessoais Sensíveis - Organizações religiosas; Uso de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa; Anonimização e pseudonimização; Regulamentação do disposto no **Art. 62** da **LGPD**.

Para uma segunda fase, a ANPD estabelece os seguintes temas que devem ser objeto de estudos e discussões, para fins de aplicação da **LGPD**: Compartilhamento de dados pelo Poder Público; Tratamento de dados pessoais de crianças e adolescentes;
Para uma terceira fase, a ANPD relaciona os temas que devem ser objeto de regulamentação e/ou orientação para fins de aplicação da **LGPD**, bem como estudo e acompanhamento, tais como: Dados Pessoais Sensíveis - Dados biométricos; Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança); Inteligência Artificial.

Por fim, para uma quarta fase, a ANPD relaciona os temas que devem ser elaborados para atendimento a determinações legais previstas na **LGPD**, incluindo as Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e a Regulamentação de critérios para reconhecimento e divulgação de regras de boas práticas e de governança.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737*

22.11 RESOLUÇÃO CD/ANPD Nº 12, DE 9 DE ABRIL DE 2024 - Institui o Programa de Integridade da Autoridade Nacional de Proteção de Dados.

Por Orestes Bacchetti Junior

Desenvolvimento

Com este normativo fica instituído, no âmbito da **ANPD**, o Programa de Integridade com o objetivo de promover a conformidade de condutas, a transparência, a priorização do interesse público e uma cultura organizacional voltada à entrega de valor público à sociedade.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-12-de-9-de-abril-de-2024-553574469*

22.12 RESOLUÇÃO CD/ANPD Nº 13, DE 9 DE ABRIL DE 2024 - Institui a Comissão de Integridade, Transparência e Acesso à Informação da Autoridade Nacional de Proteção de Dados.

Por Anna Carolina de Medeiros Silva

Desenvolvimento

A Resolução CD/ANPD Nº 13, de 9 de abril de 2024, é um passo significativo na regulamentação da segurança de dados pessoais no Brasil. Este regulamento estabelece diretrizes claras e obrigatórias para a comunicação de incidentes de segurança que afetam dados pessoais, consolidando esforços para aumentar a transparência e a responsabilidade das organizações.

Essencial para a proteção de dados pessoais, a Resolução determina que todas as organizações públicas e privadas devem notificar a **ANPD** e os titulares dos dados afetados em prazos específicos após a detecção de qualquer incidente de segurança.

Essa medida visa garantir uma resposta rápida e eficaz, mitigando possíveis danos, o que trará uma maior confiabilidade titulares de dados.

O regulamento também enfatiza a importância de adotar boas práticas de governança e segurança, como a documentação detalhada das medidas de resposta a incidentes e a implementação de estratégias proativas para prevenir futuras violações. Estas práticas são fundamentais para estabelecer uma cultura sólida de proteção de dados pessoais no país.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-13-de-9-de-abril-de-2024-553571464*

22.13 RESOLUÇÃO CD/ANPD Nº 14, DE 9 DE ABRIL DE 2024 - Aprova a Metodologia de Governança de Processos da Autoridade Nacional de Proteção de Dados.

Por Anna Carolina de Medeiros Silva

Desenvolvimento

Para reforçar as práticas de governança de dados, a **ANPD** publicou a Resolução CD/ANPD Nº 14, em 9 de abril de 2024. Esta resolução visa consolidar e aprimorar as diretrizes para organizações que tratam dados pessoais, garantindo uma gestão mais segura e responsável das informações.

A Resolução introduz normas mais estritas sobre o armazenamento, tratamento e compartilhamento de dados pessoais, impondo obrigações claras aos controladores para manter a integridade e a privacidade dos dados. As medidas incluem a exigência de políticas de segurança da informação mais desenvolvidas, auditorias regulares de dados e a necessidade de obter consentimento explícito dos titulares para qualquer nova finalidade de tratamento não autorizada previamente.

Além disso, a ANPD estabelece que todas as organizações devem nomear um encarregado de proteção de dados para supervisionar a conformidade com as normas estabelecidas, servindo como ponto de contato entre a entidade reguladora e os titulares de dados.

Ademais, a obrigatoriedade da nomeação de um encarregado de dados não se estende aos agentes de tratamento de pequeno porte, exceto àqueles que realizarem tratamento de alto risco, aufiram receita bruta superior ao limite estabelecido na Lei Complementar nº 123/2006, de 14 de dezembro de 2006, pertençam a grupo econômico de fato ou de direito, cuja receita ultrapasse os limites referidos na mesma Lei Complementar.

Concluindo, esta resolução é um passo importante para fortalecer a confiança dos titulares de dados nas instituições públicas e privadas, bem como, para impulsionar a cultura de transparência e responsabilidade em todo o ecossistema de dados no Brasil.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-13-de-9-de-abril-de-2024-553571464*

22.14 RESOLUÇÃO CD/ANPD Nº 15, DE 24 DE ABRIL DE 2024 - Aprova o Regulamento de Comunicação de Incidente de Segurança.

Por Valéria Rodrigues Reani Garcia

Desenvolvimento

A **ANPD** publicou, no dia 26 de maio de 2024, Resolução nº15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança (RCIS).

O normativo tem os objetivos de mitigar ou reverter prejuízos gerados por incidentes; de assegurar a responsabilização e a prestação de contas; de promover a adoção de boas práticas de governança, prevenção e segurança; e de fortalecer a cultura de proteção de dados pessoais no País.

Fonte: *ANPD, disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca*

22.15 RESOLUÇÃO CD/ANPD Nº 16, DE 7 DE MAIO DE 2024 - Aprova o Planejamento Estratégico Institucional da Autoridade Nacional de Proteção de Dados para os anos de 2024 a 2027.

Por Orestes Bacchetti Junior

Desenvolvimento

Com esta Resolução, a **ANPD** aprovou seu Planejamento Estratégico Institucional para os anos de 2024 a 2027.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-16-de-7-de-maio-de-2024-558531744 acesso em 26/05/2024*

22.16 RESOLUÇÃO CD/ANPD Nº 17, DE 22 DE MAIO DE 2024 – Institui o Sistema Eletrônico de Informações (SEI) no âmbito da Autoridade Nacional de Proteção de Dados e aprova seu Termo de Uso.

Por Gabriela Marangoni

Desenvolvimento

Para reforçar as práticas de governança de dados, a **ANPD** instituiu institui o Sistema Eletrônico de Informações (SEI) como o sistema de gestão de documentos e processos administrativos, eletrônicos e digitais, o que compreende as etapas de produção, edição, assinatura, recebimento, tramitação, autuação, conclusão e arquivamento.

O SEI possui como objetivos promover a utilização de meios eletrônicos para a realização dos processos administrativos com segurança, transparência e economicidade; ampliar a sustentabilidade ambiental com o uso da tecnologia da informação e comunicação; facilitar o acesso às informações e às instâncias administrativas e simplificar o atendimento prestado aos usuários dos serviços públicos.

A Coordenação-Geral de Administração (CGA) atuará como unidade de gestão organizacional do SEI, com o objetivo de coordenar os trabalhos de implantação, manutenção e evolução do SEI no âmbito da ANPD, e demais atribuições necessárias para acompanhar e monitorar a adequada utilização do sistema.

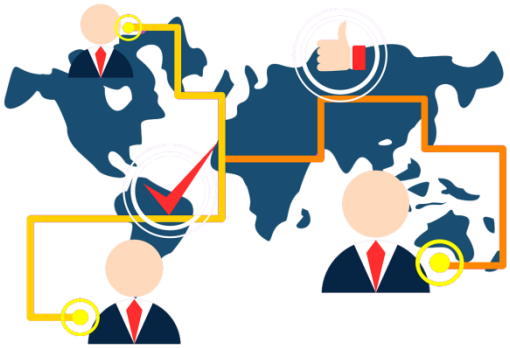
Por outro lado, a Coordenação-Geral de Tecnologia da Informação (CGTI) atuará como unidade de gestão técnica do SEI, que deverá gerir a infraestrutura de hardware e requisitos de software; bem como manter atualizada a versão do sistema e prover as condições técnicas necessárias à implantação e à utilização do SEI, garantindo sua disponibilidade, integridade, confiabilidade e segurança dos documentos eletrônicos e proporcionar a integração do SEI com outros sistemas informatizados que estejam sob sua responsabilidade.

Por fim, estabelece e anexa o Termo de Uso do Sistema Eletrônico de Informação (SEI), que está disponível no próprio sistema e no sítio eletrônico para consulta dos usuários, e possui cláusulas acerca de: aceitação do termo de uso; definições do termo de uso; arcabouço legal; descrição do serviço; direitos do usuário; responsabilidades do usuário; responsabilidade da ANPD; alterações no termo de uso; informações para contato e foro competente.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-17-de-22-de-maio-de-2024-562136962*

22.17 RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024 - Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

Por Valéria Rodrigues Reani Garcia



Desenvolvimento

A **LGPD** não define um perfil específico e detalhado para o Encarregado de Proteção de dados - EPD (chamado pelo RGPD europeu de "Encarregado da Proteção de Dados", correntemente referido como *Data Protection Officer*, ou *DPO*), sendo tal incumbência da Autoridade Nacional de Proteção de Dados (ANPD), a qual publicou, em 17/07/2024, no DOU, a **RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024** que aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais que transcrevemos de forma resumida e objetiva todos os pontos relevantes dessa Resolução;

Regulamento sobre a Atuação do Encarregado pelo Tratamento de Dados Pessoais

A Resolução CD/ANPD nº 18, de 16 de julho de 2024, aprovada pelo Conselho Diretor da ANPD, estabelece normas detalhadas sobre a atuação do encarregado pelo tratamento de dados pessoais, conforme a Lei nº 13.709, de 14 de agosto de 2018. Este regulamento entra em vigor na data de sua publicação.

Disposições Preliminares

O regulamento define a indicação, as atribuições e a atuação do encarregado, que é a pessoa designada pelo controlador e operador para servir como canal de comunicação entre estes, os titulares dos dados e a ANPD. Define também termos importantes, como agentes de tratamento, controlador, operador e titular.

Dos Agentes de Tratamento e da Indicação do Encarregado

A indicação do encarregado deve ser formal, documentada por escrito, e apresentada à ANPD quando solicitada. Agentes de pequeno porte que são dispensados de indicar um encarregado devem disponibilizar um canal de comunicação com os titulares dos dados.

Da Identidade e das Informações de Contato do Encarregado

A identidade e as informações de contato do encarregado devem ser divulgadas publicamente no site do agente de tratamento, de forma clara e objetiva. Para agentes que não possuem site, essa divulgação pode ser feita por outros meios de comunicação disponíveis.

Dos Deveres dos Agentes de Tratamento

Os agentes de tratamento são responsáveis por prover os meios necessários para o desempenho das atribuições do encarregado, garantir sua autonomia técnica, e assegurar acesso direto às pessoas de maior nível hierárquico dentro da organização.

Do Encarregado e das Características

O encarregado pode ser uma pessoa natural ou jurídica, interna ou externa ao quadro organizacional do agente de tratamento, e deve ser capaz de comunicar-se claramente em língua portuguesa.

Das Atividades e das Atribuições

O encarregado deve aceitar reclamações dos titulares, receber comunicações da ANPD, orientar os funcionários sobre práticas de proteção de dados, e executar outras atribuições determinadas pelo agente de tratamento. Deve também prestar assistência na elaboração de registros e relatórios de impacto, implementação de medidas de segurança, e outras decisões estratégicas relativas ao tratamento de dados pessoais.

Do Conflito de Interesse

O encarregado deve atuar com ética, integridade e autonomia, evitando situações de conflito de interesse. Pode acumular funções para mais de um agente de tratamento, desde que isso não comprometa suas atribuições e não haja conflito de interesse. O encarregado deve declarar qualquer situação que possa configurar conflito de interesse, e o agente de tratamento deve adotar medidas para evitar ou mitigar esses conflitos. Vale salientar que haja cautela quanto ao acúmulo das funções do EPD, vez que pode representar um **alto risco** numa organização, principalmente por gerar conflitos de interesse, o que afeta a capacidade de agir com independência.

Este regulamento reforça a importância de uma gestão ética e transparente no tratamento de dados pessoais, assegurando direitos dos titulares e a conformidade com a legislação de proteção de dados.

Quando pode haver o conflito de interesses?

O conflito de interesses pode ser verificado quando questões diversas (profissionais, financeiras, familiares, políticas ou pessoais) podem interferir no julgamento das pessoas ao exercerem suas ações dentro das organizações — com base na Norma de Certificação de Sistemas de Gestão de *Compliance* Antissuborno (NBR ISO 37001:2016).

Considerações acerca da Resolução acima que trata do Encarregado

Reforçamos que a Resolução não altera as obrigações e atribuições da LGPD, que passamos a destacar abaixo:

Para que não incorra no "conflito de Interesse "descrito na Seção III da Resolução, é recomendável que o encarregado nomeado **NÃO** atue nas áreas de tecnologia da informação, auditoria e/ou *compliance*. No entanto, convém que esta pessoa exerça tal cargo em período integral, tenha senioridade equiparável à um diretor e competência para analisar estratégias fundamentais sobre fluxo de dados.

O Encarregado também deverá sobressair-se em *soft skills* e saber transitar pelas diversas áreas da empresa. Importante, acima de tudo, que conte com o suporte da diretoria e administradores como forma de fortalecer sua atuação e aumentar a cooperação dos demais funcionários da empresa, sendo envolvido em todas as operações que envolvam o tratamento de dados pessoais, bem como participando de reuniões de diretoria e gestão da empresa.

Para cumprir seus objetivos, o Encarregado necessitará que a empresa forneça os recursos necessários ao desempenho de suas atividades e à manutenção dos seus conhecimentos, garantindo acesso aos dados pessoais e às operações de tratamento.

Dentre os recursos e suporte que a empresa deverá garantir e fornecer, destacamos os seguintes:

i. Apoio efetivo às atividades do Encarregado pela diretoria e gestores da empresa, inclusive, quando aplicável, do conselho de administração;
ii. Não penalização do encarregado e sua equipe em razão do cumprimento de suas atividades relacionadas à proteção de dados pessoais;
iii. Garantir que outras atividades exercidas pelo encarregado dentro da empresa, caso ele exerça alguma outra função além de Encarregado, não gerem um conflito de interesses;
iv. O Encarregado pode acumular funções para mais de um agente de tratamento, **desde que isso não comprometa suas atribuições e não haja conflito de interesse**. O encarregado deve declarar qualquer situação que possa configurar conflito de interesse, e o agente de tratamento deve adotar medidas para evitar ou mitigar esses conflitos.
v. O encarregado deve-se assegurar que ele tenha tempo suficiente para execução das atividades específicas relativas à proteção de dados dentro de sua jornada de trabalho;
vi. Devem ser alocados recursos humanos para formação da equipe de apoio, assim como recursos financeiros tanto para o orçamento interno dos custos rotineiros do Encarregado quanto para eventual contratação de consultores e advogados externos e de plataformas operacionais;
vii. Disponibilização de infraestrutura adequada, local de trabalho, salas privativas para condução de reuniões e entrevistas que podem abordar matérias sensíveis e sigilosas, computadores e outros equipamentos, conexão com internet, rede e telefonia, entre outros;
viii. Comunicação oficial sobre a nomeação do Encarregado, inclusive mediante disponibilização dos canais oficiais para contato, preferencialmente, mas não exclusivamente, na página da empresa na internet;
ix. Capacitação e formação contínua, viabilizando que o Encarregado esteja sempre atualizado com relação à proteção de dados e matérias relacionadas; e
x. Garantir que as recomendações, observações e considerações do Encarregado serão levadas em conta nas decisões internas da empresa, registrando e fundamentando os casos em que tais recomendações não forem acatadas.

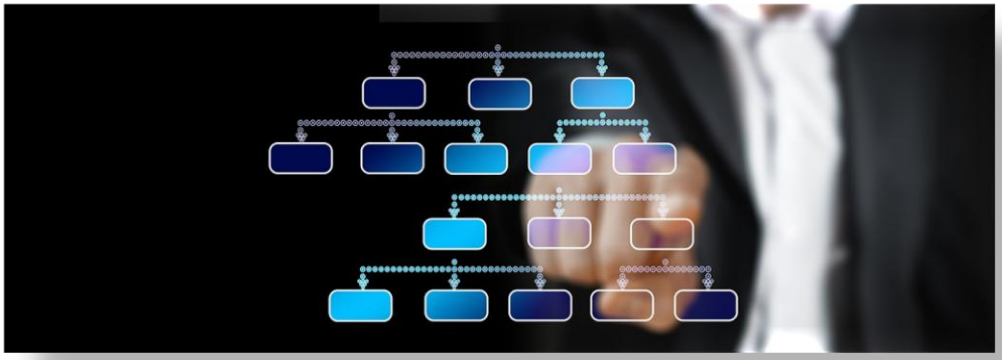
A nomeação do Encarregado (ou DPO) relevante (embora a Resolução tenha deixado essa relevância a parte, para o melhor atendimento ao titular de dados) vez que a nomeação **do EPD é objetivamente exigida pelo Art. 41 da Lei:**

> *O controlador deverá indicar encarregado pelo tratamento de dados pessoais.*
> *§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.*

Sendo clara a importância de sua atuação, trata-se de providência imediata a ser adotada pelas empresas e por escritórios de advocacia, não só visando atender a imposição legislativa, mas também direcionar as implementações necessárias e orientar, internamente, quanto à mudança de cultura e o necessário acautelamento no tratamento de dados pessoais por parte dos colaboradores.

Atividades e responsabilidades do Encarregado de Dados / *DPO*, de acordo com a **LGPD** em seu **Art. 41**, o Encarregado tem as seguintes atividades:

i. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
ii. Receber comunicações da autoridade nacional e adotar providências;
iii. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
iii. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.



Além destas, percebe-se que o **Encarregado de Proteção de Dados -EPD** é importante para todo o ecossistema de proteção de dados pessoais corporativo, em razão de que podemos incluir como atribuições adicionais:

i. Tomar as medidas necessárias para promover a cultura sobre proteção de dados pessoais dentro da organização, por meio de treinamentos periódicos, palestras, e-mails internos informativos, dentre outras atividades;
ii. Gerir a governança de dados pessoais;
iii. Providenciar que a empresa se adapte para tratar dados pessoais em conformidade com a **LGPD**;
iv. Gerir dados pessoais e os riscos relacionados ao envolver terceiros na cadeia de tratamento (operadores);
v. Gerir incidentes de segurança da informação (SI) e, especialmente, violação de dados pessoais;
vi. Auxiliar na contratação e fiscalização de terceiros, verificando se as medidas de segurança adequadas podem ser aplicadas pelo referido terceiro, bem como acompanhando a execução do contrato, solicitando informações e esclarecimentos ao encarregado do terceiro;
vii. Providenciar a criação e atualização dos relatórios de impacto à proteção de dados pessoais (DPIA - RIPD); e
viii. Revisar regularmente e cumprir a política de proteção de dados pessoais da empresa, além das normas complementares eventualmente emitidas pela ANPD.

Importante frisar que no momento a **LGPD** impõe a todos os agentes de tratamento (Controladores e Operadores), independentemente de seu porte, ramo de atividade e faturamento, a obrigação de ter um Encarregado constituído, sendo facultado à ANPD (Resolução nº 18, de 17 de julho de 2024) estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

A área e equipe **do Encarregado de proteção de dados** poderá variar conforme a estrutura e porte do agente de tratamento, mas, especialmente, em razão do volume de dados pessoais tratados e sua complexidade, inexistindo uma configuração única compatível.
Isto significa que cada um dos agentes de tratamento deverá estudar suas operações, fluxos de dados, complexidade, volume e organograma, para identificar uma estrutura que melhor supra suas necessidades e viabilize o cumprimento de suas obrigações.

Neste sentido, além dos conhecimentos sobre **LGPD**, tecnologia da informação e segurança da informação recomendáveis ao Encarregado, outros profissionais poderão ser indicados para assessorar o Encarregado, integrando ou não sua equipe.

Feitas estas considerações e com base numa análise objetiva acima, recomenda-se a criação de uma equipe multidisciplinar, **como um Comitê**, com pessoas que complementem o conhecimento do Encarregado, com o compromisso de interagir, aconselhar e auxiliar nos processos, rotinas e atividades do encarregado seja de forma proativa ou mediante demanda.

É altamente recomendado que referido Comitê conte com pessoas das principais de departamentos o que colabora não só para uma visão mais apurada das operações da respectiva área, mas também para a propagação da cultura da proteção de dados pessoais.

De forma alternativa, a Resolução 18, ainda indica que é possível a contratação de **consultoria de assessoramento ao Encarregado** (pessoa jurídica), ou um "***DPO as a service*"**, na forma do disposto na Resolução 18 de 17/07/2024 *"in verbis"*; **Capítulo III - Do Encarregado Seção I - Das Características: O encarregado pode ser uma pessoa natural *ou jurídica*,** interna ou externa ao quadro organizacional do agente de tratamento, e deve ser capaz de comunicar-se claramente em língua portuguesa.

Portanto, é assegurado pela Resolução contratação de assessoria/Consultoria (pessoa jurídica) de um *"DPO as a servisse"*, isto é , um terceiro externo que, não vinculado como colaborador, execute as atividades do Encarregado como prestador de serviços, devendo-se garantir que referido prestador possua as competências e capacidades necessárias para lidar com as demandas dos titulares, da ANPD e da organização.

A **LGPD** responsabiliza apenas os agentes de tratamento (Controlador e Operador) pelos danos patrimoniais, morais, individuais e coletivos causados que decorram do exercício de atividades de tratamento de dados pessoais, razão pela qual também são os agentes de tratamento que respondem pelas sanções administrativas. Vale dizer, a responsabilidade perante os titulares dos dados e a ANPD será dos agentes de tratamento.

No entanto, isto não significa que o Encarregado não será responsabilizado pelos danos decorrentes de suas ações ou omissões, uma vez que ele poderá ser responsabilizado tanto no caso de ser um empregado, quanto no caso de ser um prestador de serviços.

A ***Consolidação das Leis do Trabalho*** (*CLT*) faculta ao empregador efetuar descontos nos salários do empregado, no caso de dolo na conduta do empregado, ou seja, quando o empregado agir ou se omitir propositalmente com a intenção de causar um dano, assim como na hipótese de previsão expressa no contrato de trabalho.

O ***Código Civil***, por sua vez, estabelece àqueles que causarem danos, seja por culpa ou dolo, a obrigação de repararem os prejuízos causados, ainda que exclusivamente morais. Desta forma, sendo o Encarregado um empregado ou um prestador de serviços, seus atos e decisões que acarretarem danos ou prejuízos podem ser objeto de responsabilização pessoal pelo empregador ou responsabilização civil pelo tomador de serviços.

Por estes motivos, recomenda-se uma criteriosa avaliação sobre a necessidade ou não da contratação de um seguro de responsabilidade civil para o controlador, e para seu Encarregado, caso ele seja empregado, ou exigir a contratação de seguro do prestador de serviço que atuar como Encarregado, apólice esta que deverá compreender cobertura para indenizações e sanções baseadas na **LGPD**.

Art. 462 - Ao empregador é vedado efetuar qualquer desconto nos salários do empregado, salvo quando este resultar de adiantamentos, de dispositivos de lei ou de contrato coletivo.
§ 1º - Em caso de dano causado pelo empregado, o desconto será lícito, desde que esta possibilidade tenha sido acordada ou na ocorrência de dolo do empregado. (...)
Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Conclusão

A Resolução CD/ANPD nº 18 de 16 de julho de 2024, reforça a importância do encarregado no sistema de proteção de dados pessoais no Brasil. Para os empresários, entender e implementar as diretrizes desta resolução é essencial para assegurar a conformidade com a **LGPD** e proteger os direitos dos titulares dos dados. A conformidade não apenas evita sanções, mas também fortalece a confiança dos clientes e parceiros de negócios na organização.

Referências *(Acessadas a 18 de julho de 2024)*

Código Civil Brasileiro, disponível em: *https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm*
Consolidação das Leis Trabalhistas – ***CLT*** , disponível em *https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm*
Constituição Federal Brasileira **–** ***CF***, disponível em *https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm*
Resolução CD/ANPD nº 18, de 16 de julho de 2024 **-** *Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.* Disponível em *https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074*

RESOLUÇÃO Nº 19 – TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS (I)

Por Camilla do Vale Jimene e Henrique Fabretti Moraes

A **ANPD** publicou, no dia 23 de agosto, de 2024 a Resolução CD/ANPD nº 19, estabelecendo o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. A norma impacta diretamente os escritórios de advocacia que realizam transferências internacionais de dados pessoais para diversos fins, como consultorias, litígios e investigações.

A Resolução nº 19 regula os mecanismos permitidos para a transferência internacional de dados, já previstos no **Art. 33** da **LGPD**, o que inclui a transferência para países com nível de proteção adequado reconhecido pela ANPD, cláusulas contratuais específicas aprovadas pela Autoridade, cláusulas-padrão contratuais elaboradas pela ANPD e normas corporativas globais. A escolha do mecanismo adequado dependerá de uma análise criteriosa de cada caso, considerando a finalidade da transferência, a natureza dos dados, o país de destino e os riscos envolvidos.

O primeiro mecanismo de transferência, para países 'adequados', **segue os mesmos moldes utilizados no *Regulamento Geral sobre Proteção de Dados da União Europeia*** *(RGPD),* onde a ANPD, poderá reconhecer a adequação do nível de proteção de dados de outros países, permitindo a transferência livre de dados para esses territórios. A Resolução nº 19, em seu Capítulo IV, define os critérios para essa avaliação, que abrangem as normas em vigor no país, a observância dos princípios da **LGPD** e a existência de um órgão regulador independente. Escritórios que transferem dados para países reconhecidos como adequados pela ANPD estarão dispensados de obter autorizações adicionais.

Nos casos em que o país de destino não possui nível de proteção adequado, a Resolução nº 19 prevê a utilização de cláusulas contratuais em algumas modalidades.

As **cláusulas-padrão contratuais** (CPCs), são cláusulas elaboradas pela ANPD (presentes no Anexo II da Resolução) e devem ser adotadas integralmente, sem modificações, e podem ser incorporadas a contratos existentes por meio de termos aditivos. Este mecanismo apesar de mais simples que as demais modalidades de cláusulas contratuais, por não permitir alterações, carece da flexibilidade que pode ser necessária a atividades específicas da prestação de serviços jurídicos.

Ademais, apesar de não estar expressamente previsto na Resolução, considerando o disposto no artigo 2º, inciso I[1], deste normativo, pode ser necessária a avaliação da legislação do país do 'importador' de dados, para assegurar que esta não se sobreponha de forma negativa à alguma das regras previstas nas CPCs, não dando o mesmo nível de proteção aos titulares de dados do que o previsto na LGPD. Este mecanismo de avaliação prévia costuma ser denominado de *Transfer Impact Assessment* (TIA).

Ainda, a ANPD também poderá reconhecer a equivalência de cláusulas-padrão de outros países ou organismos internacionais, como as SCCs da Comissão Europeia, simplificando o processo para escritórios que já utilizam esses modelos.

Em situações específicas, quando as cláusulas-padrão contratuais não atenderem às necessidades da transferência internacional de dados, o controlador poderá solicitar à ANPD a aprovação de cláusulas contratuais específicas (Art. 21 da Resolução nº 19). Essa modalidade exige um processo mais rigoroso, devendo o controlador comprovar a impossibilidade de utilizar as cláusulas-padrão e demonstrar que as cláusulas específicas garantem nível de proteção de dados equivalente ao da legislação brasileira.

A elaboração de cláusulas contratuais específicas exige atenção redobrada por parte dos escritórios de advocacia. É fundamental que as cláusulas sejam redigidas de forma clara, precisa e abrangente, contemplando todos os aspectos relevantes da transferência, como a finalidade, os tipos de dados, as responsabilidades das partes, as medidas de segurança e os direitos dos titulares. A ANPD analisará cuidadosamente o conteúdo das cláusulas, podendo solicitar informações adicionais ou realizar diligências antes de conceder a aprovação e o processo de avaliar a legislação do país do importador também pode ser necessária.

[1] *"Art. 2° A transferência internacional de dados será realizada em conformidade com o disposto na Lei nº 13.709, de 14 de agosto de 2018, e neste Regulamento, observadas as seguintes diretrizes: I - garantia de cumprimento dos princípios, dos direitos do titular e de nível de proteção equivalente ao previsto na legislação nacional, independentemente do país onde estejam localizados os dados pessoais objeto da transferência, inclusive após o término do tratamento e nas hipóteses de transferências posteriores."*

Já as **normas corporativas globais**, similares às *Binding Corporate Rules* (BCRs) europeias, são outra opção para transferências internacionais que ocorram apenas dentro de um mesmo grupo econômico. O Capítulo VII da Resolução nº 19 detalha os requisitos para a elaboração e aprovação dessas normas pela ANPD, que devem abranger a estrutura do grupo, os direitos dos titulares, as responsabilidades pelo tratamento e as medidas de segurança. A aprovação das normas corporativas globais garante a conformidade das transferências internacionais intragrupo, dispensando novas autorizações.

A **LGPD** também prevê **outros mecanismos** para a transferência internacional de dados, como o consentimento específico e em destaque do titular (Art. 33, VIII), o cumprimento de obrigação legal ou regulatória (Art. 33, IX), a execução de contrato com o titular (Art. 33, IX) e o exercício regular de direitos em processo judicial, administrativo ou arbitral (Art. 33, IX). É crucial que os escritórios de advocacia compreendam as nuances de cada um desses mecanismos e os utilizem de forma adequada, documentando o processo para fins de comprovação.

Por fim, vale mencionar que a partir da publicação da resolução, os agentes de tratamento têm o prazo de 12 meses, para incorporar as cláusulas-padrão contratuais aos contratos existentes que envolvam transferência internacional de dados.

RESOLUÇÃO CD/ANPD Nº 19 DE 23 DE AGOSTO DE 2024 (II) - Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais

Por Raquel Elena Rinaldi Maciel

Desenvolvimento

A **ANPD** publicou Resolução CD/ANPD Nº 19, em 23 de agosto de 2024 objetivando regulamentar **Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.**

Como Principais pontos citamos:

Primeiramente a regra, passou por diversas etapas, dentre as quais destacam-se a Tomada de Subsídios, a Consulta Pública e Audiência Pública.

Consequentemente, regulamentou os **Arts. 33 a 36** da **LGPD**, disciplinando mecanismos contratuais para a realização de transferências internacionais de dados pessoais e estabeleceu procedimentos e regras para o reconhecimento de adequação de outros países ou organismos internacionais.

Sendo assim, a transferência internacional de dados ocorrerá quando o agente de tratamento (chamado de exportador), localizado no território nacional ou em país estrangeiro, transferir dados pessoais para outro agente de tratamento (chamado de importador) localizado em país estrangeiro ou organismo internacional.

A resolução chama a atenção de que a coleta internacional de dados não caracteriza transferência internacional de dados, e que a transferência internacional de dados observará o princípio da necessidade:

- Ficará limitada ao mínimo necessário para o alcance de suas finalidades, devendo ocorrer somente com os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

A transferência internacional de dados deverá estar amparada basicamente em:

- Uma das hipóteses legais previstas no **Art. 7º** da **LGPD** e

- Um dos seguintes mecanismos válidos de realização da transferência internacional:

Grau de proteção de dados pessoais adequado reconhecido por decisão de adequação da ANPD será possuir:

- cláusulas-padrão contratuais;
- normas corporativas globais ou
- cláusulas contratuais específicas.

A LGPD não será aplicada basicamente nas seguintes situações:

- Em caso de trânsito internacional de dados pessoais sem que haja comunicação ou compartilhamento com agente de tratamento no Brasil;

- Em caso de retorno dos dados pessoais tratados para o país ou para o organismo internacional de origem, desde que:

  - Haja adequado grau de proteção aos dados pessoais (o que deverá ser) reconhecido por decisão da ANPD) no país ou organismo internacional;

  - A lei do país de origem, bem como as normas do organismo internacional possam ser aplicadas ao tratamento em questão.

Dentre os mecanismos de transferência internacional regulamentados temos as cláusulas- padrão contratuais, as cláusulas contratuais específicas e as normas corporativas globais que são citadas no **Art. 33** da **LGPD**:

> "A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
> **b) cláusulas-padrão contratuais;**
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;"

DECISÃO DE ADEQUAÇÃO

É a decisão na qual a ANPD reconhece a equivalência entre o nível de proteção de dados pessoais de país estrangeiro ou organismo
internacional e a **LGPD**.

Nesse cenário, poderá ser emitida pela ANPD após o preenchimento de critérios avaliativos e a tramitação em um procedimento específico que inclui análises técnica e jurídica e a deliberação pelo Conselho Diretor.

CLÁUSULAS-PADRÃO CONTRATUAIS

São cláusulas que poderão integrar contrato celebrado para reger a transferência internacional de dados e contêm garantias e condições para a realização de transferências internacionais com o objetivo de garantir a presença de salvaguardas visando cumprir os princípios, os direitos do titular e o regime de proteção de dados previstos na LGPD.

As cláusulas-padrão contratuais constam no GDPR como **"SCC"** (*Standard Contractual Clauses*) sendo um modelo padrão de mecanismo de conformidade para a transferência de dados.

Através destas cláusulas são estabelecidos requisitos e compromissos contratuais, com o objetivo de facilitar transferência para países terceiros.

As cláusulas- padrão contratuais deverão ser:

- adotadas integralmente no contrato e sem qualquer alteração em seu texto a fim de assegurar a validade da transferência internacional de dados;

- interpretadas de forma mais favorável ao Titular e de acordo com as disposições da Legislação Nacional;

- aprovadas pela ANPD e incorporadas pelo agente de tratamento aos instrumentos contratuais no prazo de até doze meses.

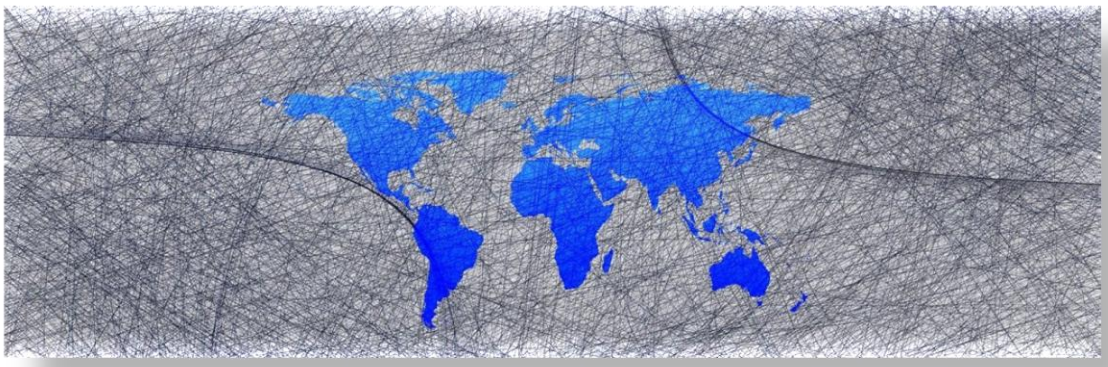
CLÁUSULAS CONTRATUAIS ESPECÍFICAS

São cláusulas contratuais criadas pelo controlador sempre que não puder utilizar as cláusulas-padrão.

Oferecem garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, devendo ser aprovadas por procedimento especifico da ANPD.

NORMAS CORPORATIVAS GLOBAIS (NCG)

São mecanismos que possibilitam transferências internacionais de dados entre organizações do mesmo grupo ou conglomerado de empresas, possuindo caráter vinculante em relação aos membros do grupo que as subscreverem.



Fonte: *ANPD – RESOLUÇÃO CD/ANPD Nº 19 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396*

23. Enunciados

23.1 ENUNCIADO CD/ANPD Nº 1, DE 22 DE MAIO DE 2023 - Edita o enunciado sobre o tratamento de dados pessoais de crianças e adolescentes.

Por Marcela Fuga Antunes Cardoso

Desenvolvimento

De acordo com o Art. 51(3) do Regimento Interno da **ANPD**, a autoridade pode se manifestar através de (**i**) resolução, (**ii**) enunciado, (**iii**) despacho decisório, (**iv**) ata de deliberação, (**v**) consulta pública e (**iv**) portaria.

Os enunciados – especificamente mencionados no art. 51, II do RIANPD –, expressam "(...) decisão quanto à interpretação da legislação de proteção de dados pessoais e fixa entendimento sobre matérias de competência da ANPD, com efeito vinculativo à Autoridade;".

Significa dizer que, ao editar um enunciado, a ANPD demonstra como determinado assunto será interpretado de acordo com legislação de proteção de dados pessoais, de sorte que os agentes de tratamento devem se atentar a esses posicionamentos para ajustar suas atividades de tratamento e evitar tratamentos ilegais, bem como eventuais penalidades em caso de fiscalização.

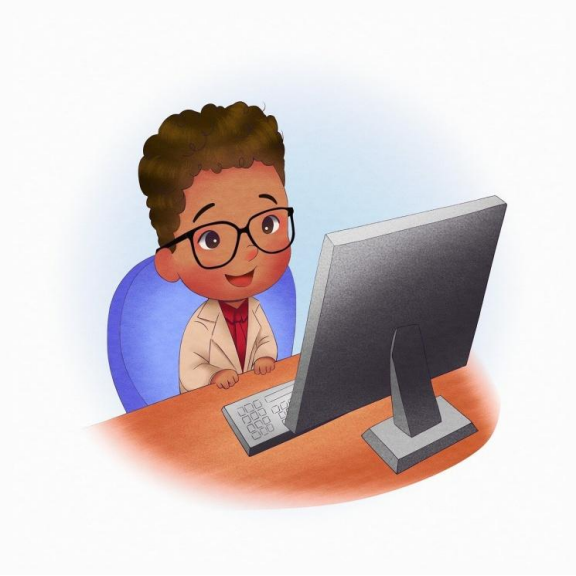
(3) Art. 51. A ANPD manifestar-se-á por meio dos seguintes instrumentos, dentre outros:
I - Resolução: expressa decisão quanto ao provimento normativo de competência da ANPD;
II - Enunciado: expressa decisão quanto à interpretação da legislação de proteção de dados pessoais e fixa entendimento sobre matérias de competência da ANPD, com efeito vinculativo à Autoridade;
III - Despacho Decisório: expressa decisão sobre matérias não abrangidas pelos demais instrumentos deliberativos previstos neste artigo;
IV - Ata de Deliberação: registra as deliberações tomadas pelo Conselho Diretor, a partir dos votos de seus Diretores, em Reuniões e Circuitos Deliberativos;
V - Consulta Pública: expressa decisão que submete proposta de ato normativo, documento ou assunto a críticas e sugestões do público em geral;
VI - Portaria: é o ato administrativo que dispõe sobre matéria relativa à gestão administrativa e ao funcionamento das unidades da ANPD;
Parágrafo único. A Resolução, o Enunciado, a Ata de Deliberação e a Consulta Pública de minuta de ato normativo são instrumentos deliberativos de competência exclusiva do Conselho Diretor.

Assim, considerando a complexidade do assunto e a necessidade de um posicionamento da Autoridade, no dia 24 de maio de 2023, a ANPD se manifestou sobre o tratamento de dados pessoais de crianças e adolescentes, através da edição do ENUNCIADO CD/ANPD Nº 1, que diz:

"*O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.*"

Para a edição do referido Enunciado, levou-se em consideração o que consta nos autos do Processo nº 00261.001880/2022-84 (Estudo Preliminar - Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes (4)) e a deliberação tomada no Circuito Deliberativo nº 11/2023 (5).

Destaca-se que a Terceira hipótese apresentada no referido Estudo Preliminar foi a que prevaleceu e era justamente a linha de raciocínio defendida pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD).



(4) *https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf*
(5) *https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/circuito-deliberativo*

A propósito, vale destacar as palavras do Diretor Relator do Enunciado, Arthur Pereira Sabbat, em seu voto durante o Circuito Deliberativo nº 11/2023:

> *4.16. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) também defende essa linha de interpretação, ressaltando que as hipóteses legais aplicáveis ao tratamento de dados de crianças e adolescentes não possuem hierarquia entre elas, sendo aplicáveis tanto as do artigo 7º quanto as do artigo 11º da LGPD, desde que seja observado o melhor interesse da criança e do adolescente. Nesse diapasão, amplia-se, sem riscos ao tratamento de dados dos titulares em lide, o rol de hipóteses legais para esse tratamento, o que permitirá o enquadramento de grande número de atividades e de políticas públicas relacionadas às crianças e aos adolescentes, sem que se verifique a mencionada obstaculização técnica e prática caso fosse adotada a primeira ou a segunda opção de interpretação. 4.17. Assim, a proposta de Enunciado veicula como melhor proposta a terceira hipótese, para dirimir lacuna a interpretativa do art. 14 da LGPD, qual seja, a aplicação das hipóteses legais previstas nos artigos 7º e 11 em leitura conjunta com o art. 14 da LGPD ao tratamento de dados de crianças e adolescentes, pois ao possibilitar o tratamento de dados, com amparo em diferentes hipóteses legais, com a inexistência de hierarquia entre elas, reforça-se a relevância do princípio do melhor interesse e aos demais princípios e regras previstas na LGPD e na legislação pertinente.*

Ao final de seu voto, o Diretor Relator do Enunciado atentou para "(...) a necessidade de a ANPD apresentar diretrizes e orientações aos agentes de tratamento de dados, conforme previsão na Agenda Regulatória 2023-2024, para assegurar uma proteção de dados pessoais de crianças e adolescentes, com efeitos *erga omnes*, considerando que o Enunciado expressa tão somente decisão quanto à interpretação da legislação de proteção de dados pessoais e fixa entendimento sobre matérias de competência da ANPD, com efeito vinculativo à Autoridade, conforme estabelece o art. 51, inciso II, do RIANPD."

Fontes: *ANPD, disponíveis em:*
https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf
https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/circuito-deliberativo
https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-11-2023-ata.pdf
https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-11-2023-votos.pdf
https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-11-2023-votos.pdf

24. Notas Técnicas

24.1 NOTA TÉCNICA Nº 20/2022/CGN/ANPD - Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais, nos termos dos **Arts. 33 e 35** da **LGPD**. É acompanhada do Aviso de Tomada de Subsídio e da Lista de Perguntas da Tomada de Subsídio.

Por Rodrigo Carvalho e Silva Canguçu de Almeida

Considerações Preliminares

O tema objeto desta Nota trata de solucionar lacuna legislativa decorrente dos **Arts 33 e 35** da **LGPD** que, apesar de determinar regras para a operação de transferência internacional de dados pessoais, deixa de esmiuçar e, por conseguinte, esclarecer pontos acerca da operação em questão.

Diante da complexidade do tema, eis que envolve diversos e diferentes níveis de proteção de dados pessoais aplicados por governos estrangeiros, a **ANPD** entendeu por bem publicar documento preliminar do "Regulamento de Transferências Internacionais de Dados Pessoais" com objetivo de obter elementos e informações relevantes por meio de tomada de subsídios propostos mediante contribuição da sociedade especializada no tema. A minuta base do regulamento possui 34 artigos e 1 anexo até o momento, tendo recebido 1.763 contribuições. A coleta de contribuições e subsídios terminou em 14 de outubro de 2023.

Desenvolvimento

O regulamento buscará estabelecer os procedimentos e regras para operações de transferência internacional de dados, contemplando países ou organismos internacional que ofereçam proteção adequada de dados.

De forma bastante objetiva, para a operação de transferência de dados pessoais, deve-se garantir o cumprimento dos princípios previstos na **LGPD**, além de adotar procedimentos compatíveis com normas internacionais e implementar medidas de responsabilidade, transparência para o titular e comprovar as medidas de segurança apropriadas que foram adotadas. Além disso, necessário lembrar que a operação deve estar amparada pelas hipóteses legais válidas pela **LGPD**.

Fica estabelecido, então, que a transferência internacional de dados pessoais ocorre quando um agente (exportador) envia dados para um agente estrangeiro (importador). A resolução também estabelece que a ANPD irá analisar e reconhecer a equivalência do nível de proteção de dados de outros países ou organismos internacionais, assim como cláusulas-padrão contratuais, elaboradas e aprovadas pela ANPD com objetivo de estabelecer garantias mínimas e condições válidas para a realização da transferência. Importante consignar que a validade da transferência necessita da adoção integral e sem alteração dos textos destas cláusulas em documento firmado entre exportador e importador. Além destas cláusulas-padrão, o regulamento estabelece normas corporativas globais, destinadas a transferência internacional dentro do mesmo grupo econômico.

Assim, o "Regulamento de Transferências Internacionais de Dados Pessoais" complementa a **LGPD** e estabelece regras específicas para a transferência internacional de dados pessoais. O regulamento define os mecanismos de transferência permitidos, os requisitos para cada mecanismo e as obrigações dos agentes de tratamento envolvidos na transferência.

O Regulamento é ainda composto pelo ANEXO I, que apresenta as cláusulas-padrão contratuais.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000968_2021_06-nota-tecnica.pdf*

Nota: entretanto, a 23 de agosto de 2024, ANPD publicou sua Resolução CD/ANPD nº 19/2024, que aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais, seguindo estes mesmos parâmetros.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396*

24.2 NOTA TÉCNICA Nº 46/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca da divulgação dos microdados do Enem e de censos escolares pelo INEP à luz da **LGPD**.

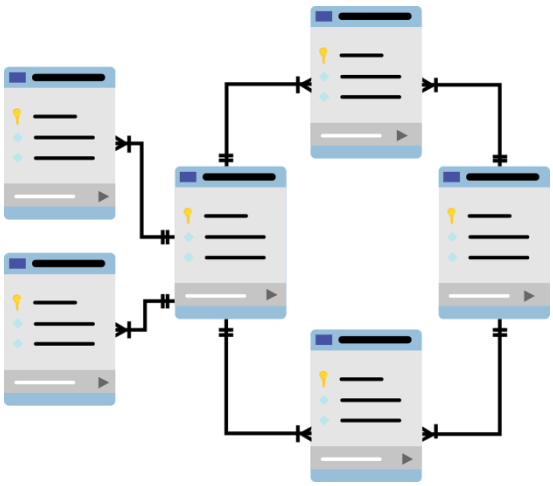
Por Renata Lima de Mattos Rocha

Desenvolvimento

A **ANPD** desenvolveu a Nota Técnica nº 46/2022, que avalia a suspensão da divulgação dos microdados do censo escolar e do Exame Nacional do Ensino Médio (Enem) pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP).

Esta Nota Técnica examina a legitimidade do INEP para o tratamento dos dados coletados para fins de censo escolar e de divulgação do Enem, bem como as hipóteses legais aplicáveis, a transparência e, primordialmente, a adoção de medidas de prevenção e segurança, a fim de evitar a ocorrência de incidentes.

A ANPD identificou que são legítimas as hipóteses legais apontadas pelo INEP para realização do tratamento, porém a prática carece de ajustes a fim de cumprir integralmente a **LGPD**, sugerindo a elaboração de Relatórios de Impacto à Proteção dos Dados (RIPD), para que o INEP tenha maior clareza quanto aos riscos que podem ser causados aos titulares e, com base nessas informações, traçar estratégia de divulgação dos microdados mais segura, transparente e eficaz.



Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf) visto em 09/07/2024*

24.3 NOTA TÉCNICA Nº 49/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca da atualização da Política de Privacidade do *Whatsapp*.

Por Anna Carolina de Medeiros Silva

Desenvolvimento

A Nota Técnica nº 49/2022/CGF, desenvolvida pela **ANPD**, aborda as práticas de tratamento de dados pelo aplicativo de mensagens *WhatsApp*, analisando diversos aspectos, entre eles, a coleta, o armazenamento, compartilhamento de dados e a transparência das práticas adotadas pelo aplicativo.

A nota enfatiza a necessidade de melhorias na comunicação com os titulares de dados e a clareza das políticas de privacidade. A ANPD apontou que o ***WhatsApp*** deve ajustar suas práticas para garantir a conformidade plena com a **LGPD**, principalmente na adequação das bases legais utilizadas e na melhoria das informações fornecidas aos titulares de dados.

Ela também discute o tratamento de dados sensíveis e de crianças e adolescentes, recomendando a implementação de medidas adicionais de segurança e transparência para esses grupos específicos, sendo que a ANPD sugere a criação de relatórios de impacto à proteção de dados (RIPD) para avaliar e mitigar os riscos associados ao tratamento desses dados.

A avaliação da ANPD é crucial para garantir que grandes plataformas, como o *WhatsApp*, adotem práticas mais eficazes e duras de proteção de dados, assegurando a privacidade e a segurança dos dados pessoais dos titulares no Brasil.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf*

24.4 NOTA TÉCNICA Nº 68/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca do tratamento de dados realizado pela Receita Federal por intermédio da Portaria RFB nº 167/2022.

Por Gabriela Marangoni

Desenvolvimento

A **ANPD**, zelando pela proteção de dados pessoais, analisou a Portaria RFB nº 167/2022, de 19 de abril de 2022, que autoriza o Serviço Federal de Processamento de Dados (SERPRO) a disponibilizar acesso, para terceiros, dos dados e informações que especifica e concluiu que o objetivo da Portaria ora analisada é instrumentalizar o acesso já existente a dados pré-determinados, tais como informações acerca de CPF, CNPJ e certidão negativa de débitos.

A Coordenação-Geral de Fiscalização acatou as justificativas da Receita Federal acerca do fato de que a simples adição da tecnologia ao acesso aos dados públicos não traria novos riscos aos direitos e garantias aos titulares, tendo em vista que o órgão já elaborou e mapeou os riscos inerentes ao tratamento. Além disso, a RFB comprovou a necessidade de compartilhamento de tais dados, especialmente no tocante à execução de políticas públicas de identificação como parte do programa de desburocratização do serviço público.

Portanto, considerando que o compartilhamento de dados está amparado por política pública e normativos legais e considerando não haver compartilhamento irrestrito de tais dados, uma vez que os dados disponibilizados são públicos e concedidos apenas aos interessados que já possuem chave de pesquisa prévia, entendeu-se que o tratamento de dados pessoais relativos ao CPF e no que tange à Portaria nº 167/2022 é lícito e adequado aos ditames da **LGPD**.

Com relação ao tratamento de dados relativo ao serviço de cadastro nacional de pessoa jurídica - CNPJ, A ANPD destacou que, embora dados de pessoas jurídicas não sejam abrangidos pela **LGPD**, há divulgação de tais dados (dados dos sócios e integrantes das entidades) por parte da Receita Federal, após a análise da defesa entendeu-se que a divulgação de dados de pessoa jurídica é feita de forma restrita, sendo publicados apenas os dados não protegidos por sigilo fiscal. Desta forma, não se vislumbrou, inicialmente, irregularidades no tratamento de dados pessoais no âmbito do acesso a dados de CNPJ, viabilizado pela Portaria nº 167/2022, da RFB.

Quanto ao tratamento de dados relativo ao serviço certidão negativa de débitos - CND, os dados divulgados não têm correlação com a **LGPD**, uma vez que tratam de dados estritamente empresariais, portanto, não há violação da Lei.

Ao final, concluiu-se que os dados considerados pessoais já eram, em sua maioria, dados públicos por força de normativos e de políticas públicas e de acordo com as informações trazidas pela Receita Federal, aqueles dados que não possuem a natureza de dado público continuam carecendo de autorização prévia de acesso, uma vez que os dados compartilhados foram mapeados pela RFB através dos Relatórios de Impacto apresentados, além de estarem inseridos em políticas públicas e possuírem finalidade definida, conforme determina a **LGPD**, não se vislumbrou incompatibilidade do tratamento pretendido pela Portaria 167/2022 com os ditames da legislação de proteção de dados pessoais.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt-68_2022_cgf_anpd.pdf*

24.5 NOTA TÉCNICA Nº 75/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca do Acordo de Cooperação nº 124.479/2022, firmado entre Serviço federal de Processamento de Dados (Serpro) e a empresa *Drumwave Brasil Tecnologia Ltd*. (*Drumwave*).

Por Renata Próximo da Silva

Desenvolvimento

Tendo conhecimento de acordo de cooperação negociado entre o Serpro e a empresa Drumwave, por meio de publicação em DOU em 10/06/2022, a CGF (Coordenação Geral de Fiscalização) da **ANPD** instaurou procedimento de fiscalização em 15 de julho de 2022, por meio do Despacho CGF/ANPD (SEI nº 3502432), com o intuito de apurar a adequação do referido acordo nos termos da **LGPD**. Na mesma data o Serpro foi oficiado para fornecimento de cópia do acordo de cooperação e outras informações.

A Serpro respondeu ao ofício em 28 de julho seguinte, informando tratar-se de contato autorizado por Regulamento, para realização de testes, experimentos, propósitos, estudos e outras medidas para avaliar a viabilidade técnica e comercial de oportunidade de negócio, de forma a reunir informações para a etapa de planejamento de oportunidade de negócio pelo Serpro. Informando ainda que a premissa desta etapa não é o compartilhamento de dados pessoais.

O documento enviado pela Serpro conta com trechos em sigilo, riscados no próprio documento disponibilizado publicamente.

Enviado também oficio a SDG, que participou da reunião havida com a Serpro e a empresa *Drumwave*, em resposta foi informado pela Encarregada do Ministério da Economia que tem atuado no fomento de transformação digital do governo, elencando a legislação que estabelece uma série de competências para a SGD relacionadas a tecnologia da informação no governo federal, e ainda a instituição da plataforma gov.br, que tem como uma de suas finalidades disponibilizar em uma única plataforma informações de serviços ao cidadão.

Em conclusão a CGF entendeu, que, no momento, não haveria necessidade de qualquer ação por parte da ANPD, uma vez que afirmado pela Serpro e SGD inexistir, na atual etapa, compartilhamento de dados pessoais.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-no-75-2022-cgf-anpd-serpro-e-drumwave.pdf*

24.6 NOTA TÉCNICA Nº 92/2022/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca da transparência e publicização das listas de requerentes e beneficiários dos auxílios Benefício Emergencial Taxistas e Benefício Emergencial Transportadores Autônomos de Carga (TAC).

Por Gabriela Marangoni

Desenvolvimento

A Nota Técnica nº 92/2022/CGF, desenvolvida pela **ANPD**, analisa e responde ao Ofício elaborado e apresentado pela Secretaria-Executiva do Ministério do Trabalho e Previdência (MTP) para dar conhecimento à Requisição em epígrafe em que o Tribunal de Contas da União (TCU) questiona o MTP sobre medidas de transparência e publicização das listas de requerentes e beneficiários dos auxílios Benefício Emergencial Taxistas e Benefício Emergencial Transportadores Autônomos de Carga (TAC).

Após analisar o Ofício citado acima, a ANPD entendeu que não há como estabelecer se o direito de proteção de dados pessoais ou o princípio da publicidade na administração pública prevalecerá e reiterou que a divulgação ou não de dados pessoais por órgãos públicos dependerá da análise dos casos concretos, no qual o órgão deverá ponderar o direito à proteção de dados pessoais de um lado e o direito dos indivíduos de acesso às atividades do Poder Público, de outro.

Em relação especificamente à divulgação de dados pessoais, concluiu que as portarias que regulam o Benefício Emergencial TAC e o Benefício Emergencial Taxista estipulam que sejam divulgados no sítio eletrônico as informações a respeito dos indivíduos que efetivamente receberam pagamento, de modo que a divulgação desses dados está de acordo com a persecução do interesse público, mencionada no **Art. 23** da **LGPD** e neste caso, a ANPD recomendou que os órgãos públicos envolvidos observem as diretrizes dispostas no Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público para compartilhamento de dados pessoais.

Por fim, tendo em vista que a hipótese legal que autoriza o tratamento de dados pessoais pelo MTP para fins de gerenciamento dos benefícios e divulgação de dados pessoais é a execução de políticas públicas, não é necessário que o MTP solicite o consentimento dos titulares, visto que o uso da hipótese legal do consentimento sequer é apropriado na situação analisada. Portanto, o MTP deve divulgar apenas dados pessoais referentes aos titulares que efetivamente recebem o benefício.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/SEI_3689701_Nota_Tecnica_92CGF.pdf*

24.7 NOTA TÉCNICA Nº 3/2023/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca da possibilidade de criação de Memorial no Portal Web da Polícia Rodoviária Federal.

Por Cecília Rezende de Freitas

Desenvolvimento

A Nota Técnica nº 3/2023 da **ANPD** tem como principal objetivo analisar a possibilidade de criar Memorial no Portal Web da Polícia Rodoviária Federal, para homenagear servidores já falecidos mediante a divulgação de nome e sobrenome, bem como foto e tempo de serviço dedicado a PRF, tendo em vista as disposições da **LGPD**.

Baseado no disposto no **Art. 1º** da **LGPD**, referente a aplicação das normas de proteção de dados, no **Artigo 5º**, inciso V, que define o titular de dados como pessoa natural a quem se referem os dados pessoais, objeto do tratamento, a Coordenação Geral de Normatização (CGN) entende que a **LGPD** somente se aplica em relação ao tratamento de dados de pessoas vivas, identificadas ou identificáveis. Ou seja, que os dados relativos a uma pessoa falecida não estão sujeitos ao nível de proteção estabelecido pela Lei.

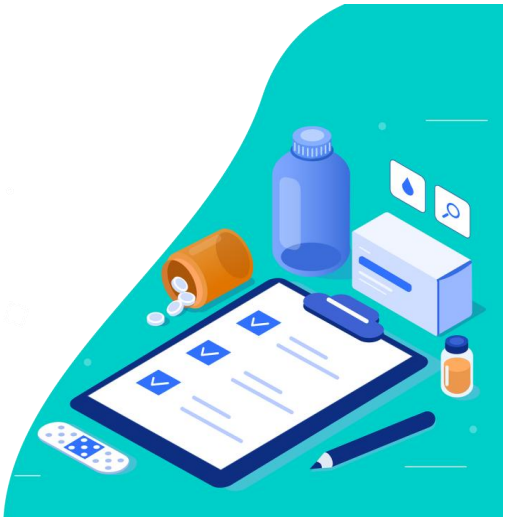
Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-no-4-2023-farmacias_ret-1.pdf*

24.8 NOTA TÉCNICA N° 4/2023/CGTP/ANPD - Manifestação técnica da Coordenação-Geral de Tecnologia e Pesquisa acerca do alinhamento de conformidade com a **LGPD** e sua aplicação no varejo farmacêutico.

Por Cecília Rezende de Freitas

Desenvolvimento

Por sua vez, a Nota Técnica nº 4/2023 da **ANPD** tem como principal objetivo identificar as práticas de tratamento de dados pessoais, incluindo dados sensíveis, no varejo farmacêutico, visando à conformidade com a **LGPD**.



A partir de monitoramentos, estudos, investigações e pesquisa, inclusive sobre acordos prévios firmados entre o Ministério Público e determinadas redes farmacêuticas, a ANPD, por sua Coordenação-Geral de Tecnologia e Pesquisa (CGTP) chegou as seguintes apurações:

Políticas de Privacidade: Foram identificadas falhas na transparência e clareza das informações sobre o tratamento de dados no âmbito de políticas de privacidade das grandes redes farmacêuticas.

Programas de Fidelidade: Foram identificadas inconsistências na utilização de dados em programas de fidelidade, especialmente quanto ao consentimento e a coleta de dados sensíveis.

Baixa Maturidade: Constatou-se uma baixa maturidade no setor farmacêutico em termos de adequação às normas da **LGPD**, evidenciando a necessidade de melhorias significativas.

Com base nas apurações acima, a CGTP promoveu workshops e reuniões com associações representativas do setor (Abrafarma, Abrafad, Febrafar e ABCFarma) para discutir boas práticas e esclarecimentos sobre a **LGPD**, bem como estudo exploratório sobre as práticas correntes e políticas de privacidade das redes farmacêuticas.

Por fim, a ANPD identificou a necessidade de uma abordagem educativa e regulatória para aumentar a maturidade do setor farmacêutico em relação à proteção de dados pessoais, destacando a importância de transparência e conformidade com a **LGPD**, mediante a manutenção de diálogos com associações representativas para incentivar a adoção de boas práticas de proteção de dados, elaboração de materiais educativos em conjunto com a Coordenação-Geral de Normatização para orientar o setor sobre conformidade à **LGPD** e realização de trabalhos em conjunto com a Secretaria Nacional do Consumidor (SENACON) para abordar questões relacionadas ao tratamento de dados pessoais no contexto de programas de fidelidade e consentimento.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-no-4-2023-farmacias_ret-1.pdf*

24.9 NOTA TÉCNICA Nº 6/2023/CGF/ANPD - Manifestação técnica da Coordenação-Geral de Fiscalização acerca dos tratamentos de dados pessoais de crianças e adolescentes, pela rede social *TikTok*, no momento em que eles se cadastram na plataforma.

Por Anna Carolina de Medeiros Silva

Desenvolvimento

A **ANPD** desenvolveu a Nota Técnica nº 6/2023, que avalia o tratamento de dados pessoais pelo *TikTok*, especialmente os dados de crianças e adolescentes que se cadastram na plataforma.

Esta Nota Técnica examina práticas de coleta, armazenamento e compartilhamento de dados, destacando a necessidade de maior clareza nas políticas de privacidade e reforço nas medidas de segurança.

A ANPD identificou que as práticas do *TikTok* precisam ser ajustadas para cumprir integralmente a **LGPD**, sugerindo a revisão dos mecanismos de verificação de idade, políticas de privacidade mais detalhadas e a apresentação de relatórios de impacto à proteção de dados para melhorar a transparência e segurança no tratamento dos dados pessoais de usuários jovens.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf*

24.10 NOTA TÉCNICA Nº 12/2023/CGF/ANPD - Avaliação dos Relatórios de Impacto à Proteção de Dados elaborados pelo INEP para fins adequação da divulgação dos microdados do censo escolar e do Enem à **LGPD**.

Por Valéria Reani Rodrigues Garcia

Desenvolvimento

A Nota Técnica nº 12/2023/CGF/ANPD da **ANPD** diz respeito a avaliação dos Relatórios de Impacto à Proteção de Dados- RIPD, elaborados pelo INEP para fins adequação da divulgação dos microdados do censo escolar e do Enem à **LGPD**.

Nesta nota Técnica figura como interessado o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP).

O Assunto discutido nesta Nota Técnica trata da Avaliação dos Relatórios de Impacto à Proteção de Dados elaborados pelo INEP para fins adequação da divulgação dos microdados do censo escolar e do Enem à **LGPD**.

As referências legais adotadas pela Autoridade:

1. Processo SEI nº 00261.000730/2022-53;
2. Nota de Esclarecimento INEP (SEI no 3289150);
3. Nota Técnica INEP 5/2021/CGCQTI/DEED (SEI no 3289210);
4. Nota Técnica INEP 14/2021/CGIM/DAEB (SEI no 3289220);
5. Termo de Execução Descentralizada UFMG (SEI no 3289230);
6. Parecer 00018/2022/PROC/PFINEP/PGF/AGU (SEI no 3289237);
7. Manifestação pública de entidades (SEI no 3289249);
8. Nota Técnica no 46/2022/CGF/ANPD (SEI no 3319546);
9. Nota Técnica no 136/2022/CGAT/DTC/STPC (SEI no 3414875), da Controladoria Geral da União (CGU);
10. Relatório de Impacto à Proteção de Dados Pessoais dos Microdados do Exame Nacional do Ensino Médio (ENEM) (SEI 3848205);
11. Relatório de Impacto à Proteção de Dados Pessoais dos Microdados dos Censos da Educação (SEI 3848206).

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-12-2023-cgf-anpd-inep.pdf/*

24.11 NOTA TÉCNICA Nº 16/2023/CGTP/ANPD - Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023.

Por Renata Proximo da Silva

Desenvolvimento

A **ANPD** desenvolveu a Nota Técnica 16/2023/CGTP/ANPD com o objetivo principal abordar e propor alterações ao Projeto de Lei nº 2338/2023, com base nas premissas estabelecidas no estudo técnico previamente conduzido e publicado em 6 de julho de 2023.

A PL 2338/2023 discute a regulação da Inteligência Artificial no Brasil, e foi apresentada pelo Senador Rodrigo Pacheco. A proposta reflete o amadurecimento, os avanços e os aprendizados acumulados desde a apresentação do PL nº 21/2020 e busca estabelecer um equilíbrio entre a promoção da inovação e a garantia dos direitos fundamentais dos cidadãos.

A Nota Técnica inicia sua análise preliminar fazendo um paralelo entre a PL nº 2338/2023 e a **LGPD**, visto que ambas as legislações, embora tenham focos distintos, convergem em diversos pontos, especialmente quando se trata da tutela de direitos dos cidadãos e da governança de tecnologias emergentes.

Os principais pontos analisados, quando feito o comparativo de proteção aos cidadãos, são:

-Tutela de direitos;

- Classificação de sistemas de IA de alto risco;

-Mecanismo de governança;

-Comunicação de incidentes;

-Coordenação com outros órgãos e autoridades;

- Processo de regulamentação.

Em conclusão, a Autoridade competente teria as funções de supervisão e fiscalização da implementação da lei relacionada à inteligência artificial. Lhe cabendo várias responsabilidades, incluindo a proteção dos direitos fundamentais afetados pela IA, a promoção e elaboração de estudos sobre boas práticas em IA, e a cooperação com outras autoridades relevantes. Em termos organizacionais e de competências funcionais, há várias semelhanças com o atual conjunto de atribuições da ANPD, como no recebimento de comunicados de incidentes e avaliação da suficiência de medidas técnicas e administrativas aptas a mitigar riscos relevantes a liberdades civis e direitos fundamentais, na condução de consultas públicas que precedam a elaboração de regulamentos e normas, na coordenação e diálogo com órgãos e entidades públicas responsáveis pela regulação de setores específicos da atividade econômica e governamental, e, finalmente, na promoção e elaboração de estudos sobre boas práticas.

A presente Nota Técnica **ainda** faz um **estudo comparado** com experiências e propostas de outros países, utilizando-se assim de modelos já existentes, o que auxilia no entendimento de efetividade da PL nº 2338/2023.

O estudo comparado levou em consideração as seguintes experiências:

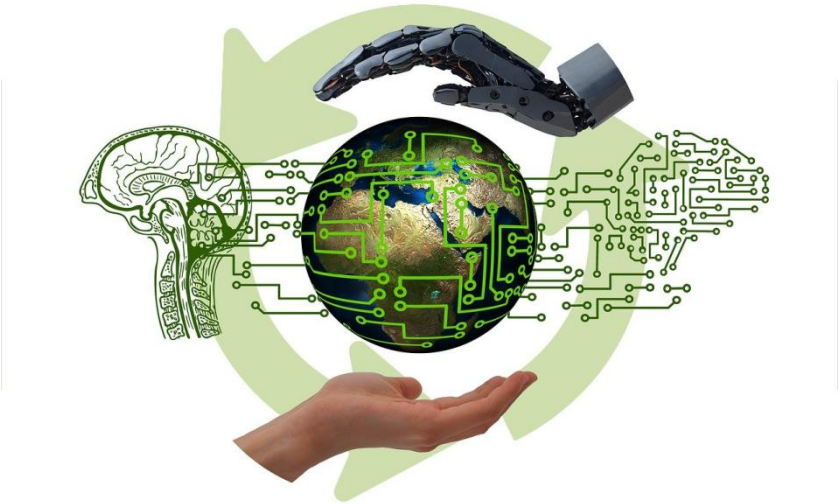
- O Regulamento da Inteligência Artificial da União Europeia;

- Os posicionamentos da Autoridade de Proteção de Dados da França – CNIL;

- A atuação da Autoridade de Proteção de Dados da Holanda (*Autoritei Persoonsgegevens*);

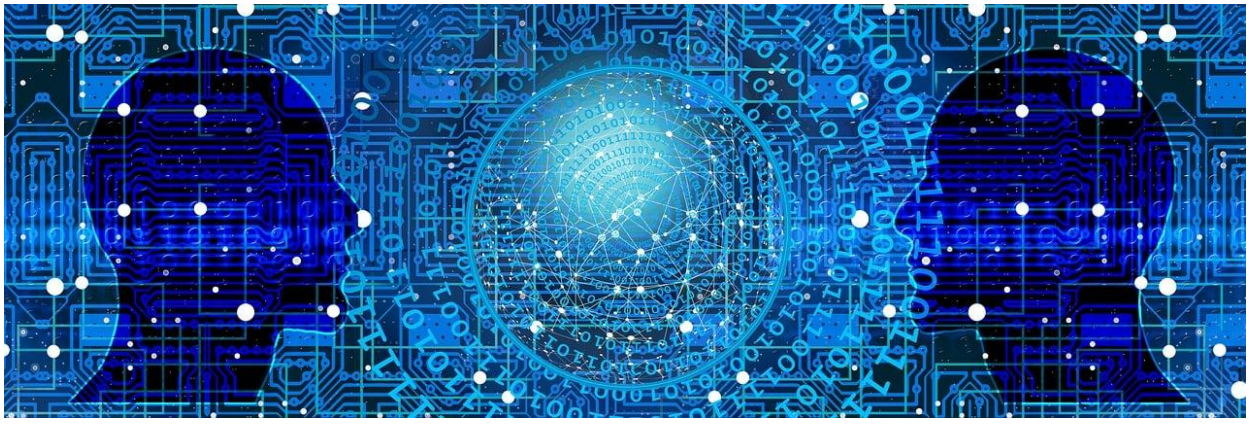
- A criação de uma agência especializada - AESIA (Espanha);

- A Proposta AIDA (Canadá).



Esse estudo comparado trouxe algumas conclusões importantes, aqui vamos transcrever alguns trechos:

> "As experiências internacionais mostram que uma abordagem centralizada, ancorada em uma única autoridade, traz benefícios inegáveis. Primeiramente, uma autoridade centralizada tem a capacidade de responder de maneira ágil e coordenada a desafios emergentes. Em um campo tão dinâmico quanto a IA, a rapidez na tomada de decisões pode ser crucial para prevenir ou mitigar riscos."
>
> "No cenário brasileiro, a ANPD já se destaca como uma entidade de referência na proteção de dados pessoais e na garantia da privacidade dos cidadãos. A IA, com suas capacidades de processamento e análise de grandes volumes de dados, se alinha diretamente às competências da ANPD. Esta interseção entre IA e proteção de dados centraliza a governança da IA sob a égide de questões técnicas e operacionais, com ênfase contínua na proteção de direitos fundamentais e na proteção de dados pessoais. Permite, ainda, formar um corpo técnico especializado em ambas as áreas, otimizando a aplicação de recursos públicos e evitando a fragmentação regulatória e a sobreposição de competências entre órgãos reguladores distintos.
>
> Dessa forma, ao considerar a trajetória e a experiência da ANPD, juntamente com os benefícios inerentes a uma abordagem centralizada, fica claro que o modelo de centralização da governança da IA em torno da ANPD é uma estratégia promissora."



Em seguida, a Nota Técnica entrega uma **proposta de modelo institucional** estruturado, com quatro instancias, que atuariam de forma articulada e coordenada, ficando assim a proposta:

(i) Autoridade competente (órgão regulador central)
Proposta de instituição da ANPD como autoridade competente, exercendo a função de órgão regulador central de interpretação da lei decorrente do PL nº 2.338/2023.
Restando destacado que, o PL nº 2338/2023 contenha expressa previsão de fortalecimento institucional da ANPD, com vistas a viabilizar a assunção de suas novas funções, com a inclusão no PL de expressa previsão de que o regime de autarquia especial a que se submete a ANPD é o mesmo previsto para as agências reguladoras e o CADE, nos termos do Art. 3º da Lei nº 13.848/2019.

(ii) Poder Executivo (elaboração de políticas públicas para o desenvolvimento de sistemas de IA)
Proposto que seja representado pelo Ministério da Ciência, Tecnologia e Inovação, Ministério da Gestão e da Inovação em Serviços Públicos e o Ministério da Justiça e Segurança Pública.
Sendo ainda sugerido que o PL atribua expressamente ao Poder Executivo – e não à autoridade competente, como previsto na atual redação do Art. 32, parágrafo único, II, do PL – a competência para elaborar, gerir, atualizar e implementar a EBIA.

(iii) Órgãos reguladores setoriais (atuação de forma coordenada com o órgão regulador central
Aqui restou proposto que os Órgãos Reguladores Setoriais, tais como Agência Nacional de Telecomunicações - Anatel, Agência Nacional de Saúde - ANS, Agência Nacional de Aviação Civil – Anac, Agência Nacional do Cinema – Ancine, e Agência Nacional do Petróleo, Gás Natural e Biocombustíveis – ANP, mantenham suas competências regulatórias específicas. Dessa forma, alia-se a expertise setorial, própria de cada órgão regulador, com a visão mais ampla e geral sobre os sistemas de IA, que decorre da atuação da ANPD, enquanto órgão central.

(iv) Conselho consultivo (órgão de natureza consultiva, que assegure a participação da sociedade nos processos decisórios das demais instâncias).

E por fim, trouxe a sugestão de criação de um Conselho Consultivo, que deve funcionar nos moldes do Conselho Nacional de Proteção de Dados (CNPD).

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf*

24.12 NOTA TÉCNICA Nº 19/2023/CGF/ANPD - Atividade de Monitoramento.

Por Renata Próximo da Silva

Desenvolvimento

De acordo com o item 3.3.3 do Plano Anual de Fiscalização (PAF) - 2022/2 a 2023/2 da **ANPD**, os setores Financeiro e de Telecomunicações foram os que receberam maior número de requerimentos, sejam petições do titular ou denúncias. Assim, julgou-se conveniente analisar os requerimentos relacionados a estes 2 (dois) setores com maior minúcia, para que, caso se julgue oportuno, incluir esses setores no Mapa de Temas Prioritários 2022/2023.

A partir da reanálise desses processos, a planilha de monitoramento dos requerimentos foi complementada com descrições precisas e detalhadas dos fatos narrados pelos interessados, sejam os titulares de dados, sejam os denunciantes. Além disso, foi adicionada uma nova coluna na planilha para indicação de padrões que mais repetiram naqueles processos.

Elaborada a planilha a Nota Técnica nº 19/2023 CGF/ANPD e com base nas fontes SUPER descreve em sua conclusão as seguintes observações:

1. Medidas educativa (o que o interessado deve saber);

2. Adequação geral à **LGPD**: Os titulares requerem que a ANPD investigue controladores que não cumprem obrigações previstas na Lei, entre elas: (i) a indicação do encarregado; (ii) a divulgação de detalhes sobre o tratamento de dados pessoais; e (iii) a adoção de medidas mínimas para segurança da informação;

3. Adequação às dificuldades de concretização de direitos dos titulares, contida no **Art. 18** da **LGPD**;

4. Adequação no compartilhamento de dados pessoais.

Foi sugerido o encaminhamento da Nota Técnica para ANATEL, à SENACON e ao Banco Central do Brasil para ciência e possível atuação conjunta para a construção de soluções que minimizem o volume de comunicações indesejadas no setor de telecomunicações e financeiro, respectivamente. Também a ao Grupo de Trabalho dedicado ao estudo e à elaboração de um plano institucional de ações educativas sobre proteção de dados pessoais e da privacidade, no âmbito da ANPD, instituído pela Portaria ANPD nº 56, de 19 de abril de 2023, no processo SUPER nº 00261.000997/2023-21.

As referências legais adotadas pela **ANPD**:

- Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

- Regimento Interno da Autoridade Nacional de Proteção de Dados (RI-ANPD), aprovado pela Portaria nº 01, de 08 de março de 2021;

- Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD (Regulamento de Fiscalização), aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021;

- Plano Anual de Fiscalização (PAF) – 2022/2 a 2023/2 (SUPER nº 3625101);

- Processo SUPER nº 00261.000403/2023-82;

- Despacho SUPER nº 3982113.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/versao_publica_sei_4161316_nota_tecnica_19.pdf*

24.13 NOTA TÉCNICA Nº 175/2023/CGF/ANPD - Contribuições da Coordenação-Geral de Fiscalização à minuta de Acordo de Cooperação entre o MJSP e a CBF para compartilhamento de dados pessoais visando ao aprimoramento do Projeto Estádio Seguro.

Por Renata Lima de Mattos Rocha

Desenvolvimento

A **ANPD** desenvolveu a Nota Técnica nº 175/2023, visando avaliar o tratamento e compartilhamento dos dados pessoais entre o MJSP e a CBF, o ente privado que realizará a venda da bilheteria e demais agentes envolvidos.

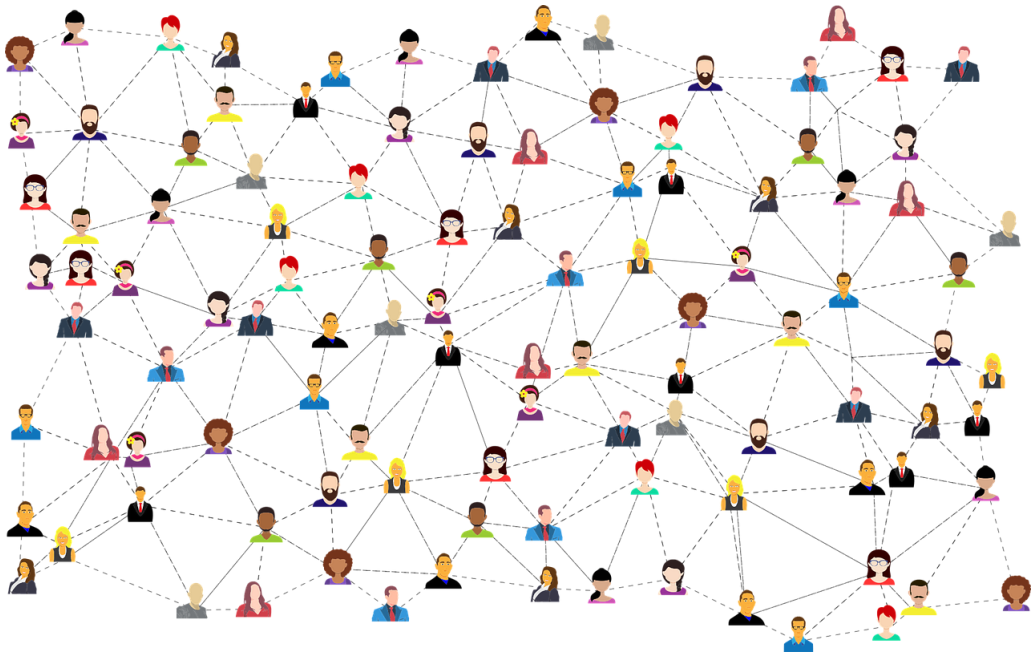
Esta Nota Técnica examina práticas de coleta, armazenamento e compartilhamento de dados, a disponibilidade de mecanismos e procedimentos estabelecidos e padronizados para assegurar o exercício dos direitos dos titulares e a indicação dos encarregados pelos entes envolvidos.

O MJSP apresentou o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) informando que os dados coletados têm por finalidade o interesse público, vez que serão coletados para (**i**) recapturar indivíduos com mandado de prisão ou medidas penais restritivas; (**ii**) auxiliar na recuperação de veículos roubados ou furtados; e (**iii**) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo.

A ANPD identificou que, no Relatório de Impacto apresentado, não restou claro a finalidade, adequação e necessidade do item iii) evitar a venda de ingressos utilizando dados de pessoas falecidas, combatendo o cambismo, requerendo, portanto, que o ente adeque o Relatório conforme considerações apontadas, reforçando, assim, a relevância da identificação e descrição dos dados coletados e relação com as hipóteses legais elencadas de forma clara, objetiva e coesa, em estrita observância aos princípios norteados da **LGPD**.

A Nota Técnica sugere ainda uma alteração no texto original para que o direito ao livre acesso do titular e a transparência sejam assegurados, ressaltando que, embora a hipótese legal aplicada seja o interesse público, dispensando, assim, a necessidade de consentimento do titular, é condição *sine qua non* que este tenha ciência de que seus dados pessoais estão sendo tratados, por quem, para quais finalidades e por quanto tempo.

Outro ponto abordado pela Nota Técnica, de exímia relevância, é que o RIPD foi apresentado apenas pelo MJSP, não restando claro, por exemplo, qual o nível de adequação da Entidade de Prática Desportiva considerando que este órgão também receberá os dados para tratamento, trazendo a luz a necessidade não apenas do ente que coletar o dado estar em conformidade com a legislação vigente, mas também buscar que o terceiro que receberá o dado também esteja, garantindo assim a segurança das informações compartilhadas.



Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdff*

24.14 NOTA TÉCNICA N° 2/2024/ FIS/CGF/ANPD - Oferta ativa de serviços de crédito a partir do tratamento de dados pessoais dos beneficiários do Instituto Nacional do Seguro Social (INSS) feita por Instituições Financeiras (IF's) e Correspondentes Bancários (Corbans).

Por Valéria Reani Rodrigues Garcia

Desenvolvimento

Nesta Nota Técnica da **ANPD** figuram os seguintes interessados

1. Banco Itaú - ITAU UNIBANCO S.A.
2. Banco Pan - PAN S.A.
3. Banco Santander - SANTANDER (BRASIL) S.A.
4. Banco Bradesco - BRADESCO S.A

O assunto discutido nessa nota trata da Oferta atividade de serviços de crédito a partir do tratamento de dados pessoais dos beneficiários do Instituto Nacional do Seguro Social (INSS) feita por Instituições Financeiras (IFs) e Correspondentes Bancários (Corbans).

As referências legais adotadas pela Autoridade Nacional de Proteção de dados

- Lei de Geral de Proteção de Dados Pessoais;

- Portaria no 1, de 8 de março de 2021 - Regimento Interno da Autoridade Nacional de Proteção de Dados (RI);

- Resolução no 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados (Regulamento de Fiscalização).

Fonte: *ANPD, disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_0049668_nota_tecnica_2_versao_publica__1_.pdf*

24.15 NOTA TÉCNICA N° 22/2024/ FIS/CGF/ANPD - Orientações aos servidores da Coordenação-Geral de Fiscalização (CGF) sobre a análise de publicidade dos documentos que instruem os processos de sua competência em atenção à Lei de Acesso à Informação.

Por Valéria Reani Rodrigues Garcia

Publicidade e Restrição de Acesso

A Lei no 12.527/2012, Lei de Acesso à Informação (LAI), pode ser compreendida como um instrumento para a construção da cidadania, uma vez que possibilita aos cidadãos a possibilidade de ter acesso a documentos e informações produzidos e custodiados por autoridades públicas, sem os quais não seria possível a participação informada nos assuntos de interesse geral.

A LAI, desse modo, garante a qualquer interessado o direito de acesso a informações contidas em registros ou documentos, produzidos ou acumulados por órgãos ou entidades públicas, recolhidos ou não a arquivos públicos, bem como a informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado.

A Lei no 12.527/2011, destarte, dispõe que é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão (art. 5º), sem a necessidade que o requerente informe aos órgãos públicos as razões subjacentes à sua solicitação (Art. 10, §3º). Nesse sentido, integram o objeto de aplicação da LAI, nos termos do seu artigo 7º, as informações sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços. O que inclui a informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; a informação relativa à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos; e ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores. Observa-se, portanto, que os processos fiscalizatórios e sancionadores instruídos por agências reguladoras ou autarquias federais encontram-se dentro do escopo de aplicação da LAI.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_0125695_nota_tecnica_22.pdf_1_.pdf*

25. Relatórios de Instrução

25.1 RELATÓRIO DE INSTRUÇÃO N° 1/2023/CGF/ANPD - Telekall Inforservice.

Por Anna Carolina de Medeiros Silva

Desenvolvimento

A **ANPD** publicou o Relatório de Instrução nº 1/2023/CGF, que investigou as práticas de tratamento de dados pela empresa *Telekall Inforservice*. Este relatório examina as conformidades e não conformidades da empresa em relação à **LGPD**.

A análise revelou diversas infrações, como a falta de comprovação de hipóteses legais para o tratamento de dados pessoais, ausência de registro das operações de tratamento e a não indicação de um encarregado pelo tratamento de dados. A investigação foi iniciada após denúncia do Ministério Público de São Paulo, que apontou a oferta de listagens de contatos de ***WhatsApp*** para campanhas eleitorais sem a devida base legal.

Com base nas infrações identificadas, a ANPD recomendou a aplicação de sanções à *Telekall Inforservice*, incluindo advertências e possíveis multas, visando garantir a conformidade com a LGPD e proteger os dados pessoais dos titulares.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf*

25.2 RELATÓRIO DE INSTRUÇÃO Nº 2/2023/CGF/ANPD - Instituto de Assistência ao Servidor Público Estadual de São Paulo - IAMSPE.

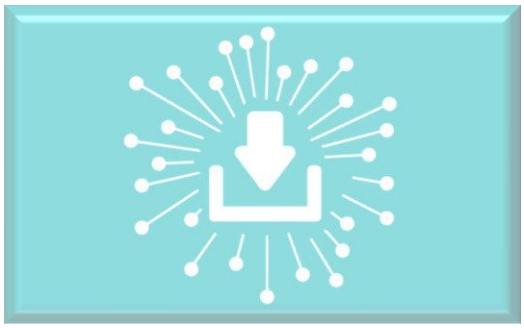
Por Renata Lima de Mattos Rocha

Desenvolvimento

A **ANPD** publicou o Relatório de Instrução nº 2/2023/CGF, que investigou as práticas de tratamento de dados pelo Instituto de Assistência ao Servidor Público Estadual de São Paulo - IAMSPE. Este relatório examina a comunicação de incidente de segurança ocorrida no IAMSPE, alegado um possível comprometimento a privacidade dos dados da organização por conta de um acesso não autorizado em dados cadastrais indicados por um usuário externo no início do ano de 2022.

A análise revelou diversas infrações, tais como a falta de comunicação ao titular dos dados em prazo razoável, conforme estipulado no **Art. 48** da **LGPD**, e bem assim a ausência de qualquer justificativa para não ter cumprido referida determinação legal. Ainda, aponta o relatório a falha na implementação de controles para garantir a confidencialidade dos dados e o acesso restrito apenas a quem fosse autorizado, o que se agrava considerando os dados sensíveis de crianças, adolescentes e idosos a que tem acesso e os possíveis danos causados em decorrência deste vazamento, infringindo o **Art. 49** da **LGPD**. Ressalta que a investigação foi iniciada após denúncia reportar a vulnerabilidade no sistema de informação mantido pelo IASMPE que permitiriam, sem o uso de credenciais válidas, o acesso a informações constantes em sua base de dados.

Com base nas infrações identificadas, a ANPD recomendou a aplicação de sanções ao administrativas ao IAMSPE, incluindo advertências e a adoção de medidas corretivas, visando garantir a conformidade com a **LGPD** e proteção dos dados pessoais dos titulares.



Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf*

25.3 RELATÓRIO DE INSTRUÇÃO N° 3/2023/CGF/ANPD - Instituto de Pesquisas Jardim Botânico do Rio de Janeiro - JBRJ

Por Gabriela Marangoni

Desenvolvimento

A **ANPD** publicou o Relatório de Instrução nº 3/2023/CGF, que apurou o suposto incidente de segurança da informação que teria afetado órgãos públicos, inclusive o Instituto de Pesquisas Jardim Botânico do Rio de Janeiro, em dezembro de 2021.

Em sua defesa, o *Jardim Botânico do Rio de Janeiro* destacou que não houve qualquer violação a **LGPD**, eis que o suposto incidente de segurança não ocorreu em sistemas que carregam em seu conteúdo dados pessoais e sim em sistemas de gestão de acervos científicos que possuem informações abertas e públicas nos moldes do plano de dados abertos ao qual o Jardim Botânico do Rio de Janeiro é signatário.

Além disso, o *Jardim Botânico do Rio de Janeiro* alegou a ausência de aviso de recebimento de notificação da ANPD e considerando que a Coordenação-Geral de Fiscalização não logrou êxito em localizá-lo junto aos Correios, não houve materialidade suficiente para caracterizar o não atendimento à requisição da ANPD, dado que a requisição nunca se completou porque ausente elemento importante que é a ciência daquele a quem ela se dirige, por conseguinte, entendeu-se que não ficou configurada a infração ao Art. 5º do Regulamento da Fiscalização conforme apontado no Auto de Infração.

Com base nas infrações identificadas, a ANPD recomendou o arquivamento deste Processo Administrativo Sancionador pela não configuração da violação do **Art. 48** da **LGPD**, eis que o *Jardim Botânico do Rio de Janeiro* comprovou nos autos que o incidente em questão não versava sobre dados pessoais, bem como pela não configuração da violação do art. 5º, corroborado pela ausência de aviso de recebimento nos autos e pela resposta negativa dos Correios.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4504630_relatorio_3.pdf*

25.4 RELATÓRIO DE INSTRUÇÃO Nº 4/2023/FIS/CGF/ANPD - Secretaria de Estado da Saúde de Santa Catarina.

Por Orestes Bacchetti Junior

Desenvolvimento

Fica instituída na Resolução a aprovação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

Fonte: *ANPD, disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077 acesso em 04/07/2024*

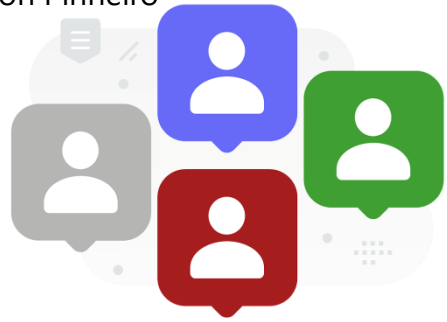
25.5 RELATÓRIO DE INSTRUÇÃO Nº 1/2024/CGF/ANPD - Instituto Nacional do Seguro Social - INSS

Por Valéria Reani Rodrigues Garcia

Desenvolvimento

O respectivo Relatório de Instrução trata do Processo no 00261.001888/2023-21 onde figuram as partes:

- Nome/Razão Social do Autuado: Instituto Nacional do Seguro Social (INSS)
- CNPJ do Autuado: 29.979.036/0001-40
- Porte do Autuado: - *Grande porte*
- Agente de Tratamento: (X) Controlador ( ) Operador
- Nome do Encarregado ou Responsável Jurídico: Edson Pinheiro
- Alvarista
- Contado do Encarregado



3. SUMÁRIO EXECUTIVO DO PROCESSO

3.1. Auto de Infração: 03/08/2023– Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146)

Dispositivo(s) Infringido(s)	Descrição da Infração
Art. 48 da Lei nº 13.709/2018.	Não comunicar aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
Art. 32, §2º da Resolução CD/ANPD nº 1/2021	Não atendimento às determinações da ANPD.

Foram adotadas Medida(s) Preventiva(s) Aplicada(s) com base no Art. 32 do Regulamento de Fiscalização.

Ante o exposto, considerando que o conjunto probatório demonstra que a autoria e a materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração no 1/2023/CGF/ANPD (4411917), conclui-se pela seguinte recomendação:

Por violação ao **Art. 48** da **LGPD**, com circunstância agravante nos termos do Art. 32, §2º, II, da Resolução CD/ANPD no 1/2021, a aplicação da sanção de PUBLICIZAÇÃO DA INFRAÇÃO ao INSS. A entidade pública autuada, assim, deverá, em até 10 dias úteis, contados a data da intimação:
a) Publicar comunicado, na primeira página do site <https://www.gov.br/inss/pt-br> que deverá permanecer acessível pelo prazo de 60 dias, contados a partir da in mação da decisão que determinar a sanção administrativa, com o seguinte teor:

O INSS, tendo em vista que foi condenado pela ANPD, por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema.

Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

- Informamos que o Instituto realizou, imediatamente, ações preventvas e corretvas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada

- A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: encarregado@inss.gov.br."

- Enviar mensagem, via recurso de notificação, a todos os usuários do aplicativo "Meu INSS", para que fique disponível no menu de 'notificações' do aplicativo "Meu INSS", com indicação visual de que há mensagem pendente de leitura/visualização, com o seguinte teor:

- "O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica a ocorrência de incidente de segurança entre agosto e setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS, saiba mais no link:" [apontar para o link criado para atender a determinação.

- Definição das sanções (inclusos agravantes e atenuantes) e a adoção de medidas corretivas restringem-se às circunstâncias deste caso em concreto. Tais decisões não vinculam, naturalmente, a análise e o posicionamento da CGF em futuros processos sancionadores.

Caso a entidade pública autuada não cumpra a referida decisão nos termos definidos pela Autoridade Nacional de Proteção de Dados, recomenda-se que o presente processo administrativo sancionador seja encaminhado para os órgãos de controle interno competentes, nos termos do **Art. 55-J,** XXII, da **LGPD**, para que sejam tomadas as medidas administrativas necessárias em relação aos agentes públicos que deram causa ao descumprimento do disposto na legislação de proteção.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-de-instrucao-1_2024.pdf*

25.6 RELATÓRIO DE INSTRUÇÃO Nº 2/2024/FIS/CGF/ANPD - Secretaria de Estado de Educação do Distrito Federal (SEEDF).

Por Cecília Rezende de Freitas

Desenvolvimento

O relatório informa sobre a instauração do processo administrativo sancionador da **ANPD** visando apurar infrações à legislação de proteção de dados por parte da Secretaria de Estado de Educação do Distrito Federal (SEEDF), a qual expôs indevidamente dados pessoais de estudantes devido a uma falha de segurança no formulário de inscrição do Programa Educação Precoce. A Coordenação-Geral de Fiscalização (CGF) determinou medidas corretivas, incluindo a comunicação do incidente à ANPD e aos titulares dos dados.

Após conclusão das análises sobre documentos apresentados nos autos do Processo Administrativo nº 00261.001192/2022-14, a CGF constatou a ocorrência de incidente de segurança envolvendo a exposição de dados, bem como a violação de dispositivos legais da **LGPD** e do Regulamento de Fiscalização, recomendando a aplicação da sanção de advertência, sem imposição de medida corretiva, em relação a cada um dos itens violados. As condutas sujeitas a sanção corresponderam a ausência de registro de operações de tratamento de dados pessoais (ROT), conforme estabelecido no **Art. 37** da **LGPD**; não elaborar relatório de impacto (RIPD) após solicitação da ANPD, conforme ao **Art. 38** da **LGPD**; não comunicar aos titulares a ocorrência de incidente de segurança, na forma estabelecida no **Art. 48** da **LGPD**; e, não apresentar informações relevantes para a avaliação das atividades de tratamento de dados pessoais no prazo estabelecido pela ANPD, nos termos do Art. 5º do Regulamento de Fiscalização.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-instrucao-2-2024_sec-educacao-gdf.pdf*

25.7 RELATÓRIO DE INSTRUÇÃO Nº 3/2024/FIS/CGF/ANPD - Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS), sucessora da Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas do Estado de Pernambuco (SDSCJPVD), que sucedeu a Secretaria de Desenvolvimento Social, Criança e Juventude de Pernambuco (SDSCJ)

Por Marcela Fuga Antunes Cardoso

Desenvolvimento

A **ANPD** publicou o Relatório de Instrução nº 3/2024/FIS/CGF/ANPD(8), que investigou uma provável falha operacional do sistema ou falha de algum usuário da Secretaria de Desenvolvimento Social, Criança e Juventude (SDSCJ), atual Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS), sucessora da Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas (SDSCJPVD), a qual teria propiciado a exposição indevida de dados cadastrais e dados de saúde de 413 cadastrados no "Programa PE Livre Acesso Intermunicipal", iniciativa que concede gratuidade a pessoas com deficiência em transportes intermunicipais.

Segundo constou, os dados sensíveis (dados de saúde, como tipo de deficiência e diagnóstico médico), bem como os dados de crianças a adolescentes teriam sido expostos em uma planilha de dados no site da Secretaria e seria possível "navegar pela planilha sem digitar senha", além de ser possível a visualização da cópia de documentos. Diante disso, o relatório examina o ocorrido de acordo a **LGPD** para entendimento das possíveis infrações, penalidades e medidas aplicáveis.

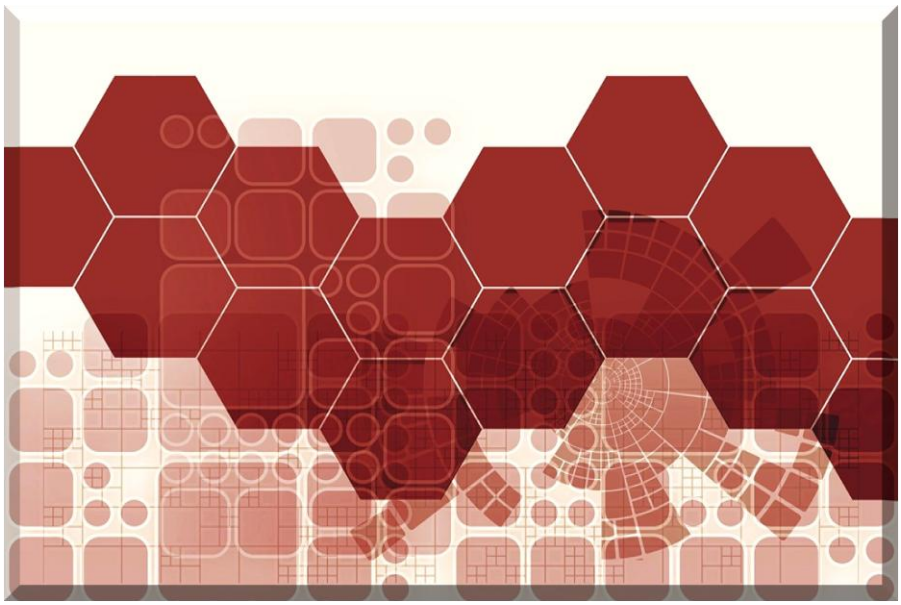
A análise revelou diversas infrações, como a ausência de comunicação individualizada dos titulares sobre o incidente, não adoção de sistemas estruturados em conformidade aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais da **LGPD**.

Com base nas infrações identificadas, a ANPD aplicou duas sanções de advertência cumulada com três medidas corretivas(9):

a) "envio de comunicação direta e individualizada a cada um dos 413 titulares afetados pela exposição dos dados no sítio eletrônico da SAS;

b) comprovação da implementação, na estrutura dos sistemas, de medidas técnicas (e administrativas, se aplicável) que já tenham sido realizadas, incluindo aquelas referentes i) à existência de mecanismos de monitoramento de tráfego à base de dados, ii) à guarda de registros de acesso à referida base de dados, e iii) ao acesso restrito ao link que contém a base de dados em discussão, a fim de atestar que sua consulta somente pode ser realizada mediante uso de senha, com nova etapa de identificação, bem como com limitação de acesso para pessoa em nível gerencial (consoante relatado pela própria autuada na CIS [0042386]); bem outras medidas que a SAS entenda ser cabível.

c) Subsidiariamente, impõe-se a seguinte medida corretiva: apresentação de um cronograma para a implementação das medidas (...), com a especificação das etapas a serem adotadas."



(8) https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf
(9) https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf pg. 13/14

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf*

26. Relatórios de Análise

26.1 RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO EMITIDO NO PROCESSO DE PROPOSIÇÃO DO REGULAMENTO DE FISCALIZAÇÃO DA ANPD.

Construção do modelo de atuação fiscalizatória da ANPD para zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais, de 25/05/2021.

Por Cecília Rezende de Freitas

Desenvolvimento

Trata-se de análise de impacto desenvolvido por equipe técnica da **ANPD** em relação a regulamentação do processo administrativo sancionatório no seu âmbito, para aplicação do **Art. 52** e seguintes **LGPD**.

Considerando as premissas do estudo, a equipe concluiu que o modelo de atuação que melhor atende aos interesses e necessidades da ANPD consiste no modelo de fiscalização ou regulação responsiva, o qual parte do pressuposto que é possível induzir comportamentos sem necessariamente fazer uso de punições, a partir de estímulos não sancionatórios.

Sob este aspecto, a atuação fiscalizatória da ANPD deve incluir atividades de monitoramento, orientação, prevenção e repressão.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2021.05.25__AIR_Fiscalizacao_Final1.pdf*

26.2 RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO EMITIDO NO PROCESSO DE PROPOSIÇÃO DO REGULAMENTO DE MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE, *STARTUPS* E PESSOAS FÍSICAS QUE TRATAM DADOS PESSOAIS - Construção do modelo regulatório para aplicação da **LGPD** a microempresas e empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais, de 17 de agosto de 2021.

Por Cecília Rezende de Freitas

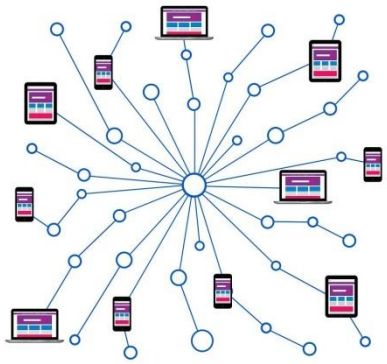
Desenvolvimento

Trata-se de análise de impacto desenvolvido por equipe técnica da **ANPD** em relação à aplicação da **LGPD** em relação a pequenas e microempresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos, conforme prevê seu **Art. 55-J**, inciso XVIII.

Considerando as premissas do estudo, a equipe dividiu a análise em três temas, sendo que em relação à definição de microempresa, empresa de pequeno porte e startup, a equipe entendeu que a flexibilização deve se dar com base no risco que esse tratamento pode causar aos titulares de dados pessoais, independentemente do faturamento.

Em relação a conformidade das obrigações impostas pela **LGPD** às microempresas, empresas de pequeno porte e startups e pessoas físicas que tratam dados pessoais, a equipe técnica considerou o modelo regulatório com simplificação e flexibilização das obrigações em uma resolução única como melhor opção.

Por fim, em relação à segurança da informação para proteção de dados pessoais e boas práticas, a equipe técnica considerou que a adoção de modelo regulatório baseado em guia de orientação de boas práticas relacionado à segurança da informação seja mais adequado.



Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2021.08.17__AIR_Reg_MPE__versao_final.pdf*

26.3 RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO SOBRE A DOSIMETRIA DAS MULTAS - Construção do modelo regulatório previsto na **LGPD** com relação à aplicação de sanções administrativas e às metodologias de cálculo do valor-base das sanções de multas, de 30 de junho de 2022.

Por Cecília Rezende de Freitas

Desenvolvimento

Trata-se de análise de impacto desenvolvido por equipe técnica da **ANPD** em relação a regulamentação do **Art. 53** da **LGPD**, o qual determina que a Autóridade, por meio de regulamento próprio sobre sanções administrativas, as metodologias que orientarão o cálculo do valor-base das sanções de multa, devendo ser previamente publicadas, para ciência dos agentes de tratamento, e apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, demonstrando a observância dos parâmetros e critérios previstos no **Art. 52** da Lei.

Considerando as premissas do estudo, a alternativa escolhida foi a adoção de modelo baseado em valoração, que consiste em determinar a espécie de sanção e o valor das sanções pecuniárias por meio de metodologia pré-definida. Com a adoção desta alternativa regulatória, a ANPD teria maior flexibilidade na aplicação das sanções administrativas, utilizando-se dos parâmetros e critérios arrolados na **LGPD** na metodologia para dosimetria da sanção a ser aplicada a cada caso concreto, presumindo-se proporcionalidade entre a sanção administrativa e a gravidade da infração.

Como parâmetros na definição da sanção a ser aplicada em cada caso concreto, a AIR concluiu que pela gravidade e a natureza das infrações e dos direitos pessoais afetados.
Com relação as circunstâncias para a aplicação das penalidades previstas na **LGPD**, em especial as sanções de multa simples e multa diária, a AIR considerou a definição de uma fórmula matemática única como a opção regulatória mais adequada neste momento, devendo considerar os parâmetros e critérios estabelecidos no **Art. 52**.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2022-06-30__air_reg_dosimetria_.pdf*

27. Estudos Técnicos

27.1 ESTUDO TÉCNICO – ANONIMIZAÇÃO DE DADOS NA LGPD: UMA VISÃO DE PROCESSO BASEADO EM RISCO E TÉCNICAS COMPUTACIONAIS, de novembro de 2023

Por Nathália Guerra de Sousa

Desenvolvimento

A **ANPD** publicou, em novembro de 2023, o "Estudo Técnico sobre Anonimização de Dados na LGPD: Uma visão de processo baseado em risco e técnicas computacionais". O documento está estruturado em 2 capítulos, abrangendo o processo de anonimização de dados na perspectiva da utilidade do dado pessoal derivada da finalidade da operação do tratamento, da documentação do processo de anonimização, da gestão do risco de reidentificação e das limitações das técnicas de anonimização. O documento contém, ainda, um apêndice com um caderno de técnicas de anonimização de dados.

O documento, apoiado no §3º do **Art. 12** da **LGPD**, que estabelece que a ANPD poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização, descreve a anonimização como um processo pelo qual os dados com capacidade de identificar um titular são transformados de maneira que a probabilidade de os associar a uma pessoa específica, direta ou indiretamente, é reduzida.

O estudo, que compõe a série de estudos técnicos a respeito da anonimização de dados na **LGPD**, objetivou apresentar a anonimização do ponto de vista da ciência da computação, contendo orientações relevantes aos agentes de tratamento no sentido de abordar a anonimização por padrão como um processo contínuo e baseado em riscos, de forma que não se limitem à aplicação das técnicas, sempre sujeitas a ataques de reidentificação.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_uma_visao_de_processo_baseado_em_risco_e_tecnicas_computacionais.pdf*

27.2 ESTUDO TÉCNICO – ANONIMIZAÇÃO DE DADOS NA LGPD: ANÁLISE JURÍDICA, de novembro de 2023

Por Anna Carolina de Medeiros Silva

Desenvolvimento

A **ANPD** publicou, também em novembro de 2023, o "Estudo Técnico sobre a Anonimização de Dados na LGPD: Análise Jurídica". Este estudo detalha os fundamentos e implicações jurídicas do processo de anonimização de dados pessoais conforme estabelecido pela própria LGPD.

O mesmo está estruturado em quatro capítulos, abrangendo desde a metodologia aplicada, passando pela definição de termos, até a análise detalhada à luz da **LGPD**.

Nele, a anonimização é apresentada como um processo essencial para garantir a privacidade dos dados, removendo identificadores diretos e indiretos, e, assim, excluindo esses dados das obrigações regulatórias previstas na Lei.

Este estudo também destaca a necessidade de transparência na aplicação das técnicas de anonimização, a fim de evitar a reidentificação de dados.

A ANPD enfatiza que, mesmo com a anonimização, é crucial que as organizações continuem a avaliar os riscos associados e adotem boas práticas de governança de dados.

Fonte: *ANPD, disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd__analise_juridica.pdf*

27.3 ESTUDO TÉCNICO – ESTUDOS DE CASOS SOBRE ANONIMIZAÇÃO DE DADOS NA LGPD, de novembro de 2023

Por Renata Lima de Mattos Rocha

Desenvolvimento

A **ANPD** publicou, ainda em novembro de 2023, o "Estudo de Casos Sobre Anonimização de Dados na LGPD".

O presente estudo apresenta 3 (três) casos, de forma simples e didática, objetivando exemplificar técnicas de anonimização de dados, em consonância com os dois estudos técnicos sobre anonimização que abordam a perspectiva jurídico-regulatória e a computacional.

O primeiro caso trata sobre a geolocalização de usuários obtida através de provedores de serviço de telefonia móvel na qual aplicam a técnica da supressão de dados, ou seja, os provedores de telefonia compartilham apenas os dados necessários em termos quantitativo, em outras palavras, não identificam quem são as pessoas que se encontram em determinado local num determinado período, mas sim a quantidade de pessoas que se encontram em determinado local num determinado período.

Já no segundo caso, além da técnica de supressão aplicou-se a técnica de pseudonimização, trazendo como exemplo a substituição de um CPF por um código interno gerado. Nesse caso, considerando que houve uma substituição de dados para tornar o documento público, a ANPD ressalta o cuidado com os dados coletados, que devem ser armazenados com segurança e mantidos em locais com controle de acesso.
Por fim, no terceiro caso, a ANPD aplicou o" Estudo Técnico sobre Anonimização de Dados na LGPD: Processo de Anonimização Baseado em Risco e Técnicas de Anonimização – Uma Introdução Computacional". O referido estudo prevê que ao anonimizar os dados, deve-se considerar o Risco de Reidentificação Aceitável (RRA), anonimizar o dado e então avaliar o Risco de Reidentificação Mensurado (RRM), e ao final, o RRM deve estar sempre abaixo do RRA.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_de_casos_sobre_anonimizacao_de_dados_na_lgpd_.pdf*

27.4 ESTUDO TÉCNICO REGULATÓRIO – SANDBOX REGULATÓRIO, de 29 de setembro de 2023

Por Nathália Guerra de Sousa

Desenvolvimento

O ambiente regulatório experimental, ou "sandbox" regulatório é uma colaboração experimental entre o regulador, a entidade regulada e outras partes interessadas. Seu objetivo é simples: gerar conhecimento e confiança em serviços e produtos inovadores a partir de testes de inovações regulatórias em um ambiente controlado, utilizando uma metodologia estruturada, facilitando a inovação de maneira segura e responsável, com acompanhamento próximo pelos reguladores, que estão atentos para avaliar benefícios e riscos à sociedade. O termo "sandbox", em inglês, refere-se a uma "caixa de areia", um espaço onde estruturas podem ser facilmente remodeladas ou reconstituídas devido à natureza flexível do material.

A Lei Complementar nº 182, de 1 de junho de 2021, institui o marco legal das startups e do empreendedorismo inovador (*Marco Legal das Startups*), define o ambiente regulatório experimental como "conjunto de condições especiais simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e de limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado".

Esse ambiente controlado permite a suspensão temporária de certas disposições ou requisitos, possibilitando a experimentação sem o risco imediato de sanções. Na prática, isso viabiliza testes em pequena escala dentro de um contexto de confiança entre os regulados e a **ANPD**, permitindo a exploração dos desdobramentos da tecnologia, viabilizando o desenvolvimento tecnológico com um viés ético.

Em razão da ampla aplicação desse conceito à proteção de dados pessoais, que busca equilibrar a proteção de direitos fundamentais com a continuidade da inovação, a ANPD está desenvolvendo um instrumento sobre o tema, que pode ser explorado especialmente por tecnologias disruptivas, como o uso de inteligência artificial, que podem apresentar incertezas quanto à conformidade com a **LGPD**. Ao final do processo, é possível identificar lacunas em termos de eficácia e desenvolver uma regulação que se adapte aos novos cenários.

A ANPD abriu, em outubro de 2023, um processo de tomada de subsídios através da consulta à sociedade, que traz questionamentos sobre critérios de elegibilidade para o projeto. Após a análise de diversas perspectivas e sugestões de melhorias, a Autoridade informará sobre as regras e estrutura do projeto, incluindo os pressupostos para participação.

Ressalta-se a importância do desenvolvimento do tema pela ANPD, uma vez que há a necessidade de viabilização de modelos de negócios como *healthtechs* e *fintechs*, que, por serem setores amplamente regulados, demandam a colaboração de reguladores específicos. Ainda, é possível apoiar-se em experiências internacionais, como o sandbox do *Information Commissioner`s Office* (ICO), do Reino Unido, que focou no design de padrões de proteção de dados voltados para menores de idade, por exemplo.

Sobre o documento da ANPD - Estudo Técnico - *Sandbox* Regulatório:

A Autoridade publicou, em setembro de 2023, o "Estudo Técnico sobre Sandbox Regulatório". O documento está estruturado em 5 capítulos, abrangendo e detalhando desde o contexto de definição e histórico dos *sandboxes* regulatórios, estudos de caso nacionais e internacionais, características relevantes dos programas, bem como a estrutura de planejamento e execução de um *sandbox*.

O documento indica que é possível considerar o *sandbox* como uma abordagem regulatória para o balanceamento de riscos, que promove, a partir de requisitos regulatórios mínimos, possibilidades de experimentação ao tempo em que orienta a regulamentação para caminhos adequados. Tudo isso através de um processo colaborativo de exploração do uso de inovações tecnológicas e novos modelos de negócios com o olhar atento dos reguladores. Esse processo permite ao regulador analisar como inovações tecnológicas interagem com regulamentos já existentes (como a **LGPD**) e verificar as possibilidades de abordagem para permitir a coexistência de modelos de inovação com a proteção de direitos fundamentais.

O estudo da ANPD tem como propósito apresentar como os *sandboxes* regulatórios podem ser utilizados por si, ou outra autoridade competente, contribuir em suas atividades relacionadas à regulação de tecnologias emergentes, tendo sido eleita pela Autoridade a inteligência artificial (IA). O documento aborda, mais especificamente, exemplos de uso de *sandboxes* regulatórios para IA, citando as experiências da Comissão Europeia e do Governo da Espanha e seus respectivos pilotos, mas não ignorando experiências nacionais, como do Sistema Financeiro Nacional e de outras agências reguladoras, como ANEEL, ANTT e ANATEL, de forma que, dos primeiros capítulos do estudo, é possível depreender uma série de elementos e características presentes em experiências de *sandboxes* regulatórios.

O texto da ANPD detalha, ainda, os seis aspectos mais relevantes na formulação e execução de programas de *sandbox* regulatório em matéria de proteção de dados pessoais, quais sejam: (i) possíveis benefícios gerados pelo programa; (ii) critérios coerentes com atribuições e prioridades regulatórias; (iii) participação colaborativa de atores interessados; (iv) consciência das limitações do programa; (v) delimitação dos riscos ensejados pelo projeto de tecnologia e mecanismos para sua mitigação; e (vi) produtos resultantes. Finalmente, o último capítulo traz resultados do benchmark realizado por meio de levantamento bibliográfico e de diálogos bilaterais com reguladores e outros atores interessados, tendo proposto um roteiro para planejamento e execução de um programa-piloto.

Fontes: *ANAPD, disponíveis em:*
https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/sandbox_regulatorio__estudo_tecnico__versao_publica_.pdf
https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-a-sociedade-sobre-sandbox-regulatorio-de-inteligencia-artificial-e-protecao-de-dados-pessoais-no-brasil
https://www.gov.br/anpd/pt-br/sandbox/o-sandbox-regulatorio
https://www.gov.br/anpd/pt-br/sandbox/para-quem-e-o-sandbox-regulatorio
ICO (Reino Unido), disponível em:
https://ico.org.uk/media/for-organisations/documents/2618112/our-key-areas-of-focus-for-regulatory-sandbox.pdf

28. Outros Documentos

28.1 TEXTO PARA DISCUSSÃO Nº 1/2022 - A **LGPD** e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa, de abril de 2022.

Por Cecília Rezende de Freitas

Desenvolvimento

Trata-se de estudo técnico, desenvolvido pela **ANPD**, contendo análise de caráter preliminar, disponibilizado à época para fomentar o debate público e subsidiar futura tomada de decisão sobre o tema pela própria Autoridade.

A **LGPD** estabelece normas específicas para o tratamento de dados pessoais para fins acadêmicos e pesquisas por órgãos de pesquisa, visando um equilíbrio entre proteção de dados e liberdade acadêmica. Este estudo técnico da ANPD aborda questões sobre sua interpretação e aplicação nesse contexto, destacando a necessidade de segurança jurídica e respeito aos direitos dos titulares.

A Lei visa também proteger a privacidade e autodeterminação informativa, garantindo a anonimização dos dados sempre que possível. As bases legais para o tratamento de dados pessoais incluem o consentimento e a realização de estudos por órgãos de pesquisa. No entanto, há incertezas jurídicas que impactam o desenvolvimento de pesquisas, como a negativa de pedidos de acesso a dados por falta de regulamentação clara.

O documento identifica diversos questionamentos sobre o tema, tais como definição e alcance dos conceitos de "tratamento de dados para fins exclusivamente acadêmicos", definição de "órgão de pesquisa" segundo a **LGPD**, bases legais que autorizam o tratamento de dados pessoais para pesquisas, delimitação de responsabilidades em relação ao tratamento dos dados pessoais e como devem ser atribuídas essas responsabilidades no contexto de pesquisas acadêmicas e científicas, quais procedimentos devem ser adotados para comprovar a identidade do pesquisador e seu vínculo com a instituição de pesquisa para acessar e tratar dados pessoais, dentre outros.

Esses questionamentos refletem as dúvidas frequentes e preocupações sobre a aplicação da **LGPD** no contexto acadêmico e de pesquisa, destacando a necessidade de clarificação e orientação para assegurar a conformidade legal e a proteção dos direitos dos titulares de dados.

Por fim, conclui-se que, mesmo com a flexibilização das regras, é necessário um regime jurídico específico e adequado às atividades acadêmicas, garantindo a segurança e a ética no tratamento dos dados pessoais.

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_2022_17.pdf*

28.2 ESTUDO PRELIMINAR - Hipóteses Legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, de setembro de 2022.

Por Marcela Fuga Antunes Cardoso

Desenvolvimento

A ANPD publicou, em setembro de 2022, o "Estudo Preliminar sobre as Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes". Este estudo "[...] foi elaborado com o intuito de analisar as hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. A partir de um levantamento das principais questões e dúvidas direcionadas à ANPD sobre o tema, a análise se concentrou em três possíveis interpretações sobre o tema:

i. a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º, da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças;
ii. (ii) a aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, haja vista a sua equiparação aos dados sensíveis; e
iii. (iii) a aplicação das hipóteses legais previstas nos arts. 7º e 11 da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse.
iv. A partir da análise dos argumentos favoráveis e contrários a cada uma dessas interpretações, apresentados e discutidos ao longo do estudo, conclui-se que a terceira alternativa expressa a melhor interpretação da LGPD, de modo que se entende pela possibilidade de tratamento de dados pessoais de crianças e adolescentes com base nas hipóteses previstas nos arts. 7º e 11, desde que observado o princípio do melhor interesse, conforme previsto no art. 14 da Lei. (...)

Assim, a fim de dirimir a controvérsia sobre a questão, bem como formalizar e sintetizar a interpretação da ANPD sobre a matéria, entende-se que seria possível a edição de enunciado, sugerindo-se a seguinte redação preliminar:

"O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD, desde que observado o seu melhor interesse, a ser avaliado no caso concreto, nos termos do caput do art. 14 da Lei."

Dessa forma, a fim de conferir maior transparência e subsidiar o processo decisório da ANPD, propõe-se a disponibilização pública do presente estudo técnico e da proposta de enunciado acima exposta, visando promover a discussão pública e colher contribuições da sociedade." (10)

Fonte: *ANPD, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf*

28.3 REGIMENTO INTERNO DA ANPD - A Resolução CNPD nº 1, de 06 de maio de 2022, estabeleceu o Regimento Interno do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD).

Por Marcela Antunes Fuga Cardoso

Desenvolvimento

Conforme ao explicitado no Relatório de Atividades 2022 da CNPD, "o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD é um órgão consultivo, vinculado à Autoridade Nacional de Proteção de Dados – ANPD, conforme disposto na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14 de agosto de 2018)".

Conforme Art. 2º do Regulamento em pauta, "o CNPD é composto por 23 (vinte e três) membros, designados por ato do Presidente da República, permitida a delegação, indicados conforme o estabelecido no art. 58-A da Lei nº 13.709, de 14 de agosto de 2018, e art. 15 do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, da seguinte forma:

I - um da Casa Civil da Presidência da República, que o presidirá;
II - um do Ministério da Justiça e Segurança Pública;
III - um do Ministério da Economia;
IV - um do Ministério da Ciência, Tecnologia e Inovações;
V - um do Gabinete de Segurança Institucional da Presidência da República;
VI - um do Senado Federal;
VII - um da Câmara dos Deputados;
VIII - um do Conselho Nacional de Justiça;
IX - um do Conselho Nacional do Ministério Público;
X - um do Comitê Gestor da Internet no Brasil;
XI - três de organizações da sociedade civil com atuação comprovada em proteção de dados pessoais; produtivo;
XII - três de instituições científicas, tecnológicas e de inovação; XIII - três de confederações sindicais representativas das categorias econômicas do setor XIV - dois de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e
XV - dois de entidades representativas do setor laboral."

Composto por membros da sociedade e do poder público, o CNPD tem como principais atribuições:

- Propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Sugerir ações a serem realizadas pela ANPD;
- Elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;
- Disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade.

Além do mencionado, o Regulamento ainda dispõe sobre (i) as Atribuições do Presidente, (ii) dos Membros, (iii) sobre o funcionamento das Reuniões (as quais ocorrem três vezes ao ano, sem prejuízo de convocações extraordinárias), (iv) sobre a Secretaria-Geral, (v) sobre a Perda de Mandato e (vi) sobre os Grupos de Trabalho.
O CNPD poderá criar Grupos de Trabalho, "de caráter temporário, para realizar análises, estudos e fazer proposições a respeito das matérias de sua competência", os quais seguirão as condições dispostas nos incisos do Art. 24 do Regulamento:

I - os grupos de trabalho serão compostos por, no máximo, 7 (sete) membros, e sempre de número ímpar;
II - a composição dos grupos de trabalho priorizará a pluralidade de setores, sempre que possível, observada a proporcionalidade da composição do CNPD;
III - duração não superior a 6 (seis) meses, prorrogável por igual período; e
IV - finalidade determinada.

Ainda sobre o assunto, ficou determinado que, em regra, somente pode haver até 5 (cinco) grupos de trabalho simultâneos (art. 24, § 4º) e que "os Grupos de Trabalho poderão reunir-se com os grupos de trabalho de outros colegiados para a realização de discussão integrada de matérias de interesse do CNPD" (art. 26, caput), podendo haver o convite para que especialistas não membros possam contribuir, sem remuneração e sem direito à voto (art. 26, parágrafo único).

Por fim, restou estabelecido que as dúvidas e casos omissos serão resolvidos pelo Presidente do CNPD (art. 33).

Fontes: *ANPD, disponíveis em:*
https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/regimento-interno-cnpd.pdf

28.4 PORTARIAS

Por Marcela Antunes Fuga Cardoso

28.4.1 Portarias CNPD nº 01 a 05, de 1º de abril de 2022, publicadas no dia 5 de abril de 2022 instituem os Grupos de Trabalho temporários.

28.4.2 Portarias CNPD nº 06 a 10, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022, prorrogam os prazos para encerramento das atividades dos Grupos de Trabalho instituídos pelas Portarias CNPD nº 01 a 05, de 1º de abril de 2022, e estabelecem regras de participação dos membros.[11]

28.4.3 Portaria CNPD nº 11, de 4 de julho de 2022, publicada no dia 04 de julho de 2022, prorroga o prazo para encerramento das atividades do Grupo de Trabalho instituído pela Portaria CNPD nº 02, de 1º de abril de 2022.

28.4.4 Portaria CNPD nº 12, de 8 de agosto de 2022, publicada no dia 10 de agosto de 2022, prorroga o prazo para encerramento das atividades do Grupo de Trabalho instituído pela Portaria CNPD nº 03, de 1º de abril de 2022.

28.4.5 Portaria CNPD nº 13, de 8 de agosto de 2022, publicada no dia 10 de agosto de 2022, prorroga o prazo para encerramento das atividades do Grupo de Trabalho instituído pela Portaria CNPD nº 05, de 1º de abril de 2022.

28.4.6 Portaria CNPD nº 14, de 14 de outubro de 2022, publicada no dia 17 de outubro de 2022, prorroga o prazo para encerramento das atividades dos Grupos de Trabalho instituídos pelas Portarias CNPD nº 01, nº 03, nº 04 e nº 05, de 1º de abril de 2022, altera a Portaria CNPD nº 05, de 1º de abril de 2022, e revoga a Portaria CNPD nº 13, de 24 de agosto de 2022.

28.4.7 Portaria CNPD nº 15, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022, prorroga o prazo para encerramento das atividades dos Grupos de Trabalho instituídos pelas Portarias CNPD nº 01, nº 02, nº 03, nº 04 e nº 05, de 1º de abril de 2022 e altera as Portarias CNPD nº 02, CNPD nº 04 e CNPD nº 05, de 1º de abril de 2022.

Desenvolvimento

Conforme disposto no Relatório de Atividades 2022 da CNPD, "uma das primeiras deliberações do colegiado do CNPD foi a formação de Grupos de Trabalho para realizar estudos em temáticas consideradas relevantes para a o fortalecimento da cultura de proteção de dados no Brasil". [12]

"Diante do estágio inicial de implementação da LGPD no país, os temas a serem tratados são numerosos e de considerável complexidade. Desse modo, a atuação em Grupos de Trabalho foi pensada como estratégia multiplicadora da capacidade de atuação do CNPD. [13]

A partir disso, foram criados os seguintes Grupos de Trabalho por meio das Portarias nº 01, 02, 03, 04 e 05 CNPD[14] , e após a publicação da Portaria CNPD nº 15, de 13 de dezembro de 2022, publicada em 13 de dezembro de 2022,[15] os Grupos de Trabalho se encontram da seguinte forma:

PORTARIA DE INSTITUIÇÃO	GT	EIXO	OBJETO	MEMBROS	PREVISÃO DE ENCERRAMENTO
Portaria CNPD nº 01, de 01 de abril de 2022	1	Política Nacional de Proteção de Dados	Proposição de Diretrizes Estratégicas e fornecimento de subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.	• DAVIS SOUZA ALVES - COORDENADOR • DÉBORA SIROTHEAU SIQUEIRA RODRIGUES • RODRIGO LANGE • CLÁUDIO EDUARDO LOBATO ABREU ROCHA • MARTA JUVINA DE MEDEIROS • MARCOS CESAR DE OLIVEIRA PINTO • FÁBIO AUGUSTO ANDRADE	31 de março de 2023 (conforme alteração dada pela Portaria CNPD nº 15, de 13 de dezembro de 2022, art. 1º)
Portaria CNPD nº 02, de 01 de abril de 2022	2	Direitos de Titulares (conforme alteração dada pela Portaria CNPD nº 15, de 13 de dezembro de 2022, art. 2º)	Proposição de diretrizes estratégicas sobre direitos de titulares, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.	• PATRÍCIA PECK GARRIDO PINHEIRO - Coordenadora • BRUNO RICARDO BIONI • CLÁUDIO SIMÃO DE LUCENA NETO • MICHELE NOGUEIRA LIMA • HARTMUT RICHARD GLASER • TAÍS CARVALHO SERRALVA • CLÁUDIO EDUARDO LOBATO ABREU ROCHA	
Portaria CNPD nº 03, de 01 de abril de 2022	3	Agenda regulatória	Acompanhamento da agenda regulatória relacionada a proteção de dados.	• CÁSSIO AUGUSTO BORGES - Coordenador • NATASHA TORRES GIL NUNES • MARCELO DE LIMA E SOUZA • ANNETTE MARTINELLI DE MATOS PEREIRA • RODRIGO BADARÓ ALMEIDA DE CASTRO • FABRO BOAZ STEIBEL • EMERSON ROCHA	
Portaria CNPD nº 04, de 01 de abril de 2022	4	Transferência internacional de dados pessoais	Proposição de Diretrizes Estratégicas relacionadas à transferência internacional de dados.	• ANA PAULA BIALER - Coordenadora • FABIANO MENKE • FERNANDO ANTONIO SANTIAGO JÚNIOR • LAURA SCHERTEL MENDES • MARCOS VINÍCIUS BARROS OTTONI • NATASHA TORRES GIL NUNES[1]	
Portaria CNPD nº 05, de 01 de abril de 2022	5	LGPD no setor público	Proposição de Diretrizes Estratégicas Relacionadas aos impactos da Lei Geral de Proteção de Dados Pessoais no setor público.	• FABRÍCIO DA MOTA ALVES - Coordenador • FABRO BOAZ STEIBEL • CAITLIN SAMPAIO MULHOLLAN • LEONARDO NETTO PARENTONI • MARTA JUVINA DE MEDEIROS • WEDERSON ADVINCULA SIQUEIRA[2]	

Até a data da edição deste Guia, ainda não foram atualizadas as informações sobre os Grupos de Trabalho.

Assim, também até a data da edição deste Guia, o histórico de Portarias é o seguinte:

PORTARIA DE INSTITUIÇÃO	GT	OBJETO	HISTÓRICO DE PORTARIAS CORRELATAS AOS GT's
Portaria CNPD nº 01, de 01 de abril de 2022	1	Proposição de Diretrizes Estratégicas e fornecimento de subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.	➢ **Portaria CNPD nº 06**, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022: • prorrogou o prazo de encerramento das atividades do GT para 02/10/2022; • estabeleceu regras de participação dos membros. ➢ **Portaria CNPD nº 14**, de 14 de outubro de 2022, publicada no dia 17 de outubro de 2022: • prorrogou o prazo de encerramento das atividades do GT para 18/10/2022; ➢ **Portaria CNPD nº15**, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022: • prorrogou o prazo para encerramento das atividades do GT para 31 de março de 2023;
Portaria CNPD nº 02, de 01 de abril de 2022	2	Proposição de diretrizes estratégicas sobre direitos de titulares, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.	➢ **Portaria CNPD nº 06**, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022: • prorrogou o prazo de encerramento das atividades do GT-1 para 04/07/2022; • estabeleceu regras de participação dos membros. ➢ **Portaria CNPD nº 11**, de 4 de julho de 2022, publicada no dia 04 de julho de 2022: • prorrogou o prazo de encerramento das atividades do GT para 27/07/2022; ➢ **Portaria CNPD nº15**, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022: • prorrogou o prazo para encerramento das atividades do GT para 31 de março de 2023; • alterou o eixo do GT-2 de "Ações educativas" para "Direitos de Titulares", sendo seu objeto "proposição de diretrizes estratégicas sobre direitos de titulares, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.".

Portaria CNPD nº 03, de 01 de abril de 2022	3	Acompanhamento da agenda regulatória relacionada a proteção de dados.	➢ **Portaria CNPD nº 06**, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022: • prorrogou o prazo de encerramento das atividades do GT-3 para 04/09/2022; • estabeleceu regras de participação dos membros. ➢ **Portaria CNPD nº 12**, de 8 de agosto de 2022, publicada no dia 10 de agosto de 2022: • prorrogou o prazo de encerramento das atividades do GT para 23/09/2022; ➢ **Portaria CNPD nº 14**, de 14 de outubro de 2022, publicada no dia 17 de outubro de 2022: • prorrogou o prazo de encerramento das atividades do GT para 11/11/2022; ➢ **Portaria CNPD nº15**, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022: • prorrogou o prazo para encerramento das atividades do GT para 31 de março de 2023;
Portaria CNPD nº 04, de 01 de abril de 2022	4	Proposição de Diretrizes Estratégicas relacionadas à transferência internacional de dados.	➢ **Portaria CNPD nº 06**, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022: • prorrogou o prazo de encerramento das atividades do GT-4 para 01/11/2022; • estabeleceu regras de participação dos membros. ➢ **Portaria CNPD nº 14**, de 14 de outubro de 2022, publicada no dia 17 de outubro de 2022: • prorrogou o prazo de encerramento das atividades do GT para 01/12/2022; ➢ **Portaria CNPD nº15**, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022: • prorrogou o prazo para encerramento das atividades do GT para 31 de março de 2023; • alterou 06 membros.

Portaria CNPD nº 05, de 01 de abril de 2022	5	Proposição de Diretrizes Estratégicas Relacionadas aos impactos da Lei Geral de Proteção de Dados Pessoais no setor público.	➢ **Portaria CNPD nº 06**, de 15 de junho de 2022, publicadas no dia 15 de junho de 2022: • prorrogou o prazo de encerramento das atividades do GT-5 para 03/08/2022; • estabeleceu regras de participação dos membros. ➢ **Portaria CNPD nº 13**, de 8 de agosto de 2022, publicada no dia 10 de agosto de 2022: • prorrogou o prazo de encerramento das atividades do GT para 08/09/2022; ➢ **Portaria CNPD nº 14**, de 14 de outubro de 2022, publicada no dia 17 de outubro de 2022: • prorrogou o prazo de encerramento das atividades do GT para 24/10/2022; • revogou a Portaria CNPD nº 13, de 8 de agosto de 2022, publicada no dia 10 de agosto de 2022; • alterou 02 membros. ➢ **Portaria CNPD nº15**, de 13 de dezembro de 2022, publicada no dia 13 de dezembro de 2022: • prorrogou o prazo para encerramento das atividades do GT para 31 de março de 2023; • alterou 06 membros.

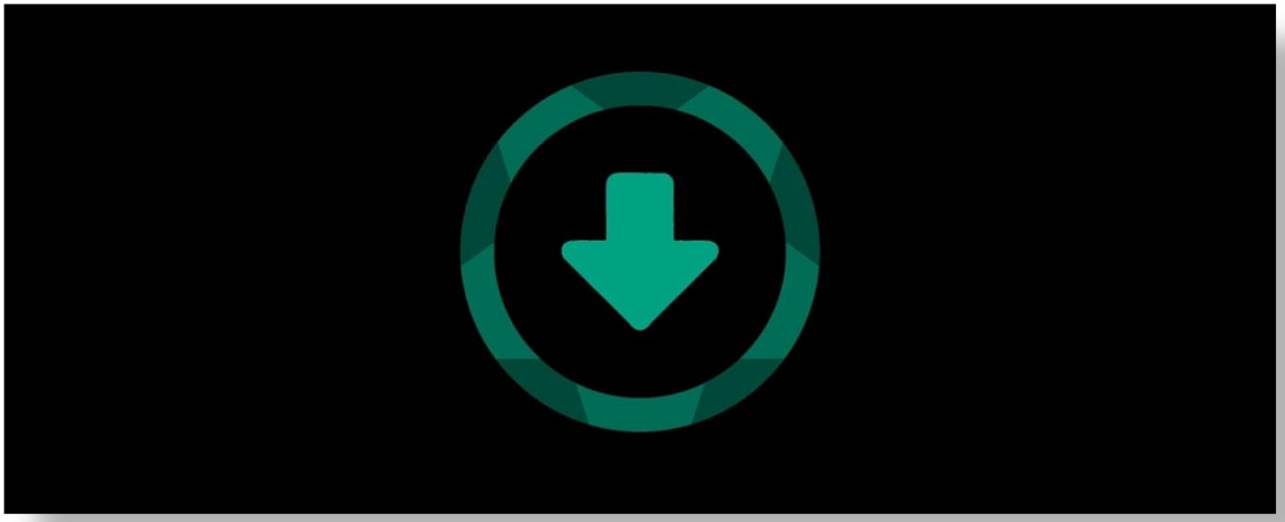
https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf *fls. 08.*

https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf *fls. 08.*
https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf *fls. 08.*
https://www.gov.br/anpd/pt-br/cnpd-2/portaria-cnpd-no-15-de-13-12-2022.pdf

Art. 1º *"Prorrogar, até o dia 31 de março de 2023, o prazo para encerramento das atividades dos Grupos de Trabalho temporários instituídos pelas seguintes Portarias: I - Portaria CNPD nº 01, de 1º de abril de 2022; II - Portaria CNPD nº 02, de 1º de abril de 2022; III - Portaria CNPD nº 03, de 1º de abril de 2022; IV - Portaria CNPD nº 04, de 1º de abril de 2022; e V - Portaria CNPD nº 05, de 1º de abril de 2022. Quando da publicação da Portaria CNPD nº 02, de 01 de abril de 2022, o eixo do GT-2 era "o das Ações educativas", sendo seu objeto "Proposição de ações educativas e fomento à cultura de proteção de dados e da privacidade.". Após a alteração dada pela Portaria CNPD nº 15, de 13 de dezembro de 2022, art. 2º, o eixo do GT-2 passou a ser "Direitos de Titulares", sendo seu objeto "proposição de diretrizes estratégicas sobre direitos de titulares, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.";* Art. 2º *"A Portaria CNPD nº 02, de 2022, passa a vigorar com as seguintes alterações: "Institui Grupo de Trabalho dedicado à proposição de diretrizes estratégicas sobre direitos de titulares, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade" (NR) "Art. 1º Fica instituído o Grupo de Trabalho temporário dedicado à proposição de diretrizes estratégicas sobre direitos de titulares, para realizar análises e estudos e, ao final, apresentar relatório" (NR) "Art. 2º Compete ao Grupo de Trabalho realizar análises, estudos e fazer proposições de diretrizes estratégicas sobre direitos de titulares" (NR)* Art. 3º *"O Grupo de Trabalho temporário dedicado à proposição de diretrizes estratégicas sobre direitos de titulares é composto por:*

I - Ana Paula Martins Bialer, membro titular representante de entidades representativas do Setor Empresarial relacionado à área de Tratamento de Dados, que o coordenará; II - Fabiano Menke, membro titular representante de Instituições Científicas, Tecnológicas e de Inovação; III - Fernando Antônio Santiago Júnior, membro suplente representante de Outros Poderes, Órgãos ou Instituições Públicas; IV - Laura Schertel Ferreira Mendes, membro titular representante de Instituições Científicas, Tecnológicas e de Inovação; V - Marcos Vinícius Barros Ottoni, membro suplente representante de Confederações Sindicais representativas das categorias econômicas do Setor Produtivo; VI - Natasha Torres Gil Nunes, membro titular representante de Confederações Sindicais representativas das categorias econômicas do Setor Produtivo" (NR).

Depois, com o art. 4º. A Portaria CNPD nº 05, de 2022, passa a vigorar com a seguinte alteração: "*Art. 3º ..... I - Fabrício da Mota Alves, membro titular representante de Outros Poderes, Órgãos ou Instituições Públicas, que o coordenará; II - Fabro Boaz Steibel, membro suplente representante Organizações da Sociedade Civil com atuação comprovada em Proteção de Dados; III - Caitlin Sampaio Mulhollan, membro suplente representante de Instituições Científicas, Tecnológicas e de Inovação; IV - Leonardo Netto Parentoni, membro suplente representante de Instituições Científicas, Tecnológicas e de Inovação; V - Marta Juvina de Medeiros, membro suplente representante do Poder Executivo Federal; VI - Wederson Advincula Siqueira, membro suplente representante de Outros Poderes, Órgãos ou Instituições Públicas" (NR).*



Fontes: *ANPD, disponíveis em:*
https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/portarias-de-prorrogacao-dos-gts.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/portaria-cnpd-no-11-de-04-de-julho-de-2022-prorrogacao-gt-2.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/prorrogacao-do-prazo-de-encerramento-do-gt3.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/prorrogacao-do-prazo-de-encerramento-do-gt5.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/portaria-cnpd-no-14-de-14-10-2022.pdf
https://www.gov.br/anpd/pt-br/cnpd-2/portaria-cnpd-no-15-de-13-12-2022.pdf

29. Apêndice

ADEQUAÇÃO DO REGULAMENTO DE PROTEÇÃO DE DADOS (RGPD) NOS ESCRITÓRIOS DE ADVOGADOS NA UNIÃO EUROPEIA, EM PARTICULAR EM PORTUGAL (Escrito de acordo com a variante portuguesa do Acordo Ortográfico de 1990.)

Por Angelina Teixeira

"Numa sociedade baseada no respeito pelo primado da lei, o advogado desempenha um papel especial. Os deveres do advogado não se esgotam no cumprimento rigoroso do seu mandato dentro dos limites da lei. O advogado deve servir o propósito de uma boa administração da justiça ao mesmo tempo que serve os interesses daqueles que lhe confiaram a defesa e afirmação dos seus direitos e liberdades. Um advogado não deve ser apenas um pleiteador de causas, mas também um conselheiro do cliente. O respeito pela função do advogado assume-se como uma condição essencial para a garantia do Estado de Direito Democrático." - Preâmbulo do *Código de Deontologia dos Advogados Europeus*.

I – Do Regulamento Geral Sobre a Proteção de Dados (RGPD) da União Europeia (UE)

O Regulamento Geral sobre a Proteção de Dados (RGPD) é um diploma da União Europeia (UE)[2] que **entrou em vigor a 25 de maio de 2018**, dotado de um regime jurídico relativo à proteção de pessoas singulares [naturais] no que diz respeito ao tratamento de dados pessoais[3] e à livre circulação desses dados, revogando a Diretiva 95/46/CE do Parlamento Europeu e do Conselho[4].

Com o RGPD, foram introduzidas um conjunto de novas regras, entre as quais, a obrigação de designar um encarregado para a proteção de dados, pseudonimização de dados, obtenção de consentimento, consentimento de menores, eliminação do sistema de notificações e autorizações, implementação do direito ao esquecimento, criação de obrigações acrescidas para os subcontratados, a introdução de coimas de valor muito significativo e obrigações de informação relativas a quebras de segurança.

Antes de tudo, a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. Assim, o artigo 8.º, n.º 1, da ***Carta dos Direitos Fundamentais da União Europeia*** («Carta»)[5] e o artigo 16.º, n.º 1, do ***Tratado sobre o Funcionamento da União Europeia*** (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito[6].

O RGPD tem como objetivo contribuir para a realização de um espaço de liberdade, segurança, justiça, união económica, progresso económico e social, consolidação e convergência das economias a nível do mercado interno e, bem-estar[7].

Tal Regulamento prevê que o **tratamento dos dados pessoais** deverá ser concebido para servir as pessoas, não sendo um direito absoluto. Deve ser considerado **em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais** - princípio da proporcionalidade[8].

Por outro lado, o intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na última década na União Europeia. As autoridades nacionais dos Estados Membros - Portugal - são chamadas, por força do Direito da União Europeia, a colaborar e a trocar dados pessoais entre si[9].

A rápida evolução tecnológica e a globalização criaram muitos desafios em matéria de proteção de dados pessoais onde a recolha e a partilha proliferam[10]. As pessoas singulares [naturais] disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global, do qual o legislador exige uma proteção reforçada, segurança jurídica e transparência através das especificações ou restrições previstas no RGPD.

Os escritórios de advocacia em Portugal não podem desconhecer, porque não lhes aproveita, sejam de prática isolada ou de outra natureza, que o tratamento de dados pessoais deve ser mais pormenorizado, seja em termos contratuais com obrigações jurídicas, seja para o exercício de funções de interesse público[11] ou da autoridade pública de que está investido o responsável pelo seu tratamento.

O legislador português através da chama ***Lei de Execução*** do RGPD[12] fez estender a sua vertente prática a um leque muito vasto de matérias do direito, como é o caso da contratação pública[13].

O princípio da proteção de dados aplica-se assim a qualquer informação relativa a uma pessoa singular [natural] identificada ou identificável[14]. O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito[15].

Em síntese, o tratamento de dados pessoais deverá ser efetuado de forma lícita, equitativa e transparente, seja por recolha, utilização, consulta ou qualquer outro tipo de tratamento e medida em que são ou virão a ser tratados[16] com a salvaguarda do «direito a serem esquecidos»[17].

Ainda persiste nos escritórios de advocacia - sobretudo – na prática individual ou isolada dúvidas quanto à materialização das medidas mais adequadas e eficazes para a promoção de atividades quanto à natureza, âmbito, contexto e finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares[18].

Na prática, podemos afirmar que **a maioria dos escritórios de advocacia em Portugal não é dotado de uma equipa dedicada e especialidade em temas de privacidade e segurança da informação**, **nem** são detentores de uma **gestão diária da conformidade** com as orientações emitidas pela entidade reguladora[19].

Recordamos que o próprio RGPD concedeu dois anos entre a sua entrada em vigor e a respectiva aplicação, ou seja, para que cada entidade procedesse à identificação das alterações necessárias para efeitos de conformidade *(Compliance)* com o novo regime de proteção de dados e à sua implantação, incluindo a adoção e a aplicação de novas medidas em matéria de segurança[20].

Foi através referida ***Lei de Execução***, publicada decorridos mais de três anos após a entrada em vigor do RGPD (2016) e mais de um ano após a sua publicação (2018), que Portugal viria a conhecer as normas de execução e algumas novidades, nomeadamente:
i. a designação da Comissão Nacional de Proteção de Dados (CNPD)[21] como autoridade de controlo nacional para efeitos de RGPD e da lei (artigo 57.º do RGPD);

ii. o esclarecimento de quais as entidades obrigadas a nomear um Encarregado de Proteção de Dados ou EPD (artigo 37.º do RGPD)[22];

iii. a dispensa de certificação profissional do EPD[23];

iv. consentimento de menores[24];

v. videovigilância com autorização prévia da CNPD[25].

Chegados aqui, acolhendo o rol de definições previsto no artigo 4.º do RGPD, passaremos abordar, ainda que de forma perfunctória, o perfil dos escritórios de advocacia em Portugal e, por último concluir sobre a adequação àquele Regulamento.

1 Advogada, com inscrição em vigor na Ordem dos Advogados Portuguesa (OAP), também coordenadora de Departamento na área da Privacidade, Proteção de Dados, IA e Compliance na ATA advogados, formadora e árbitra em Direito.

[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (UE) n.º 679/2016, de 27 de abril, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

[3] São exemplos, nome, apelido, número de identificação fiscal, foto, domicílio fiscal ou pessoal, endereço pessoal de correio eletrônico; número de telefone, número de cartão de identificação, rendimento, dados de localização, endereço IP, perfil social.

[4] De 24 de outubro de 1995, esta Diretiva visa harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AOJ.L_.1995.281.01.0031.01.POR.

[5] Estabelece, no seu art.º 8.º - Proteção de Dados Pessoais, que a todas as pessoas foi concedido o direito de proteger os dados de caráter pessoal que lhe digam respeito. Além disso, é determinado que, tais dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, disponível em https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html?locale=pt.

[6] Considerando 1 do RGPD e, na ausência de citação do diploma, deve-se ler como parte deste.

[7] Considerando 2.

[8] Observando as liberdades, princípios da Carta e dos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística - (4) do RGPD.

[9] A fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro – (5) do RGPD.

[10] As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As mesmas transformaram a economia e a vida social e o RGPD visa contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

[11] A Constituição da República Portuguesa (CRP), de 2 de abril de 1976, atribui à advocacia uma função de interesse público, sem precedente noutras profissões liberais, como elemento essencial na administração da justiça (art. 208.º), espelhado no Estatuto da Ordem dos Advogados Portuguesa - Lei n.º 145/2015, de 9 de setembro, em vigor. Determina a Lei fundamental em Portugal, no Art. 35.º "Utilização da Informática" constante na Parte I do Título II, Capítulo I, que, todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

[12] A Lei n.º 58/2019, de 8 de agosto, assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, disponível em: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982.

[13] Está prevista uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividade. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não estão abrangidos pelo RGPD – Considerandos 13, 15 e 78 do RGPD.

[14] *Por associação a identificadores por via eletrónica, através de aparelhos, aplicações, ferramentas e protocolos (IP) ou testemunhos de conexão ou outros identificadores - considerando 30.*

[15] *Pode ser feito através de uma declaração escrita ou em formato eletrónico ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido – considerando 32.*

[16] *Considerandos 39, 43, 58 e 60.*

[17] *Considerandos 64 a 67.*

[18] *Considerandos 74, 76 e 77.*

[19] *O cenário ideal seria o de todos os escritórios de advocacia terem em curso formas de avaliação de impacto em matéria de Cibersegurança e de Privacidade, com uma verificação regular.*

[20] *Tarefas como o levantamento de todas as atividades que envolvesse tratamento de dados pessoais e catalogar as bases de dados, nomeadamente, trabalhadores, clientes, fornecedores, destinatários de newsletters. Para cada base, a verificação da licitude, transparência, lealdade, minimização dos dados, limitação das finalidades, limites da conservação, confidencialidade e integridade, com tratamento jurídico fundamentado. Falamos de consentimento dos titulares dos dados, diligências pré-contratuais, obrigações jurídicas, execução de contratos, revisão dos formulários de consentimento, contratos, mecanismos de garantia do exercício dos direitos dos titulares dos dados e definição de procedimentos internos de notificação de violações dos pessoais face às novas exigências do RGPD.*

[21] *Lei n.º 43/2004, de 18 de agosto estabelece a organização e funcionamento da Comissão Nacional de Proteção de Dados em Portugal. As entidades públicas e privadas devem prestar a sua colaboração à CNPD, facultando-lhes todas as informações que por esta lhes sejam solicitadas, bem como o acesso ao sistema informático, a ficheiros de dados pessoais e a documentação relativa ao tratamento de dados pessoais. A CNPD age com independência na prossecução das suas atribuições e competências e exercício dos seus poderes (previstos designadamente nos artigos 57.º e 58.º do RGPD, 6.º e 8.º da Lei 58/2019, e 44.º da Lei 59/2019). A CNPD é um órgão colegial, composto por sete membros de integridade e mérito reconhecidos, cujo estatuto garante a independência das suas funções. Os membros da CNPD têm um mandato de cinco anos e tomam posse perante o Presidente da Assembleia da República. Veja-se ainda o sítio da Internet disponível em: https://www.cnpd.pt/*

[22] *Obrigatório para algumas entidades privadas, sendo obrigatório nomear um EPD quando a atividade privada desenvolvida, a título principal, implicar tratamentos que exijam um controlo regular e sistemático dos titulares dos dados em grande escala ou tratamentos, escala das categorias especiais de dados nos termos do artigo 9.º do RGPD, ou de dados pessoais relacionados com condenações penais e contraordenacionais nos termos do artigo 10.º daquele regulamento.*

[23] *Esclarece que o exercício das funções de encarregado da proteção de dados não carece de certificação profissional e reforça que, independentemente da natureza da sua relação jurídica com o responsável pelo tratamento de dados, aquele mantém autonomia técnica. Foi determinado que o Instituto Português de Acreditação (IPAC, I.P.) é a autoridade competente para a acreditação dos organismos de certificação em matéria de proteção de dados, conforme exigido no artigo 43.º do RGPD.*

[24] *O consentimento prestado por menores no que respeita à oferta direta de serviços da sociedade da informação é lícito se os menores tiverem, pelo menos, 13 anos. Com menos idade, o tratamento só é lícito se o consentimento for dado pelos titulares das responsabilidades parentais, com recurso a meios de autenticação segura.*

[25] *Foi determinada proibição de captação de som por parte de câmaras de videovigilância, exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD.*

II – Da Adequação RGPD aos Escritórios de Advocacia de Portugal

Segundo dados da Direção-Geral da Política de Justiça (DGPJ) do Ministério da Justiça, em 2021 estavam inscritos na Ordem dos Advogados em Portugal, 33.937 advogados[26].

Estima-se que em Portugal, cerca de 85% dos escritórios de advocacia é exercida em prática individual ou isolada e de acordo com os dados de 2024 partilhados pela Ordem dos Advogados Portuguesa[27] a atividade incide sobretudo no plano do sistema de acesso ao direito (SADT) [28].

Este regime individual é apontado como aquele que traz ao advogado um sentimento de liberdade, flexibilidade, proximidade com o cliente e sentido de criatividade intelectual na busca de soluções, em detrimento dos projetos societários [29].

Em Portugal os processos na sua maioria são tramitados nas plataformas judiciais CITIUS[30] e SITAF[31] através de uma *interface* de acesso ao sistema de suporte à atividade dos tribunais por mandatários e representantes em juízo designado *eTribunal*[32].

Os desafios dos escritórios de advocacia também passam pela necessidade de compartilhar informações com terceiros, as quais podem conter dados pessoais, incluindo dados sensíveis, como as próprias instâncias judiciárias, as entidades administrativas ou outros advogados, daí que o mapeamento dos processos ou dossiês de clientes seja prioritário[33].

Independentemente da dimensão dos escritórios de advocacia em Portugal, é ainda uma matéria jurídica e na prática com alguma sensibilidade, sobretudo no desafio na proteção de dados aquando da tomada de decisão de, como efetivamente salvaguardar a confidencialidade dos titulares dos dados, nomeadamente, clientes.

No entanto, são notórios os avanços na busca de formas de implementação de medidas de segurança e adaptação que passem da teoria à prática, a par de um reforço na linguagem jurídica e vocabulário gerador de uma nova forma de comunicação.

Como é também crescente a procura de gestão de acesso aos dados, formas de garantia da robustez, privacidade, integridade de dados, cifragem, monitorização, além de uma formação especializada em matéria de RGPD.

Nessa medida, reconhecemos o esforço dos Centros Distritais da Ordem dos Advogados em Portugal, seja pelas iniciativas facilitadoras, na maioria de acesso online e gratuitas na área da formação em RGPD.

Mais recentemente, foram apresentados protocolos, no intuito de permitir a todos os advogados com inscrições em vigor em Portugal, sobretudo aos profissionais em prática individual ou isolada, passarem a dispor a plataformas de gestão de clientes e processos, de acesso gratuito ou de subscrição a preços inferiores ao habitual.

Noutro cenário, temos os projetos societários que utilizam programas de gestão feitos à medida, de acordo com o seu perfil, volume de clientes e faturação, contratando para o efeito empresas do sector informático e muitas das vezes a contratação de *players* que assumam o papel de encarregado de proteção de dados[34].

A adequação do RGPD tem vindo a ser fortalecida, sobretudo através de aplicações e campos em plataformas tecnológicas que permitem o envio de formulário-tipo para a obtenção do consentimento expresso de autorização do tratamento dos dados pessoais mais eficiente[35].

Em síntese, falamos da transformação dos escritórios de advocacia em centros de maior eficiência. Por isso, cremos que a manutenção do exercício da profissão de advocacia passa - sem retorno - por soluções digitais, informáticas, em particular com recursos com capacidade de adequar a regulamentação em proteção de dados, seja aquela que está em vigor no plano nacional e comunitário ou internacional.

Apesar das mudanças muito significativas e até positivas, a **mentalidade preventiva em termos de cumprimento do RGPD ainda é um parente pobre**, a par da adopção de programas de *Compliance*.

Mas, temos a convicção de que a transparência em matéria de proteção de dados é a chave para consolidar a relação de confiança entre advogado (a) e cliente (s) como um dos pilares fundamentais no exercício da profissão de advocacia, sob pena de colocar em causa o próprio mandato forense.

Assim, independentemente da dimensão dos escritórios em Portugal, a matéria do RGPD anda de mãos dadas com os princípios éticos e deontológicos da profissão, razão pela qual, deve ser reforçada.

De sua parte, a nossa **Ordem** fez publicar, na sua "Ficha Técnica e Termos Legais", a "**Política de Privacidade**" aplicável. Esta, estabelece as regras de garantia de todos os dados pessoais rececionados e retidos por esta na sequência da admissão dos seus trabalhadores, estagiários, prestadores de serviços e qualquer outro tipo de colaboradores e parceiros, clientes e fornecedores[36].

Desde então, **a maioria dos escritórios de advocacia em Portugal seguem uma efetiva implementação de políticas de privacidade** que representam uma manifesta declaração com natureza pública, partilhados através dos suportes de comunicação inclusive nas redes sociais.

Nessa medida, a mensagem de que o responsável pelo tratamento de dados está empenhado (a) na proteção da privacidade e dos dados pessoais dos seus clientes e utilizadores do *website*, adotando casa escritório de advocacia a sua política pública de práticas utilizadas é cada vez mais uma realidade prática e sem precedentes[37].

Assiste-se também a uma maior sensibilidade jurídica em matéria de RPGD, nomeadamente nos escritórios de prática isolada. Passou a ser mais comum acautelar que tipo de informação recolhem, qual a finalidade, com quem é partilhado, por quanto tempo é mantida a informação, qual o fundamento, qual o enquadramento para tratamento dos dados e que direitos existem relativamente aos dados recolhidos.

E na prática, há uma crescente preocupação generalizada em envolver os clientes, tratando o RGPD de forma global, seja no plano documental (físico/digital), no dos recursos humanos, com os seus colaboradores internos ou externos, das parcerias ou de outras realidades.

E aqui, falamos de recolha, armazenamento com origem no processamento cada vez mais digital e cujas medidas vão sendo cada vez mais apertadas, sem descurarmos que a adequação do RGPD nos escritórios de advogados tem de estar **em articulação com a matéria do segredo e sigilo profissionais**[38].

Sobretudo a partir da Pandemia do Covid 19, **a Cibersegurança tem-se revelado uma das maiores preocupações em Portugal nos clientes e para os próprios escritórios de advogados.** São conhecidas já as interrupções da atividade, danos relacionados com a reputação face à vulnerabilidade de segurança, perda de registo de dados, tarefas, contas correntes, perda de documentos digitalizados, etc.

Mas. nem sempre proceder a cópias de segurança remotas é a melhor solução, pois estando dependentes da «nuvem» ou de dispositivos eletrónicos, os mesmos não são infalíveis, podendo provocar dissabores, sendo necessárias redundâncias com discos externos no próprio escritório [39].

É ainda de notar que o próprio RGPD aponta alguns alertas a implementar nas entidades, aqui extensível aos escritórios de advocacia em Portugal, nomeadamente, dotar os mesmos de mecanismos para cifrar os dados pessoais, sistemas e serviços de tratamento.

Assim, temos conhecimento de que os escritórios de advocacia em Portugal têm redobrado as medidas de segurança, com a criação regular de novas *passwords*, alargam os procedimentos de certificação, adotam instrumentos de *compliance*, tais como, regulamentos, normas e procedimentos específicos.

Podemos estar a falar em escritórios de advocacia dividido em áreas, departamentos ou a título isolado com as plataformas disponíveis pelos protocolos celebrados e já citados, para a promoção da aplicação do RGPD.

Por outro lado, registamos que as medidas que matéria de implementação do RGPD nos escritórios de advocacia vai sendo mais conhecidas, seja em projetos societários ou, com as devidas ressalvas, nos escritórios de advocacia em prática individual/isolada. O que passa por:

i. a utilização a ferramentas de arquivo físico e digital e de proteção dos arquivos;
ii. o recurso a procedimentos internos transversais de tratamento de dados e segurança informática elaborados à medida da dimensão do escritório;
iii. a introdução de procedimentos internos de classificação de informação e gestão de acessos ao arquivo de acordo com essa classificação;
iv. a formação continua sobre o RGPD e procedimentos de segurança;
v. as auditorias internas de Cibersegurança e de RGPD;
vi. a designação de DPO (*Data Protection Officer)* e / ou CSO *(Chief Securiy Officer)*; e
vii. a destruição de processos físicos.

Destacamos que em território português já são vários os escritórios de advogados que prestam assessoria jurídica especializada sobre o enquadramento do RGPD[40].

Há, uma efetiva preocupação na centralização da confidencialidade e no tratamento e manuseamento dos dados pessoais, conduzindo a novas formas de digitalização e destruição de documentação física. Na prática, esta matéria não é apenas uma inquietação dos escritórios de advogados da União Europeia, aqui em destaque de Portugal, mas sabemos que tem vindo a ser também no Brasil.

Em suma, **a proteção de dados é** (deve ser) **uma prioridade em qualquer escritório de advocacia**.

Concluindo. O saldo em matéria de adequação ao RGPD nos escritórios de advocacia em Portugal é, na nossa perspetiva, positivo. Porém, apesar do conhecimento das normas ISO27001 e 27701, enquanto padrões de referência internacional para a gestão da Segurança da Informação e da Privacidade, o processo de implementação continuar a estar na base de que ***mais vale prevenir, para não remediar*** em matéria de Proteção de Dados Pessoais.

[26]*Fonte: Relatório Justiça 2015-2021, de fevereiro 2022. Ao longo dos últimos anos, este número tem vindo a crescer, verificando-se apenas sete quebras dos advogados inscritos nos anos de 1988, 1991, 1996, 2002, 2007, 2009 e 2019, correspondendo a 57% de mulheres, recordando-se aqui, que a advocacia esteve durante vários anos restringida às mulheres que só em 1918 é que viram assegurado o seu direito de acesso à profissão. Apesar destes dados quantitativos demonstrarem um progressivo domínio da mulher na advocacia, nem sempre os números são traduzidos de forma igualitária na progressão de carreira, no equilíbrio entre género nos cargos de topo e na conciliação da vida profissional com a pessoal.*

[27]*Na publicação online Advocatus, 16/05/2024, disponível em: https://eco.sapo.pt/advocatus/. Acrescento que a Ordem dos Advogados em Portugal é uma associação pública representativa dos profissionais que, em conformidade com os preceitos do presente Estatuto e demais disposições legais aplicáveis, exercem a advocacia. É uma pessoa coletiva [jurídica] de direito público que, no exercício dos seus poderes públicos, desempenha as suas funções, incluindo a função regulamentar, de forma independente dos órgãos do Estado, sendo livre e autónoma na sua atividade. Em Portugal, uma sociedade de advogados tem natureza de sociedade civil e não comercial, estando em curso diversos debates para a possibilidade da multidisciplinariedade, cuja reflexão se tem mantido entre a necessidade de equilibrar a inovação com preservação dos valores da profissão, assegurando a modernização do setor e a missão de interesse público em que assenta.*

[28]*O regulamento da Lei de Acesso ao Direito foi aprovado pela Portaria n.º 10/2008, de 3 de janeiro, o apoio judiciário pela Lei n.º 34/20004, de 29 de julho e pela Portaria n.º 1386/2004, de 10 de novembro. Para mais desenvolvimentos, aconselhamos a consulta do sítio da Internet: https://justica.gov.pt/Servicos/Pedir-apoio-judiciario.*

[29] *Apesar de se regist[r]ar um aumento do abandono da prática individual ou isolada, não raras vezes, por razões financeiras, apontadas pelas despesas correntes ou investimento para dar continuidade ao exercício da profissão, a verdade é que continua a ser uma realidade predominante. A par disso, ainda se regista de forma significativa escritórios de advogados que mantêm práticas mais tradicionais, sem apoio administrativo ou financeiro. Mas, sobretudo, no plano informático da gestão de processos judiciais. Do outro lado, ainda que em menor percentagem, emergem as sociedades de advogados e o caminho célere para a multidisciplinariedade que fará na nossa perspetiva que muitos escritórios de advocacia encerem a sua actividade.*

[30]*Ferramenta que permite ao advogado/solicitador, através da Internet proceder à apresentação de peças processuais e respectivos documentos, consultar processos judiciais e as diligências que lhes respeitam.*

[31] *Sistema de informação integrado criado para cada um dos tribunais, acedido através de um site, tendo como principal objetivo a criação do processo electrónico a partir de documentos/articulados entrados e digitalizados, com automatização de procedimentos, utilizando mecanismos de Workflow.*

[32]*Acessível neste endereço https://portal.tribunais.org.pt/, o sistema possibilita ver as notificações eletrónicas e aceder a documentos enviados pelos tribunais, pelas secretarias do Balcão Nacional de Injunções (BNI), Balcão Nacional do Arrendamento (BNA) e Serviço de Injunção em Matéria de Arrendamento (SIMA). Prevê-se que em 2025 o sistema disponibilize novas funcionalidades, tais como, a inteligência artificial passará a reconhecer o tipo de peça processual submetida, serão desenvolvidos mecanismos que vão permitir a comunicação entre os sistemas internos e a possibilidade de alterar a morada profissional do mandatário nas duas jurisdições. Esta é uma das fases de transformação digital dos tribunais que está prevista no Plano de Recuperação e Resiliência (PRR), aprovado pela União Europeia em sequência da Pandemia do Covid 19. A parte relativa a Portugal está disponível em: https://recuperarportugal.gov.pt/.*

[33]*Nomeadamente, acompanhando o ciclo de vida dos dados pessoais e implementação de medidas destinadas a mitigar eventuais riscos, tornando-se uma vantagem competitiva e demonstração de compromisso e de excelência ao proteger os dados dos seus clientes e a realização de constantes due diligence.*

[34]*O qual tem inúmeras funções, designadamente as de assegurar o cumprimento das políticas de privacidade e proteção de dados pessoais, sensibilização e informar todos os que tratem dos dados pessoais, controlo e regular a conformidade do RGPD, recolher informação para identificar atividades de tratamento, controlar os escritórios de contratos escritos subcontratante, ser o ponto de contacto com os titulares de forma a esclarecer as questões, ser o ponto de contacto com as autoridades de controlo.*

[35]*Starter OA | DataLEX e iBASE Jurídico, Protocolos divulgados quer pelo Conselho Geral da Ordem dos Advogados, quer pelo Conselho Regional de Lisboa (consultado a 14/07/2024.*
https://portal.oa.pt/comunicacao e https://www.linkedin.oacrlisboa_advogados.

[36]*Trata-se de facultar um quadro orientador de ação que permita, por um lado referir os mecanismos de controlo e garantia implementados e, por outro, informar dos direitos que assistem às partes interessadas, no sentido de promover o total cumprimento da legislação aplicável, estando disponível em: https://portal.oa.pt/ficha-tecnica-e-termos-legais/politica-de-privacidade/*

[37] *Aparecendo, por regra, no final de cada página de Internet num campo próprio de acesso.*

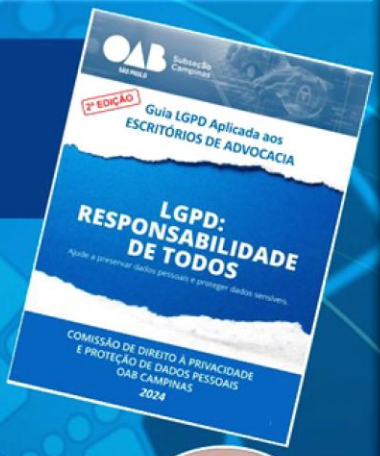
[38]*Patente no Estatuto da Ordem dos Advogados (artº 92.º da Lei n.º 145/2015, de 09 de setembro).*

[39]*E tal cenário, além dos cenários acima citados, somam-se as eventuais despesas de consultoria especializada, aquisição de apólices de seguro de responsabilidade civil por danos causados por terceiros quanto a eventos nos sistemas informáticos, cobertura por danos aos sistemas Informáticos, cobertura de assistência tecnológica, coberturas de Ciberproteção, mitigação de danos decorrentes de ameaça de extorsão cibernética, gastos derivados de restituição de imagem após sanções impostas pela Comissão nacional de Proteção de Dados (CNPD), cujas entidades de seguros são várias em Portugal nesta divulgação.*

[40]*Ora, da implementação do RGPD nas suas próprias estruturas, também já é uma realidade em território português, muitos escritórios de advogados transpuseram a sua experiência na implementação do RGPD para a prestação desse serviço e de assessoria jurídica especializada sobre o enquadramento do RGPD aos seus clientes, dele se destacando, políticas e avisos de privacidade, códigos de conduta, direitos de portabilidade dos dados, direito a "ser esquecido", registos de atividade de tratamento de dados, funções de encarregado de proteção de dados, notificações em matéria de segurança de dados pessoais, responsabilidade e consequência das infrações [até 4% do volume de negócios anual ou a Euros 20.0000.000,00*

LGPD: RESPONSABILIDADE DE TODOS

2ª Edição do Guia LGPD aplicada aos Escritórios de Advocacia - 2024



17/10 17h00 às 19h30

evento online

VALÉRIA REANI RODRIGUES GARCIA
Presidente da CDPPDP
Moderadora

ORESTES BACCHETTI JUNIOR
Vice-presidente da CDPPDP
Mediador

ALINE ANDRIETTA
1ªSecretária da CDPPDP
Comentarista

SPENCER ALVES ALMEIDA NETO
2º Secretario da CDPPDP
Comentarista

CARLOS ALBERTO CASANOVA CAMPOS
Presidente da Comissão de Direito Digital
Mediador

RODRIGO CARVALHO CANGUÇU DE ALMEIDA
Vice-presidente da Comissão de Direito Digital
Mediador

ANA CRISTINA OLIVARI
Secretária da Comissão de Direito Digital
Comentarista

GABRIELA MARANGONI
Membro da da CDPPDP
Representante dos autores

ANNA CAROLINA DE MEDEIROS SILVA
Colaboradora da CDPPDP
Suporte Referência

MANUEL DAVID MASSENO
Membro Consultor da CDPPDP
Coordenação Técnica Científica

Transmissão zoom

Comissão de Direito à Privacidade e Proteção de Dados Pessoais
Apoio
Comissão de Direito Digital

OAB SÃO PAULO Subseção Campinas

Luciana Freitas
Presidente

PATROCINADORES

Internethic®
Privacidade e Proteção de Dados Pessoais

Anna Medeiros
ADVOCACIA

PRIMO & CAMPOS
SOCIEDADE DE ADVOGADOS

gov DADOS

Angelina Teixeira
e Associados
Sociedade de Advogados, SP, RL.

Aline Andrietta
ADVOGADA

CA 20 ANOS
CANGUÇU DE ALMEIDA
ADVOGADOS
OAB/SP Nº 28.375

APOIO

RONCARATI 50 Anos
EDITORA

OAB Subseção Campinas
SÃO PAULO
Comissão de Direito Digital

ALEXANDRE ATHENIENSE ADVOGADOS
DIREITO DIGITAL
37 ANOS

Verifact®

CANTO DE LIMA
ADVOCACIA

OLIVARI
ADVOCACIA

3ª SUBSEÇÃO DA ORDEM DOS ADVOGADOS DO BRASIL

GESTÃO 2022/2024

Diretoria

Luciana Freitas
Presidente

Paulo Braga
Vice-Presidente

Cláudio Vieira
Secretário Geral

André Amin Teixeira Pinto
Secretário Geral-Adjunto

Stella Vicente Serafini
Diretora Tesoureira

OAB SÃO PAULO Subseção Campinas

Comissão de Direito a Privacidade e Proteção de dados Pessoais